IEC 63154

Edition 1.0 2021-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

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.

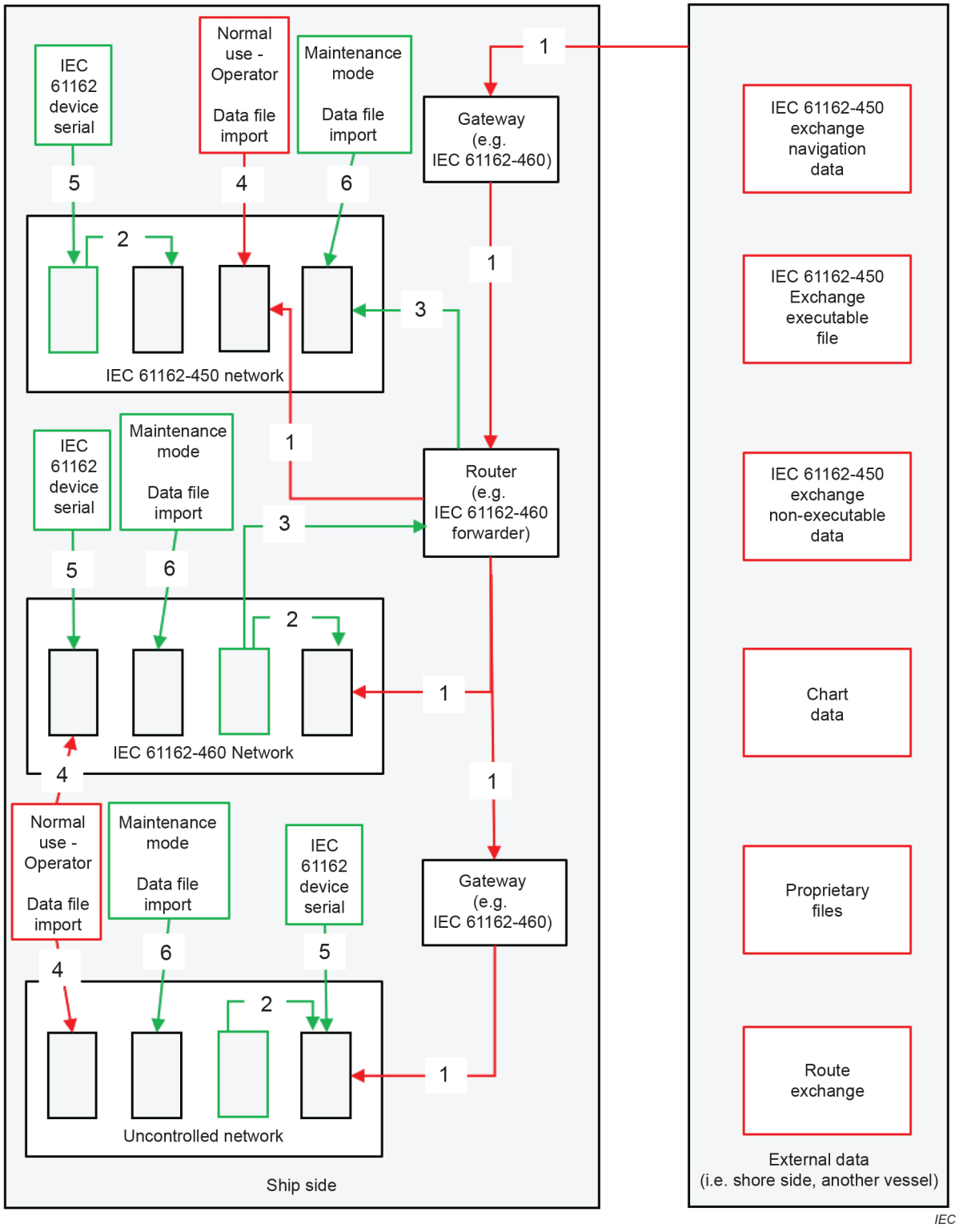


Figure 1 – Some examples of data transfer

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*

SOMMAIRE

AVANT-PROPOS 67
INTRODUCTION 69
1 Domaine d'application 72
2 Références normatives 72
3 Termes, définitions et termes abrégés 73
3.1 Termes et définitions 73
3.2 Termes abrégés 77
4 Module A: Fichiers de données 77
4.1 Généralités 77
4.2 Exigences 77
4.2.1 Intégrité du transport 77
4.2.2 Authentification de la source 78
4.3 Méthodes d'essai et résultats d'essai exigés 79
5 Module B: Exécution des fichiers exécutables 80
5.1 Généralités 80
5.2 Exigences 80
5.3 Méthodes d'essai et résultats d'essai exigés 80
6 Module C: Authentification de l'utilisateur 81
6.1 Généralités 81
6.2 Exigences 81
6.3 Méthodes d'essai et résultats d'essai exigés 83
7 Module D: Défense du système 84
7.1 Généralités 84
7.2 Protection contre les programmes malveillants 84
7.2.1 Exigences 84
7.2.2 Méthodes d'essai et résultats d'essai exigés 87
7.3 Protection contre le déni de service 89
7.3.1 Exigences 89
7.3.2 Méthodes d'essai et résultats d'essai exigés 92
8 Module E: Accès au réseau 94
8.1 Généralités 94
8.2 Matériel qui se connecte à un réseau 94
8.2.1 Exigences 94
8.2.2 Méthodes d'essai et résultats d'essai exigés 94
8.3 Matériel fournissant un accès réseau entre des réseaux contrôlés 95
8.3.1 Exigences 95
8.3.2 Méthodes d'essai et résultats d'essai exigés 95
8.4 Matériel fournissant un accès réseau entre des réseaux contrôlés et non contrôlés 96
8.4.1 Exigences 96
8.4.2 Méthodes d'essai et résultats d'essai exigés 96
9 Module F: Accès au système d'exploitation 97
9.1 Généralités 97
9.2 Exigences 97
9.3 Méthodes d'essai et résultats d'essai exigés 97
