IEC 63154

Edition 1.0 2021-03

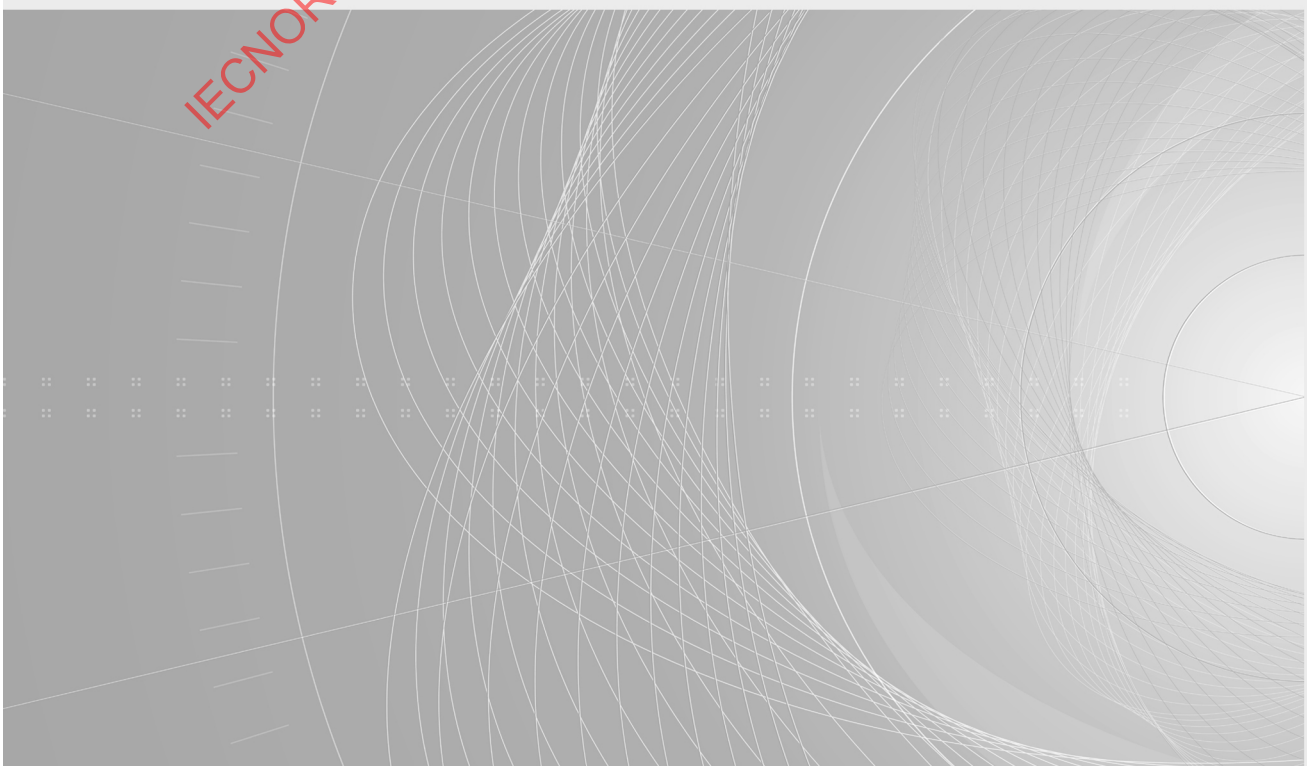
INTERNATIONAL STANDARD

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



IEC 63154:2021-03(en-fr)

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

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

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

CONTENTS

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.

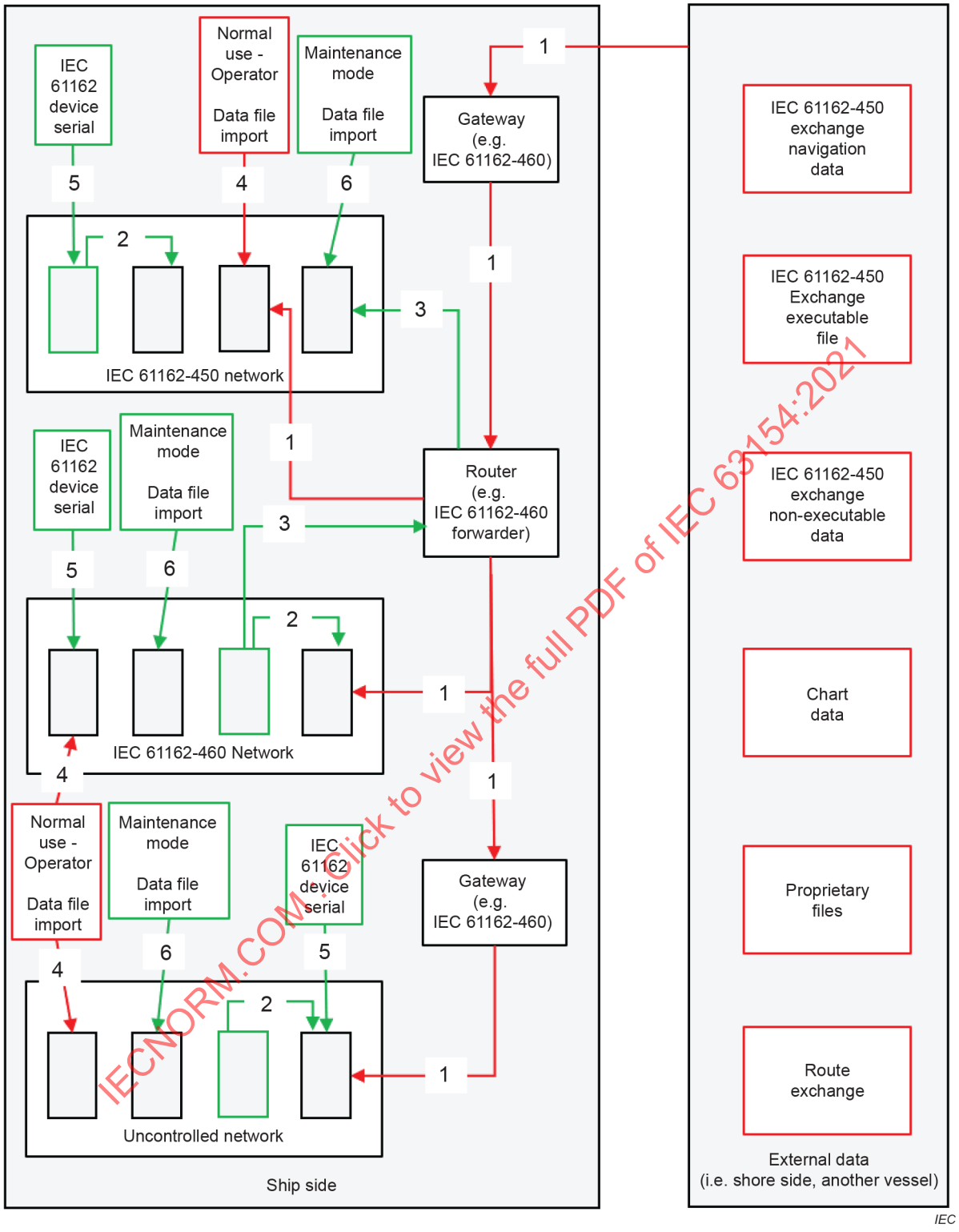


Figure 1 – Some examples of data transfer

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*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Terms and definitions

3.1.1
address space layout randomization authentication
ASLR
memory-protection process for operating systems that guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory

3.1.2
authentication
provision of assurance that a claimed characteristic of an identity is correct

Note 1 to entry: Authentication is usually a prerequisite to allowing access to resources in a system.

3.1.3
authenticator
means used to confirm the identity of a user (human, software process or device)

Note 1 to entry: For example, a password or token may be used as an authenticator.

3.1.4
authenticity
property that an entity is what it claims to be

Note 1 to entry: Authenticity is typically used in the context of confidence in the identity of an entity, or the validity of a transmission, a message or message originator.

3.1.5
basic input/output system
BIOS
non-volatile firmware used to perform hardware initialization during the booting process (power-on startup), and to provide runtime services for operating systems and programs

Note 1 to entry: Examples include legacy BIOS (historical IBM PC compliant), UEFI (unified extensible firmware interface).

3.1.6
controlled network
network compliant to the controlled network requirements of IEC 61162-460

3.1.7
closed network
network which is physically isolated from other networks

Note 1 to entry: A closed network is also known as an "air gapped network".

Note 2 to entry: A closed network cannot contain equipment that connects to different networks. A closed network may be controlled or uncontrolled.

Note 3 to entry: This includes but is not limited to Ethernet networks.

3.1.8
cryptographic key
sequence of symbols that controls the operations of a cryptographic

EXAMPLE Encipherment, decipherment, cryptographic check-function computation, signature calculation and signature verification.

3.1.9
data execution prevention
DEP
implementation of execution space protection on Microsoft Windows operating systems

Note 1 to entry: Execution space protection technique allows memory to be marked as non-executable such that attempts to add executable code results in an error.

3.1.10
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.1.11
digital signature
data appended to, or cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[SOURCE: ISO 7498-2:1989, 3.3.26]

3.1.12
external data source
EDS
network or non-network data source, including, but not limited to, REDS and SIM cards

3.1.13
hash-code
string of bits which is the output of a hash-function

Note 1 to entry: The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples.

Note 2 to entry: NIST SP 800-63B uses message digest for this.

[SOURCE: ISO/IEC 10118-1:2016, 3.3, modified – Note 2 to entry has been added.]

3.1.14
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

– for a given output, it is computationally infeasible to find an input which maps to this output;
– for a given input, it is computationally infeasible to find a second input which maps to the same output

Note 1 to entry: Used as part of data authentication, integrity and non-repudiation.

[SOURCE: ISO/IEC 10118-1:2016, 3.4, modified – Note 1 to entry has been replaced by a new note.]

3.1.15
maintenance mode
mode reserved for qualified and authorized persons, or authorised remote devices for the purposes of installation, commissioning, repair or maintenance of the system

3.1.16
manufacturer's configuration
part of setup, installation or configuration parameters/selections/settings which the manufacturer has specified in their documentation as being available only in the maintenance mode

3.1.17
network storm
unplanned excessive transmission of traffic in a network causing the network to be overwhelmed and degrading the planned performance

3.1.18
normal operation
use of functionality which is described as being available for an operator by the documentation of the manufacturer

3.1.19
private key
cryptographic key of an entity's asymmetric key pair which can only be used by that entity

3.1.20
public key
cryptographic key of an entity's asymmetric key pair which can be made public

3.1.21
remote maintenance
maintenance access to equipment by any user (human, software process or device) communicating from outside the perimeter of the controlled network being addressed that can result in changes to the manufacturer's configuration and operator settings

3.1.22
removable external data source
REDS
user removable non-network data source, including, but not limited to, compact discs, memory sticks and Bluetooth®[1] data storage devices

[SOURCE: IEC 61162-460:2018, 3.32, modified – The words "data storage" have been added in the definition, and the note to entry has been deleted.]

3.1.23
secret key
cryptographic key used with symmetric cryptographic techniques and usable only by a set of specified entities

[1] Bluetooth is the trademark of a product supplied by Bluetooth Special Interest Group. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

3.1.24
security strength
number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system

EXAMPLE 80 bits, 112 bits, 128 bits, 192 bits, 256 bits.

Note 1 to entry: Security strength of a 2048-bit RSA key is 112 bits.

3.1.25
signer
entity generating a digital signature

[SOURCE: ISO/IEC 13888-1:2020, 3.52]

3.1.26
session
semi-permanent stateful and interactive information interchange between two or more communicating devices

3.1.27
trust
relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well-defined way (with respect to the activities) that does not violate the given security policy

3.1.28
trusted third party
security authority, or its agent, trusted by other entities with respect to security-related activities

Note 1 to entry: In the context of ISO/IEC 13888 (all parts), a trusted third party is trusted by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as an adjudicator.

3.1.29
user
any person that is using the equipment as intended

3.2 Abbreviated terms

EUT equipment under test
IMO International Maritime Organization
IP Internet protocol
LAN local area network
MAC media access control
TCP transmission control protocol
UDP user datagram protocol
USB universal serial bus
VDR voyage data recorder
VLAN virtual LAN

4 Module A: Data files

4.1 General

This module applies during normal operation.

During normal operation, transport integrity and source identification shall be implemented for all non-executable data files, for example chart or route data files, when they are made available for the first time for operational use in the equipment from the outside of a controlled network. Non-executable files which intentionally contain executable code, for example scripts or executable files embedded in a compressed file, shall comply with the requirement of module B instead.

4.2 Requirements

4.2.1 Transport integrity

For a data file transfer into the equipment, a mechanism of verifying transport integrity shall be employed such that files are transferred without being corrupted, for example hash-codes or checksums in Ethernet frames, IP packets or communication protocols such as IEC 61162-450. Files which fail this integrity check shall not be made available for operational use in the equipment.

NOTE 1 Transport method can include the possibility of requesting resend of a part of a data file. In such case, the integrity check is passed when all parts of data file have been transferred correctly.

Where a recognised data file format supports a means for verifying the integrity of the file, such as a checksum, hash-code or digital signature such as IHO S-100, the integrity of the file shall be checked using this means. Files which fail this integrity check shall not be made available for operational use in the equipment.

NOTE 2 Recording or logging of network traffic including IEC 61162-450 data files, for example by VDR, is not subject to authentication.

NOTE 3 Integrity checking is implicit in the use of digital signatures. See Annex C for details.

NOTE 4 In addition to data integrity check, to protect against malformed data files, the end equipment can validate the data before use (for example by checking against the data structure – also known as schema – in accordance with individual equipment standards).

4.2.2 Source authentication

At least one of the alternatives below shall be implemented.

a) The manufacturer shall apply source authentication when a data file is made available for operational use in the equipment in accordance with the requirements of Annex B.

d) The manufacturer shall state in the operator's manual the type(s) of data file(s) and the risk posed to the equipment. Only stated data file type(s) shall be importable into equipment. The manufacturer shall assess the risk posed by the permitted file types, considering the risk to integrity and availability of equipment, and its functions shall implement additional technical controls that may be required to mitigate the risk and shall identify any additional procedural steps that the user should take, documenting these in the operator's manual.

   Some examples of technical controls are given below.

1) The parsing of escape or other special characters and sequences to ensure that they are correctly interpreted.
2) An XML parser which is configured to limited expansion of user defined entities.
3) Disabling macros.
4) Disabling JavaScript.
5) Employing exploit mitigation techniques such as ASLR and DEP.

6) Performing data validation in accordance with individual equipment standards.
7) Scanning files externally to the equipment using an anti-malware scanner.
8) Use of controlled external tools such as dedicated cables.

NOTE 1 There are many different controls which can be used individually or in combination, depending upon the file type, equipment type and functions provided by the equipment and the controlled network. This document expects the manufacturer to demonstrate that a detailed analysis of the risks has been performed and that appropriate mitigations have been put in place.

Where alternative a) has been implemented, at least one of the source authentication alternatives below shall be implemented.

1) IEC 61162-460 compliant equipment that is intended to be installed in an IEC 61162-460 compliant network using IEC 61162-460 compliant methods

NOTE 2 A 450-node can be also an IEC 61162-460 compliant node.

Within the controlled network of IEC 61162-460, the identification of the source by one or more of the source MAC address, the source IP address or the source identifier (SFI) of IEC 61162-450 shall be used. Data files from the outside of the controlled network shall be authenticated.

For this alternative, the installation manuals provided by the manufacturer shall contain appropriate installation instructions including a warning that, if used in other environments, the equipment may not be cyber secure.

2) IEC 61162-450 compliant equipment that is intended to be installed in a closed network using IEC 61162-450 compliant methods

NOTE 3 A 450-node can be also an IEC 61162-460 compliant node.

Within the closed network of IEC 61162-450, the identification of the source by one or more of the source MAC address, the source IP address or the source identifier (SFI) of IEC 61162-450 shall be used. Data files from the outside of the closed network shall be authenticated.

The installation manuals provided by the manufacturer shall contain appropriate installation instructions (e.g. this equipment shall be installed within a closed network, where all interfaces including those in use of this closed network are physically blocked from easy access by a user without a tool or key) including a warning that, if used in other environments, the equipment may not be cyber secure.

3) Equipment not compliant with IEC 61162-450 or IEC 61162-460 that is intended to be installed in a network or equipment that is not intended to be installed in a network

Such equipment may include for example an Ethernet based interface for a network or may be without any interface to any local area network.

The manufacturer shall declare for which alternative(s) the equipment has been designed.

4.3 Methods of testing and required test results

Confirm by analytical evaluation that a mechanism of verifying transport integrity has been employed.

Confirm by analytical evaluation that files that fail the transport integrity check are not made available for operational use in the equipment.

Confirm by observation that, where data files containing a means for verifying the integrity of the file fail the integrity check, they are not made available for operational use in the equipment.

Where source authentication is implemented in accordance with 4.2.2 a):

– confirm by observation that the requirements of Annex B are complied with;

– confirm by observation that the manufacturer provides a declaration for which authentication method the EUT is designed;

– confirm by observation that non-executable files are not made available for operational use in the EUT in the following cases:

  • an attempt to import a file from non-authorized source;

  • an attempt to import a file with invalid content (i.e. not passing integrity check), for example an attempt to import a file with invalid hash-code or certificate.

Where data files can be made available for operational use in the EUT without first passing source authentication in accordance with 4.2.2 b):

– use the manufacturer's documentation to obtain the list of non-executable files that can be made available for operational use in the EUT;

– confirm by analytical evaluation that non-executable files not listed by the manufacturer are not made available for operational use in the EUT;

– confirm by observation that the operator's manual specifies supported file types and risks together with procedural steps for their mitigation; confirm by analytical evaluation that only the stated files are made available for operational use in the equipment;

– confirm by observation that the manufacturer's documentation includes the risk assessment; confirm by observation that the operator's manual specifies risks together with procedural steps for their mitigation.

Confirm by analytical evaluation that all non-executable files are verified as described in the manufacturer's documentation before use by the EUT.

5 Module B: Execution of executables

5.1 General

This module applies both during normal operation and in maintenance mode.

5.2 Requirements

In normal operation:

1) all automatic execution from EDS, including auto-run and booting, shall be prohibited;
2) manual execution of any type of executables from EDS shall only be possible after passing source authentication and integrity check of the executable content of the EDS, for example by using digital signatures or secret keys (i.e. authentication) as defined by Annex B;
3) in the event of a catastrophic equipment failure, cryptographically authenticated software may boot and run from EDS as a reversionary measure;
4) if the execution of the executable will affect the normal operation of the device, sufficient indication shall be given before execution; the execution shall only be possible in case of confirmation by the operator. The manufacturer shall provide a list of executables which are possible to execute during normal operation.

NOTE Firmware or application software can automatically authenticate executables without user intervention, provided that an informative indication is given when those executables are executed.

In maintenance mode, auto-run of executables and booting from EDS is permitted.

Annex C contains examples of technical methods to perform authentication.

5.3 Methods of testing and required test results

Use an EDS that, when used in an unrestricted computer, would cause an automatic action. One by one, attach a device to the connection points for REDS, which are accessible by the operator without using a tool or key, or insert a media into the REDS (disc drives, etc.) and confirm by observation that all automatic executions at the EUT are prohibited.

If the EUT provides manual execution of any type of files from EDS, confirm by analytical evaluation that manual execution is only possible for files which have been verified by digital signatures or secret keys.

If the EUT provides execution of executable during normal operation, use the list of such executions provided by the manufacturer and confirm by observation that either there is no recognizable affect for normal operation or that the EUT requested confirmation from the user to execute an executable affecting normal operation.

The relevant tests regarding digital signatures and secret keys are defined in Annex B.

6 Module C: User authentication

6.1 General

This module applies both during normal operation and for entering maintenance mode.

Where user authentication is needed, it is described in the individual equipment standard or in the relevant paragraphs of this document (see module G, module H and module N; see Annex B).

User authentication involves making a claim to an identity and verifying that claim by providing proof in the form of an authenticator which is often based upon some secret such as a password or private key.

It is acceptable for the identity to be generic to a "role" associated with all users rather than a single "individual" user.

6.2 Requirements

Where provided, user authentication shall be implemented by at least one of the alternatives below.

a) Passwords

This method is applicable for equipment which includes an alphanumeric keyboard functionality or other data entry device capable of entering passwords during normal operation.

User authentication with log-in information shall be provided, for example passwords used with usernames, password used with key cards, etc.

Where passwords based user authentication is used, the minimum password length shall be 8 characters. Additional password restrictions may be enforced at the manufacturer's discretion, including length, character complexity, periodic changes and excluded word lists.

NOTE 1 NIST SP 800-63B recommends a password length of at least 8 characters and no specific requirements on complexity (mix of letters, symbols, and figures) because highly complex memorized secrets introduce a new potential vulnerability, for example password written on paper.

The operator's manual shall include guidance such as: "Passwords should not contain the users name or parts of the user's full name such as first name, company name, product name, etc. Dictionary words should not be used. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd') should not be used."

Passwords intended for user authentication shall be stored securely (e.g. non-reversible using a hash-function) and shall not be readily accessible (e.g. human readable) if access to the storage medium is obtained.

e) Secret key or other symmetric cryptographic method

Where secret keys are used, the key length shall be 128 bits or longer, and shall have a security strength of at least 128 bits and the key shall be random in nature.

NOTE 2 An example is authentication using a token containing a symmetric authentication key.

NOTE 3 Security strength is a comparable measure of the complexity of breaking a given cipher and is distinct from cipher key lengths. For example, RSA 3072 and ECDSA 256 are considered to have a comparable security strength of 128 bits despite very different key lengths.

NOTE 4 Random in nature means that the creation of the next secret key is not the next value in alphanumeric order (i.e. the new value is unpredictable based on the previous value).

f) Smart card or other asymmetric cryptographic method

Where asymmetric cryptography is used, for example in smart cards, the security strength of the cipher shall be at least 112 bits.

g) Identification

For equipment for which full user authentication is impractical due to it not having alphanumeric keyboard functionality or other data entry device capable of entering passwords during normal operation and lacks the capability for entering a password, the equipment shall provide one of following alternatives:

- the user interface for special modes (for example maintenance mode, software updates readily available) is accessible only by intentional and multiple operator action, for example pressing multiple buttons simultaneously, multiple buttons in a sequence, etc.;
- other means than log-in information described by the manufacturer.

For alternatives a), b) and c), where applicable, means shall be provided for an authenticated user to change a password or secret key used for user authentication or to revoke the public key associated with a compromised private key.

If practicable, means shall be provided to restrict repeated failed user authentication attempts, for example introducing a delay before a new attempt can be accepted, locking access after a specified number of attempts, etc. These means shall not impact normal operation, for example by introducing any delay for operation of normal operation, locking any functionality of normal operation, etc. These means shall leave the equipment in the same state as before the failed attempt. Where appropriate, an informative indication that user authentication is restricted (for example by delay, account locking, etc.) shall be provided when in force.

NOTE 5 Although an informative indication as to the reason for an authentication failure can be helpful to typical users of the equipment, more information than is necessary can assist malicious users in attacking the equipment. For this reason, the manufacturer can determine a level of detail appropriate for the equipment. Useful indication can provide information about what is the current state, for example blocked for a delay, account has been locked, etc.

If practicable, compliant equipment shall record activation of maintenance mode into an internal log, which is capable of recording the last 10 activations, or into the syslog which may be external to the equipment.

NOTE 6 Description of the syslog is available in IEC 61162-450 and RFC 5424.

Where applicable, for alternatives a), b) and c), the equipment shall provide the capability for user account management applicable to the type of user authentication provided (e.g. creation of accounts, update of passwords, deletion of accounts).

6.3 Methods of testing and required test results

Execute tests for all alternatives provided by the EUT.

a) If the EUT provides user authentication based on passwords:

- confirm by observation that the user authentication is based on at least an 8-character long password;
- confirm by inspection of the manufacturer's documentation that the operator's manual includes guidance on the use of passwords;
- confirm by analytical evaluation that passwords intended for user authentication are stored securely and are not readily accessible; for example, analytical evaluation could include attempts to operate the EUT, attempts to gain access to things for which access should not be available, study of documentation provided by the manufacturer or request to the manufacturer to clarify any detail.

h) If the EUT provides user authentication based on secret key or other symmetric cryptographic method, confirm by inspection of the manufacturer's documentation that the key length is 128 bits or longer, the security strength of the key is at least 128 bits or longer, and that the key is random by nature.

i) If the EUT provides user authentication based on smart card or other asymmetric cryptographic method, confirm by inspection of the manufacturer's documentation that the security strength of the cipher is at least 112 bits.

j) If the EUT provides user authentication based on identification, confirm by observation that the user interface for special modes is accessible only by:

- intentional and multiple operator actions; or
- other means described in the manufacturer's documentation.

Confirm by observation, if applicable, that the user can change password(s) used for user authentication.

Where applicable, confirm by analytical evaluation that compromised passwords, private or other secret keys can be revoked by the method defined by the manufacturer.

Confirm by observation that new passwords, private and secret keys in normal operation are not accepted and their acceptance is limited to a specific part of the user interface requiring separate user authentication as defined by the manufacturer.

If practicable, confirm by observation that means are provided to restrict repeated failed attempts of user authentication. Confirm by observation that the means provided do not impact normal operation by causing delays in normal operation or locking of any functionality of normal operation. Confirm by observation that these means leave the equipment a similar state as before the failed attempt. If appropriate, confirm by observation that an informative indication that user authentication is restricted is provided when in force.

