This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

BSI Standards Publication

Maritime navigation and radiocommunication equipment and systems — Cybersecurity — General requirements, methods of testing and required test results

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

National foreword

This British Standard is the UK implementation of EN IEC 63154:2021. It is identical to IEC 63154:2021.

The UK participation in its preparation was entrusted to Technical Committee EPL/80, Maritime navigation and radiocommunication equipment and systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 580 51931 4

ICS 35.030; 47.020.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2021.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD **EN IEC 63154**

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

EUROPÄISCHE NORM

April 2021

ICS 35.030; 47.020.70

English Version

Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results (IEC 63154:2021)

Matériels et systèmes de navigation et de radiocommunication maritimes - Sécurité informatique - Exigences générales, méthodes d'essai et résultats d'essai exigés (IEC 63154:2021)

Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt - Cyber-Security - Allgemeine Anforderungen, Prüfverfahren und geforderte Prüfergebnisse (IEC 63154:2021)

This European Standard was approved by CENELEC on 2021-04-13. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

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

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

© 2021 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 63154:2021 E

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

European foreword

The text of document 80/984/FDIS, future edition 1 of IEC 63154, prepared by IEC/TC 80 "Maritime navigation and radiocommunication equipment and systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 63154:2021.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2022-01-13
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2024-04-13

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

Endorsement notice

The text of the International Standard IEC 63154:2021 was approved by CENELEC as a European Standard without any modification.

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

IEC 61162-1	NOTE	Harmonized as EN 61162-1
IEC 61162-2	NOTE	Harmonized as EN 61162-2
IEC 61162-3	NOTE	Harmonized as EN 61162-3
IEC 61993-2:2018	NOTE	Harmonized as EN IEC 61993-2:2018 (not modified)
IEC 62443 (series)	NOTE	Harmonized as EN IEC 62443 (series)

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

(normative)

Normative references to international publications with their corresponding European publications

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

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

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

Publication	Year	Title	EN/HD	Year
IEC 60945	2002	Maritime navigation and radiocommunication equipment and systems - General requirements - Methods of testing and required test results	EN 60945	2002
IEC 61162-450	-	Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection	EN IEC 61162-450	-
IEC 61162-460	2018	Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection –Safety and security	EN IEC 61162-460	2018

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

This page deliberately left blank

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 9
2 Normative references 9
3 Terms, definitions and abbreviated terms 10
3.1 Terms and definitions 10
3.2 Abbreviated terms 13
4 Module A: Data files 14
4.1 General 14
4.2 Requirements 14
4.2.1 Transport integrity 14
4.2.2 Source authentication 14
4.3 Methods of testing and required test results 15
5 Module B: Execution of executables 16
5.1 General 16
5.2 Requirements 16
5.3 Methods of testing and required test results 17
6 Module C: User authentication 17
6.1 General 17
6.2 Requirements 17
6.3 Methods of testing and required test results 19
7 Module D: System defence 20
7.1 General 20
7.2 Malware protection 20
7.2.1 Requirements 20
7.2.2 Methods of testing and required test results 23
7.3 Denial of service protection 25
7.3.1 Requirements 25
7.3.2 Methods of testing and required test results 27
8 Module E: Network access 29
8.1 General 29
8.2 Equipment which connects to a network 29
8.2.1 Requirements 29
8.2.2 Methods of testing and required test results 29
8.3 Equipment providing network access between controlled networks 30
8.3.1 Requirements 30
8.3.2 Methods of testing and required test results 30
8.4 Equipment providing network access between controlled and uncontrolled networks 31
8.4.1 Requirements 31
8.4.2 Methods of testing and required test results 31
9 Module F: Access to operating system 32
9.1 General 32
9.2 Requirements 32
9.3 Methods of testing and required test results 32
10 Module G: Booting environment 32

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

10.1 General 32
10.2 Requirements 32
10.3 Methods of testing and required test results 33
11 Module H: Maintenance mode 33
11.1 General 33
11.2 Requirements 33
11.3 Methods of testing and required test results 34
12 Module I: Protection against unintentional crash caused by user input 35
12.1 General 35
12.2 Requirements 35
12.3 Methods of testing and required test results 36
13 Module J: Interfaces for removable devices including USB 36
13.1 General 36
13.2 Requirements 36
13.2.1 Physical protection 36
13.2.2 Operational protection 37
13.3 Methods of testing and required test results 37
13.3.1 Physical protection 37
13.3.2 Operational protection 37
14 Module K: IEC 61162-1 or IEC 61162-2 as interface 38
15 Module L: IEC 61162-450 as interface 38
15.1 General 38
15.2 IEC 61162-1 sentences 38
15.3 IEC 61162-450 used for file transfer 38
16 Module M: Other interfaces 39
17 Module N: Software maintenance 39
17.1 General 39
17.2 Software maintenance in maintenance mode 40
17.2.1 Requirements 40
17.2.2 Methods of testing and required test results 40
17.3 Semi-automatic software maintenance by the crew onboard the vessel 40
17.3.1 General 40
17.3.2 Requirements 40
17.3.3 Methods of testing and required test results 41
18 Module O: Remote maintenance 42
18.1 General 42
18.2 Requirements 42
18.3 Methods of testing and required test results 42
19 Module P: Documentation 43
19.1 Requirements 43
19.2 Methods of testing and required test results 43
Annex A (informative) Guidance on implementing virus and malware protection on type approved equipment 44
Annex B (normative) File authentication 46
B.1 General 46
B.2 Digital signatures 46
B.2.1 Requirements 46
B.2.2 Methods of testing and required test results 47

