

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN IEC 63154:2021 sisaldab Euroopa standardi EN IEC 63154:2021 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 63154:2021 consists of the English text of the European standard EN IEC 63154:2021.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 23.04.2021.	Date of Availability of the European standard is 23.04.2021.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030, 47.020.70

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele. Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation: Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC 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)

Annex ZA (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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Matériels et systèmes de navigation et de radiocommunication maritimes –
Sécurité informatique – Exigences générales, méthodes d'essai et résultats
d'essai exigés**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2021 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Matériels et systèmes de navigation et de radiocommunication maritimes –
Sécurité informatique – Exigences générales, méthodes d'essai et résultats
d'essai exigés**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 35.030; 47.020.70

ISBN 978-2-8322-9471-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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

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

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

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 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.

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.

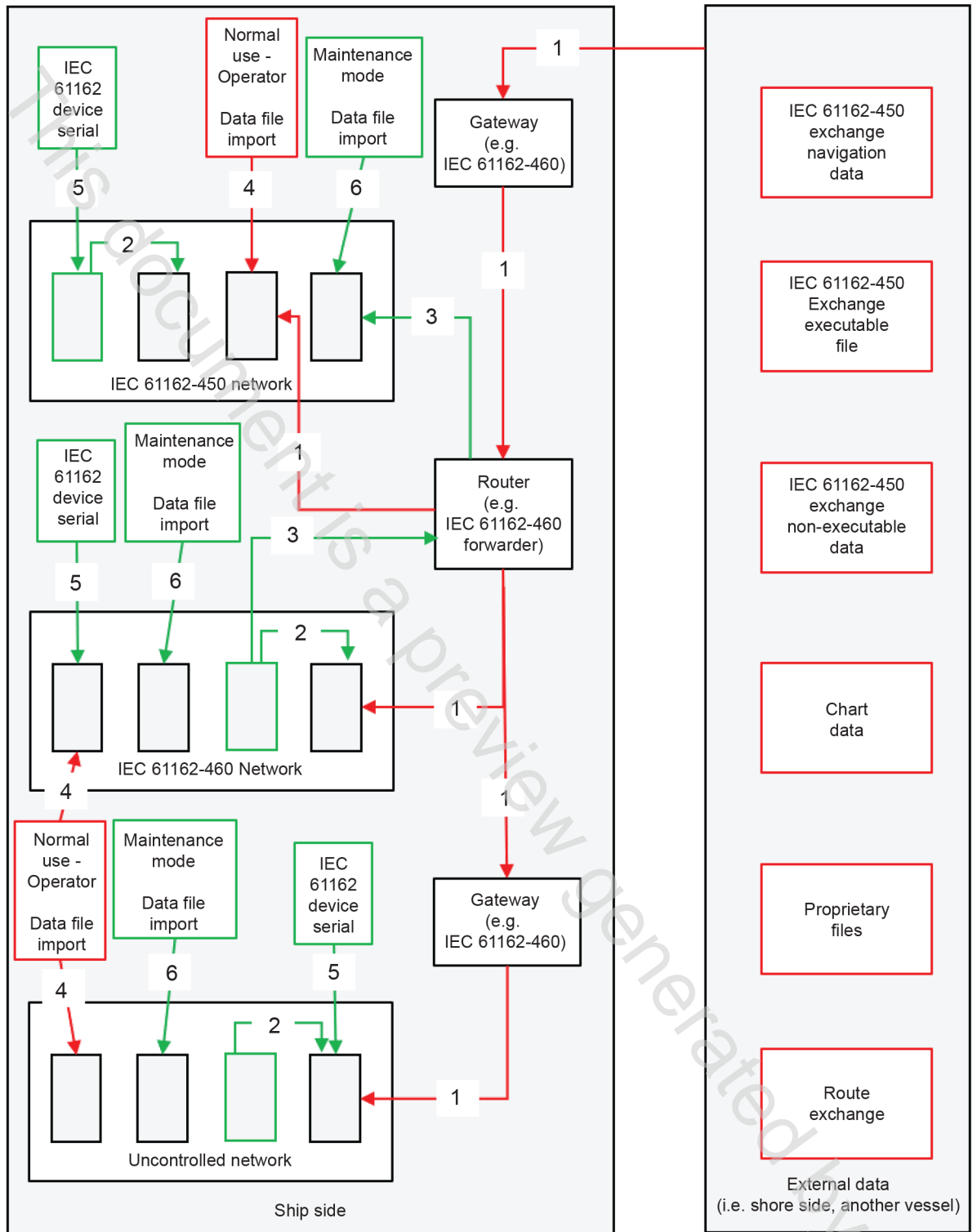


Figure 1 – Some examples of data transfer