Confirm by observation that access to make changes to the manufacturer's configuration requires user authentication.

If practicable, confirm by observation that the last 10 activations of maintenance mode are available in an internal log or in syslog. Syslog may be part of the simulation environment around the equipment.

If applicable, for alternatives a), b) and c), confirm by observation that the EUT provides user account management.

7 Module D: System defence

7.1 General

This module applies during normal operation.

System defence consists of malware prevention, host firewall, host intrusion prevention and user notification, where practical, if malware or other software infection is detected. Host related items are related to the installation environment of the equipment. Malware prevention can be provided by equipment or by the installation environment of the equipment. An example of environment providing system defence is IEC 61162-460 compliant equipment installed in an IEC 61162-460 compliant network.

NOTE 1 A 450-node can be also an IEC 61162-460 compliant node.

NOTE 2 Disaster and recovery plans are the responsibility of the owner of the ship and are assumed to be included in the ship's integrated safety management plan (ISMP).

Denial of service (DoS) is a broad category of cyber-attacks intended to prevent use of network-connected systems, compromise their security and ultimately cause damage. Via a network-connection, a successful DoS attack can be used as a stepping stone to first silence a target device which the attacker may then impersonate to gain further access or control. Attacks can be based on direct methods and indirect methods that increase network traffic to the point where errors occur or a victim can no longer perform intended functions. This may accomplish the attacker's goal or present further opportunities to exploit. DoS attacks can harness normally useful and benign network protocols and standard network services to interact with additional network nodes in a way that multiplies the resulting spike of traffic addressed to the victim while hiding the source of the attack. Attacks can take place that cause a flood of traffic but use low bandwidth functions that never establish a typical transaction channel and do not get logged.

Although not addressed here, in the broadest sense DoS also includes actions to disable equipment directly by physical attack or indirectly by attacking elements critical to its function like power supply or thermal management devices.

7.2 Malware protection

7.2.1 Requirements

7.2.1.1 General

System defence for malware protection shall be provided by one of the alternatives A, B, C, D.1 or D.2, or any combination of them, described in 7.2.1.2 to 7.2.1.5.

The manufacturer shall declare for which alternatives A, B, C, D.1 and/or D.2 the equipment has been designed.

For each alternative, the installation and operator's manuals provided by the manufacturer shall contain appropriate installation and operating instructions including a warning that the equipment may be vulnerable to a cybersecurity threat and could result in a cybersecurity risk for other equipment if used outside of its intended environment.

7.2.1.2 Alternative A

IEC 61162-460 compliant equipment intended for installation in an IEC 61162-460 compliant network.

NOTE A 450-node can be also an IEC 61162-460 compliant node.

For this alternative, there are no additional requirements.

7.2.1.3 Alternative B

Equipment intended for installation in a controlled network other than IEC 61162-460.

For this alternative, security measures equivalent or exceeding those of IEC 61162-460 shall be provided. An example is IEEE 802.1X in place of MAC address filtering prescribed by IEC 61162-460.

7.2.1.4 Alternative C

Equipment with no accessible interfaces through which malware could penetrate inside or through which intrusion could be possible.

For this alternative, there are no additional requirements.

NOTE 1 This applies for example to embedded systems without an operating system or to embedded systems with such physical interfaces which do not form a platform for malware penetration nor form a platform for intrusion. Such interfaces are for example IEC 61162-1 serial lines, or radio air interfaces for maritime radiocommunication or navigation equipment where such interfaces are not capable of transferring files.

NOTE 2 An "accessible interface" is an interface which is physically accessible without the use of a tool or key and not normally connected to other equipment in normal operation. Examples include USB port used to load data files, serial programming or "debug" ports or network ports.

7.2.1.5 Alternative D

7.2.1.5.1 General

Equipment with accessible interfaces through which malware could penetrate inside or through which intrusion could be possible.

NOTE This alternative is typical for off-the-shelf computers without any special configuration.

The manufacturer shall consider the risks associated with the equipment's function and the environment it is designed to operate in when determining the applicable protections.

The manufacturer shall detail the methods employed to reduce the cybersecurity risks associated with the equipment.

The principle of least privilege shall be applied so that in normal operation the equipment provides only the necessary access to functionality required to perform its intended function. For example, read, write and execute access to files may be configured appropriately for the functionality intended to be available in normal operation.

Equipment shall provide basic hardening against attacks or damage. All unused interfaces, network ports, services and applications not necessary for normal operation shall be disabled.

This alternative requires at least one of the alternatives D.1 or D.2 as a method to mitigate risk in such equipment.

7.2.1.5.2 Alternative D.1

Protection by anti-malware is provided.

a) The equipment shall include malware protection software module and, if applicable, include the possibility to update the malware prevention. Manufacturers shall provide documented procedures for the installation and update of this software module.

k) The equipment with its anti-malware software shall meet its performance requirements under normal operation.

l) The manufacturer shall agree a documented procedure with the type approval body, which details the method for evaluating and recording the effect of applying anti-malware definition file updates or software updates to the equipment.

m) This procedure shall provide assurance that the updates of a particular type will not adversely affect the intended functionality or compliance of the equipment. Annex A provides guidance relating to the type approval of equipment where anti malware definition files or software is updated.

NOTE This update process can be equivalent to the documented quality procedure for evaluating the effect of chart updates (data files) and chart engine updates (software) on the equipment.

n) For anti-malware software updates, the requirements of module N apply. It is not necessary for updates of definition files or other anti-malware data files to comply with the subclauses defined in module N.

o) The installation and operator's manuals shall describe how to update the malware prevention, as applicable. The manuals shall also describe the conditions under which the update should be performed.

p) The malware prevention module shall inform the user about outdated malware prevention after the maximum time since the last update has been reached.

q) The manufacturer shall document the process implemented to assure that updates to anti-malware software do not affect the intended functionality or compliance of the equipment with applicable performance standards and testing standards.

r) If practical, the equipment shall have means for indicating to the user if the system has detected the presence of malware as a result of either continuous or periodic or on demand processes, for example by comparison against white list, etc.

7.2.1.5.3 Alternative D.2

Protection by firewall is provided.

For equipment communicating over Internet protocol (IP) interfaces, the installation manuals and, where applicable, operator's manuals shall contain instructions that the equipment shall be installed in an environment which is protected by a correctly configured firewall (for example a firewall compliant with 460-Gateway requirements). The detailed configuration instructions may be available in a separate confidential security configuration document (see Annex E).

NOTE The optional security configuration document could contain additional essential information for a system integrator (for example a shipyard) so that they can install the equipment with the necessary protection.

The instructions for correct configuration shall:

a) state that the default policy shall be to drop network packets which are not explicitly permitted;

s) detail how to configure TCP and UDP based packet filtering based upon source and destination IP address and destination port for each network flow;

t) detail the average network bandwidth utilisation for each network flow;

u) where supported by the firewall, detail how to prevent bandwidth utilisation exceeding a pre-defined threshold (e.g. broadcast storm, denial of service prevention);

v) detail any other layer 3 protocols that need to be allowed by the firewall;

w) explain how to configure and how to test the least promiscuous set of firewall rules required for the equipment's intended function, for example so that wildcards and aliases are not misconfigured.

Where the equipment has one or more essential services or applications known to be susceptible to high risk vulnerabilities, for example remote code execution, the manuals shall provide additional guidance for protecting the navigation network, for example, how to configure an intrusion detection/prevention system in addition to the firewall described in 7.2.1.5.3.

7.2.2 Methods of testing and required test results

7.2.2.1 General

Confirm by inspection of the manufacturer's documentation that it identifies which alternative A, B, C, D.1 and/or D.2 for which the EUT has been designed.

Confirm by inspection of manufacturer's documentation that for each alternative the installation and/or operator's manuals provided contain appropriate installation and operating instructions including a warning that the equipment may be vulnerable to a cybersecurity threat and could result in a cybersecurity risk for other equipment if used outside of its intended environment.

7.2.2.2 Alternative A

Confirm by inspection of a test report or certificate of compliance, submitted with the EUT, that the EUT complies with IEC 61162-460 and confirm by inspection that the manufacturer's documentation describes installation in an IEC 61162-460-compliant network.

NOTE A 450-node can be also an IEC 61162-460 compliant node.

7.2.2.3 Alternative B

Confirm by analytical evaluation of the manufacturer's documentation that:

– it states that the unit is intended for use in a controlled network;

– it identifies requirements of IEC 61162-460 with which the EUT complies and the exceptions where the EUT does not, and that for each such exception it clearly specifies an alternative implemented by the EUT and provides an analysis of the equivalence or improvement to security provided by the alternative in the intended network compared with IEC 61162-460.

7.2.2.4 Alternative C

Confirm by analytical evaluation of the manufacturer's documentation that the EUT has no accessible interfaces capable of providing a means for malware data files to enter the EUT or be passed through to other equipment.

7.2.2.5 Alternative D

7.2.2.5.1 General

Confirm by inspection of the manufacturer's documentation that:

– it identifies the functions, interfaces, network ports, services and applications necessary for normal operation; and

– it identifies the functions that are removed or restricted.

Select a representative sample, for example 5 pieces or more if appropriate, of removed or restricted access to functions, services and applications, and confirm by analytical evaluation that the documented access limitations have been implemented.

Confirm by analytical evaluation that unused physical interfaces and logical network ports are disabled.

Confirm by analytical evaluation of the EUT that the protection of these unused items cannot be circumvented or disabled during normal operation without using a tool or key.

Confirm one or more of the alternatives D.1 or D.2 as explained in 7.2.2.5.2 and 7.2.2.5.3.

7.2.2.5.2 Alternative D.1

Confirm by observation that malware protection is functioning, for example by use of EICAR test string (click on "Download anti-malware testfile" on http://www.eicar.org).

Confirm:

a) if applicable, by inspection that the manufacturer has provided a documented procedure for installing anti-malware definition file updates or anti-malware software updates on the EUT;

x) by analytical evaluation that the procedure is capable of maintaining compliant operation of the EUT;

y) by inspection of manufacturer's documentation that documented procedures are provided, agreed with type approval body, describing the details of the methods for evaluating and recording the effect of applying anti-malware definition file updates or software updates to the equipment;

z) by analytical evaluation that installation and actions undertaken by the malware protection software assures that the updates of a particular type will not adversely affect the intended functionality or compliance of the equipment with the relevant rules for type approval;

aa) by analytical evaluation that the update procedure complies with the requirements of module N;

bb) if applicable, by observation that installation and operator's manuals describe how to update the malware prevention including the conditions under which this update should be performed;

cc) by observation that means are provided to inform the operator of the date of the most recent update or the date when the next update is due;

dd) if applicable, by inspection that manufacturer's documentation describes the process implemented to assure that updates to anti-malware do not affect intended functionality or compliance with applicable performance standards and testing standards;

ee) if implemented, by analytical evaluation that the equipment provides means for indicating to the user if the system has detected the presence of malware as a result of either continuous or periodic or on demand processes, for example by comparison against white lists, etc.

7.2.2.5.3 Alternative D.2

Confirm by inspection of installation manuals and, where applicable, operator's manuals that they contain instructions that the EUT shall be installed in an environment protected by a correctly configured firewall.

Confirm by inspection of installation manuals and, where applicable, operator's manuals and, where applicable, a confidential security configuration document that the instructions for configuration include:

a) a statement that the default policy is to drop network packets which are not explicitly permitted;

ff) how to configure TCP and UDP based packet filtering based upon source and destination IP address and destination port for each network flow;

gg) the average network bandwidth utilisation for each network flow;

hh) how to prevent bandwidth utilisation exceeding a pre-defined threshold, where supported by the firewall;

ii) identification of any other layer 3 protocols that need to be allowed by the firewall;

jj) how to configure and how to test the least promiscuous set of firewall rules required for the equipment's intended function, for example so that wildcards and aliases are not misconfigured.

If the EUT include one or more essential services or applications known to be susceptible to high risk vulnerabilities, then confirm by inspection of installation and operator's manuals that they provide additional guidance for the protection of the navigation network.

7.3 Denial of service protection

7.3.1 Requirements

7.3.1.1 General

System defence against DoS attacks shall be provided by one of the alternatives A, B, C, D, or any combination of them, described in 7.3.1.2 to 7.3.1.5.

The manufacturer shall declare for which alternatives A, B, C or D, or any combination of them, the equipment has been designed.

7.3.1.2 Alternative A

IEC 61162-450 or IEC 61162-460 compliant equipment intended to be installed in an IEC 61162-460 compliant network.

NOTE A 450-node can be also an IEC 61162-460 compliant node.

There are no additional requirements for protection against DoS attacks over a network.

7.3.1.3 Alternative B

Equipment without network interfaces for which DoS attacks are relevant.

There are no additional requirements for protection against DoS attacks over a network for equipment which is within a physically secure area.

The installation manuals shall state that the equipment is to be installed in a physically secure area.

7.3.1.4 Alternative C

Internal interfaces within a closed network.

For equipment that is intended to be installed within a closed network which is outside a physically secure area, the equipment shall at least be protected by compensating measures, for example network defences in case the control network gets compromised. The equipment shall be protected via internal input rate limitation or be protected by external protection method described in the installation manual (e.g. a switch with rate limitation, use of Controller Area Network (CAN)-bus which has measures by design, etc.).

There are no requirements for equipment which is intended to be installed within a closed network which is physically secured.

The installation manuals shall state that the equipment is to be installed in a physically secure area.

7.3.1.5 Alternative D

Any other equipment.

The manufacturer shall determine appropriate perimeter, network and host based measures to assist in mitigating DoS attacks.

NOTE 1 These measures can be provided by the EUT or by the environment in which the EUT is installed.

For example, relevant attacks may include:

– amplification attacks which cause excessive traffic for a network host by manipulating network protocols used within the network including, but not limited to, Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Domain Name System (DNS), Simple Network Management Protocol (SNMP) and multicast or broadcast discovery protocols;
– spoofing attacks whereby the source address of a frame or packet is spoofed such that the network infrastructure components appear to see traffic from many sources directed to one or more network hosts;
– network storm.

The installation manual of the equipment shall detail any such measures required in the installation environment of the equipment to assist in mitigating DoS attacks. The installation manual shall include a warning that, if these measures are not present in the environment in which the equipment is installed, the equipment may not be secure.

Measures that shall be considered include:

1) traffic filtering, for example by firewalls, routers or switches;
2) restricting bandwidth (quality of service);
3) physical isolation of network components;
4) physical access controls.

Optionally, the following measures may be considered, but are not limited to:

5) intrusion detection and prevention software;
6) redundant network connections;
7) authenticated connections;
8) load balancing;
9) traffic or application monitoring, analysis and alerting.

NOTE 2 Quality of service protects parts of a system not directly targeted by DoS attack.

NOTE 3 In some circumstances, such as saturation of an equipment's network links, it is possible that equipment's services cannot be prevented from being degraded or made unavailable. However, equipment and systems can be designed to minimise the lasting impact to services in such circumstances.

For DoS attacks other than caused by network storm, the manufacturer shall identify and document vulnerabilities and measures necessary to mitigate the risk of those vulnerabilities being exploited. Some examples of DoS attacks other than network storm are:

– repeated attempt to log in with wrong password;
– transmission of items more often than assumed by receiver;
– transmission of items with intentionally malformed content;
– database (e.g. structured query language – SQL) wildcard query attacks;
– locking customer accounts;
– buffer overflows;
– user specified object allocation;
– user input as a loop counter;
– writing user provided data to disk;
– failure to release resources;
– storing too much data in session.

NOTE 4 Guidance about mitigation for above is available from OWASP[2]:
http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf,
https://www.owasp.org/index.php/Testing_for_Denial_of_Service

7.3.2 Methods of testing and required test results

7.3.2.1 General

Confirm by inspection of the manufacturer's documentation that it identifies for which alternative A, B, C or D the EUT has been designed.

7.3.2.2 Alternative A

Confirm by inspection of a test report or certificate of compliance, submitted with the EUT, that the EUT complies with IEC 61162-460.

NOTE A 450-node can be also an IEC 61162-460 compliant node.

Confirm by inspection of manufacturer's documentation that the equipment is only intended to be installed in an IEC 61162-460 compliant network and that the manufacturer's documentation contains a clear warning that the equipment may not be secure if installed in an environment other than an IEC 61162-460 compliant network.

7.3.2.3 Alternative B

Confirm by inspection that installation manual states that the equipment is to be installed in a physically secure area.

7.3.2.4 Alternative C

If the equipment has built-in protection:

1) confirm by inspection of the manufacturer's documentation that the maximum operational input data rate is declared by the manufacturer;
2) use simulation arrangements to create traffic up to the maximum that is declared by the manufacturer; confirm by observation that the EUT meets its performance requirements;
3) use simulation arrangements to create traffic of 200 % of the maximum that is declared by the manufacturer but not over 90 % of the maximum available for the network interface for a period of at least 10 min; after 10 min, return to the maximum traffic as declared by the manufacturer; confirm by analytical evaluation that the EUT returns to intended functionality or compliance after the change in traffic.

If the equipment requires external protection, confirm by inspection of the installation manual that it describes the installation environment.

If the equipment is intended to be installed within a closed network which is physically secured:

1) confirm by inspection of manufacturer's documentation that the equipment is only intended to be used within a closed network and that the documentation contains a clear warning that the equipment may not be secure if installed in any other environment;
2) confirm by inspection that installation manual states that the equipment is to be installed in a physically secure area.

[2] Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software.

7.3.2.5 Alternative D

Confirm by analytical evaluation of the manufacturer's documentation that appropriate perimeter, network and host based measures to assist in mitigating the risk of DoS attacks have been identified. This may include spoofing, amplification and network storms.

Confirm by analytical evaluation that the measures the manufacturer has identified as being provided by the EUT to assist in mitigating the risk of DoS attacks, including spoofing, amplification and network storms, are present in the EUT.

Confirm by inspection that the installation manual of the equipment describes detailed measures required in the installation environment of the EUT, if any of the following are not provided by the EUT:

1) traffic filtering, for example by firewalls, routers or switches;
2) restricting bandwidth (quality of service);
3) physical isolation of network components;
4) physical access controls; or
5) additional measures as identified by the manufacturer.

Confirm by inspection of the installation manual that a warning is provided that, if these measures are not present in the environment in which the EUT is installed, the EUT may not be secure.

To test declared and excessive amount of network traffic at EUT level:

6) confirm by inspection of the manufacturer's documentation that the maximum operational input data rate is declared by the manufacturer;
7) use simulation arrangements to create traffic up to the maximum that is declared by the manufacturer; confirm by observation that the EUT meets its performance requirements;
8) use simulation arrangements to create traffic of 200 % of the maximum that is declared by the manufacturer but not over 90 % of the maximum available for the network interface for a period of at least 10 min; after 10 min, return to the maximum traffic as declared by the manufacturer; confirm by analytical evaluation that the EUT returns to intended functionality or compliance after the change in traffic;

   NOTE The 90 % limit is to enable practical simulation environments to create enough network traffic.

9) confirm by inspection of the manufacturer's documentation that the maximum operational output data rate is declared by the manufacturer;
10) confirm by analytical evaluation of the documented evidence or confirm by analytical evaluation of the EUT itself that the EUT does not exceed the declared maximum operational output bandwidth.

To test mitigation of DoS attacks other than caused by excessive amount of network traffic at EUT:

11) confirm by inspection of the manufacturer's documentation that it describes the measures taken to mitigate DoS attacks other than DoS by excessive traffic;
12) confirm by analytical evaluation that measures taken to mitigate DoS attacks other than DoS by excessive traffic address each identified vulnerability in the EUT.

8 Module E: Network access

8.1 General

This module applies both during normal operation and in maintenance mode.

This module applies to equipment designed to be connected to a network external to the equipment including networks carrying non-IP based traffic. Guidance on interconnecting networks can be found in Annex F.

8.2 Equipment which connects to a network

8.2.1 Requirements

The installation manuals or confidential security configuration document (see Annex E) shall contain the following information:

a) network services, i.e. ports and protocols necessary for the intended functionality of the equipment, for example for IP-based networks UDP, TCP, Simple Network Management Protocol (SNMP), Internet Group Management Protocol (IGMP), Network Time Protocol (NTP) time synchronization;

NOTE 1 Where manufacturer proprietary protocols are used, it is sufficient to declare their use without providing details of such a protocol but specifying the carrier, for example UDP multicast.

kk) the typical rate at which the equipment transmits data onto the network over a representative time period determined by the manufacturer;

NOTE 2 The description for the above can provide this information over multiple time periods, for example to inform periods of use of maximum technical rate and information about average over a longer period.

ll) the maximum sustained rate at which the equipment can receive traffic from the network averaged over a representative time period determined by the manufacturer;

mm) the effect on the equipment of exceeding the maximum input rate at which the equipment can receive traffic;

NOTE 3 The description for above could be as simple as that there is loss of normal functionality of named items.

nn) all necessary physical security requirements for installation of the equipment;

oo) all necessary network architecture (e.g. requirements for gateways) and equipment configuration requirements (e.g. network access controls such as MAC address filtering and default IP addresses).

8.2.2 Methods of testing and required test results

Confirm by inspection that the installation manuals or confidential security configuration documents contain:

a) detail of the network services necessary for the intended functionality of the EUT;

pp) detail of the typical rate at which the equipment transmits data onto the network over a representative time period determined by the manufacturer;

qq) detail of the maximum sustained rate at which the equipment can receive traffic from the network averaged over a representative time period determined by the manufacturer;

rr) detail of the effect on the equipment of exceeding the maximum input rate at which the equipment can receive traffic;

ss) detail of the physical security requirement for the installation of the equipment;

tt) detail of the network architecture and equipment configuration setups.

8.3 Equipment providing network access between controlled networks

8.3.1 Requirements

8.3.1.1 General

Communication between equipment on different controlled networks shall be provided by one of the alternatives described in 8.3.1.2 to 8.3.1.4. See Annex F for guidance.

8.3.1.2 Alternative A

Connections between IP based networks: an IEC 61162-460 compliant forwarder (460-Forwarder) intended to be installed between two IEC 61162-460 compliant networks or between an IEC 61162-460 compliant network and another controlled network.

For this alternative, there are no additional requirements.

8.3.1.3 Alternative B

Connections between IP based networks: a managed switch or router consistent with the principles of a 460-Forwarder as described in IEC 61162-460 for network traffic management, VLAN, security and network monitoring.

Manufacturer's documentation shall clearly identify how network traffic management, VLAN, security, and network monitoring are implemented so that a comparison with IEC 61162-460 can be made.

8.3.1.4 Alternative C

Connection between an IP based network and a non-IP based network and connection between two non-IP based networks.

The data transfer between the two networks shall be based on the principles of the IEC 61162-460-Forwarder.

8.3.2 Methods of testing and required test results

8.3.2.1 General

Depending of the alternative implemented in the EUT, one of the alternatives described in 8.3.2.2 to 8.3.2.4 shall be tested.

8.3.2.2 Alternative A

Confirm by inspection of a test report or certificate of compliance, submitted with the EUT, that the EUT complies with IEC 61162-460 and confirm by inspection that the manufacturer's documentation describes the installation in an IEC 61162-460-compliant network.

8.3.2.3 Alternative B

Confirm by analytical evaluation that the manufacturer's documentation identifies applicable requirements of the following items of IEC 61162-460 with which the EUT complies and the exceptions where the EUT does not comply:

1) network traffic management;
2) VLAN;
3) security;
4) network monitoring.

For each applicable exception, confirm by analytical evaluation that the manufacturer's documentation clearly specifies the alternative implemented by the EUT and provides an analysis of the equivalence or improvement to security provided by the alternative in the intended network compared with IEC 61162-460. See Annex F for guidance.

8.3.2.4 Alternative C

Confirm by analytical evaluation that the data transfer between the two networks follows the principles of the IEC 61162-460-Forwarder.

8.4 Equipment providing network access between controlled and uncontrolled networks

8.4.1 Requirements

8.4.1.1 General

Communication between equipment on controlled and uncontrolled networks shall be provided by one of the alternatives described in 8.4.1.2 and 8.4.1.3 or equivalent where applicable. See Annex F for guidance.

8.4.1.2 Alternative A

An IEC 61162-460 compliant gateway (460-Gateway) or wireless gateway (460-Wireless Gateway) intended to be installed in an IEC 61162-460 compliant network.

For this alternative, there are no additional requirements.

8.4.1.3 Alternative B

A network gateway or router consistent with following principles of 460-Gateway or 460-Wireless Gateway:

1) for all gateways: 460-Gateway functions: firewall, application server, demilitarized zone (DMZ), direct communication;
2) for all gateways: 460-Gateway security requirements;
3) additional for wireless gateways: 460-Wireless gateway functions: gateway function requirements plus limits on traffic forwarding, client-only, encryption, and 460-Node.

8.4.2 Methods of testing and required test results

8.4.2.1 General

Depending of the alternative implemented in the EUT, one of the alternatives described in 8.4.2.2 and 8.4.2.3 shall be tested.

8.4.2.2 Alternative A

If the EUT is compliant to the applicable requirements for a 460-Gateway, confirm by inspection of a test report or certificate of compliance, submitted with the EUT, that the EUT complies with IEC 61162-460 and confirm by inspection that the manufacturer’s documentation describes installation in an IEC 61162-460-compliant network.

8.4.2.3 Alternative B

Confirm by analytical evaluation that the manufacturer's documentation identifies applicable requirements of the following items of IEC 61162-460 with which the EUT complies and the exceptions where the EUT does not comply:

1) 460-Gateway functions: firewall, application server, DMZ, direct communication;
2) 460-Gateway security;
3) wireless gateways: functions: 460-Wireless Gateway function requirements plus limits on traffic forwarding, client-only, encryption, and 460-Node.