10 Module G: Environnement de démarrage 97

10.1 Généralités 97
10.2 Exigences 97
10.3 Méthodes d'essai et résultats d'essai exigés 98
11 Module H: Mode entretien 98
11.1 Généralités 98
11.2 Exigences 99
11.3 Méthodes d'essai et résultats d'essai exigés 99
12 Module I: Protection contre le plantage involontaire provoqué par une entrée d'utilisateur 100
12.1 Généralités 100
12.2 Exigences 101
12.3 Méthodes d'essai et résultats d'essai exigés 101
13 Module J: Interfaces des dispositifs amovibles, y compris USB 102
13.1 Généralités 102
13.2 Exigences 102
13.2.1 Protection physique 102
13.2.2 Protection opérationnelle 102
13.3 Méthodes d'essai et résultats d'essai exigés 103
13.3.1 Protection physique 103
13.3.2 Protection opérationnelle 103
14 Module K: IEC 61162-1 ou IEC 61162-2 en tant qu'interface 103
15 Module L: IEC 61162-450 en tant qu'interface 104
15.1 Généralités 104
15.2 Sentences IEC 61162-1 104
15.3 IEC 61162-450 utilisé pour le transfert de fichier 104
16 Module M: Autres interfaces 105
17 Module N: Entretien du logiciel 105
17.1 Généralités 105
17.2 Entretien du logiciel en mode entretien 106
17.2.1 Exigences 106
17.2.2 Méthodes d'essai et résultats d'essai exigés 106
17.3 Entretien semi-automatique du logiciel par l'équipage embarqué sur le navire 106
17.3.1 Généralités 106
17.3.2 Exigences 107
17.3.3 Méthodes d'essai et résultats d'essai exigés 108
18 Module O: Entretien à distance 108
18.1 Généralités 108
18.2 Exigences 108
18.3 Méthodes d'essai et résultats d'essai exigés 109
19 Module P: Documentation 109
19.1 Exigences 109
19.2 Méthodes d'essai et résultats d'essai exigés 109
Annexe A (informative) Recommandations relatives à la mise en œuvre d'une protection contre les virus et les programmes malveillants sur un matériel ayant fait l'objet d'un agrément de type 110
Annexe B (normative) Authentification de fichier 112
B.1 Généralités 112