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

B.3 Symmetric means based upon pre-shared secret keys 48
B.3.1 Requirements 48
B.3.2 Methods of testing and required test results 49
Annex C (informative) Methods of authentication of data files and executables – Examples 51
C.1 General 51
C.2 Explanations of terms 51
C.3 Asymmetric cryptography 51
C.4 Digital signatures 52
C.5 Public key infrastructure 53
C.5.1 General theory 53
C.5.2 Notes about shipboard use 55
C.6 Symmetric key authentication based on "pre-shared secret key" 55
Annex D (normative) USB class codes 57
Annex E (informative) Cyber security configuration document for equipment 58
E.1 General for the document 58
E.2 Document parts 58
E.2.1 Hardening of the operating system 58
E.2.2 Update strategy for cyber security reasons 58
E.2.3 Strategies for detecting and reacting to future vulnerabilities 58
Annex F (informative) Guidance on interconnection between networks 59
F.1 General 59
F.2 Guidance 59
Bibliography 61

Figure 1 – Some examples of data transfer 8
Figure F.1 – Examples for different types of network and associated interconnecting devices 60

Table D.1 – USB class codes 57

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

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.

IEC 63154 has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems. It is an International Standard.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
80/984/FDIS	80/989/RVD

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

The language used for the development of this International Standard is English

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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

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

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.

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

INTRODUCTION

IMO resolution MSC.428(98) on maritime cyber risk management in safety management systems affirms the need for cyber risk management on vessels subject to the SOLAS Convention. This document addresses the basic cybersecurity requirements for shipborne navigation and radiocommunication equipment falling within that need.

Shipborne navigation and radiocommunication equipment are generally installed in restricted areas, for example at the bridge where access is defined by the IMO International Ship and Port Facility Security (ISPS) Code or in an electronic locker room or in a closed cabinet. These restricted areas are referred to as secure areas in this document. This is based on the importance of navigation and radiocommunication equipment for the safety of navigation. These restricted areas are considered as areas with implemented security and access measures. These measures are defined in the ship security plan of the individual vessel derived from ISPS code, they are not part of this document and not specified or tested in the context of this document. Accordingly, equipment installed in these physically restricted access areas are understood to benefit from these security measures. This document provides mitigation against the remaining cyber vulnerabilities for equipment installed in such areas.

Following from the above, this document includes consideration of cyber threats from unauthorized users, from removable external data sources (REDS) like USB sticks, from network segments installed outside of the restricted areas including interfaces to external networks, for example ship to shore, ship to ship.

The risk of an incident is different for each equipment/system boundary, and the mitigating security measures required should be appropriate to the identified risk of incident and proportional to the identified adverse consequences. Boundaries take the form of both physical, such as direct access to the equipment via its ports (e.g. network, USB, import of digital files, software installation) and logical (e.g. connections over a network, transfer of data, operator use). A key tenet of cyber security is authentication of who has provided the data and verification that what is being provided has not been tampered with.

To reflect the difference in cyber security risk, the needs for authentication and verification between secure and non-secure areas are illustrated in Figure 1. The methods for achieving authentication and verification are described in each module of this document.

In Figure 1, the colour red means a source requiring authentication and verification. The colour green means a source not requiring authentication and verification.

The explanation of the numbers in Figure 1 is:

1) external communication that requires authentication and verification as the source is not a local secure area and its provenance cannot be trusted;
2) local network message interfacing that does not require authentication and verification as they are part of normal operation defined by configuration in a local secure area, for example VDR binary transfer, IEC 61162 interfacing, internal proprietary data exchange;
3) local message and data import between networks that does not require authentication and verification as they are part of normal operation defined by configuration in local secure areas;
4) external data import by an operator from an external source via REDS that requires authentication and verification of data import; this applies to executable or non-executable data;
5) local serial interface messaging that does not require authentication and verification as it is part of normal operation defined by configuration in a local secure area;
6) updates applied via external data source or REDS in maintenance mode that does not require authentication and verification but does require user authentication to change configuration.