For each applicable exception, confirm that the documentation clearly specifies an alternative implemented by the EUT and provides an analysis of the equivalence or improvement to security provided by the alternative in the intended network compared with IEC 61162-460.

9 Module F: Access to operating system

9.1 General

This module applies during normal operation if an operating system is provided on the equipment.

9.2 Requirements

The system shall conform to 4.2.3.2 of IEC 60945:2002 about access to the operating system.

NOTE 1 More detailed requirements are available in module G.

NOTE 2 Changes to the configuration of the operating system are understood to happen in maintenance mode (see module H).

This document does not contain requirements for limiting access to the operating system while in maintenance mode.

9.3 Methods of testing and required test results

Confirm by observation that an IEC 60945:2002 test report is provided and comprises the relevant subclause (4.2.3.2). Otherwise, perform the test according to IEC 60945.

10 Module G: Booting environment

10.1 General

This module applies both during normal operation and in maintenance mode.

The booting environment includes for example boot loader, operating system and BIOS.

There is no requirement to restrict access to the booting environment when in maintenance mode.

10.2 Requirements

During normal operation, repeated attempts of power on/power off/power on cycles shall not result in access to the internal storage, operating system or BIOS.

During normal operation, special key codes, i.e. pressing a control or multiple controls in a user interface, shall not result in access to the internal storage, operating system or BIOS unless the user has successfully passed authentication as defined in module C.

During normal operation, at booting phase, a connection to an external device (for example USB device, network, etc.) shall not result in access to the internal storage, operating system or BIOS unless the user has successfully passed authentication as defined in module C.

Optionally, the maintenance mode may include a configuration to enable and disable booting from an external device.

NOTE An unsuccessful user authentication attempt does not constitute access to the operating system or BIOS.

Equipment design may be based on firmware, operating system and/or application software being stored in a removable storage device, for example CompactFlash (CF)-card, Secure Digital (SD) card, etc. In this case, module J applies.

10.3 Methods of testing and required test results

Confirm by observation that repeating power on/power off/power on cycle 3 consecutive times does not result to access to the internal storage, operating system or BIOS.

Confirm by inspection of manufacturer's documentation that, during normal operation, there are no special key codes available to access the internal storage, operating system or BIOS without passing user authentication.

If available, confirm by observation that, during normal operation at booting phase, connection to an external device does not cause access to the internal storage, operating system or BIOS of the EUT without passing user authentication as defined in module C.

If applicable, confirm by observation that access to removable storage used for firmware, operating system or application software complies with module J.

11 Module H: Maintenance mode

11.1 General

This module applies when accessing and in maintenance mode.

The maintenance mode is intended to be accessible only by users authorized by the manufacturer or the manufacturer's authorised representatives who have the competencies that ensure that maintenance activities do not compromise the compliance of the equipment with the applicable international standards and regulations.

NOTE Authorized users are typically those working for a company which performs initial installation or later maintenance. They are not necessarily employees of the manufacturing organisation.

11.2 Requirements

Access to maintenance mode shall only be possible following successful user authentication (see module C).

A failed user authentication attempt shall not provide access to the operating system or BIOS. This includes ensuring that the following actions do not provide access to maintenance mode unless the user has successfully passed authentication as defined in module C:

– repeated power cycling without a tool or key;
– insertion or removal of a device or cable available to a typical user during normal operation without a tool or key; for example, USB device, network connections, etc.

If practicable:

a) the equipment shall record activation of maintenance mode into an internal log, which is capable of recording at least the last 10 activations; or

uu) the activation of the maintenance mode shall be transmitted via syslog message so that other devices are able to record such events. Where the equipment relies upon syslog messages, either equipment capable of receiving and processing syslog messages shall be provided as part of the deployed system or the installation manuals shall contain an instruction that the equipment shall be interfaced to other equipment with such capabilities.

NOTE 1 Description of the syslog is available in IEC 61162-450 and RFC 5424. IEC 61162-460 requires implementation of syslog functionality.

Additional logs may be provided as applicable, for example firewall logs, operating system event logs, install/uninstall logs, malware/intrusion event logs, REDS connectivity logs, application logs.

If applicable, the integrity of the change of the manufacturer's configuration shall be verified for all changes received from external sources. Integrity verification may be implemented by procedural means (e.g. by using means provided by the manufacturer to confirm applicability prior to deployment).

During normal operation, there shall be no access to change the manufacturer's configuration without user authentication as defined in module C or using a tool or key.

NOTE 2 Sometimes, simple devices have no maintenance mode. For example, it is possible that they have only dip switches to change configuration (for example dip switches for CAN-bus addresses). In such cases, the protection could be by no free access to the dip switches. See module C in 6.2 d).

NOTE 3 During maintenance mode, there is no restriction on changing the manufacturer's configuration.

If the equipment includes a graphical display and if the equipment is in the maintenance mode, then the maintenance mode shall be permanently indicated or be distinctively obvious.

11.3 Methods of testing and required test results

If the equipment provides a maintenance mode, confirm by inspection of the manufacturer's documentation which of the user authentication methods listed in module C is provided to access the maintenance mode.

Confirm by observation that it is not possible to enter maintenance mode without first successfully passing user authentication as defined in module C.

Confirm by observation that a failed attempt to access the maintenance mode does not result in access to the operating system or BIOS.

Confirm by observation that repeating a power on/power off/power on cycle three times does not result in access to maintenance mode.

Confirm by observation that insertion or removal of devices or cables without a tool or key does not result in access to maintenance mode unless that device or cable is associated with user authentication as defined in module C.

If practicable, confirm by observation that the equipment is able to record at least the last 10 activations of the maintenance mode or that such activations are sent by the equipment using syslog messages. If syslog messages are used, either confirm by observation that the handling of syslog messages are provided within the system or confirm by inspection that the installation manual contains instruction about installation into an environment which provide handling of syslog messages.

If provided, confirm by observation that the equipment has recorded manufacturer specified events in the optional logs or that such events are sent by the equipment using syslog messages.

Confirm by analytical evaluation that it is not possible to change the manufacturer's configuration during normal operation without first successfully passing user authentication as defined in module C or using a tool or key.

If the EUT provides a mode to change the manufacturer's configuration from an external source, confirm by observation that a manufacturer's configuration with an invalid format is rejected by the EUT. Examples of invalid format include an incorrect file or message checksum, an incorrect hash or an incompatible parameter setting.

NOTE An example of a message is a UDP datagram on Ethernet.

If the equipment provides a maintenance mode and a graphical display, activate the maintenance mode and confirm by observation that maintenance mode is permanently indicated on the graphical display or is visibly distinct from the normal operation.

12 Module I: Protection against unintentional crash caused by user input

12.1 General

This module applies during normal operation.

Software which does not validate user input properly could result in parts of the system receiving unintended input which may result in unexpected code behaviour or crashes.

Checking the valid syntax and semantics of user inputs (e.g., character sets, string lengths, numerical ranges and validities, and acceptable values) verifies that those inputs match the application's expected definitions for format and content. Prescreening inputs prior to passing the data on to internal software algorithms and processes prevents the content from being unintentionally interpreted as commands or from behaving in an unexpected manner.

Malicious attacks such as structured query language (SQL) injection, transmission of data with intentionally malformed content and buffer overflow are already covered in module D (see Clause 7). The scope of this module is the validation of data entered through the user interface.

NOTE The requirements in module I are based upon controls referenced in the National Institute of Standards and Technology Special Publication 800-53, Rev. 4 (NIST SP 800-53). Specifically, two of the Control Enhancements for security control SI-10 "Information Input Validation": SI-10(3) "Predictable Behaviour in the face of invalid inputs" and SI-10(5) "Restrict inputs to trusted sources and approved formats."

12.2 Requirements

For user-entered data, a method of validation shall be applied to verify all relevant properties of the data including length, type of input, full range of acceptable values, missing or extra inputs, syntax and consistency across related fields, for example:

– "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if the input is only expected to contain colours such as "red" or "blue";

– acceptable values: while the value "361" is a valid integer, it is not a valid value for a ship's course or heading.

Data that does not pass the input validation method shall be rejected for use and shall not adversely affect the normal operation of the equipment.

12.3 Methods of testing and required test results

Confirmation of user input validation shall be based on one of the alternatives below.

a) For each of the relevant properties of the user input data (e.g. length, type of input, range of acceptable values, missing or extra inputs, syntax and consistency), attempt to make invalid entries to a representative number of different user entry fields and confirm by observation that the EUT has employed a data validation mechanism which prevents malformed data from impacting the operation of the equipment.

b) Confirm by inspection of manufacturer's documentation that the manufacturer has employed techniques such as fuzz testing (e.g. OWASP®[3] fuzz testing), robustness testing and/or fault injection or alternatively a penetration test report highlighting input validation results, to confirm that user input is adequately validated.

NOTE Fuzz testing is a software testing methodology used to automate the testing of a software application's inputs. The fuzz tester provides invalid, unexpected, or random data as inputs to a computer program and then monitors for software exceptions such as crashes, failures of built-in code assertions, or potential memory leaks. More information can be found at:
https://www.owasp.org/index.php/Fuzzing
https://www.owasp.org/index.php/OWASP_Testing_Guide_Appendix_C:_Fuzz_Vectors

13 Module J: Interfaces for removable devices including USB

13.1 General

This module applies during normal operation.

This document does not contain requirements for limiting USB functionality or functionality of other removable interfaces while in maintenance mode. The other removable interfaces in this context means any user removable technology for which a user could remove the original device from the interface and replace the original device by another device which may have different functionality or different data content, for example hot-swappable Peripheral Component Interconnect (PCI) Express card or firewire device.

The vulnerability addressed by Clause 13 for other removable interfaces is related to the implementation of physical interfaces including USB ports where a connected device may be removed by the user leaving the interface physically exposed for connection with any other device.

This document accepts that the protection of the USB interface or other removable interface shall be addressed by physical protection (see 13.2.1) or by operational protection (see 13.2.2) or both.

The manufacturer shall declare which alternatives have been provided for each interface.

13.2 Requirements

13.2.1 Physical protection

The number of connection points for REDS (for example keyboard/mice ports, printer ports, USB ports, Secure Digital (SD)-cards, disc drives, (hot swappable) drive bays, etc.) shall be limited to the minimum required for the operation of the system and its lifetime maintenance and support. An exception is USB ports providing only the functionality of charging. All other points shall either:

[3] Open Web Application Security Project (OWASP) fuzz testing or fuzzing is an example of a black box software testing technique. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

– be physically blocked from easy access without a tool or key; or
– be subject to an instruction in the manufacturer's installation manual that the equipment shall only be installed in a closed console or cabinet requiring additional tools or keys to open; the manufacturer's installation manual shall include a notice of cyber security risk if not installed as described by the manufacturer.

13.2.2 Operational protection

Interfaces for removable devices (for example storage, keyboards, printers, etc.) as required for operation and lifecycle maintenance shall be minimized and restricted by one or more of the alternatives listed below:

– logical blocking (i.e. software or firmware or operating system) of the interface;
– preventing device drivers from installing; this means that the device drivers can only be installed in maintenance mode;
– cryptographic authentication with a security strength of at least 128 bits prior to use of any content or functionality from USB devices;
– restriction of the interface to specific USB device classes (see Annex D);
– restriction of the interface to a specific hardware identifier (i.e. same model of equipment);
– restriction of the interface to specific instance identifiers (i.e. individual equipment).

For any removable device which cannot practically be restricted using the options detailed above, the manufacturer shall provide information about how they have limited the interface to its intended functionality and protected against misuse.

Interfaces for REDS (including USB ports) shall be protected against unauthenticated data files (see module A) and auto-run of executables (see module B).

13.3 Methods of testing and required test results

13.3.1 Physical protection

Where physical protection is provided, refer to the manufacturer's documentation and confirm by inspection of the documented evidence that the number of connection points for REDS are limited to the minimum required for the operation of the system and its lifetime maintenance and support.

For all other connection points, either:

– confirm by observation that they are physically blocked from easy access without a tool or key, or that they can be used for charging only; or
– confirm by inspection of the manufacturer's documentation that there is an instruction in the manufacturer's installation manual that the equipment shall only be installed in a closed console or cabinet requiring additional tools or keys to open and that there is a notice of cyber security risk if not installed as described by the manufacturer.

13.3.2 Operational protection

Where operational protection is provided, for USB connection points, use the manufacturer's documentation and confirm by analytical evaluation that the EUT refuses to perform any other functionality than that specified in the manufacturer's documentation.

Refer to manufacturer's documentation and confirm by inspection that a declaration is included about which alternative of operational protection for each removable interface is provided.

If it is possible for a REDS technology to have functionality other than data storage (for example from keyboard to data storage), then attach one by one an example of such a non-data storage device to the connection point and confirm by analytical evaluation that the EUT only performs functions specified in the manufacturer's documentation.

If applicable, refer to the manufacturer's documentation and confirm by inspection that information is available as to how the interface is limited to its intended functionality and protected against misuse for any removable device which cannot practically be restricted using the options listed in 13.2.

14 Module K: IEC 61162-1 or IEC 61162-2 as interface

This module applies both during normal operation and in maintenance mode.

IEC 61162-1 or IEC 61162-2 compliant interfaces are hardwired from one equipment to another. Existing equipment standards already manage such issues as protection of parameters setup, etc. which may be vulnerable to a cyber threat.

NOTE An example of protection of parameter setup is IEC 61993-2:2018 AIS Class A.

Requirements for checksum verification and handling of malformed sentences are fully specified in existing equipment standards and IEC 61162-1.

Requirements for traffic converted between an IEC 61162-1 or IEC 61162-2 interface and IEC 61162-450 interface are specified in module L.

15 Module L: IEC 61162-450 as interface

15.1 General

This module applies during normal operation.

For any file received through this interface, module A and module B apply.

For malware protection and intrusion prevention, module D applies.

15.2 IEC 61162-1 sentences

An example of an external threat related to IEC 61162-450 interfaces and the IEC 61162-1 sentences distributed in the Local Area Network (LAN) is an unauthorized command to perform an action or to set a manufacturer's configuration parameter. Requirements for this issue are covered by module H.

Requirements for checksum verification and handling of malformed sentences are covered by module K.

Requirements for authentication and identification are fully specified in IEC 61162-450.

Authentication may be used as described for TAG block parameter "General authentication – a" in IEC 61162-450.

15.3 IEC 61162-450 used for file transfer

15.3 applies both to IEC 61162-450 binary file transfer and to any file transfer based on ONF as defined by IEC 61162-450.

For the transfer of data files, module A applies. Recording or logging of data files, for example by VDR, is not restricted.

For the transfer of executables, module B applies.

16 Module M: Other interfaces

This module applies during normal operation.

This module applies to any other interface than mentioned in module J, module K or module L such as firewire, thunderbolt, Small Computer System Interface (SCSI), etc. including wireless interfaces such as Bluetooth®[4], Wi-Fi®[5], Near Field Communication (NFC), etc. which is not part of module J, module K or module L.

NOTE Wi-Fi is a family of wireless networking technologies, based on the IEEE 802.11 family of standards.

All relevant modules of this document apply when an interface provides applicable functionality.

17 Module N: Software maintenance

17.1 General

This module applies both during normal operation and in maintenance mode.

NOTE 1 Equipment can change in build standard during its life cycle. For example, new feature can be added, existing feature can be amended or design mistakes – often known as bugs – can be fixed. The type approval certificate is valid for an identified version of the product. Therefore, a new test of compliance and resulting new certificate can be required when the software is changed.

NOTE 2 The local conformity assessment laws, for example within the European Union, can require reporting of any modification to the conformity assessment authority.

Security related updates to software are an important part of protecting a system against attack, whilst bug fixes and new functionality are often important in maintaining equipment. It is important however to ensure that changes to software do not adversely impact the intended functionality of the equipment or its compliance to applicable regulations, prior to their deployment.

Software maintenance may be performed by:

– authorized persons local to the equipment, in maintenance mode;
– the crew in normal operation, where semi-automated means are provided;
– authorized persons remote from the equipment in maintenance mode for remote access (see Clause 18).

Maintenance mode is intended to be available only to personnel authorized by the manufacturer.

---

4 Bluetooth is the trademark of a product supplied by Bluetooth SIG, Inc. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

5 Wi-Fi is the trademark of a product supplied by Wi-Fi Alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

17.2 Software maintenance in maintenance mode

17.2.1 Requirements

The requirements of module H shall apply.

The manufacturer shall ensure that, where updates to software have the potential to impact the intended functionality of the equipment, the service documentation describes any limitations to the application of the updates.

Facilities or procedures, either external or internal to the equipment, shall be provided for restoring the equipment to a known good state, for example to recover from corruption or malware infection. This shall be described in the installation manual and may, for example, involve restoration from a backup or replacing and re-configuring affected equipment.

17.2.2 Methods of testing and required test results

If the equipment provides a means to update the software in maintenance mode:

1) confirm that EUT complies with module H;
2) refer to manufacturer's documentation and confirm that the means to update the software in maintenance mode is described in the installation manual;
3) confirm by analytical evaluation that it is not possible to carry out the described software update procedure in normal operation;
4) refer to manufacturer's documentation and confirm that any limitations on application of the update that might affect normal operation of the equipment are clearly described;
5) refer to manufacturer's documentation and confirm that the means to restore the equipment to a known good state are described in the installation manual, and in the operator's manual where appropriate;
6) confirm by observation that it is possible to carry out the described procedure to restore the EUT to a known good state.

17.3 Semi-automatic software maintenance by the crew onboard the vessel

17.3.1 General

Semi-automatic software maintenance may be provided by the equipment.

Semi-automatic software maintenance may be performed by authorised persons on board the vessel including members of the crew or other users authorised by the manufacturer.

This kind of software maintenance may be based on files classified as data files or as executables. Such files are subject to source authentication and integrity check (see module A and module B).

The software maintenance related files may arrive to a remote system (for example by post, email attachment) from which the files are required to be moved to the equipment (for example by using EDS) or the software maintenance related files may arrive to be readily available for the equipment (i.e. no additional manual transfer of the files by the user is required).

17.3.2 Requirements

The operator's manual shall describe instructions for semi-automatic software maintenance.

The files associated with the maintenance shall be authenticated as applicable (see module A and module B.

The execution of a software update shall begin only after successful user authentication (see module C).

Access to semi-automatic software maintenance shall not lead to access to maintenance mode.

Semi-automatic software maintenance can be launched from the maintenance mode.

The equipment shall request and receive positive user confirmation prior to commencing the software update.

Two steps are required before execution of an update, user authentication and obtaining express permission to begin installing the update. Both of these steps may be performed at the same time.

Where maintenance to software have the potential to impact the intended functionality of the equipment, the impact and/or any limitations to the application(s) shall be indicated to the operator and the equipment shall request and receive positive user confirmation prior to commencing the software update.

The user shall be notified if, once initiated, the software update fails to successfully occur.

After completion of the update, the authenticated user shall be able to roll back to the manufacturer's previous configuration. This capability to roll back shall be possible also after power off/power on sequence. As minimum, the roll back shall be available at least for the manufacturer's working configuration.

Roll back procedures may include storing of the manufacturer's previous configuration (i.e. software and setup) in another shipboard equipment or EDS. If this method is provided, the operator's manual shall include instructions on how to execute the roll back procedure including the storage of the manufacturer's previous configuration and shall include instructions for storing the copy of the manufacturer's previous configuration for future use (for example, mark and store the used USB memory stick in a safe place from where it is available for the future roll back). All data files or executables of this method including the manufacturer's previous configuration shall be subject to source authentication and integrity check (see module A and module B).

The equipment may inform the user about a software update readily available or the user may initiate the process of software update.

If provided, informing the user about a readily available software update:

a) shall not obscure or prevent normal functionality of the equipment;

NOTE An indicator, small icon or small dialog can comply with above.

vv) may provide the possibility to accept initiation of the procedure to update software;

ww) shall include the possibility to acknowledge the information without initiation of the procedure to update software;

xx) may include a repeated reminder, but this shall comply with the above requirements from a) to c).

17.3.3 Methods of testing and required test results

Refer to the operator's manual and confirm by inspection that it contains instructions for software maintenance.

Confirm by analytical evaluation that only files with correct authentication are accepted for maintenance (see module A and module B).

Follow the procedure described in the operator's manual and confirm by observation that the EUT requires both of the following before the update is initiated:

– successful user authentication; and

– user confirmation to initiate the software update.

Confirm by observation that the identity used above cannot be used to access maintenance mode.

Confirm by observation that a software update which has impact and/or any limitations to the application(s) generates an indication to the operator and the software update only starts after the equipment has requested and received positive user confirmation from the operator prior to commencing the software update.

Use manufacturer provided test data set which will prevent an update from successfully completing and confirm by observation that the software update notifies the user that it was unsuccessful.

Use the manufacturer provided test data set and follow the procedure described in the operator's manual to perform a software update. Then power off and power on. Follow the procedure described in the operator's manual to perform roll back and confirm by observation that it is possible to roll back to the manufacturer's working configuration.

If the EUT provides the means to inform the user about an update that is ready to install:

a) confirm by observation that it does not obscure or prevent normal functionality of the EUT;

yy) if provided, confirm by observation that it is possible to initiate the procedure of software update;

NOTE The authenticated user's consent is needed before initiation of any software update, even if it has previously been delayed or scheduled for a different time.

zz) confirm by observation that it is possible to acknowledge the information without initiation of the procedure to update software;

aaa) if provided, confirm by observation that the repeated reminder complies with requirements from a) to c).

18 Module O: Remote maintenance

18.1 General

This module applies both during normal operation and in maintenance mode.

18.2 Requirements

Equipment shall comply with principles described for security requirements for direct communication in IEC 61162-460 or equivalent.

18.3 Methods of testing and required test results

Confirm by inspection of documented evidence that remote maintenance follows the principles of IEC 61162-460 or equivalent regarding direct communication.

19 Module P: Documentation

19.1 Requirements

The operator's manual shall contain guidance regarding cyber security practices. Some examples are:

– do not write down passwords;
– do not leave secure doors unlocked;
– do not disconnect interface cables;
– do not charge your USB devices except from ports that are intended for charging.

The operator's manual shall explicitly prescribe operation of equipment during normal operation and shall not include cyber security information listed in E.2.1 and E.2.3.

Documentation, for example user and/or installation manuals, if publicly accessible, for example Internet downloadable, shall not contain any default password information, unless the change of the password is possible and required by the manufacturer's installation instructions.

Optionally, manufacturers may provide a cyber security configuration document for equipment (see Annex E) to document cyber security related system design decisions. This documentation shall not be publicly accessible, for example by publicly accessible Internet download.

19.2 Methods of testing and required test results

Confirm by inspection of the manufacturer's documentation that the operator's manual:

a) contains user guidance regarding cyber security practices relevant to the EUT;

bbb) provides only information limited to normal operation and does not contain:

1) cyber security relevant information needed for installation and maintenance, for example information listed in Annex E;

2) any default password information, unless change of the password is possible and required by the manufacturer's installation instructions.

Confirm by inspection of the manufacturer's documentation that the installation manuals, if publicly accessible, for example Internet downloadable, do not contain any default password information, unless the change of the password is possible and required by the manufacturer's installation instructions.

If applicable, confirm by inspection that the manufacturer has provided a declaration that they will not make the cyber security configuration document for equipment publicly available, for example publicly accessible Internet download.

Annex A
(informative)

Guidance on implementing virus and malware protection on type approved equipment

The purpose of Annex A is to tailor the application of cyber security best practices for the maritime shipborne environment on equipment required to be carried by the IMO SOLAS Convention and subject to type approval.

IEC TC 80 has been established to create international standards related to IMO Conventions. IMO member states have agreed the rules in the SOLAS Convention. SOLAS specifies performance requirements of technical arrangements, specifies carriage requirements (i.e. which of the technical arrangements are mandatory to implement onboard vessels operating in international traffic) and requires approval by administration for these technical arrangements. In this context, "administration" means the responsible flag country of the vessel. Typical for approval by administrations is that special test houses and certification bodies recognized by governments perform testing of SOLAS compliance. This process is often called "type approval" and the result is often called a" type approval certificate".

Equipment may change in build standard during its life cycle. For example, new feature may be added, existing feature may be amended or design mistakes – often known as bugs – may be fixed. The type approval certificate is valid for an identified version of the product. Therefore, a new test of compliance and resulting new certificate may be required when the software or hardware is changed.

Issues to consider include the following.

- Frequency of update

  Some virus and malware protection strategies require regular updates of malware data definition files. These updates can be daily or even more frequent. Re-approval of type approved software at this frequency is clearly not practical.

- Impact of false positives

  There is a risk that some types of virus or malware protection software may falsely identify parts of type approved software as malware and thereby interfere with the conformance of the type approved equipment to the applicable standards.

  Mechanisms should be in place to minimise the likelihood of such "false-positives"; these could include manufacturer testing of malware data definition files prior to deployment on equipment. The ability to be able to revert updates of data files should be considered in order to mitigate this risk.

- Continuous operation

  There are only limited periods of time available for possible updates of the equipment. Typically, type approved equipment is required to be available 24/7 while the ship is operational. Interruption of the normal operation to update virus or malware protection software or data definition files cannot be allowed to affect safe operation of the vessel.

  Manufacturers should ensure that, if updates have the potential to impact the operation of the equipment, the user documentation describes precautions, for example it may need to wait until the vessel is moored safely.