B.2 Signatures numériques 112
B.2.1 Exigences 112
B.2.2 Méthodes d'essai et résultats d'essai exigés 113
B.3 Moyens symétriques reposant sur des clés secrètes prépartagées 115
B.3.1 Exigences 115
B.3.2 Méthodes d'essai et résultats d'essai exigés 115
Annexe C (informative) Méthodes d'authentification des fichiers de données et des fichiers exécutables – Quelques exemples 117
C.1 Généralités 117
C.2 Explications des termes 117
C.3 Cryptographie asymétrique 118
C.4 Signatures numériques 119
C.5 Infrastructure de clé publique 120
C.5.1 Théorie générale 120
C.5.2 Notes à propos de l'utilisation à bord 121
C.6 Authentification de clé symétrique en fonction de la "clé secrète prépartagée" 122
Annexe D (normative) Codes de classe USB 124
Annexe E (informative) Document de configuration de la sécurité informatique du matériel 125
E.1 Généralités concernant le document 125
E.2 Parties du document 125
E.2.1 Renforcement de la sécurité du système d'exploitation 125
E.2.2 Mise à jour de la stratégie pour des raisons de sécurité 125
E.2.3 Stratégies de détection et de réactions aux vulnérabilités futures 125
Annexe F (informative) Recommandations relatives à l'interconnexion entre les réseaux 126
F.1 Généralités 126
F.2 Recommandations 126
Bibliographie 129

Figure 1 – Quelques exemples de transfert de données 71
Figure F.1 – Exemples de différents types de réseaux et de dispositifs d'interconnexion associés 128

Tableau D.1 – Codes de classe USB 124

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

MATÉRIELS ET SYSTÈMES DE NAVIGATION ET DE RADIOCOMMUNICATION MARITIMES – SÉCURITÉ INFORMATIQUE – EXIGENCES GÉNÉRALES, MÉTHODES D'ESSAI ET RÉSULTATS D'ESSAI EXIGÉS

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme IEC 63154 a été établie par le comité d'études 80 de l'IEC: Matériels et systèmes de navigation et de radiocommunication maritimes. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
80/984/FDIS	80/989/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

La langue utilisée pour l'élaboration de la présente Norme internationale est l'anglais

Le présent document a été rédigé conformément aux Directives ISO/IEC, Partie 2, et développé conformément aux Directives ISO/IEC, Partie 1, et aux Directives ISO/IEC, Supplément IEC, disponibles à l'adresse www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail à l'adresse www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La Résolution MSC.428(98) de l'OMI sur la gestion des cyberrisques maritimes dans le cadre des systèmes de gestion de la sécurité affirme la nécessité de gérer les cyberrisques sur les vaisseaux soumis à la Convention SOLAS. Le présent document traite des exigences de base en matière de sécurité informatique pour le matériel de navigation et de radiocommunication de bord qui répondent à ce besoin.

Le matériel de navigation et de radiocommunication de bord est en général installé dans des zones réglementées, par exemple sur le pont dont l'accès est défini par le Code international pour la sûreté des navires et des installations portuaires (ISPS) de l'OMI, dans un vestiaire électronique ou dans une armoire fermée. Ces zones réglementées sont appelées zones protégées dans le présent document. Il s'agit de souligner l'importance du matériel de navigation et de radiocommunication pour la sécurité de la navigation. Ces zones réglementées sont considérées comme des espaces dans lesquels des mesures de sécurité et d'accès ont été mises en place. Ces mesures étant définies dans le plan de sûreté du navire, lequel est déduit du code ISPS, elles ne font pas partie intégrante du présent document et ne sont pas spécifiées ni soumises à essai dans le contexte du présent document. En conséquence, le matériel installé dans ces zones à accès physiquement restreint est réputé bénéficier de ces mesures de sécurité. Le présent document donne les mesures d'atténuation des vulnérabilités informatiques restantes pour le matériel installé dans ce type de zones.

Il en découle de ce qui précède que le présent document prend en considération les menaces informatiques provenant d'utilisateurs non autorisés, de sources de données externes amovibles (REDS) (des clés USB, par exemple) et de segments de réseau installés à l'extérieur des zones réglementées comportant des interfaces avec des réseaux externes (navire à station côtière, entre navires, par exemple).