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

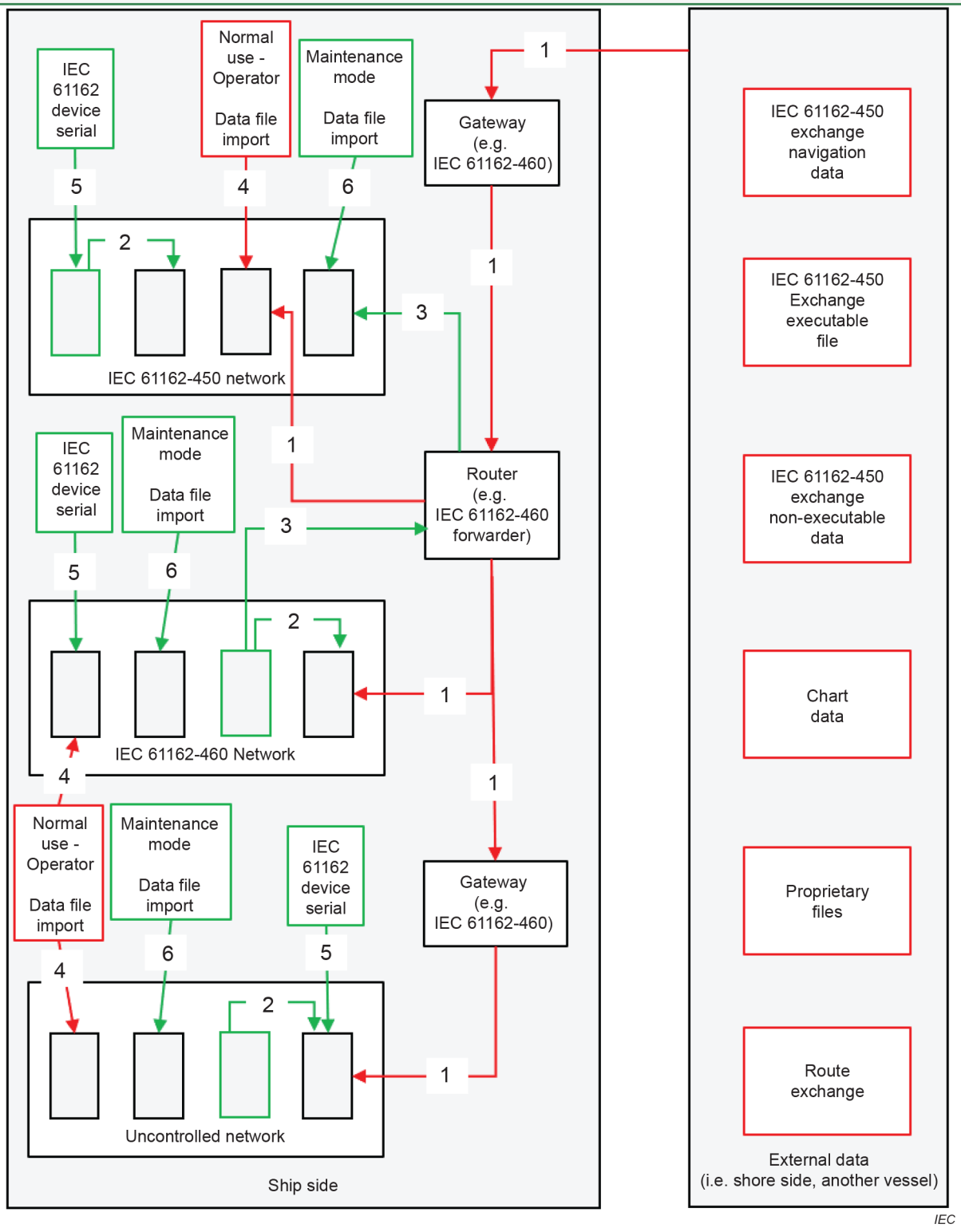

Figure 1 – Some examples of data transfer

This is a preview of "BS EN IEC 63154:2021". Click here to purchase the full version from the ANSI store.

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

1 Scope

This document specifies requirements, methods of testing and required test results where standards are needed to provide a basic level of protection against cyber incidents (i.e. malicious attempts, which actually or potentially result in adverse consequences to equipment, their networks or the information that they process, store or transmit) for:

a) shipborne radio equipment forming part of the global maritime distress and safety system (GMDSS) mentioned in the International Convention for Safety of Life at Sea (SOLAS) as amended, and by the Torremolinos International Convention for the Safety of Fishing Vessels as amended, and to other shipborne radio equipment, where appropriate;

b) shipborne navigational equipment mentioned in the International Convention for Safety of Life at Sea (SOLAS) as amended, and by the Torremolinos International Convention for the Safety of Fishing Vessels as amended,

c) other shipborne navigational aids, and Aids to Navigation (AtoN), where appropriate.

The document is organised as a series of modules dealing with different aspects. The document considers both normal operation of equipment and the maintenance of equipment. For each module, a statement is provided indicating whether the module applies during normal operation or in maintenance mode.

Communication initiated from navigation or radiocommunication equipment outside of items a), b) and c) above, for example ship side to other ship or shore side, are outside of the scope of this document.

This document does not address cyber-hygiene checks, for example anti-malware scanning, etc., performed outside of the cases defined in this document.

2 Normative references

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

IEC 60945:2002, *Maritime navigation and radiocommunication equipment and systems – General requirements – Methods of testing and required test results*

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

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