- Distinction between executable and data files

  Virus and malware protection solutions often distinguish between executable and data files. Updating the virus/malware data definition files can be considered a modification of the data in the equipment – with parallels to the update of electronic chart data. It may be possible for users to carry out these data file updates as they become available. In contrast, updating the virus or malware detection executable is a change to a type-approved software image that should only be carried out under the control of the manufacturer of the equipment.

The manufacturer should carry out tests to confirm that performance of the type approved equipment is not adversely affected by updates to virus and malware protection software and data definition files and that the equipment remains in conformance with the applicable standards after an update.

- Deep scans

  Some virus and malware protection solutions perform deep scans over an extended period of time that have the potential to interfere with system performance. This can be a concern particularly because navigation equipment does not have a predictable period of low activity.

  Manufacturers should ensure that, if deep scans have the potential to impact the operation of the equipment, the user documentation describes precautions, for example, it may need to wait until the vessel is moored safely.

- Impact on network traffic

  Some malware protection solutions, including anti-virus, firewalls and intrusion protection systems, can adversely interfere with network traffic. To minimise this, messages that can be received during normal operation should not be inspected unless it has been demonstrated that this can be done without impacting system performance and conformance to the applicable standards.

- Type approval

  Virus and malware protection solutions can be an important part of protecting a system from external attacks.

  However, manufacturers should take the above issues into account before implementing virus and malware protection solutions as part of type approved equipment. Where implemented, the manufacturer should:

  – declare the protection mechanisms implemented on the equipment;

  – agree with the type approval body when re-testing and re-approval is needed;

  – document the risks of the protection solution to equipment performance and conformance to the applicable standards and the actions taken to mitigate the risks (including, but not limited to, the issues identified in Annex A);

  – describe any requirements for keeping virus/malware definitions up to date in the user and installation manuals.

Annex B
(normative)

File authentication

B.1 General

Annex B describes the technical alternatives for source authentication and integrity check. See module A and module B for the cases when source authentication and integrity check as specified by Annex B is required.

Source authentication and integrity check of files shall be provided either by digital signatures, which make use of public and private cryptographic key pairs, or under specific circumstances by symmetric algorithms or hash-functions, which make use of a pre-shared secret key. The manufacturer shall declare which of the alternative methods are implemented. Depending on the manufacturer's declaration, Clause B.2 or Clause B.3 apply.

B.2 Digital signatures

B.2.1 Requirements

Digital signatures shall be used to provide a means of source authentication and integrity checking for both executable and non-executable files. This is achieved by encrypting a hash-code using the signer's private key, known as "signing".

In normal operation, it shall only be possible to install a signer's public key or trusted root certificate authority (CA) following successful user authentication as defined in module C or file authentication as defined in Annex B.

Alternatives for providing the public key for the data source are as follows.

1) Non X.509 certificate based

   The public keys may be pre-installed during manufacturing.

   NOTE 1 The format of an X.509 certificate is described in ISO/IEC 9594-8.

2) X.509 certificate based

   In normal operation, it may be possible to install certificates which are signed by a root CA that is already installed or "trusted". These certificates are known as intermediate or leaf certificates.

   Certificates for root CAs may be pre-installed during manufacturing.

   The signer shall provide their public key within an X.509 certificate file separately from, or along with the file to be checked.

   The signer's certificate shall make use of least permissive X.509 extensions appropriate to the certificate's purpose.

   The X.509 certificate corresponding to the private key used for the signing operation shall be signed by a root or intermediate certificate authority unless reasonable justification is provided. Use of self-signed leaf certificates are not encouraged and shall only be used with reasonable justification.

   A signing certificate shall only be considered valid if it chains back to a trusted root CA, i.e. the entire path from the selected certificate to the root certification authority is valid and the root certificate is trusted by the equipment.

As an exception to 1) and 2) above, it shall be possible to install and revoke IHO S-63 and S-100 certificates and public keys on the equipment in normal operation (i.e. outside of maintenance mode) after passing user authentication.

The digital signature algorithm employed shall make use of asymmetric cryptography and shall have equivalent security strength of at least 128 bits.

NOTE 2 Equivalent security strength is different from key length.

The signature may be embedded within the signed file or may be contained within a separate file that is provided with the signed file. Where the signature is not embedded within the signed file and the format of the signature is not already standardised, for example IHO S-63 or GnuPG/OpenPGP, the preferred format of the separate signature file is <name of signed file>.<hash-function type>.snd.

A file with an invalid signature shall not be processed further by the equipment.

NOTE 3 Data integrity check, although useful, is not sufficient to protect against malformed data files and the end equipment needs to validate the data before use (for example by check against data structure also known as schema) in accordance with individual equipment standards.

The ISO and IEC have issued guidance within ISO/IEC 10118 (all parts) and ISO/IEC 14888 (all parts), which shall be considered when selecting a cryptographic hash-function for cryptographic signing operations. Digital signatures making use of MD4, MD5 and SHA1 hash-functions are widely regarded as insecure and they shall not be used in new digital signatures; however, these algorithms may be used for verifying "old" digital signatures (those created before 01 January 2018).

NOTE 4 ISO/IEC 10118-3 details hash-functions including RIPEMD-160, SHA-256, SHA-384, SHA-512, and WHIRLPOOL. Other potentially suitable hash-functions include; SHA3 "Keccak" (FIPS 202), BLAKE2 (RFC 7693).

A method of revoking compromised public key shall be provided. The method shall include user authentication.

B.2.2 Methods of testing and required test results

Confirm by inspection of the manufacturer's documentation that digital signatures are declared as a means by which executable or non-executable files can be made available for operational use in the EUT in normal operation.

Confirm by observation for executable and non-executable files (as applicable) that when attempting to import files into the EUT:

1) unsigned files are not made available for operational use in the EUT;
2) files signed by an untrusted authority are not made available for operational use in the EUT;
3) files signed by a trusted authority, but modified after they were signed (so the signature is not valid) are not made available for operational use in the EUT;
4) files signed by a trusted authority are made available for operational use in the EUT.

NOTE 1 A trusted authority is the entity whose public key is used to decrypt the file.

For non-certificate based means:

1) confirm by observation that it is possible to install (trust) or remove/revoke (untrust) public keys from the EUT in maintenance mode;
2) confirm by observation that the method(s) of installing (trusting) public keys in maintenance mode is unavailable in normal operation.

For certificate based means:

1) confirm by observation that it is possible to install (trust) or remove (untrust) a root certificate from the EUT in maintenance mode;
2) confirm by observation that the method(s) of installing (trusting) a root certificate in maintenance mode is unavailable in normal operation;

3) confirm by inspection of the manufacturer's documentation that the public keys used to authenticate files are contained in X.509 certificates;

NOTE 2 The certificate file itself can be encoded in different ways, for example binary/base64.

4) confirm by inspection of the manufacturer's documentation that the least permissive X.509 extensions appropriate a certificate's purpose are used;

NOTE 3 A certificate can be used for multiple purposes where multiple purposes are necessary.

5) with the exception of leaf or intermediate certificates signed by a root CA, confirm by observation that files authenticated by self signed certificates are not made available for operational use in the EUT;

NOTE 4 A root CA's certificate is necessarily self signed.

6) confirm that a file is made available for operational use in the EUT only when the signing certificate chains back to a trusted root CA's certificate.
   a) Generate a root certificate, intermediate certificate and leaf certificate to be used for file authentication.
   b) Install the root certificate but not the intermediate certificate.
   c) Sign the file using the leaf certificate.
   d) Attempt to make the file available for operational use in the EUT and show that the file is not made available for operational use in the EUT.
   e) Install the intermediate certificate and show that the file is made available for operational use in the EUT.

Confirm by observation that, following successful user authentication, it is possible to install or revoke the IHO S-63 and S-100 certificates and/or public keys on the EUT whilst in normal operation.

Confirm by inspection of manufacturer's documentation that the digital signature algorithm uses asymmetric cryptography and has a security strength of at least 128 bits.

Confirm by observation that, as applicable, the system:

a) is able to handle files where the signature is embedded within the file;

ccc) is able to handle files where the signature is not embedded within the file, but is standardised (e.g. IHO S-63 or GnuPG/OpenPGP);

ddd) is able to handle files where the signature is not embedded but is named <name of signed file>.<hash function type>.snd.

Confirm by observation that, following successful user authentication, it is possible to revoke, uninstall, or otherwise untrust a public key or certificate such that subsequent attempts to import a file into the EUT which is authenticated using the revoked public key or certificate are not successful.

B.3 Symmetric means based upon pre-shared secret keys

B.3.1 Requirements

Clause B.3 provides alternatives for source authentication and integrity check of files using a pre-shared secret key and explains the differing requirements in normal and in maintenance modes.

Symmetric encryption or hash-function algorithms may be used to provide a means of source authentication and integrity checking for both executable and non-executable files. This is achieved by encrypting a hash-code using the shared secret key. Annex C discusses source authentication and integrity check based upon pre-shared secret keys and its limitations.

In normal operation, where reasonable justification can be provided, symmetric methods may be used in place of digital signatures provided that either item 1) or item 2) below is observed. For example, within a controlled network, additional source authentication and integrity check may be provided between navigation equipment over and above the requirements of module A.

1) "One-time pads" may be used for source authentication and integrity check of files. For this alternative, a set of pre-shared secret keys shall only be shared with a single source, individual or organisation and specific destination vessel's navigation system. Each secret pre-shared key shall only be used once to authenticate the source of a file.
2) Source authentication and integrity check using pre-shared secret keys as the method of source authentication and integrity check shall only be used within the onboard systems of a vessel, not to transfer files from any source external to the vessel.

In maintenance mode, symmetric algorithms or hash-functions may be used for source authentication and integrity check of data and executable files since the pre-shared secret key is under the control of the manufacturing organisation.

In all cases, the cryptographic method of source authentication and integrity check employed shall have equivalent security strength of at least 128 bits.

In all cases, a method of revoking a compromised pre-shared secret key shall be provided. The method shall include user authentication.

NOTE This does not exclude using "session keys" or "tokens" for symmetric encryption and hash-code based techniques, provided that they are not used for source authentication and integrity check in normal operation.

B.3.2 Methods of testing and required test results

Confirm by inspection of manufacturer's documentation that pre-shared secret keys are declared as a means by which executable or non-executable files can have their source authenticated by a "source authenticator" and be made available for operational use in the EUT in normal operation.

Confirm by inspection of manufacturer's documentation that justification is provided for the use of symmetric means of file integrity check and authentication.

Confirm by observation for executable and non-executable files (as applicable) that when attempting to import files into the EUT:

– files are not made available for operational use in the EUT without a source authenticator;
– files with a source authenticator for an untrusted pre-shared secret key are not made available for operational use in the EUT;
– files with a source authenticator for a trusted pre-shared secret key, but modified such that the source authenticator is not valid, are not made available for operational use in the EUT.

NOTE A trusted pre-shared secret key is a pre-shared secret key installed in the EUT and used for the purpose of authenticating the source of a file from the group of entities in control of the pre-shared secret key.

Where one-time pre-shared secret keys are used for file authentication:

1) confirm by inspection of the manufacturer's documentation that a method is provided for generating and installing a unique set of pre-shared keys that are shared only between a single vessel's systems and a single individual or organisation;
2) confirm by observation that, once a one-time pre-shared secret has been used to authenticate a file, the same shared secret cannot be used again to authenticate another file.

Where pre-shared secret keys are used for file authentication, confirm by inspection of the manufacturer's documentation (including installation and operator's manuals as appropriate) that technical and/or procedural means are described such that shared secret keys are not used to authenticate files external to the vessel.

Confirm by inspection of manufacturer's documentation that the cryptographic methods used for authentication and integrity check have a security strength of at least 128 bits.

Confirm by observation that, following successful user authentication, it is possible to revoke, uninstall, or otherwise untrust a pre-shared secret key such that subsequent attempts to import a file into the EUT which is authenticated using the revoked pre-shared key are not successful.

Annex C
(informative)

Methods of authentication of data files and executables – Examples

C.1 General

This document requires in many cases authentication of data files and executables in normal operation. In principle, both are files and similar technical methods can be used to authenticate both types. Annex C gives some examples of how this authentication could be implemented.

The integrity of a file may be covered by a checksum or a separate hash-code. These methods do not protect the file against intentional hacking.

In authentication, a file is signed using some secret data that is only known to the creator and intended recipient of the file.

In normal operation, the source to be authenticated is the equipment, individual or organisation, from which the file originates. If any intermediate entity could sign files destined for the navigation system, the process could result in malicious third parties tricking intermediary signing parties into signing malicious content, or themselves sign malicious content prior to being transferred onto the navigation system.

ISO/IEC 10118-3 and ISO/IEC 14888-1 provide further guidance on the topics discussed here.

C.2 Explanations of terms

In Annex C, the following apply.

– MAC algorithm (message authentication code algorithm)

  Algorithm for computing a function that maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

  - for any secret key and any input string, the function can be computed efficiently;
  - for any fixed secret key, and given no prior knowledge of the secret key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the i^{th} input string may have been chosen after observing the value of the first $i - 1$ function values.

  NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2).

  NOTE 2 Computational feasibility depends on the user's specific security requirements and environment.

  NOTE 3 Source: ISO/IEC 9797-1.

– Non-repudiation of origin

  service intended to protect against the originator's false denial of having created the content of a message and of having sent a message

  NOTE 4 Source: ISO/IEC 13888-1.

C.3 Asymmetric cryptography

Asymmetric cryptography involves the generation and use of two cryptographic keys, a "key pair". One cryptographic key is known as the "private key" and as its name suggests, is kept secure or "secret" by its owner. The other cryptographic key is known as the public key and is generally made publicly available.

When the private key is used to encrypt data, only the associated public key can be used to decrypt that data. Since the public key is provided to the recipient to decrypt data, the owner can always maintain control of the private key. The cryptographic key size, related to the algorithm's security strength, is chosen so that the private key cannot be obtained in a reasonable amount of time, given certain computing power assumptions.

If the owner of the private key can be trusted to secure their private key, then the ability to decrypt data with the public key proves that the data has come from the owner of the private key.

The most commonly used algorithm asymmetric cipher is known as RSA.

Asymmetric cryptography, particularly the RSA algorithm, is slow compared to symmetric cryptography. In addition, if someone is able to obtain very large amounts of encrypted data, they may be able to discover the private key. For these reason, public-private key pairs are often used as a means to prove identity by encrypting and decrypting symmetric cryptographic keys, message authentication codes, or challenges, rather than files themselves or large streams of data.

An earlier algorithm known as Diffie-Hellman, named after its creators, allows two parties to agree upon a shared secret by using a method that makes it impossible for an eavesdropper to determine what that secret key is, given certain computing power assumptions. The algorithm cannot however be used to "prove the identity" or authenticate either participant. While this algorithm is an effective means for generating a shared symmetric secret key, without authentication of the participants it is vulnerable to man in the middle attacks, where an eavesdropper can masquerade as each of the participants, generating a shared secret key for communicating from the first participant to the eavesdropper and from the eavesdropper to the second participant. Neither participant would be aware of the eavesdropper.

In order to authenticate either, or both, of the participants, they should first exchange certificates and then prove that they are in possession of the associated private key to encrypt a random array of data known as a "challenge". This allows the generation of a unique session cryptographic key which is used for symmetric cryptographic key encryption between the two participants.

C.4 Digital signatures

A digital signature is a means for mathematically proving message or file authenticity, i.e. an authenticator. A valid digital signature gives the recipient reason to believe that a message or file originates from a trusted sender "data origin authentication", that the sender cannot deny having sent the message or file "non-repudiation of origin", and that the message or file has not been altered in transit "data integrity".

The integrity of a file may be demonstrated by a checksum or a "message digest" of the file content, also known as a "hash-code". The hash-code or checksum may be contained within the file or within a separate file. To check that the file has not unintentionally been modified, the integrity check value is recomputed and compared with the original value. A match indicates that the file is unchanged.

While integrity checks do indicate corruption of the file content after the integrity check value has been computed, these methods do not identify deliberate changes to the file as the hash-code or checksum can be recomputed and the original value replaced with a new value. If a file were corrupted before the original integrity check was computed, the integrity check value would provide no indication of the corruption.

To authenticate the source and integrity of a file, a strong integrity check algorithm is used, typically a dedicated hash-function although, for example, symmetric ciphers may also be used.

Hash-functions used for the digital signatures need to be collision-resistant. The security strength for the selected hash-function needs to meet or exceed the security strength of the parameters used in asymmetric cryptographic key generation.

These integrity codes (hash-codes) are then encrypted using an asymmetric cryptographic algorithm, using the private key associated with the source of a file, the originating entity. The encrypted integrity code is known as a signature. The signature can be contained within the file or as a separate file.

The source's public key needs to be distributed securely to the recipient either by some trusted out of band path or via a trusted third party. The reason for taking care when distributing the public key is so that it is not substituted by an eavesdropper for their own public key. This would allow the eavesdropper to intercept signed data, modify the data and resign the data with their own private key. The file and signature may be sent via an untrusted path.

The recipient of the file uses the sender's public key to decrypt the signature, revealing the integrity code. The recipient then computes the integrity code from the file and compares the two. If the cryptographic key can be decrypted by the sender's public key, then the file has to be from whoever is in possession of the signer's private key, the originating entity. If the two codes match, then the file can be considered unchanged since the integrity code was generated.

The file itself is not encrypted as part of the signing process, although it can be encrypted prior to being signed if confidentiality is required as well as authentication and integrity.

A number of drawbacks from this relatively simple approach will be evident and are discussed in further detail in Clause C.5, which discusses certificates as a means to overcome these issues whilst adding administrative complexity.

NOTE An example of successful onboard use of this method is IHO S-63 used for authentication of ENC charts and updates weekly loaded into the ECDIS onboard. The public keys are also provided within an X.509 certificate.

C.5 Public key infrastructure

C.5.1 General theory

Digital signature is a relatively simple means for verifying some data, such as a file or email, originated from the sender and were not modified during transit from the sender to the recipient. It is however limited in that every sender needs to be trusted independently from every other and if a sender were to lose control of their private key, another individual could impersonate the sender and the authentication can no longer be relied upon.

These problems can to some extent be overcome by the use of validity periods, revocation of the public keys associated with a compromised private key and use of a trusted third party to assist in the distribution of public keys, by verifying the identity of the owner of a public key and then by signing the sender's public key. This process is performed in a standardised and globally recognised manner by using public key infrastructure to manage certificates.

A certificate typically refers to a standardised method of embedding metadata around a public key. The X.509 format is prevalent (see ISO/IEC 9594-8 for specification and technical corrigenda) with DER and PEM encoding used frequently. For DER-encoded X.509, see ISO/IEC 9594-8 and for base 64-encoded X.509 (often called PEM), see section 6.8 of IETF RFC 2045.

The recipient of a certificate can check whether the certificate's metadata is valid and the claimed identity is trusted before making use of the public key it contains to decrypt data, i.e. a certificate contains a unique identifier and details the validity of that public key to provide further guarantees to the recipient.

A certificate contains a validity period. Outside of its validity period, it should not be trusted. A shorter validity period is preferred on security grounds, months rather than years, but this requires regular "renewal" or distribution of new certificates and cryptographic keys.

Version three of the X.509 certificate incorporates extensions which permit only certain types of cryptographic operations, so for example a certificate for email signing cannot be used for server authentication. This way the loss of a private key is not so detrimental. The recipient of some encrypted data, such as a signature, can check to see if that operation is permitted by the certificate and to determine whether the sender is permitted to do so.

An X.509 certificate is signed by a private key, which can be the private key associated with the certificate's public key in the case of self-signed certificates. Self-signed certificates should be trusted on a case by case basis and often software warns the user that the certificate is from an untrusted source and therefore potentially insecure.

Alternatively, a "special" self-signed certificate called a root certificate authority (CA) may be generated. This certificate can be pre-installed into equipment, for example during software install, and may have a long validity period. The CA certificate's private key is used only to sign or revoke other certificates. These "other" certificates are known as leaf certificates and are the ones that are used for a variety of asymmetric encryption operations defined by their extensions and constraints. This may include code signing for example.

The fact that this leaf certificate is now signed by another certificate means that a recipient of the leaf certificate can trust it implicitly along with any permitted encryption functions performed by its private key, as it was issued "signed" by a trusted CA installed on the equipment.

CAs can issue certificate revocation lists (CRLs) which identify certificates which have been revoked, for example if they are no longer needed or if the owner has lost control over them. The CA signs the revocation list and either provides the list at regular intervals or permits others to query any certificate status via a protocol known as OCSP, which operates over Internet protocol.

It is normal practise for a root CA to sign another certificate which also acts as a CA, known as an intermediary CA. This allows the root CA's private key to be stored securely and to be used only to revoke the intermediary CA, while the intermediary CA is used to sign leaf certificates. It is possible to have a number of intermediary CAs, which are each signed by the CA at one level above, forming a chain of certificates from a leaf certificate through each intermediate CA back to the root CA. The recipient can verify each certificate in turn is both valid and signed by a certificate one level up. Provided that all certificates associated with leaf and intermediary CAs are available, the root CA is trusted and no certificates have been revoked.

Once this process is successfully completed, the data encrypted by the private key associated with the leaf certificate can be assumed to be from the source. For the case where a file has been signed, the next process of verifying the now-decrypted authentication code can begin.

Whilst this approach generates significant administrative complexities, namely certificate issuance, renewal and revocation, it provides a means for two independent parties to trust one another with strong security guarantees.

This mechanism is widely used to provide secure communication across an untrusted network. For example, this mechanism is widely used to provide secure browsing, email and financial transactions using the Internet.

C.5.2 Notes about shipboard use

C.5.2.1 Effect of common proxy servers used in communication between ship and shore

In general, where the revocation status of a certificate is checked via a communication path to a trusted authority or distribution point, that communication path has to be available for the check to succeed.

C.5.2.2 Usability of chain of trust for certificates

Public keys and certificates (which contain public keys) can be used to identify vessels, equipment, software applications and users.

In this case, a trusted authority is needed to issue public keys or certificates to vessels, shore centers and authorities and to provide information on their revocation status. For the status of the key or certificate to be checked, the authenticator needs to establish communications with the trusted authority which may reside ashore.

The challenge onboard with the chain of the trust of certificates is long lag times and packet loss in communication between shore and vessel.

Protocols other than TCP are available which seek to provide a perceived performance improvement over a communication medium with higher latency or packet loss than a wired network, such as some wireless interfaces. One example of such a protocol is QUIC, which uses UDP at the transport layer.

C.5.2.3 Usability of automatic check of certificate or public key revocation

In general, where the revocation status of a certificate is checked via a communication path to a trusted authority or distribution point, that communication path has to be available for the check to succeed. Not all vessels have on-line broadband connection available. If available, the on-line broadband connection typically suffers from short and longer (even multiple days) breaks in the connection.

An alternative means of obtaining certificate or public key revocation status may be provided where either:

1) the primary means for an equipment to communicate with a trusted authority in order to check revocation status are unavailable; or
2) the equipment does not itself regularly check a certificate's revocation status.

For example, an ECDIS is not required to check the IHO root CA's periodically. It is assumed that IHO will use the Maritime Safety Information (MSI) distribution to inform revoking of the IHO root CA (the IHO root CA is often referred to as the "IHO public key"). Onboard radio communication facilities to receive MSI are part of the mandatory carriage rules of the Global Maritime Distress and Safety System (GMDSS) and in this instance are deemed to be fit for the purpose of certificate revocation and certificate distribution by an authority responsible for the IHO root CA.

C.6 Symmetric key authentication based on "pre-shared secret key"

This symmetric cryptographic mechanism relies upon two or more participants having knowledge of a shared secret key. The same secret key is used to both encrypt and decrypt data, in a similar fashion to a password. The secret key has to be provided securely to each participant, as obtaining the secret key would allow an eavesdropper to decrypt, modify and encrypt data.

To prove that a participant has knowledge of a secret key, that participant can encrypt some data which is only decipherable by any participant with knowledge of the secret key, with appropriate computing power assumptions. Typically, this requires that the size and entropy of a secret key are sufficiently high for the intended application and that the secret key is stored by and transferred securely to participants.

This mechanism can be used by two parties to prove they are part of a group of two or more participants with knowledge of the secret key. Once the group identity has been established, it is possible to generate a shared session secret key using the Diffie-Hellman or similar method.

A hash-code based message authentication code can be generated by a sender for an array of data or a file, where a shared secret key can be included with a file prior to hashing operations. The fixed length result of a hash-function "considered to be secure" bears no resemblance to the input, is always the same for the same input and is different even with a single change to the input file.

This process results in a keyed-hash based message authentication code, which can be used to verify that the creator of the keyed HMAC has knowledge of the cryptographic key and that the file is unmodified since the time keyed HMAC was computed. An alternative but similar method might involve encrypting an HMAC with a symmetric cryptographic key rather than appending the cryptographic key during the hash-function operation. The code may be stored within the file or in a separate file.

NOTE 1 For some hash-function algorithms, a slightly more complex operation is needed when generating the HMAC to avoid length extension attacks. See ISO/IEC 9797-1 for MACs.

The receiver of the data array or file performs the same keyed HMAC operation on the received file and compares the output to the sender's keyed-HMAC. If the two are identical, then the file can be assumed to be unchanged in transit and from a sender who has knowledge of the shared secret key.

In a similar way to a signature, it is therefore possible to use this keyed-HMAC mechanism with pre-shared cryptographic key to verify the "group identity" of the source of a file. However, because the sender, receiver and any other participants necessarily know the pre-shared cryptographic key, it cannot be asserted that the file has come from an individual party. In addition, there is no "public key" that can be revoked should the pre-shared cryptographic key become known to third parties. These are important disadvantages of any pre-shared cryptographic key method compared to a public-private cryptographic key pair and underscore why the invention of the RSA algorithm was so significant to the field of cryptography.