Le risque d'incident est différent pour chaque matériel/système délimité, et il convient que les mesures de sécurité d'atténuation exigées soient adaptées au risque d'incident identifié et qu'elles soient proportionnelles aux conséquences néfastes identifiées. Les limites sont physiques, comme un accès direct au matériel par l'intermédiaire de ses accès (réseau, USB, importation de fichiers numériques, installation logicielle, par exemple) et logique (connexions sur un réseau, transfert de données, utilisation de l'opérateur, par exemple). Un principe essentiel de la sécurité informatique est l'authentification de la personne qui a fourni les données, et la vérification que les éléments qui ont été fournis n'ont pas été falsifiés.

Pour refléter la différence en matière de risque pour la sécurité informatique, les besoins d'authentification et de vérification entre des zones protégées et non protégées sont représentés à la Figure 1. Les méthodes d'authentification et de vérification sont décrites dans chaque module du présent document.

A la Figure 1, la couleur rouge matérialise une source exigeant l'authentification et la vérification. La couleur verte matérialise une source n'exigeant pas d'authentification et de vérification.

Les nombres de la Figure 1 sont expliqués ci-dessous:

1) communication externe qui exige une authentification et une vérification, la source n'étant pas une zone protégée locale et sa provenance ne pouvant pas être digne de confiance;
2) interfaçage de messagerie de réseau local qui n'exige pas d'authentification et de vérification étant donné qu'elle entre dans le cadre du fonctionnement normal défini par la configuration dans une zone protégée locale (transfert binaire VDR, interfaçage IEC 61162, échange de données propriétaires internes, par exemple);
3) importation locale de message et de données entre des réseaux qui n'exige pas d'authentification et de vérification, étant donné qu'elle entre dans le cadre du fonctionnement normal défini par la configuration dans des zones protégées locales;

4) importation de données externes par un opérateur depuis une source externe par l'intermédiaire de REDS et qui exige une authentification et une vérification. Cela s'applique aux données exécutables ou non exécutables;

5) messagerie d'interface série locale qui n'exige pas d'authentification et de vérification, étant donné qu'elle entre dans le cadre du fonctionnement normal défini par la configuration dans une zone protégée locale;

6) mises à jour appliquées par l'intermédiaire de la source de données externe ou de la REDS en mode entretien et qui n'exigent pas d'authentification et de vérification, mais qui exigent une authentification de l'utilisateur pour modifier la configuration.

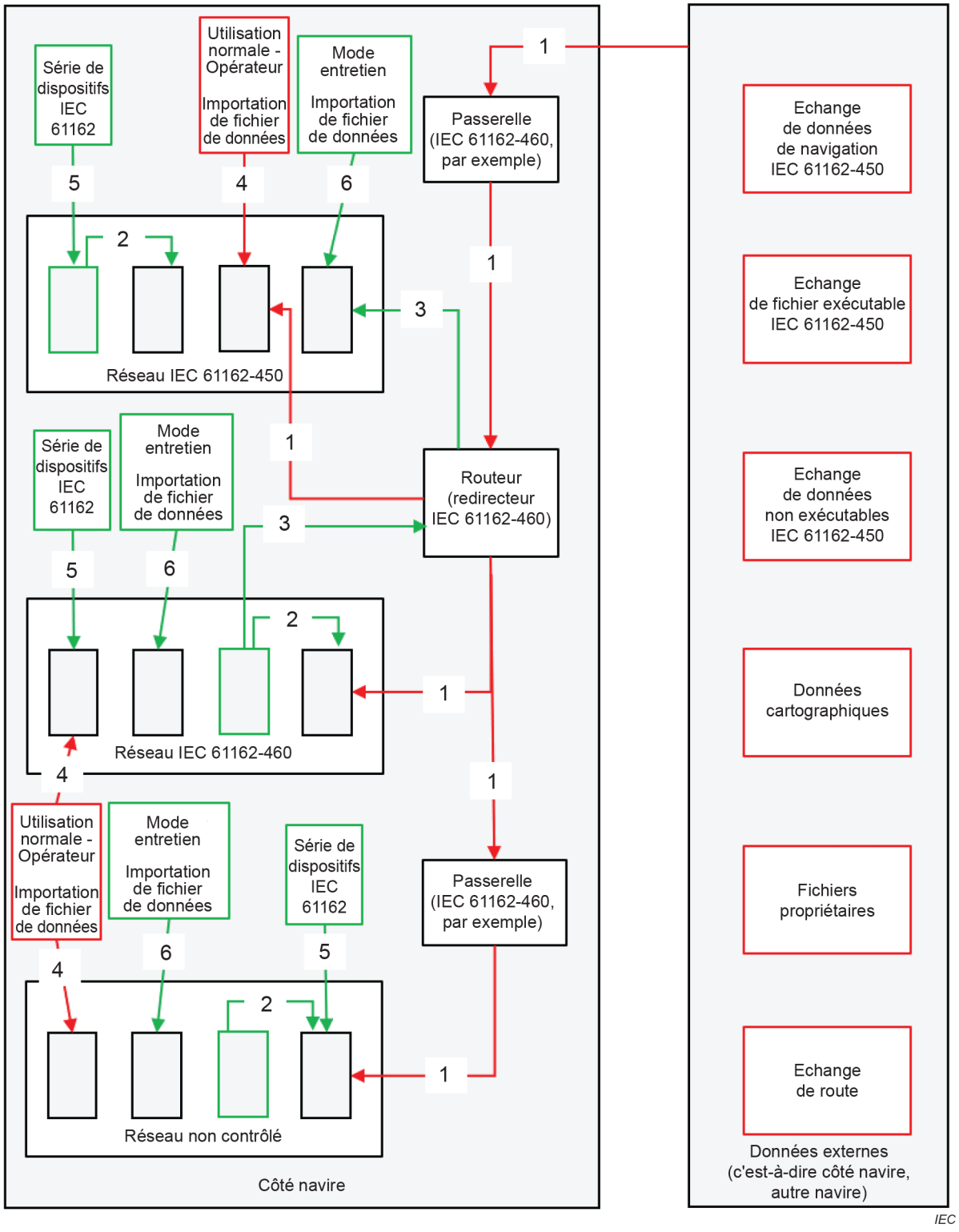


Figure 1 – Quelques exemples de transfert de données

MATÉRIELS ET SYSTÈMES DE NAVIGATION ET DE RADIOCOMMUNICATION MARITIMES – SÉCURITÉ INFORMATIQUE – EXIGENCES GÉNÉRALES, MÉTHODES D'ESSAI ET RÉSULTATS D'ESSAI EXIGÉS

1 Domaine d'application

Le présent document spécifie les exigences, les méthodes d'essai et les résultats d'essai exigés lorsque des normes sont nécessaires pour fournir un niveau de protection de base contre les incidents de sécurité informatique (c'est-à-dire les tentatives malveillantes, qui ont un effet réellement ou potentiellement néfaste sur les matériels, sur leurs réseaux ou sur les informations qu'ils traitent, stockent ou transmettent) pour:

a) le matériel radioélectrique de bord faisant partie du système mondial de détresse et de sécurité en mer (SMDSM) mentionné dans la Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS), telle que modifiée, et par la Convention internationale de Torremolinos pour la sécurité des bateaux de pêche, telle que modifiée, et d'autres matériels radioélectriques de bord, le cas échéant;

b) le matériel de navigation de bord mentionné dans la Convention Internationale pour la sauvegarde de la vie humaine en mer (SOLAS), telle que modifiée, et par la Convention internationale de Torremolinos pour la sécurité des bateaux de pêche, telle que modifiée,

c) les autres aides à la navigation de bord, le cas échéant (AtoN), le cas échéant.

Le document est organisé en une série de modules traitant différents aspects. Le document prend en considération tant le fonctionnement normal que l'entretien du matériel. Pour chaque module, un énoncé est fourni indiquant si le module s'applique pendant le fonctionnement normal ou pendant l'entretien.

La communication initiée à partir d'un matériel de navigation ou de radiocommunication hors des points a), b) et c) ci-dessus (entre un navire et un autre navire ou le quai, par exemple) ne relève pas du domaine d'application du présent document.

Le présent document ne porte pas sur les contrôles d'hygiène informatique (les analyses de détection des programmes malveillants, etc.) réalisés hors des cas définis dans le présent document.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60945:2002, *Matériels et systèmes de navigation et de radiocommunication maritimes – Spécifications générales – Méthodes d'essai et résultats exigibles*

IEC 61162-450, *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques – Partie 450: Emetteurs multiples et récepteurs multiples – Interconnexion Ethernet*

IEC 61162-460:2018, *Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques – Partie 460: Emetteurs multiples et récepteurs multiples – Interconnexion Ethernet – Sûreté et sécurité*