Once a pre-shared cryptographic key has been used and distributed between participants, it no longer provides guarantees of the authenticity of the data source as any participant could be the source. Instead, an asymmetric mechanism is needed for source authentication, such that every receiver can verify the authenticity of messages it receives, without being able to generate authentic messages.

With the exception of "one-time pads" where a set of pre-shared cryptographic keys are known only to a single source individual or organisation and specific destination vessel's navigation system, authentication of data sources using pre-shared cryptographic keys as the method of authentication are only used within the vessel's systems, i.e. in normal operation, pre-shared cryptographic keys are not used to transfer data onto the navigation system from any source external to the vessel.

ISO/IEC 20648:2016 provides further explanation on this aspect of authentication using pre-shared cryptographic keys in 7.5.

NOTE 2 This does not exclude using symmetric cryptographic key encryption and hash based techniques as part of a "cipher suite", provided that they are not used for authentication of the data source in normal operation.

Annex D
(normative)

USB class codes

Universal Serial Bus (USB) includes class code information that is used to identify a device's functionality and to nominally load a device driver based on that functionality.

Examples are given in Table D.1. A complete list of USB base classes is available from search "defined class" at http://www.usb.org.

Table D.1 – USB class codes

Base class	Descriptor usage	Description
00h	Device	Use class information in the Interface Descriptors
01h	Interface	Audio
02h	Both	Communications and CDC Control
03h	Interface	HID (Human Interface Device)
05h	Interface	Physical
06h	Interface	Image
07h	Interface	Printer
08h	Interface	Mass Storage
09h	Device	Hub
0Ah	Interface	CDC-Data
0Bh	Interface	Smart Card
0Dh	Interface	Content Security
0Eh	Interface	Video
0Fh	Interface	Personal Healthcare
10h	Interface	Audio/Video Devices
11h	Device	Billboard Device Class
12h	Interface	USB Type-C Bridge Class
DCh	Both	Diagnostic Device
E0h	Interface	Wireless Controller
EFh	Both	Miscellaneous
FEh	Interface	Application Specific
FFh	Both	Vendor Specific

Annex E
(informative)

Cyber security configuration document for equipment

E.1 General for the document

A document prepared by the manufacturer. This document is considered confidential between the manufacturer and recipient (e.g. type approval body and system integrator).

E.2 Document parts

E.2.1 Hardening of the operating system

If applicable, it may be listed what has been done to harden the operating system, for example by disabling some part of operating system functionality (for example ftp, smb, http, etc.) or by complying with another named standard.

E.2.2 Update strategy for cyber security reasons

If supported, it may be described which strategy will be employed to inform or provide users of security updates.

EXAMPLE Cyber security related software updates available during warranty period, cyber security related updates available for annual service contract customers, etc.

E.2.3 Strategies for detecting and reacting to future vulnerabilities

If supported, it may be described which strategy will be employed to avoid future vulnerabilities.

EXAMPLE Cyber security related follow-up of cyber threats and creation of related mitigation available for annual service contract customers, etc.

Annex F
(informative)

Guidance on interconnection between networks

F.1 General

Annex F provides guidance on interconnecting one or more networks which utilise technologies not addressed by IEC 61162-450 or IEC 61162-460.

NOTE IEC 61162-450 addresses IEC 61162-1, IEC 61162-2 and IEC 61162-3.

F.2 Guidance

When physically connecting networks together, it is important to consider the effect of the traffic on the devices connected to each network. Depending upon the specifics of the connected network devices and their function, this can affect:

– communications latency;
– integrity of transmitted data (for example loss or corruption);
– traffic throughput of other devices;
– forwarding decisions via conflicts in device identifiers (e.g. IP address conflicts);
– computing resources of other devices.

Within this document, IP networks which require protection are considered to be closed networks or controlled networks. Controlled networks include IEC 61162-460 compliant networks.

A key principle of IEC 61162-460 is that a device which provides interconnections between two networks adequately protects the devices on the two networks by filtering, rate limiting and prioritising traffic.

This interconnecting device may be a discreet device or may be part of some equipment which carries out other functions. For example, an ECDIS may include IEC 61162-1, IEC 61162-2, IEC 61162-3 and Ethernet adapters. This allows the ECDIS to effectively interconnect these networks if the ECDIS provides SNGF and PNGF functions as defined in IEC 61162-450.

An IEC 61162-460 Forwarder is an example of an interconnecting device between two or more controlled networks. An IEC 61162-460 Gateway is an example of a device which may be used to interconnect uncontrolled and IEC 61162-460 networks with alternative stricter constraints.

When interconnecting networks other than those based on Ethernet and Internet protocol, it is important for the system integrator to be made aware of:

– relevant limitations of the equipment, such as the maximum sustained rate at which it can receive traffic and continue to carry out its intended function;
– the effect on the network of that equipment, such as the average rate at which the equipment transmits data onto the network.

An interconnecting device used to connect a controlled network to another controlled network, known as a forwarder, may consider the following:

– access control lists;
– traffic shaping (i.e. bandwidth limiting);
– logical segregation;

– overprovisioning of bandwidth;
– traffic prioritisation (often referred to as "quality of service").

An interconnecting device used to connect an uncontrolled network to a controlled network, known as a gateway, may consider the following:

– blocking direct communications between networks;
– facilitating encrypted and authenticated communication between devices;
– providing common data access to authenticated devices on each network;
– protection from malware appropriate to the computing platform.

Figure F.1 provides some examples for different types of network and associated interconnecting devices.

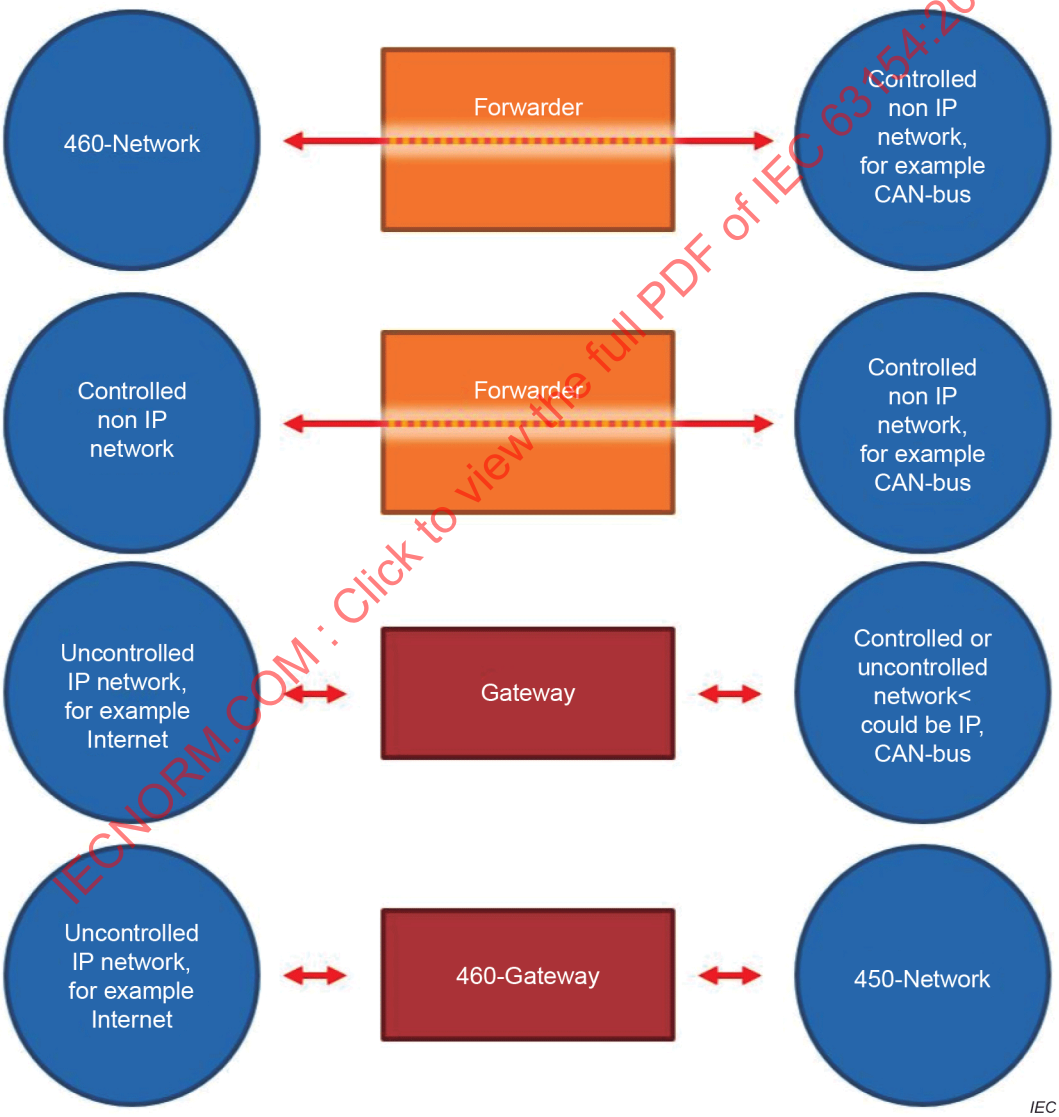


Figure F.1 – Examples for different types of network and associated interconnecting devices

Bibliography

IEC 61162-1, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 1: Single talker and multiple listeners*

IEC 61162-2, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 2: Single talker and multiple listeners, high-speed transmission*

IEC 61162-3, *Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 3: Serial data instrument network*

IEC 61993-2:2018, *Maritime navigation and radiocommunication equipment and systems – Automatic identification systems (AIS) – Part 2: Class A shipborne equipment of the automatic identification system (AIS) – Operational and performance requirements, methods of test and required test results*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*

ISO/IEC 10118 (all parts), *Information technology – Security techniques – Hash-functions*

ISO/IEC 10118-1, *Information technology – Security techniques – Hash-functions – Part 1: General*

ISO/IEC 10118-3, *IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions*

ISO/IEC 10181-1, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*

ISO/IEC 11770-3:2015, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 13888 (all parts), *Information technology – Security techniques – Non-repudiation*

ISO/IEC 13888-1:2020, *Information technology – Security techniques – Non-repudiation – Part 1: General*

ISO/IEC 14888 (all parts), *Information technology – Security techniques – Digital signatures with appendix*

ISO/IEC 14888-1, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*

ISO/IEC 20648:2016, *Information technology – TLS specification for storage systems*

ISO/IEC 9797-1, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks*

IEEE 802.1X, *Standard for Local and metropolitan area networks – Port-Based Network Access Control*

IETF RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*

IETF RFC 5424, *The Syslog Protocol*

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

IHO S-63, *Data protection scheme*

IHO S-100, *Universal hydrographic data model*

IMO, *International Ship and Port Facility Security (ISPS) Code*

IMO resolution MSC.428(98), *Maritime cyber risk management in safety management systems*

IMO, *International convention for the safety of life at sea (SOLAS)*

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*

NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*

Torremolinos International Convention for the Safety of Fishing Vessels

SOMMAIRE

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.

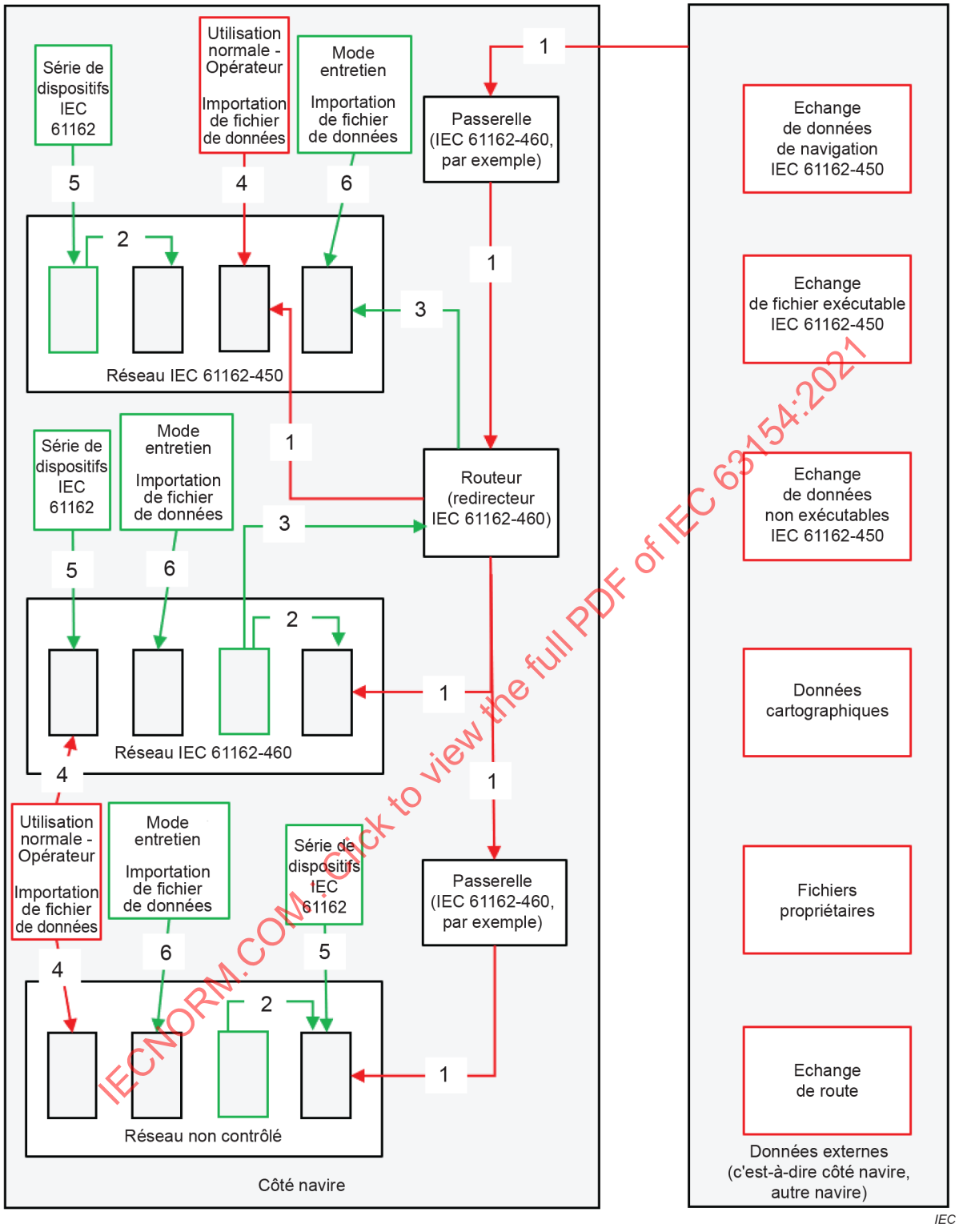


Figure 1 – Quelques exemples de transfert de données

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*

3 Termes, définitions et termes abrégés

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1 Termes et définitions

3.1.1
authentification par distribution aléatoire de l'espace d'adressage
ASLR
processus de protection de mémoire des systèmes d'exploitation qui assure la protection contre les attaques de dépassement de mémoire tampon en randomisant l'emplacement dans lequel les fichiers exécutables sont chargés dans la mémoire

Note 1 à l'article: L'abréviation "ASLR" est dérivée du terme anglais développé correspondant "Address Space Layout Randomization authentication''.

3.1.2
authentification
fourniture de l'assurance qu'une caractéristique revendiquée d'une identité est correcte

Note 1 à l'article: L'authentification est en général une condition préalable à l'autorisation d'accéder à des ressources dans un système.

3.1.3
authentifiant
moyen permettant de confirmer l'identité d'un utilisateur (humain, processus logiciel ou dispositif)

Note 1 à l'article: Par exemple, un mot de passe ou un jeton peut être utilisé comme authentifiant.

3.1.4
authenticité
propriété qu'une entité est bien ce qu'elle revendique être

Note 1 à l'article: L'authenticité est en général utilisée dans le contexte de la confiance en l'identité d'une entité ou de la validité d'une transmission, d'un message ou de l'expéditeur d'un message.

3.1.5
système d'entrée/sortie de base
BIOS
micrologiciel non volatil utilisé pour initialiser le matériel au cours du processus de démarrage (démarrage à la mise sous tension) et pour fournir des services d'exécution aux systèmes d'exploitation et aux programmes

Note 1 à l'article: Il s'agit, par exemple, de l'ancien BIOS (assurant historiquement la conformité avec les IBM PC) et de l'UEFI (Unified Extensible Firmware Interface - Interface micrologicielle extensible unifiée).

3.1.6
réseau contrôlé
réseau satisfaisant aux exigences de l'IEC 61162-460 relatives au réseau contrôlé

3.1.7
réseau fermé
réseau qui est physiquement isolé des autres réseaux

Note 1 à l'article: Un réseau fermé est également appelé un "réseau espacé dans l'air".

Note 2 à l'article: Un réseau fermé ne peut pas contenir de matériel qui se connecte à différents réseaux. Un réseau fermé peut être contrôlé ou non contrôlé.

Note 3 à l'article: Cela inclut, mais sans exhaustivité, les réseaux Ethernet.

3.1.8
clé cryptographique
suite de symboles commandant les opérations d'une transformation cryptographique

EXEMPLE Chiffrement, déchiffrement, calcul de fonction de contrôle cryptographique, calcul de signature et vérification de signature.

3.1.9
prévention de l'exécution des données
DEP
mise en œuvre de la protection de l'espace d'exécution sous Microsoft Windows

Note 1 à l'article: La technique de protection de l'espace d'exécution permet de marquer la mémoire comme étant non exécutable, de sorte que toute tentative d'ajout d'un code exécutable génère une erreur.

Note 2 à l'article: L'abréviation "DEP" est dérivée du terme anglais développé correspondant "Data Execution Prevention".

3.1.10
intégrité des données
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.1.11
signature numérique
données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)

[SOURCE: ISO 7498-2:1989, 3.3.26]

3.1.12
source de données externe
EDS
source de données de réseau ou hors réseau, y compris, entre autres, des REDS et des cartes SIM

Note 1 à l'article: L'abréviation "EDS" est dérivée du terme anglais développé correspondant "External Data Source".

3.1.13
code de hachage
chaîne de bits qui est la sortie d'une fonction de hachage

Note 1 à l'article: La documentation de référence sur ce sujet contient un éventail de termes dont la signification est identique ou similaire à celle de code de hachage. Code de détection de modification, code de détection de manipulation, condensé, résultat de hachage, valeur de hachage et empreinte en sont des exemples.

Note 2 à l'article: NIST SP 800-63B utilise la condensation de message pour cela.

[SOURCE: ISO/IEC 10118-1:2016, 3.3, modifiée – La Note 2 à l'article a été ajoutée.]

3.1.14
fonction de hachage
fonction mettant en correspondance des chaînes de bits de longueur variable (mais généralement avec une limite supérieure) avec des chaînes de bits de longueur fixe, conformément aux deux propriétés suivantes:

– pour une sortie donnée, il est informatiquement impossible de trouver une entrée établissant une correspondance avec cette sortie;
– pour une entrée donnée, il est informatiquement impossible de trouver une seconde établissant une correspondance avec la même sortie

Note 1 à l'article: Utilisée comme partie de l'authentification, de l'intégrité et de la non-répudiation des données.

[SOURCE: ISO/IEC 10118-1:2016, 3.4, modifiée – La Note 1 à l'article a été remplacée par une nouvelle note.]

3.1.15
mode entretien
mode réservé aux personnes qualifiées et autorisées ou aux dispositifs distants autorisés pour les besoins de l'installation, de la mise en service, de la réparation ou de l'entretien du système

3.1.16
configuration du fabricant
partie des paramètres/sélections/réglages du montage, de l'installation ou de la configuration que le fabricant a spécifiée dans sa documentation comme étant disponible uniquement en mode entretien

3.1.17
tempête de réseau
transmission ou trafic excessif imprévu dans un réseau, provoquant la saturation du réseau et la dégradation des performances prévues

3.1.18
fonctionnement normal
utilisation d'une fonctionnalité décrite par la documentation du fabricant comme étant disponible pour un opérateur

3.1.19
clé privée
clé cryptographique de la paire de clés asymétriques d'une entité qui peut uniquement être utilisée par ladite entité

3.1.20
clé publique
clé cryptographique de la paire de clés asymétriques d'une entité qui peut être rendue publique

3.1.21
entretien à distance
accès au matériel par tout utilisateur (humain, processus logiciel ou dispositif) pour l'entretien, communiquant depuis l'extérieur du périmètre du réseau contrôlé concerné et qui peut donner lieu à des modifications de la configuration du fabricant et des réglages de l'opérateur

3.1.22
source de données externe amovible
REDS
source de données qui n'appartient pas au réseau et qui est amovible par l'utilisateur, comprenant, entre autres, les disques compacts, les clés USB et les périphériques de stockage de données Bluetooth®[1]

Note 1 à l'article: L'abréviation "REDS" est dérivée du terme anglais développé correspondant "Removable External Data Source".

[SOURCE: IEC 61162-460:2018, 3.32, modifiée – Dans la définition, l'expression "dispositifs Bluetooth" a été remplacée par "périphériques de stockage de données Bluetooth".]

3.1.23
clé secrète
clé cryptographique utilisée avec des techniques cryptographiques symétriques et utilisable uniquement par un ensemble d'entités spécifiées

3.1.24
force de la sécurité
nombre associé à la quantité de travail exigée (c'est-à-dire le nombre d'opérations) pour casser un algorithme cryptographique ou un système

EXEMPLE 80 bits, 112 bits, 128 bits, 192 bits, 256 bits.

Note 1 à l'article: La force de la sécurité d'une clé RSA 2 048 bits est de 112 bits.

3.1.25
signataire
entité qui génère une signature numérique

[SOURCE: ISO/IEC 13888-1:2020, 3.52]

3.1.26
session
échange d'informations dynamiques et interactives semi-permanentes entre au moins deux dispositifs de communication

3.1.27
confiance
relation entre deux éléments, un ensemble d'activités et une politique de sécurité dans laquelle l'élément x fait confiance à y si et seulement si x a confiance dans le fait que y se comporte d'une manière bien définie (au regard de certaines activités) qui n'enfreint pas la politique de sécurité donnée

3.1.28
tiers de confiance
autorité de sécurité ou son agent auquel il est fait confiance au regard de certaines activités liées à la sécurité

Note 1 à l'article: Dans le contexte de l'ISO/IEC 13888 (toutes les parties), la confiance est accordée au tiers de confiance par l'initiateur, le destinataire et/ou l'autorité de livraison pour les besoins de la non-répudiation, ainsi que par une autre partie telle qu'un arbitre.

[1] Bluetooth est le nom commercial d'un produit fourni par Bluetooth Special Interest Group. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il est démontré qu'ils conduisent aux mêmes résultats.

3.1.29
utilisateur
toute personne qui utilise le matériel de la manière prévue

3.2 Termes abrégés

EUT Equipment Under Test (équipement soumis à essai)
OMI Organisation Maritime Internationale
IP Internet Protocol (protocole Internet)
LAN Local Area Network (réseau local)
MAC Medium Access Control (commande d'accès au support)
TCP Transmission Control Protocol (protocole de commande de transmission)
UDP User Datagram Protocol (protocole de datagramme utilisateur)
USB Universal Serial Bus (bus série universel)
VDR Voyage Data Recorder (enregistreur des données de navigation)
VLAN Virtual LAN (réseau local virtuel)

4 Module A: Fichiers de données

4.1 Généralités

Ce module s'applique pendant le fonctionnement normal.

Pendant le fonctionnement normal, l'intégrité du transport et l'identification de la source doivent être mises en œuvre pour tous les fichiers de données non exécutables (les fichiers de données de carte ou de route, par exemple), lors de leur première mise à disposition pour une utilisation opérationnelle dans le matériel depuis l'extérieur d'un réseau contrôlé. Les fichiers non exécutables qui contiennent délibérément du code exécutable (des scripts ou des fichiers exécutables intégrés dans un fichier compressé, par exemple) doivent plutôt satisfaire aux exigences du module B.

4.2 Exigences

4.2.1 Intégrité du transport

Pour un transfert de fichier de données dans le matériel, un mécanisme de vérification de l'intégrité du transport doit être utilisé de manière à ne pas transférer de fichiers corrompus (codes de hachage ou sommes de contrôle dans des trames Ethernet, des paquets IP ou des protocoles de communication tels que l'IEC 61162-450, par exemple). Les fichiers dont ce contrôle d'intégrité n'a pas été concluant ne doivent pas être mis à disposition pour une utilisation opérationnelle dans le matériel.

NOTE 1 La méthode de transport peut inclure la possibilité de demander un renvoi d'une partie d'un fichier de données. Dans ce cas, le contrôle d'intégrité est réussi lorsque toutes les parties du fichier de données ont été correctement transférées.

Lorsqu'un format de fichier de données reconnu prend en charge un moyen de vérifier l'intégrité du fichier (une somme de contrôle, un code de hachage ou une signature numérique telle que l'OHI S-100, par exemple), l'intégrité du fichier doit être vérifiée par ce moyen. Les fichiers dont ce contrôle d'intégrité n'a pas été concluant ne doivent pas être mis à disposition pour une utilisation opérationnelle dans le matériel.

NOTE 2 L'enregistrement ou la consignation du trafic du réseau incluant les fichiers de données IEC 61162-450 (par un VDR, par exemple) ne fait pas l'objet d'une authentification.

NOTE 3 Le contrôle d'intégrité est implicite lors de l'utilisation des signatures numériques. Voir l'Annexe C pour plus de détails.

NOTE 4 Outre le contrôle d'intégrité des données, pour assurer la protection contre les fichiers de données malformés, le matériel final peut valider les données avant l'utilisation (par exemple en procédant à une vérification par rapport à la structure de données [également appelée schéma] conformément aux normes individuelles s'appliquant au matériel).

4.2.2 Authentification de la source

Au moins l'une des alternatives ci-dessous doit être mise en œuvre:

a) Le fabricant doit appliquer l'authentification de la source lorsqu'un fichier de données est mis à disposition pour une utilisation opérationnelle dans le matériel conformément aux exigences de l'Annexe B.

b) Le fabricant doit indiquer dans le manuel de l'opérateur le ou les types de fichiers de données et le risque auquel s'expose le matériel. Seuls les types de fichiers de données indiqués doivent pouvoir être importés dans le matériel. Le fabricant doit évaluer le risque que posent les types de fichiers autorisés, en prenant en considération le risque pour l'intégrité et la disponibilité du matériel, et ses fonctions doivent mettre en œuvre des contrôles techniques supplémentaires qui peuvent être exigés pour atténuer le risque et doivent identifier toutes les étapes supplémentaires de la procédure qu'il convient que l'utilisateur suive, en les documentant dans le manuel de l'opérateur.

   Des exemples de contrôles techniques sont donnés ci-dessous.

   1) L'analyse syntaxique de l'échappement ou d'autres caractères et séquences spéciaux pour vérifier qu'ils sont correctement interprétés.
   2) Un analyseur XML configuré à une croissance limitée des entités définies par l'utilisateur.
   3) Désactivation des macros.
   4) Désactivation de JavaScript.
   5) Utilisation de techniques de limitation de l'exploitation de failles (ASLR et DEP par exemple).
   6) Validation des données conformément aux normes individuelles du matériel.
   7) Analyse des fichiers en externe du matériel à l'aide d'un analyseur antifichiers malveillants.
   8) Utilisation d'outils externes contrôlés tels que des câbles dédiés.

   NOTE 1 Il existe de nombreux contrôles différents qui peuvent être utilisés individuellement ou en combinaison, suivant le type de fichier, le type de matériel et les fonctions fournies par le matériel et le réseau contrôlé. Le présent document attend du fabricant qu'il démontre qu'une analyse détaillée des risques a été réalisée et que des mesures d'atténuation appropriées ont été mises en place.

Si l'alternative a) a été mise en œuvre, au moins l'une des alternatives d'authentification de la source ci-dessous doit être mise en œuvre.

1) Matériel conforme à l'IEC 61162-460 destiné à être installé dans un réseau conforme à l'IEC 61162-460 à l'aide de méthodes conformes à l'IEC 61162-460.

   NOTE 2 Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

   A l'intérieur du réseau contrôlé de l'IEC 61162-460, l'identification de la source par au moins une adresse MAC source, une adresse IP source ou un identificateur source (SFI) de l'IEC 61162-450 doit être utilisé. Les fichiers de données provenant de l'extérieur du réseau contrôlé doivent être authentifiés.

   Pour cette alternative, les manuels d'installation fournis par le fabricant doivent contenir des instructions d'installation appropriées, y compris une mise en garde selon laquelle une utilisation du matériel dans d'autres environnements ne permet pas de garantir sa sécurité informatique.

2) Matériel conforme à l'IEC 61162-450 destiné à être installé dans un réseau fermé à l'aide de méthodes conformes à l'IEC 61162-450.

NOTE 3 Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

A l'intérieur du réseau fermé de l'IEC 61162-450, l'identification de la source par au moins une adresse MAC source, une adresse IP source ou un identificateur source (SFI) de l'IEC 61162-450 doit être utilisé. Les fichiers de données provenant de l'extérieur du réseau fermé doivent être authentifiés.

Les manuels d'installation fournis par le fabricant doivent contenir des instructions d'installation appropriées (par exemple, ce matériel doit être installé dans un réseau fermé, dans lequel l'accès à toutes les interfaces, y compris celles utilisées dans ce réseau fermé, est physiquement bloqué pour les utilisateurs sans outil ou clé) incluant une mise en garde selon laquelle une utilisation du matériel dans d'autres environnements ne permet pas de garantir sa sécurité informatique.

3) Matériel non conforme à l'IEC 61162-450 ou l'IEC 61162-460 qui est destiné à être installé dans un réseau ou matériel qui n'est pas destiné à l'être.

Ce type de matériels peut inclure, par exemple, une interface Ethernet pour un réseau ou peut être dépourvu d'une interface avec tout réseau local.

Le fabricant doit déclarer l'alternative ou les alternatives pour lesquelles le matériel a été conçu.

4.3 Méthodes d'essai et résultats d'essai exigés

Confirmer par évaluation analytique qu'un mécanisme de vérification de l'intégrité du transport a été utilisé.

Confirmer par évaluation analytique que les fichiers dont la vérification de l'intégrité de transport n'est pas concluante ne sont pas mis à disposition pour une utilisation opérationnelle dans le matériel.

Confirmer par observation que lorsque des fichiers de données contenant un moyen de vérifier l'intégrité du fichier ne satisfont pas au contrôle d'intégrité, ils ne sont pas mis à disposition pour une utilisation opérationnelle dans le matériel.

Lorsque l'authentification de la source est mise en œuvre conformément au paragraphe 4.2.2, option a):

– confirmer par l'observation que les exigences de l'Annexe B sont satisfaites;
– confirmer par l'observation que le fabricant fournit une déclaration à propos de la méthode d'authentification pour laquelle l'EUT est conçu;
– confirmer par l'observation que les fichiers non exécutables ne sont pas mis à disposition pour une utilisation opérationnelle dans l'EUT dans les cas suivants:
  - tentative d'importation d'un fichier à partir d'une source non autorisée;
  - tentative d'importation d'un fichier dont le contenu n'est pas valide (c'est-à-dire dont le contrôle d'intégrité n'est pas concluant), par exemple une tentative d'importation d'un fichier contenant un code de hachage ou un certificat non valide.

Si les fichiers de données peuvent être mis à disposition pour une utilisation opérationnelle dans l'EUT sans avoir préalablement réussi l'authentification de la source conformément au paragraphe 4.2.2, option b):

– consulter la documentation du fabricant pour obtenir la liste des fichiers non exécutables qui peuvent être mis à disposition pour une utilisation opérationnelle dans l'EUT;
– confirmer par évaluation analytique que les fichiers non exécutables ne figurant pas dans la liste du fabricant ne sont pas mis à disposition pour une utilisation opérationnelle dans l'EUT;

– confirmer par observation que le manuel de l'opérateur spécifie les types de fichiers pris en charge et les risques, ainsi que la procédure pour les atténuer. Confirmer par évaluation analytique que seuls les fichiers indiqués sont mis à disposition pour une utilisation opérationnelle dans le matériel;

– confirmer par observation que la documentation du fabricant contient l'appréciation du risque. Confirmer par observation que le manuel de l'opérateur spécifie les risques, ainsi que la procédure à suivre pour les atténuer.

Confirmer par évaluation analytique que tous les fichiers non exécutables sont vérifiés comme indiqué dans la documentation du fabricant avant leur utilisation par l'EUT.

5 Module B: Exécution des fichiers exécutables

5.1 Généralités

Ce module s'applique tant pendant le fonctionnement normal qu'en mode entretien.

5.2 Exigences

En fonctionnement normal:

1) toutes les exécutions automatiques à partir de l'EDS, y compris l'exécution automatique et le démarrage, doivent être interdites;
2) l'exécution manuelle de tout type de fichier à partir de l'EDS ne doit être possible qu'après avoir procédé à l'authentification de la source et au contrôle d'intégrité du contenu exécutable de l'EDS, par exemple à l'aide de signatures numériques ou de clés secrètes (c'est-à-dire l'authentification) telles que définies à l'Annexe B;
3) en cas de défaillance catastrophique du matériel, un logiciel authentifié cryptographiquement peut être démarré et exécuté depuis l'EDS en tant que mesure réversible;
4) si l'exécution du fichier exécutable a un impact sur le fonctionnement normal du dispositif, une indication suffisante le signalant doit être donnée avant l'exécution. L'exécution doit uniquement être possible après confirmation par l'opérateur. Le fabricant doit fournir une liste des fichiers exécutables qu'il est possible d'exécuter pendant le fonctionnement normal.

NOTE Le micrologiciel ou le logiciel d'application peut authentifier automatiquement les fichiers exécutables sans intervention de l'utilisateur, à condition qu'une indication informative soit donnée lors de l'exécution de ces fichiers exécutables.

En mode entretien, l'exécution automatique des fichiers exécutables et le démarrage à partir de l'EDS sont autorisés.

L'Annexe C contient des exemples de méthodes techniques d'authentification.

5.3 Méthodes d'essai et résultats d'essai exigés

Utiliser une EDS qui, lorsqu'elle est utilisée dans un ordinateur dont l'accès n'est pas restreint, déclencherait une action automatique. Relier l'un après l'autre des dispositifs aux points de connexion pour la REDS, qui sont accessibles par l'opérateur sans outil ni clé, ou insérer un support dans la REDS (lecteurs de disques, etc.) et confirmer par observation que toutes les exécutions automatiques de l'EUT sont interdites.

Si l'EUT permet une exécution manuelle de tout type de fichier à partir de l'EDS, confirmer par une évaluation analytique que l'exécution manuelle est uniquement possible pour les fichiers qui ont été vérifiés par des signatures numériques ou des clés secrètes.

Si l'EUT permet l'exécution de fichiers exécutables pendant le fonctionnement normal, utiliser la liste de ces fichiers exécutables fournie par le fabricant et confirmer par l'observation soit

qu'ils n'affectent pas le fonctionnement normal, soit que l'EUT a demandé une confirmation par l'utilisateur de l'exécution d'un fichier exécutable qui affecte le fonctionnement normal.

Les essais correspondants relatifs aux signatures numériques et aux clés secrètes sont définis à l'Annexe B.

6 Module C: Authentification de l'utilisateur

6.1 Généralités

Ce module s'applique pendant le fonctionnement normal et pour l'entrée en mode entretien.

Si une authentification de l'utilisateur s'avère nécessaire, elle est décrite dans la norme du matériel individuel ou dans les alinéas correspondants du présent document (voir le module G, le module H, le module J et le module N; voir l'Annexe B).

L'authentification de l'utilisateur implique de déclarer une identité et de vérifier cette déclaration en apportant la preuve sous la forme d'un authentifiant qui repose souvent sur un secret (un mot de passe ou une clé privée, par exemple).

Il est acceptable que l'identité soit générique à un "rôle" plutôt qu'à un utilisateur "individuel" unique.

6.2 Exigences

Le cas échéant, l'authentification de l'utilisateur doit être mise en œuvre par au moins l'une des alternatives ci-dessous.

a) Mots de passe

Cette méthode s'applique au matériel intégrant une fonctionnalité de clavier alphanumérique ou un autre dispositif d'entrée de données permettant de saisir des mots de passe pendant le fonctionnement normal.

Une authentification de l'utilisateur avec des informations relatives à l'ouverture d'une session doit être prévue (par exemple, des mots de passe utilisés avec des noms d'utilisateur, un mot de passe avec des cartes-clés, etc.).

Si une authentification de l'utilisateur basée sur des mots de passe est utilisée, le mot de passe doit contenir au moins 8 caractères. Des restrictions de mot de passe supplémentaires peuvent être mises en place à la discrétion du fabricant, y compris la longueur, la complexité des caractères, les modifications régulières et les listes de mots exclus.

NOTE 1 NIST SP 800-63B recommande d'utiliser des mots de passe d'au moins 8 caractères et ne formule aucune exigence particulière en matière de complexité (mélange de lettres, de symboles et de chiffres), car les secrets mémorisés très complexes introduisent une nouvelle vulnérabilité potentielle (mot de passe écrit sur une feuille de papier, par exemple).

Le manuel de l'opérateur doit inclure une recommandation telle que: "Il convient que le mot de passe ne contienne pas le nom d'utilisateur ou des parties du nom complet de l'utilisateur telles que le prénom, le nom de la société, le nom de produit, etc. Il convient de ne pas utiliser de mots du dictionnaire. Il convient de ne pas utiliser de caractères répétitifs ou séquentiels ("aaaaaa", "1234abcd", par exemple)".

Les mots de passe destinés à l'authentification de l'utilisateur doivent être stockés de manière sécurisée (non réversibles à l'aide d'une fonction de hachage, par exemple) et ne doivent pas être aisément accessibles (lisible par l'homme, par exemple) en cas d'accès au support de stockage.

b) Clé secrète ou autre méthode cryptographique symétrique

Si des clés secrètes sont utilisées, la longueur de clé doit être d'au moins 128 bits, la clé doit avoir une force de la sécurité d'au moins 128 bits et être de nature aléatoire.

NOTE 2 Il s'agit, par exemple, d'une authentification à l'aide d'un jeton contenant une clé d'authentification symétrique.

NOTE 3 La force de la sécurité est une mesure comparable de la complexité pour casser un chiffrement donné et elle est distincte des longueurs de la clé de chiffrement. RSA 3072 et ECDSA 256, par exemple, sont considérées posséder une force de sécurité comparable de 128 bits malgré des longueurs de clé très différentes.

NOTE 4 De nature aléatoire, cela signifie que la création de la clé secrète suivante n'est pas la valeur suivante dans l'ordre alphanumérique (c'est-à-dire qu'il est impossible de prédire la nouvelle valeur en se basant sur la valeur précédente).

c) Carte à puce ou autre méthode cryptographique asymétrique

Si la cryptographie asymétrique est utilisée (dans les cartes à puce, par exemple), la force de la sécurité du chiffrement doit être d'au moins 112 bits.

d) Identification

Pour un matériel dont l'authentification complète de l'utilisateur est impossible à mettre en œuvre en pratique en raison de l'absence de fonctionnalité de clavier alphanumérique ou d'un autre dispositif de saisie de données permettant d'entrer des mots de passe pendant le fonctionnement normal, et du manque de capacité de saisie d'un mot de passe, le matériel doit fournir l'une des alternatives suivantes:

- l'interface utilisateur pour les modes spéciaux (le mode entretien, les mises à jour de logiciel aisément disponibles, par exemple) est accessible uniquement par une action volontaire et multiple de l'opérateur (en appuyant sur plusieurs boutons en même temps, sur plusieurs boutons à la suite, etc.);
- d'autres moyens que les informations relatives à l'ouverture d'une session décrites par le fabricant.

Pour les alternatives a), b) et c), le cas échéant, des moyens doivent être fournis pour permettre à un utilisateur authentifié de modifier un mot de passe ou une clé secrète pour l'authentification de l'utilisateur ou de révoquer la clé publique associée à une clé privée corrompue.

Dans la mesure du possible, des moyens doivent être prévus pour limiter les tentatives infructueuses d'authentification de l'utilisateur, par exemple en introduisant un délai avant de pouvoir accepter une nouvelle tentative, en verrouillant l'accès après un certain nombre de tentatives, etc. Ces moyens ne doivent pas avoir d'impact sur le fonctionnement normal (introduction d'un délai de fonctionnement normal, verrouillage d'une fonctionnalité du fonctionnement normal, etc.). Ces moyens doivent laisser le matériel dans le même état qu'avant la tentative avortée. Le cas échéant, une indication informative que l'authentification de l'utilisateur fait l'objet d'une restriction (par un délai, un verrouillage de compte, etc.) doit être prévue une fois entrée en vigueur.

NOTE 5 Même si une indication informative de la raison pour laquelle l'authentification n'a pas abouti peut s'avérer utile pour des utilisateurs classiques du matériel, davantage d'informations que nécessaire peut aider les utilisateurs malveillants à attaquer le matériel. C'est la raison pour laquelle le fabricant peut déterminer un niveau de détail approprié pour le matériel. Une indication utile peut donner des informations relatives à l'état en cours (par exemple bloqué pendant un certain délai, le compte a été verrouillé, etc.).

Dans la mesure du possible, un matériel conforme doit consigner l'activation du mode entretien dans un journal interne, qui est capable de consigner au moins 10 activations, ou dans le syslog qui peut être externe au matériel.

NOTE 6 Une description du syslog est disponible dans l'IEC 61162-450 et RFC 5424.

Le cas échéant, pour les alternatives a), b) et c), le matériel doit offrir la capacité de gestion de compte d'utilisateur applicable au type d'authentification de l'utilisateur prévu (création de comptes, mise à jour des mots de passe, suppression de comptes, par exemple).

6.3 Méthodes d'essai et résultats d'essai exigés

Exécuter les essais pour toutes les alternatives fournies par l'EUT.

a) Si l'EUT prévoit l'authentification de l'utilisateur basée sur des mots de passe:
   - confirmer par observation que l'authentification de l'utilisateur repose sur un mot de passe d'au moins 8 caractères;
   - confirmer par examen de la documentation du fabricant que le manuel de l'opérateur contient une recommandation relative à l'utilisation de mots de passe;
   - confirmer par évaluation analytique que les mots de passe destinés à l'authentification de l'utilisateur sont stockés en toute sécurité et ne sont pas aisément accessibles. Par exemple, l'évaluation analytique peut inclure des tentatives de faire fonctionner l'EUT, des tentatives d'accès à des éléments dont il convient qu'ils ne soient pas accessibles, une étude de la documentation fournie par le fabricant ou une demande au fabricant de préciser certains détails.

b) Si l'EUT prévoit une authentification de l'utilisateur basée sur une clé secrète ou une autre méthode cryptographique symétrique, confirmer par examen de la documentation du fabricant que la longueur de clé est d'au moins 128 bits, que la force de la sécurité de la clé est d'au moins 128 bits et que la clé est de nature aléatoire.

c) Si l'EUT prévoit une authentification de l'utilisateur basée sur une carte à puce ou une autre méthode cryptographique asymétrique, confirmer par examen de la documentation du fabricant que la force de la sécurité du chiffrement est d'au moins 112 bits.

d) Si l'EUT prévoit une authentification de l'utilisateur basée sur l'identification, confirmer par observation que l'interface utilisateur pour les modes spéciaux est accessible uniquement par:
   - des actions volontaires et multiples de l'opérateur; ou
   - d'autres moyens décrits dans la documentation du fabricant.

Confirmer par observation, le cas échéant, que l'utilisateur peut modifier le ou les mots de passe utilisés pour son authentification.

Le cas échéant, confirmer par évaluation analytique que les mots de passe, clés privées ou autres clés secrètes compromis peuvent être révoqués par la méthode définie par le fabricant.

Confirmer par observation que de nouveaux mots de passe, clés privées et clés secrètes en fonctionnement normal ne sont pas acceptés et que leur acceptation est limitée à une partie spécifique de l'interface utilisateur exigeant une authentification séparée de l'utilisateur telle que définie par le fabricant.

Dans la mesure du possible, confirmer par observation que des moyens sont prévus pour limiter les tentatives avortées répétées d'authentification de l'utilisateur. Confirmer par observation que les moyens prévus n'ont pas d'impact sur le fonctionnement normal à cause de retards de fonctionnement normal ou du verrouillage d'une fonctionnalité du fonctionnement normal. Confirmer par observation que ces moyens laissent le matériel dans le même état que celui dans lequel il se trouvait avant la tentative avortée. Le cas échéant, confirmer par observation qu'une indication informative signalant que l'authentification de l'utilisateur est limitée est fournie une fois entrée en vigueur.

Confirmer par observation que l'accès pour procéder à des modifications de la configuration du fabricant exige une authentification de l'utilisateur.

Dans la mesure du possible, confirmer par observation que les 10 dernières activations du mode entretien sont disponibles dans un journal interne ou dans le syslog. Le syslog peut faire partie de l'environnement de simulation autour du matériel.

Le cas échéant, pour les alternatives a), b) et c), confirmer par observation que l'EUT permet la gestion de compte d'utilisateur.

7 Module D: Défense du système

7.1 Généralités

Ce module s'applique pendant le fonctionnement normal.

La défense du système est composée de la prévention des programmes malveillants, d'un pare-feu hôte, d'une prévention des intrusions hôte et d'une notification de l'utilisateur, le cas échéant, si un programme malveillant ou autre infection logicielle est détecté(e). Les éléments liés à l'hôte sont relatifs à l'environnement d'installation du matériel. La prévention des programmes malveillants peut être assurée par le matériel ou son environnement d'installation. Un exemple d'environnement assurant la défense du système est un matériel conforme à l'IEC 61162-460 installé dans un réseau conforme à l'IEC 61162-460.

NOTE 1 Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

NOTE 2 Les plans de reprise après sinistre relèvent de la responsabilité du propriétaire du navire et sont par hypothèse inclus dans le plan de gestion intégrée de la sécurité (ISMP) du navire.

Un déni de service (DoS) est une catégorie importante de cyberattaques destinées à empêcher l'utilisation de systèmes connectés au réseau, à compromettre leur sécurité et, à terme, à provoquer des dommages. Par l'intermédiaire d'une connexion réseau, une attaque par DoS réussie peut être utilisée comme un tremplin pour, en premier lieu, réduire au silence un dispositif cible, que le pirate informatique peut ensuite imiter pour obtenir un accès supplémentaire ou une commande. Les attaques peuvent s'appuyer sur des méthodes directes et indirectes qui accroissent le trafic du réseau jusqu'au point où des erreurs se produisent ou qu'une victime ne peut plus accomplir les fonctions prévues. Cela peut permettre au pirate d'atteindre son objectif ou présenter d'autres opportunités à exploiter. Les attaques par DoS peuvent exploiter des protocoles réseau normalement utiles et de portée limitée ainsi que des services de réseau normalisés pour interagir avec des nœuds de réseau supplémentaires de manière à multiplier les pics de trafic résultants adressés à la victime tout en masquant la source de l'attaque. Les attaques peuvent provoquer un afflux de trafic, mais utiliser des fonctions à faible largeur de bande qui n'établissent jamais une voie de transaction classique et ne sont pas journalisées.

Même si le sujet n'est pas traité ici, le DoS au sens large du terme inclut des actions visant à désactiver le matériel directement par des attaques physiques ou indirectement en attaquant des éléments critiques pour son fonctionnement (l'alimentation électrique ou les dispositifs de gestion thermique, par exemple).

7.2 Protection contre les programmes malveillants

7.2.1 Exigences

7.2.1.1 Généralités

La défense du système pour la protection contre les programmes malveillants doit être assurée par l'une des alternatives A, B, C, D.1 ou D.2, ou par toute combinaison de celles-ci, décrites aux paragraphes 7.2.1.2 à 7.2.1.5.

Le fabricant doit déclarer pour quelles alternatives A, B, C, D.1 et/ou D.2 le matériel a été conçu.

Pour chaque alternative, le manuel d'installation et le manuel de l'opérateur fournis par le fabricant doivent contenir les instructions d'installation et de fonctionnement appropriées incluant une mise en garde selon laquelle le matériel peut être vulnérable à une menace informatique et peut présenter un risque lié à la sécurité informatique pour d'autres matériels s'il est utilisé à l'extérieur de son environnement prévu.

7.2.1.2 Alternative A

Matériel conforme à l'IEC 61162-460 prévu pour une installation dans un réseau conforme à l'IEC 61162-460.

NOTE Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

Cette alternative ne fait l'objet d'aucune exigence supplémentaire.

7.2.1.3 Alternative B

Matériel destiné à être installé dans un réseau contrôlé autre que l'IEC 61162-460.

Pour cette alternative, des mesures de sécurité équivalentes ou allant au-delà de celles présentées dans l'IEC 61162-460 doivent être prévues. Il s'agit, par exemple, de l'IEEE 802.1X utilisée en lieu et place du filtrage d'adresse MAC préconisé par l'IEC 61162-460.

7.2.1.4 Alternative C

Matériel dépourvu d'interface accessible par laquelle le programme malveillant peut pénétrer ou par laquelle une intrusion pourrait être possible.

Cette alternative ne fait l'objet d'aucune exigence supplémentaire.

NOTE 1 Cela s'applique, par exemple, à des réseaux intégrés sans système d'exploitation ou à des réseaux intégrés dont les interfaces physiques ne constituent pas une porte d'entrée pour un programme malveillant ou pour une intrusion. Il s'agit, par exemple, des lignes série IEC 61162-1 ou des interfaces hertziennes pour la radiocommunication maritime ou le matériel de navigation lorsque ce type d'interfaces ne peut pas transférer de fichiers.

NOTE 2 Une "interface accessible" est une interface qui est physiquement accessible sans l'aide d'un outil ou d'une clé et qui n'est en principe pas connectée à un autre matériel en fonctionnement normal. Il s'agit, par exemple, d'un accès USB utilisé pour charger des fichiers de données, d'un accès de programmation série ou "de débogage" ou d'un accès réseau.

7.2.1.5 Alternative D

7.2.1.5.1 Généralités

Matériel avec des interfaces accessibles par l'intermédiaire desquelles le programme malveillant peut pénétrer ou par lesquelles une intrusion peut être possible.

NOTE Cette alternative est classique pour les ordinateurs disponibles dans le commerce sans configuration particulière.

Au moment de déterminer les protections applicables, le fabricant doit prendre en considération les risques liés à la fonction du matériel, ainsi que l'environnement dans lequel il est destiné à être utilisé.

Le fabricant doit décrire les méthodes utilisées pour réduire les risques liés à la sécurité informatique associés au matériel.

Le principe du moindre privilège doit être appliqué de sorte que, en fonctionnement normal, le matériel fournisse uniquement l'accès nécessaire aux fonctionnalités exigées pour exécuter sa fonction prévue. L'accès en lecture, en écriture et d'exécution aux fichiers, par exemple, peut être configuré de manière appropriée pour la fonctionnalité destinée à être disponible en fonctionnement normal.

Le matériel doit assurer un renforcement de base contre les attaques ou les dommages. Toutes les interfaces, tous les accès réseau, tous les services et applications non utilisés et qui ne sont pas nécessaires pour le fonctionnement normal doivent être désactivés.

Cette alternative exige au moins l'un des moyens D.1 ou D.2 comme méthode d'atténuation du risque dans ce type de matériels.

7.2.1.5.2 Alternative D.1

La protection contre les programmes malveillants est assurée.

a) Le matériel doit inclure un module logiciel de protection contre les programmes malveillants et, le cas échéant, la possibilité de mettre à jour la prévention des programmes malveillants. Les fabricants doivent fournir des procédures documentées d'installation et de mise à jour de ce module logiciel.

b) Le matériel et son logiciel de protection contre les programmes malveillants doivent satisfaire aux exigences de performances en fonctionnement normal.

c) Le fabricant doit convenir d'une procédure documentée avec l'organisme d'agrément de type, qui décrit la méthode d'évaluation et de consignation des effets liés à l'application des mises à jour de fichier de définition anti programme malveillant et des mises à jour logicielles sur le matériel.

d) Cette procédure doit fournir l'assurance que des mises à jour d'un type particulier ne compromettent pas la fonctionnalité prévue ou la conformité du matériel. L'Annexe A donne des recommandations relatives à l'agrément de type du matériel lorsque des fichiers de définition ou logiciels anti programmes malveillants sont mis à jour.

   NOTE Ce processus de mise à jour peut être équivalent à la procédure de qualité documentée permettant d'évaluer les effets des mises à jour de graphique (fichiers de données) et des mises à jour de moteur de graphique (logiciels) sur le matériel.

e) Pour les mises à jour de logiciels anti programmes malveillants, les exigences du module N s'appliquent. Il n'est pas nécessaire que les mises à jour des fichiers de définition ou d'autres fichiers de données anti programmes malveillants satisfassent aux paragraphes définis dans le module N.

f) Le manuel d'installation et le manuel de l'opérateur doivent décrire la manière de mettre à jour la prévention des programmes malveillants, suivant le cas. Ils doivent également décrire les conditions dans lesquelles il convient de procéder à la mise à jour.

g) Le module de prévention des programmes malveillants doit informer l'utilisateur que la prévention n'est plus à jour lorsque la durée maximale depuis la dernière mise à jour a été dépassée.

h) Le fabricant doit documenter le processus mis en œuvre pour être sûr que les mises à jour du logiciel anti programmes malveillants n'ont aucun impact sur la fonctionnalité prévue ou la conformité du matériel aux normes de performances et normes d'essai applicables.

i) Dans la mesure du possible, le matériel doit disposer de moyens permettant d'indiquer à l'utilisateur que le système a détecté la présence d'un programme malveillant dans le cadre de processus permanents, périodiques ou sur demande (par comparaison avec une liste blanche, etc.).

7.2.1.5.3 Alternative D.2

La protection par un pare-feu est assurée.

Dans le cas d'un matériel communiquant sur des interfaces IP (protocole Internet), les manuels d'installation et, le cas échéant, les manuels de l'opérateur doivent contenir des instructions selon lesquelles le matériel doit être installé dans un environnement protégé par un pare-feu correctement configuré (un pare-feu satisfaisant aux exigences relatives aux Passerelles 460, par exemple). Les instructions de configuration détaillées peuvent être disponibles dans un document confidentiel de configuration de la sécurité séparé (voir l'Annexe E).

NOTE Le document de configuration de la sécurité facultatif peut contenir d'autres informations essentielles destinées à l'intégrateur de système (un chantier naval, par exemple) de sorte qu'il puisse installer le matériel avec la protection nécessaire.

Les instructions de configuration correcte doivent:

a) indiquer que la stratégie par défaut doit consister à abandonner les paquets de réseau qui ne sont pas explicitement autorisés;

b) décrire en détail la manière de configurer le filtrage de paquets basé sur TCP et UDP en fonction de l'adresse IP source et destinataire et de l'accès destinataire pour chaque flux de réseau;

c) décrire l'utilisation moyenne de la largeur de bande de réseau pour chaque flux de réseau;

d) si le pare-feu le prend en charge, décrire la manière d'éviter que l'utilisation de la largeur de bande ne dépasse un seuil prédéfini (tempête de transmission, prévention des dénis de service, par exemple);

e) décrire en détail tous les autres protocoles de couche 3 nécessitant d'être autorisés par le pare-feu;

f) expliquer comment configurer et soumettre à essai l'ensemble le moins banalisé de règles de pare-feu exigées pour le fonctionnement prévu du matériel (pour que les caractères génériques et les alias ne soient pas mal configurés, par exemple).

Si un ou plusieurs services ou applications essentiels du matériel sont réputés présenter d'éventuelles vulnérabilités à haut risque (exécution d'un code à distance, par exemple), les manuels doivent fournir des recommandations supplémentaires en matière de protection du réseau de navigation (comment configurer un système de protection contre/de détection des intrusions en plus du pare-feu décrit en 7.2.1.5.3).

7.2.2 Méthodes d'essai et résultats d'essai exigés

7.2.2.1 Généralités

Confirmer par examen de la documentation fournie par le fabricant que l'alternative A, B, C, D.1 et/ou D.2 pour laquelle l'EUT a été conçu y est identifiée.

Confirmer par examen de la documentation du fabricant que pour chaque alternative, le manuel d'installation et/ou de l'opérateur fourni contient des instructions d'installation et d'exploitation appropriées, y compris une mise en garde selon laquelle le matériel peut être vulnérable à une menace informatique, ce qui peut présenter un risque lié à la sécurité informatique pour un autre matériel s'il est utilisé hors de son environnement prévu.

7.2.2.2 Alternative A

Confirmer par examen d'un rapport d'essai ou d'un certificat de conformité, qui accompagne l'EUT, que ce dernier satisfait à l'IEC 61162-460, et confirmer par examen que la documentation fournie par le fabricant décrit l'installation dans un réseau conforme à l'IEC 61162-460.

NOTE Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

7.2.2.3 Alternative B

Confirmer par évaluation analytique de la documentation fournie par le fabricant:

– qu'elle indique que l'unité est destinée à être utilisée dans un réseau contrôlé;

– qu'elle identifie les exigences de l'IEC 61162-460 auxquelles l'EUT satisfait et les exceptions dans lesquelles l'EUT ne satisfait pas aux exigences, et que pour chaque exception, elle spécifie clairement une alternative mise en œuvre par l'EUT et elle donne une analyse de l'équivalence ou de l'amélioration de la sécurité offerte par l'alternative dans le réseau prévu par rapport à l'IEC 61162-460.

7.2.2.4 Alternative C

Confirmer par évaluation analytique de la documentation fournie par le fabricant que l'EUT ne dispose d'aucune interface accessible pouvant permettre à des fichiers de données de programme malveillant d'entrer dans l'EUT ou d'être transmis à un autre matériel.

7.2.2.5 Alternative D

7.2.2.5.1 Généralités

Confirmer par examen de la documentation du fabricant:

– qu'elle identifie les fonctions, interfaces, accès réseau, services et applications nécessaires au fonctionnement normal; et

– qu'elle identifie les fonctions supprimées ou restreintes.

Choisir un échantillon représentatif (5 éléments ou plus, selon le cas, par exemple) d'accès supprimé ou restreint à des fonctions, services et applications, et confirmer par évaluation analytique que les limitations d'accès documentées ont été mises en œuvre.

Confirmer par évaluation analytique que les interfaces physiques et accès de réseau logique non utilisés sont désactivés.

Confirmer par évaluation analytique de l'EUT que la protection de ses éléments non utilisés ne peut pas être contournée ou désactivée pendant le fonctionnement normal sans l'aide d'un outil ou d'une clé.

Confirmer une ou plusieurs des alternatives D.1 ou D.2, comme expliqué en 7.2.2.5.2 et en 7.2.2.5.3.

7.2.2.5.2 Alternative D.1

Confirmer par observation que la protection contre les programmes malveillants fonctionne, en utilisant par exemple la chaîne d'essais EICAR [cliquer sur "Download anti-malware testfile" (Télécharger un fichier d'essai antiprogrammes malveillants) sur http://www.eicar.org].

Confirmer:

a) le cas échéant, par examen, que le fabricant a fourni une procédure documentée d'installation de mises à jour de fichier de définition anti programmes malveillants ou de logiciel anti programmes malveillants sur l'EUT;

b) par évaluation analytique que la procédure peut maintenir le fonctionnement conforme de l'EUT;

c) par examen de la documentation du fabricant que les procédures documentées sont fournies, qu'elles font l'objet d'un accord avec l'organisme d'agrément de type, en décrivant les détails des méthodes d'évaluation et de consignation des effets liés à l'application des mises à jour de fichier de définition ou de logiciel anti programmes malveillants sur le matériel;

d) par évaluation analytique que l'installation et les actions entreprises par le logiciel de protection contre les programmes malveillants assurent que les mises à jour d'un type particulier ne compromettent pas la fonctionnalité prévue ou sur la conformité du matériel aux règles correspondantes d'agrément de type;

e) par évaluation analytique que la procédure de mise à jour satisfait aux exigences du module N;

f) le cas échéant, par observation que les manuels d'installation et manuels de l'opérateur décrivent la manière de mettre à jour la prévention des programmes malveillants, y compris des conditions dans lesquelles il convient de procéder à cette mise à jour;

g) par observation que des moyens sont prévus pour informer l'opérateur de la date de la dernière mise à jour ou de la date de la prochaine mise à jour;

h) le cas échéant, par examen que la documentation du fabricant décrit le processus mis en œuvre pour vérifier que les mises à jour anti programmes malveillants n'ont pas d'impact sur la fonctionnalité prévue ou sur la conformité aux normes de performances ou d'essai applicables;

i) si mise en œuvre, par évaluation analytique que le matériel fournit des moyens permettant d'indiquer à l'utilisateur que le système a détecté la présence d'un programme malveillant dans le cadre de processus permanents, périodiques ou sur demande (par comparaison à des listes blanches, etc.).

7.2.2.5.3 Alternative D.2

Confirmer par examen des manuels d'installation et, le cas échéant, des manuels de l'opérateur, qu'ils contiennent des instructions selon lesquelles l'EUT doit être installé dans un environnement protégé par un pare-feu correctement configuré.

Confirmer par examen des manuels d'installation et, le cas échéant, des manuels de l'opérateur et, selon le cas, d'un document confidentiel de configuration de la sécurité que les instructions de configuration incluent:

a) une déclaration que la stratégie par défaut consiste à abandonner les paquets de réseau qui ne sont pas explicitement autorisés;

b) la manière de configurer le filtrage des paquets basé sur TCP et UDP en fonction de l'adresse IP source et de destination et de l'accès de destination pour chaque flux de réseau;

c) l'utilisation moyenne de la largeur de bande de réseau pour chaque flux de réseau;

d) la manière d'éviter que l'utilisation de la largeur de bande ne dépasse un seuil prédéfini, si cela est pris en charge par le pare-feu;

e) l'identification de tous les autres protocoles de couche 3 nécessitant d'être autorisés par le pare-feu;

f) la manière de configurer et de soumettre à essai l'ensemble le moins banalisé de règles de pare-feu exigées pour le fonctionnement prévu du matériel (pour que les caractères génériques et les alias ne soient pas mal configurés, par exemple).

Si l'EUT inclut un ou plusieurs services ou application essentiels réputés présenter d'éventuelles vulnérabilités à haut risque, confirmer par examen du manuel d'installation et du manuel de l'opérateur qu'ils fournissent des recommandations supplémentaires en matière de protection du réseau de navigation.

7.3 Protection contre le déni de service

7.3.1 Exigences

7.3.1.1 Généralités

La défense du système contre les attaques par DoS doit être assurée par l'une des alternatives A, B, C, D ou une combinaison de ces alternatives, décrites aux paragraphes 7.3.1.2 à 7.3.1.5.

Le fabricant doit déclarer les alternatives A, B, C ou D, ou toute combinaison de celles-ci, pour lesquelles le matériel a été conçu.

7.3.1.2 Alternative A

Matériel conforme à l'IEC 61162-450 ou à l'IEC 61162-460 prévu pour une installation dans un réseau conforme à l'IEC 61162-460.

NOTE Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

La protection contre les attaques par DoS sur un réseau ne fait l'objet d'aucune exigence supplémentaire.

7.3.1.3 Alternative B

Matériel sans interfaces de réseau pour lesquelles des attaques par DoS sont pertinentes.

La protection contre les attaques par DoS sur un réseau d'un matériel se trouvant à l'intérieur d'une zone physiquement protégée ne fait l'objet d'aucune exigence supplémentaire.

Les manuels d'installation doivent indiquer que le matériel doit être installé dans une zone physiquement protégée.

7.3.1.4 Alternative C

Interfaces internes à l'intérieur d'un réseau fermé.

Dans le cas d'un équipement dont l'installation est prévue au sein d'un réseau fermé qui se trouve en dehors d'une zone physiquement protégée, le matériel doit au moins être protégé par des mesures compensatoires (défenses du réseau dans le cas où le réseau de commande est compromis, par exemple). Le matériel doit être protégé par une limitation du débit d'entrée interne ou par la méthode de protection externe décrite dans le manuel d'installation (commutateur de limitation de débit, utilisation d'un bus CAN [Controller Area Network] qui possède des mesures en raison de sa conception, etc.).

Le matériel destiné à être installé à l'intérieur d'un réseau fermé physiquement sécurisé ne fait l'objet d'aucune exigence.

Les manuels d'installation doivent indiquer que le matériel doit être installé dans une zone physiquement protégée.

7.3.1.5 Alternative D

Tous les autres matériels.

Le fabricant doit déterminer les mesures appropriées basées sur le périmètre, le réseau et l'hôte pour faciliter l'atténuation des attaques par DoS.

NOTE 1 Ces mesures peuvent être fournies par l'EUT ou par l'environnement dans lequel l'EUT est installé.

Des attaques pertinentes peuvent inclure, par exemple:

– les attaques par amplification, qui provoquent un trafic excessif pour un hôte du réseau en manipulant les protocoles réseau utilisés dans le réseau, y compris, entre autres, ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), DNS (Domain Name System), SNMP (Simple Network Management Protocol) et les protocoles de découverte multicast ou de diffusion;
– les attaques par imposture, par lesquelles l'adresse source d'une trame ou d'un paquet est mystifiée, de telle sorte que les composants d'infrastructure du réseau constatent que le trafic provenant de nombreuses sources est dirigé vers un ou plusieurs hôtes du réseau;
– la tempête de réseau.

Le manuel d'installation du matériel doit décrire les mesures exigées dans l'environnement d'installation du matériel pour aider à atténuer les attaques par DoS. Le manuel d'installation doit inclure une mise en garde selon laquelle le matériel peut ne pas être sécurisé en l'absence de ces mesures dans son environnement d'installation.

Les mesures qui doivent être prises en considération incluent:

1) le filtrage du trafic (par des pare-feu, des routeurs ou des commutateurs, par exemple);
2) la restriction de la largeur de bande (Qualité de service);
3) l'isolation physique des composants du réseau;
4) les contrôles d'accès physiques.

Les mesures suivantes peuvent éventuellement être prises en considération, mais ne sont pas exhaustives:

5) logiciels de détection et de prévention des intrusions;
6) connexions redondantes au réseau;
7) connexions authentifiées;
8) équilibrage des charges;
9) surveillance du trafic ou de l'application, analyse et alerte.

NOTE 2 La Qualité de Service protège les parties du système qui ne sont pas directement ciblées par une attaque par DoS.

NOTE 3 Dans certaines circonstances (la saturation des liaisons de réseau d'un matériel, par exemple), il peut s'avérer impossible de prévenir la dégradation ou l'indisponibilité des services du matériel. Toutefois, le matériel et les systèmes peuvent être conçus pour réduire le plus possible l'impact durable sur les services dans ces circonstances.

Pour les attaques par DoS autres que celles provoquées par une tempête de réseau, le fabricant doit identifier et documenter les vulnérabilités et les mesures nécessaires pour atténuer le risque de les exploiter. Des exemples d'attaques par DoS autres qu'une tempête de réseau sont donnés ci-dessous:

– tentative répétée d'ouvrir une session avec un mot de passe erroné;
– transmission plus fréquente d'éléments que ne le suppose le destinataire;
– transmission d'éléments dont le contenu est volontairement malformé;
– attaques par requête d'un caractère générique de base de données (SQL – Structured Query Language, par exemple);
– verrouillage de comptes d'utilisateur;
– saturations de mémoire tampon;
– allocation d'objet spécifié par l'utilisateur;
– entrée d'utilisateur en tant que compteur de boucle;
– écriture sur le disque de données fournies par l'utilisateur;
– échec de la libération de ressources;
– quantité excessive de données stockées dans une session.

NOTE 4 Des recommandations à propos de l'atténuation des attaques ci-dessus sont disponibles auprès de l'OWASP[2]:
http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf,
https://www.owasp.org/index.php/Testing_for_Denial_of_Service

[2] Open Web Application Security Project (OWASP) est une fondation sans but lucratif qui travaille pour améliorer la sécurité des logiciels.

7.3.2 Méthodes d'essai et résultats d'essai exigés

7.3.2.1 Généralités

Confirmer par examen de la documentation fournie par le fabricant qu'elle identifie l'alternative A, B, C ou D pour laquelle l'EUT a été conçu.

7.3.2.2 Alternative A

Confirmer par examen d'un rapport d'essai ou d'un certificat de conformité, qui accompagne l'EUT, que l'EUT est conforme à l'IEC 61162-460.

NOTE Un nœud 450 peut également être un nœud conforme à l'IEC 61162-460.

Confirmer par examen de la documentation du fabricant que le matériel est uniquement destiné à être installé dans un réseau conforme à l'IEC 61162-460, et que la documentation du fabricant contient une mise en garde claire selon laquelle le matériel peut ne pas être sûr s'il est installé dans un environnement autre qu'un réseau conforme à l'IEC 61162-460.

7.3.2.3 Alternative B

Confirmer par examen que le manuel d'installation indique que le matériel est à installer dans une zone physiquement protégée.

7.3.2.4 Alternative C

Si le matériel comporte une protection intégrée:

1) confirmer par examen de la documentation du fabricant que le débit de données d'entrée opérationnel maximal est déclaré par le fabricant;
2) utiliser les dispositions de simulation générant des trafics jusqu'à atteindre la limite maximale déclarée par le fabricant. Confirmer par observation que l'EUT satisfait à ses exigences de performances;
3) utiliser les dispositions de simulation générant des trafics jusqu'à atteindre 200 % de la limite maximale déclarée par le fabricant, mais pas plus de 90 % de la limite maximale disponible pour l'interface réseau pendant au moins 10 min. Après 10 min, repasser au trafic maximal déclaré par le fabricant. Confirmer par évaluation analytique que l'EUT repasse à la fonctionnalité prévue ou redevient conforme après la modification du trafic.

Si le matériel exige une protection externe, confirmer par examen du manuel d'installation que l'environnement d'installation est décrit.

Si le matériel est prévu pour être installé à l'intérieur d'un réseau fermé qui est physiquement sécurisé:

1) confirmer par examen de la documentation du fabricant que le matériel est uniquement destiné à être utilisé dans un réseau fermé et que la documentation contient une mise en garde claire selon laquelle le matériel peut ne pas être sécurisé s'il est installé dans tout autre environnement;
2) confirmer par examen que le manuel d'installation indique que le matériel est à installer dans une zone physiquement protégée.

7.3.2.5 Alternative D

Confirmer par évaluation analytique de la documentation du fabricant que des mesures basées sur le périmètre, le réseau et l'hôte ont été identifiées pour aider à atténuer le risque d'attaques par DoS. Cela peut inclure l'imposture, l'amplification et les tempêtes de réseau.

Confirmer par évaluation analytique que les mesures identifiées par le fabricant comme étant fournies par l'EUT pour aider à atténuer le risque d'attaques par DoS (y compris l'imposture, l'amplification et les tempêtes de réseau) sont présentes dans l'EUT.

Confirmer par examen que le manuel d'installation du matériel décrit les mesures détaillées exigées dans l'environnement d'installation de l'EUT, si l'une de celles indiquées ci-dessous n'est pas fournie par l'EUT:

1) le filtrage du trafic (par des pare-feu, des routeurs ou des commutateurs, par exemple);
2) la restriction de la largeur de bande (Qualité de service);
3) l'isolation physique des composants du réseau;
4) les contrôles d'accès physiques; ou
5) les mesures supplémentaires identifiées par le fabricant.

Confirmer par examen du manuel d'installation qu'une mise en garde est fournie selon laquelle, si ces mesures ne sont pas présentes dans l'environnement d'installation de l'EUT, l'EUT peut ne pas être sécurisé.

Pour soumettre à essai la quantité déclarée et excessive de trafic du réseau au niveau de l'EUT:

6) confirmer par examen de la documentation du fabricant que le débit de données d'entrée opérationnel maximal est déclaré par le fabricant;
7) utiliser les dispositions de simulation générant des trafics jusqu'à atteindre la limite maximale déclarée par le fabricant. Confirmer par observation que l'EUT satisfait à ses exigences de performances;
8) utiliser les dispositions de simulation générant des trafics jusqu'à atteindre 200 % de la limite maximale déclarée par le fabricant, mais pas plus de 90 % de la limite maximale disponible pour l'interface réseau pendant au moins 10 min. Après 10 min, repasser au trafic maximal déclaré par le fabricant. Confirmer par évaluation analytique que l'EUT repasse à la fonctionnalité prévue ou redevient conforme après la modification du trafic;

   NOTE La limite de 90 % est destinée à permettre des environnements de simulation pratiques pour générer suffisamment de trafic du réseau.

9) confirmer par examen de la documentation du fabricant que le débit de données de sortie opérationnel maximal est déclaré par le fabricant;
10) confirmer par évaluation analytique des preuves documentées ou par évaluation analytique de l'EUT lui-même que l'EUT ne dépasse pas la largeur de bande de sortie opérationnelle maximale déclarée.

Pour soumettre à essai l'atténuation d'attaques par DoS autres que celles provoquées par une quantité excessive de trafic du réseau au niveau de l'EUT:

11) confirmer par examen de la documentation du fabricant qu'elle décrit les mesures prises pour atténuer les attaques par DoS autres que le DoS par trafic excessif;
12) confirmer par évaluation analytique que les mesures prises pour atténuer les attaques par DoS autres que le DoS par trafic excessif traitent chaque vulnérabilité identifiée dans l'EUT.

8 Module E: Accès au réseau

8.1 Généralités

Ce module s'applique tant pendant le fonctionnement normal qu'en mode entretien.

Ce module s'applique au matériel conçu pour être connecté à un réseau externe, y compris à des réseaux transportant un trafic non IP. Des recommandations relatives à l'interconnexion des réseaux peuvent être consultées à l'Annexe F.

8.2 Matériel qui se connecte à un réseau

8.2.1 Exigences

Les manuels d'installation ou le document confidentiel de configuration de la sécurité (voir l'Annexe E) doivent contenir les informations suivantes:

a) les services de réseau, c'est-à-dire les accès et protocoles nécessaires à la fonctionnalité prévue du matériel, par exemple, pour les réseaux IP, UDP, TCP, SNMP (Simple Network Management Protocol), IGMP (Internet Group Management Protocol) et la synchronisation d'horloge NTP (Network Time Protocol);

NOTE 1 Si les protocoles propriétaires du fabricant sont utilisés, il est suffisant de déclarer leur utilisation sans donner de détails les concernant, mais en spécifiant la porteuse (UDP multicast, par exemple).

b) la vitesse de transmission classique des données par le matériel sur le réseau sur une période représentative déterminée par le fabricant;

NOTE 2 La description des éléments ci-dessus peut donner ces informations sur plusieurs périodes, par exemple pour indiquer les périodes d'utilisation du taux technique maximal et donner des informations relatives à la moyenne sur une plus longue période.

c) la vitesse normale maximale à laquelle le matériel peut recevoir le trafic depuis le réseau, moyennée sur une période représentative déterminée par le fabricant;

d) l'effet sur le matériel d'un dépassement de la vitesse d'entrée maximale à laquelle le matériel peut recevoir le trafic;

NOTE 3 La description ci-dessus peut simplement signaler une perte de fonctionnalité normale des éléments indiqués.

e) toutes les exigences nécessaires en matière de sécurité physique pour l'installation du matériel;

f) toutes les exigences nécessaires en matière d'architecture réseau (exigences relatives aux passerelles, par exemple) et de configuration du matériel (contrôles d'accès au réseau tels qu'un filtrage d'adresse MAC et des adresses IP par défaut, par exemple).

8.2.2 Méthodes d'essai et résultats d'essai exigés

Confirmer par examen que les manuels d'installation ou les documents confidentiels de configuration de la sécurité contiennent:

a) les détails des services de réseau nécessaires à la fonctionnalité prévue de l'EUT;

b) les détails de la vitesse de transmission classique des données par le matériel sur le réseau sur une période représentative déterminée par le fabricant;

c) les détails de la vitesse normale maximale à laquelle le matériel peut recevoir le trafic depuis le réseau, moyennée sur une période représentative déterminée par le fabricant;

d) les détails de l'effet sur le matériel d'un dépassement de la vitesse d'entrée maximale à laquelle le matériel peut recevoir le trafic;

e) les détails des exigences de sécurité physique pour l'installation du matériel;

f) les détails de l'architecture du réseau et de la configuration du matériel.

8.3 Matériel fournissant un accès réseau entre des réseaux contrôlés

8.3.1 Exigences

8.3.1.1 Généralités

La communication entre des matériels installés sur différents réseaux contrôlés doit être assurée par l'une des alternatives décrites aux paragraphes 8.3.1.2 à 8.3.1.4. Voir l'Annexe F pour des recommandations.

8.3.1.2 Alternative A

Connexions entre des réseaux IP: un redirecteur conforme à l'IEC 61162-460 (Redirecteur 460) destiné à être installé entre deux réseaux conformes à l'IEC 61162-460 ou entre un réseau conforme à l'IEC 61162-460 et un autre réseau contrôlé.

Cette alternative ne fait l'objet d'aucune exigence supplémentaire.

8.3.1.3 Alternative B

Connexions entre des réseaux IP: un commutateur ou routeur géré satisfaisant aux principes d'un Redirecteur 460 (voir l'IEC 61162-460) pour la gestion du trafic du réseau, le réseau local virtuel (VLAN), la sécurité et la surveillance du réseau.

La documentation du fabricant doit clairement identifier la manière dont sont mis en œuvre la gestion du trafic du réseau, le VLAN, la sécurité et la surveillance de réseau afin qu'une comparaison avec l'IEC 61162-460 soit possible.

8.3.1.4 Alternative C

Connexion entre un réseau IP et un réseau non IP, et connexion entre deux réseaux non IP.

Le transfert de données entre les deux réseaux doit s'appuyer sur les principes du redirecteur IEC 61162-460.

8.3.2 Méthodes d'essai et résultats d'essai exigés

8.3.2.1 Généralités

En fonction de l'alternative mise en œuvre dans l'EUT, l'une des alternatives décrites aux paragraphes 8.3.2.2 à 8.3.2.4 doit être soumise à essai.

8.3.2.2 Alternative A

Confirmer par examen d'un rapport d'essai ou d'un certificat de conformité, qui accompagne l'EUT, que ce dernier satisfait à l'IEC 61162-460, et confirmer par examen que la documentation fournie par le fabricant décrit l'installation dans un réseau conforme à l'IEC 61162-460.

8.3.2.3 Alternative B

Confirmer par évaluation analytique que la documentation du fabricant identifie les exigences applicables des éléments suivants de l'IEC 61162-460 que l'EUT satisfait et les exceptions dans lesquelles l'EUT n'est pas conforme:

1) gestion du trafic du réseau;
2) VLAN;
3) sécurité;
4) surveillance de réseau.

Pour chaque exception applicable, confirmer par évaluation analytique que la documentation du fabricant spécifie clairement l'alternative mise en œuvre par l'EUT et qu'elle fournit une analyse de la sécurité équivalente ou améliorée offerte par l'alternative dans le réseau prévu par rapport à l'IEC 61162-460. Voir l'Annexe F pour des recommandations.

8.3.2.4 Alternative C

Confirmer par évaluation analytique que le transfert de données entre les deux réseaux respecte les principes du Redirecteur IEC 61162-460.

8.4 Matériel fournissant un accès réseau entre des réseaux contrôlés et non contrôlés

8.4.1 Exigences

8.4.1.1 Généralités

La communication entre le matériel sur des réseaux contrôlés et non contrôlés doit être assurée par l'une des alternatives décrites aux paragraphes 8.4.1.2 et 8.4.1.3 ou des alternatives équivalentes selon le cas. Voir l'Annexe F pour des recommandations.

8.4.1.2 Alternative A

Une passerelle conforme à l'IEC 61162-460 (une "Passerelle 460") ou une passerelle sans fil conforme à l'IEC 61162-460 (une "Passerelle sans fil 460") prévue pour être installée dans un réseau conforme à l'IEC 61162-460.

Cette alternative ne fait l'objet d'aucune exigence supplémentaire.

8.4.1.3 Alternative B

Une passerelle ou un routeur de réseau conforme aux principes suivants d'une Passerelle 460 ou d'une Passerelle sans fil 460:

1) pour toutes les passerelles: Fonctions de Passerelle 460: Pare-feu, Serveur d'application, Zone démilitarisée (DMZ), Communication directe;
2) pour toutes les passerelles: exigences de sécurité de la Passerelle 460;
3) éléments supplémentaires pour les passerelles sans fil: fonctions de la Passerelle sans fil 460: exigences de fonction de passerelle plus limites sur la redirection du trafic, client uniquement, cryptage et Nœud 460.

8.4.2 Méthodes d'essai et résultats d'essai exigés

8.4.2.1 Généralités

En fonction de l'alternative mise en œuvre dans l'EUT, l'une des alternatives décrites aux paragraphes 8.4.2.2 et 8.4.2.3 doit être soumise à essai.

8.4.2.2 Alternative A

Si l'EUT satisfait aux exigences applicables pour une Passerelle 460, confirmer par examen d'un rapport d'essai ou d'un certificat de conformité, qui accompagne l'EUT, que l'EUT est conforme à l'IEC 61162-460, puis confirmer par examen que la documentation fournie par le fabricant décrit l'installation dans un réseau conforme à l'IEC 61162-460.

8.4.2.3 Alternative B

Confirmer par évaluation analytique que la documentation du fabricant identifie les exigences applicables des éléments suivants de l'IEC 61162-460 que l'EUT satisfait et les exceptions dans lesquelles l'EUT n'est pas conforme:

1) fonctions de Passerelle 460: Pare-feu, Serveur d'application, Zone démilitarisée (DMZ), Communication directe;
2) sécurité de la Passerelle 460;
3) passerelles sans fil: fonctions: exigences de fonction de la Passerelle sans fil 460 plus limites sur la redirection du trafic, client uniquement, cryptage et Nœud 460.

Pour chaque exception applicable, confirmer que la documentation spécifie clairement une alternative mise en œuvre par l'EUT et fournit une analyse de la sécurité équivalente ou améliorée offerte par l'alternative dans le réseau prévu par rapport à l'IEC 61162-460.

9 Module F: Accès au système d'exploitation

9.1 Généralités

Ce module s'applique pendant le fonctionnement normal si un système d'exploitation est prévu sur le matériel.

9.2 Exigences

Le système doit être conforme à 4.2.3.2 de l'IEC 60945:2002 en ce qui concerne l'accès au système d'exploitation.

NOTE 1 Le module G contient des exigences plus détaillées.

NOTE 2 Il est entendu que la configuration du système d'exploitation est modifiée en mode entretien (voir le module H).

Le présent document ne contient aucune exigence de limitation d'accès au système d'exploitation en mode entretien.

9.3 Méthodes d'essai et résultats d'essai exigés

Confirmer par observation qu'un rapport d'essai IEC 60945:2002 est fourni et qu'il contient le paragraphe concerné (4.2.3.2). Sinon, procéder à l'essai selon l'IEC 60945.

10 Module G: Environnement de démarrage

10.1 Généralités

Ce module s'applique tant pendant le fonctionnement normal qu'en mode entretien.

L'environnement de démarrage inclut, par exemple, le programme d'amorçage, le système d'exploitation et le BIOS.

La limitation d'accès à l'environnement d'amorçage en mode entretien ne fait l'objet d'aucune exigence.

10.2 Exigences

Pendant le fonctionnement normal, des cycles répétés de mise sous tension/mise hors tension/mise sous tension ne doivent pas permettre d'accéder au stockage interne, au système d'exploitation ou au BIOS.

Pendant le fonctionnement normal, des codes de touches spéciaux, c'est-à-dire des pressions sur une ou plusieurs commandes dans une interface utilisateur, ne doivent pas permettre d'accéder au stockage interne, au système d'exploitation ou au BIOS, sauf si l'authentification de l'utilisateur a réussi (voir le module C).

En fonctionnement normal, au moment de la phase de démarrage, la connexion à un dispositif externe (par exemple un dispositif USB, un réseau, etc.) ne doit pas permettre d'accéder au stockage interne, au système d'exploitation ou au BIOS, sauf si l'authentification de l'utilisateur a réussi (voir le module C).

Le mode entretien peut éventuellement inclure une configuration permettant d'activer et de désactiver le démarrage à partir d'un dispositif externe.

NOTE Une tentative infructueuse d'authentification de l'utilisateur n'établit pas un accès au système d'exploitation ou au BIOS.

La conception du matériel peut prévoir de stocker un micrologiciel, un système d'exploitation et/ou un logiciel d'application dans un dispositif de stockage amovible (par exemple une carte mémoire CompactFlash [CF], une carte mémoire Secure Digital [SD], etc.). Dans ce cas, le module J s'applique.

10.3 Méthodes d'essai et résultats d'essai exigés

Confirmer par observation que le fait de répéter le cycle mise sous tension/mise hors tension/mise sous tension 3 fois consécutives ne permet pas d'accéder au stockage interne, au système d'exploitation ou au BIOS.

Confirmer par examen de la documentation du fabricant que, pendant le fonctionnement normal, aucun code de touches n'est disponible pour accéder au stockage interne, au système d'exploitation ou au BIOS sans authentification de l'utilisateur.

Si disponible, confirmer par observation que pendant le fonctionnement normal, et au moment de la phase de démarrage, la connexion à un dispositif externe ne permet pas d'accéder au stockage interne, au système d'exploitation ou au BIOS de l'EUT sans authentification de l'utilisateur (voir le module C).

Le cas échéant, confirmer par observation que l'accès au stockage amovible utilisé pour le micrologiciel, le système d'exploitation ou le logiciel d'application est conforme au module J.

11 Module H: Mode entretien

11.1 Généralités

Ce module s'applique lors de l'accès et en mode entretien.

Le mode entretien est destiné à être accessible uniquement par les utilisateurs autorisés par le fabricant ou par les représentants agréés du fabricant dont les compétences permettent d'être sûr que les activités d'entretien ne compromettent pas la conformité du matériel aux normes et règlements internationaux en vigueur.

NOTE Les utilisateurs autorisés sont en général ceux qui travaillent pour une société qui procède à l'installation initiale ou à l'entretien ultérieur. Il ne s'agit pas nécessairement des employés de l'entreprise de fabrication.

11.2 Exigences

L'accès au mode entretien doit uniquement être possible après l'authentification réussie de l'utilisateur (voir le module C).

Une tentative infructueuse d'authentification de l'utilisateur ne doit pas permettre d'accéder au système d'exploitation ou au BIOS. Il s'agit de vérifier que les actions suivantes ne permettent pas d'accéder au mode entretien, sauf si l'authentification de l'utilisateur a réussi conformément au module C:

– cycle d'alimentation répété sans outil ni clé;
– insertion ou dépose, sans outil ni clé, d'un dispositif ou d'un câble à la disposition d'un utilisateur classique pendant le fonctionnement normal. Par exemple un dispositif USB, des connexions réseau, etc.

Si possible en pratique:

a) le matériel doit consigner l'activation du mode entretien dans un journal interne, qui est capable de consigner au moins les 10 dernières activations; ou
b) l'activation du mode entretien doit être transmise par l'intermédiaire d'un message syslog de sorte que les autres dispositifs puissent consigner ces événements. Si le matériel dépend des messages Syslog, des matériels en mesure de les recevoir et de les traiter doivent être prévus dans le système déployé ou les manuels d'installation doivent contenir une instruction selon laquelle le matériel doit être interfacé avec un autre matériel pourvu de ces capacités.

NOTE 1 Une description du syslog est disponible dans l'IEC 61162-450 et RFC 5424. L'IEC 61162-460 exige la mise en œuvre d'une fonctionnalité de syslog.

Des journaux supplémentaires peuvent être fournis suivant le cas (des journaux de pare-feu, d'événement du système d'exploitation, d'installation/désinstallation, d'événement de programme malveillant/intrusion, de connectivité REDS, d'application, par exemple).

Le cas échéant, l'intégrité de la modification de la configuration du fabricant doit être vérifiée pour toutes les modifications provenant de sources externes. La vérification d'intégrité peut être mise en œuvre par des moyens procéduraux (à l'aide des moyens fournis par le fabricant pour confirmer l'applicabilité avant le déploiement, par exemple).

Pendant le fonctionnement normal, aucun accès ne doit permettre de modifier la configuration du fabricant sans authentification de l'utilisateur (voir le module C) ou sans l'aide d'un outil ou d'une clé.

NOTE 2 Des dispositifs simples sont parfois dépourvus de mode entretien. Par exemple, ils peuvent disposer uniquement de microcommutateurs pour modifier la configuration (des microcommutateurs pour les adresses de bus CAN, par exemple). Dans ces cas, la protection peut être assurée par l'absence d'accès libre aux microcommutateurs. Voir le module C en 6.2 d).

NOTE 3 En mode entretien, la modification de la configuration du fabricant ne fait l'objet d'aucune restriction.

Si le matériel inclut un affichage graphique et se trouve en mode entretien, le mode entretien doit alors être indiqué en permanence ou apparaître clairement d'une manière distincte.

11.3 Méthodes d'essai et résultats d'essai exigés

Si le matériel dispose d'un mode entretien, confirmer par examen de la documentation du fabricant laquelle des méthodes d'authentification de l'utilisateur présentées dans le module C est fournie pour accéder au mode entretien.

Confirmer par observation qu'il n'est pas possible d'entrer en mode entretien sans préalablement réussir l'authentification de l'utilisateur définie dans le module C.

Confirmer par observation qu'une tentative infructueuse d'accéder au mode entretien ne permet pas d'accéder au système d'exploitation ou au BIOS.

Confirmer par observation qu'un cycle de mise sous tension/mise hors tension/mise sous tension répété trois fois ne permet pas d'accéder au mode entretien.

Confirmer par observation que l'insertion ou la dépose de dispositifs ou de câbles sans l'aide d'un outil ou d'une clé ne permet pas d'accéder au mode entretien, sauf si ledit dispositif ou câble est associé à une authentification de l'utilisateur telle que définie dans le module C.

Le cas échéant, confirmer par observation que le matériel est capable de consigner au moins les 10 dernières activations du mode entretien ou que ces activations sont envoyées par le matériel à l'aide de messages syslog. Si des messages syslog sont utilisés, confirmer par observation que le traitement des messages syslog est assuré au sein du système ou confirmer par examen que le manuel d'installation contient une instruction relative à l'installation dans un environnement qui permet le traitement des messages syslog.

Le cas échéant, confirmer par observation que le matériel a consigné les événements spécifiés par le fabricant dans les journaux facultatifs ou que lesdits événements sont envoyés par le matériel à l'aide des messages syslog.

Confirmer par évaluation analytique que la configuration du fabricant ne peut pas être modifiée pendant le fonctionnement normal sans préalablement réussir l'authentification de l'utilisateur telle que définie dans le module C ou à l'aide d'un outil ou d'une clé.

Si l'EUT propose un mode de modification de la configuration du fabricant à partir d'une source externe, confirmer par observation qu'une configuration du fabricant dont le format n'est pas valide est rejetée par l'EUT. Des exemples de format non valide incluent un fichier ou une somme de contrôle de message incorrect, un hachage incorrect ou un paramètre incompatible.

NOTE Un exemple de message est un datagramme UDP sur Ethernet.

Si le matériel dispose d'un mode entretien et d'un affichage graphique, activer le mode entretien et confirmer par observation qu'il est indiqué en permanence sur l'affichage graphique ou qu'il se distincte clairement du fonctionnement normal.

12 Module I: Protection contre le plantage involontaire provoqué par une entrée d'utilisateur

12.1 Généralités

Ce module s'applique pendant le fonctionnement normal.

Si un logiciel n'a pas correctement validé une entrée d'utilisateur, certaines parties du système peuvent recevoir une entrée inattendue, ce qui peut provoquer un comportement imprévu du code ou des plantages.

Le contrôle de la validité de la syntaxe et de la sémantique des entrées utilisateur (le jeu de caractères, les longueurs de chaînes, les plages et validités numériques et les valeurs acceptables, par exemple) permet de vérifier que ces entrées correspondent à la définition prévue de l'application en ce qui concerne le format et le contenu. L'examen préalable des entrées avant de transmettre les données dans des algorithmes et processus logiciels internes empêche l'interprétation involontaire du contenu comme des instructions ou évite tout comportement imprévu.

Les attaques malveillantes (injection SQL, transmission de données dont le "contenu est volontairement malformé" et "dépassement de mémoire tampon", par exemple) sont déjà traitées dans le module D (voir l'Article 7). Le domaine d'application du présent module est la validation des données entrées par l'intermédiaire de l'interface utilisateur.

NOTE Les exigences du présent module reposent sur les commandes référencées dans le document National Institute of Standards and Technology Special Publication 800-53, Rev. 4 (NIST SP 800-53). En particulier, deux des améliorations de commande pour le contrôle de sécurité SI-10 "Information Input Validation" (Validation d'entrée des informations): SI-10(3) "Predictable Behavior in the face of invalid inputs" (Comportement prévisible en cas d'entrées non valides) et SI-10(5) "Restrict inputs to trusted sources and approved formats" (Limiter les entrées à des sources dignes de confiance et à des formats approuvés).

12.2 Exigences

Pour les données entrées par l'utilisateur, une méthode de validation doit être appliquée pour vérifier toutes les propriétés pertinentes des données, y compris la longueur, le type d'entrées, la plage complète de valeurs acceptables, les entrées manquantes ou supplémentaires, la syntaxe et la cohérence entre les champs connexes, par exemple:

– "bateau" peut être valide d'un point de vue syntaxique, car il ne contient que des caractères alphanumériques, mais il n'est pas valable s'il est prévu que l'entrée contienne uniquement des couleurs ("rouge" ou "bleu", par exemple);

– valeurs acceptables: même si la valeur "361" est un entier valide, il ne l'est pas pour le trajet ou le cap d'un navire.

Les données dont la méthode de validation des entrées n'est pas concluante doivent être rejetées et ne doivent pas compromettre le fonctionnement normal du matériel.

12.3 Méthodes d'essai et résultats d'essai exigés

La confirmation de la validation des entrées utilisateur doit reposer sur l'une des alternatives ci-dessous.

a) Pour chacune des propriétés correspondantes des données d'entrée utilisateur (longueur, type d'entrées, plage de valeurs acceptables, entrées manquantes ou supplémentaires, syntaxe et cohérence, par exemple), tenter de rendre des entrées non valides dans un nombre représentatif de champs d'entrée utilisateur différents, puis confirmer par observation que l'EUT a utilisé un mécanisme de validation de données qui empêche les données malformées d'avoir un impact sur le fonctionnement du matériel.

b) Confirmer par examen de la documentation du fabricant que ce dernier a utilisé des techniques telles que l'essai à données aléatoires (par exemple l'essai à données aléatoires de l'OWASP®[3]), l'essai de robustesse et/ou l'injection d'un défaut ou, en variante, un rapport d'essai de pénétration mettant en évidence les résultats de validation d'entrée, pour confirmer que l'entrée utilisateur est validée de manière adéquate.

NOTE L'essai à données aléatoires est une méthode d'essai des logiciels utilisée pour automatiser les essais des entrées d'une application logicielle. Il s'agit d'entrer des données non valides, imprévues ou aléatoires dans un programme informatique, puis de surveiller les exceptions logicielles telles que les plantages, les défaillances des assertions intégrées dans le code ou les fuites de mémoire potentielles. De plus amples informations peuvent être obtenues à l'adresse suivante:
https://www.owasp.org/index.php/Fuzzing
https://www.owasp.org/index.php/OWASP_Testing_Guide_Appendix_C:_Fuzz_Vectors

3 L'essai à données aléatoires de l'Open Web Application Security Project (OWASP) est un exemple de technique d'essai par boîte noire des logiciels. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il est démontré qu'ils conduisent aux mêmes résultats.

13 Module J: Interfaces des dispositifs amovibles, y compris USB

13.1 Généralités

Ce module s'applique pendant le fonctionnement normal.

Le présent document ne contient aucune exigence de limitation de fonctionnalité USB ou de fonctionnalité d'autres interfaces amovibles en mode entretien. Dans ce contexte, les autres interfaces amovibles entrent dans le cadre d'une technologie amovible par l'utilisateur, le dispositif d'origine pouvant être retiré de l'interface et remplacé par un autre dispositif dont la fonctionnalité peut être différente ou dont le contenu de données peut être différent (carte PCI Express [Peripheral Component Interconnect] remplaçable à chaud ou dispositif FireWire, par exemple).

La vulnérabilité traitée à l'Article 13 pour d'autres interfaces amovibles est liée à la mise en œuvre d'interfaces physiques, y compris des accès USB, dans lesquelles un dispositif connecté peut être retiré par l'utilisateur, laissant l'interface physiquement exposée pour la connexion avec un autre dispositif.

Le présent document estime que la protection de l'interface USB ou d'une autre interface amovible doit être assurée par une protection physique (voir 13.2.1) et/ou par une protection opérationnelle (voir 13.2.2).

Le fabricant doit déclarer quelles alternatives ont été fournies pour chaque interface.

13.2 Exigences

13.2.1 Protection physique

Le nombre de points de connexion pour REDS (accès de clavier/souris, accès d'imprimante, accès USB, cartes mémoires Secure Digital [SD], unités de disque, baies [remplaçables à chaud], etc.) doit être limité au minimum exigé pour le fonctionnement du système et son entretien et support sur toute sa durée de vie. Les accès USB n'offrant qu'une fonctionnalité de charge constituent une exception. Tous les autres points doivent:

– être physiquement bloqués contre tout accès facile sans l'aide d'un outil ou d'une clé; ou
– faire l'objet d'une instruction dans le manuel d'installation du fabricant selon laquelle le matériel doit uniquement être installé dans une console ou armoire fermée dont l'ouverture exige l'utilisation d'outils ou de clés supplémentaires. Le manuel d'installation du fabricant doit inclure une notice de risque lié à la sécurité informatique si le matériel n'est pas installé selon les instructions du fabricant.

13.2.2 Protection opérationnelle

Les interfaces des dispositifs amovibles (stockage, claviers, imprimantes, etc.) telles qu'exigées pour le fonctionnement et l'entretien sur la durée de vie doivent être réduites le plus possible et restreintes par une ou plusieurs des alternatives ci-dessous:

– blocage logique (c'est-à-dire logiciel, micrologiciel ou système d'exploitation) de l'interface;
– prévention de l'installation des pilotes. Cela signifie que les pilotes peuvent uniquement être installés en mode entretien;
– authentification cryptographique avec une force de la sécurité d'au moins 128 bits avant l'utilisation d'un contenu ou d'une fonctionnalité provenant de dispositifs USB;
– restriction de l'interface à des classes de dispositifs USB spécifiques (voir l'Annexe D);
– restriction de l'interface à un identifiant matériel spécifique (c'est-à-dire le même modèle de matériel);
– restriction de l'interface à des identificateurs d'instance spécifiques (c'est-à-dire le matériel individuel).

Si un dispositif amovible ne peut pas être restreint dans la pratique à l'aide des options détaillées ci-dessus, le fabricant doit donner des informations relatives à la manière dont il a limité l'interface à sa fonctionnalité prévue et assuré sa protection contre les mauvaises utilisations.

Les interfaces pour REDS (y compris les accès USB) doivent être protégées contre les fichiers de données non authentifiés (voir le module A) et l'exécution automatique des fichiers exécutables (voir le module B).

13.3 Méthodes d'essai et résultats d'essai exigés

13.3.1 Protection physique

Lorsqu'une protection physique est prévue, consulter la documentation du fabricant et confirmer par examen de la preuve documentée que le nombre de points de connexion pour REDS est limité au minimum exigé pour le fonctionnement du système et son entretien et support sur toute sa durée de vie.

Pour tous les autres points de connexion:

– confirmer par observation qu'ils sont physiquement bloqués contre tout accès facile sans l'aide d'un outil ou d'une clé ou qu'ils ne peuvent être utilisés que pour la charge; ou

– confirmer par examen de la documentation du fabricant que le manuel d'installation du fabricant contient une instruction selon laquelle le matériel doit uniquement être installé dans une console ou armoire fermée dont l'ouverture exige l'utilisation d'outils ou de clés supplémentaires, et qu'il y a une notice de risque lié à la sécurité informatique si le matériel n'est pas installé selon les instructions du fabricant.

13.3.2 Protection opérationnelle

Lorsqu'une protection physique est prévue, pour les points de connexion USB, utiliser la documentation du fabricant et confirmer par évaluation analytique que l'EUT refuse d'exécuter une autre fonctionnalité que celle spécifiée dans la documentation du fabricant.

Consulter la documentation du fabricant et confirmer par examen qu'une déclaration est incluse quant à l'alternative de protection opérationnelle fournie pour chaque interface amovible.

Si une technologie REDS peut disposer d'une fonctionnalité autre que le stockage de données (du clavier au stockage de données, par exemple), associer l'un après l'autre un exemple de ce type de dispositifs de non-stockage de données au point de connexion et confirmer par évaluation analytique que l'EUT exécute uniquement les fonctions spécifiées dans la documentation du fabricant.

Le cas échéant, consulter la documentation du fabricant et confirmer par examen que des informations sont disponibles quant à la manière dont l'interface est limitée à sa fonctionnalité prévue et est protégée contre toute mauvaise utilisation pour un dispositif amovible quelconque qui ne peut pas, dans la pratique, être restreint à l'aide des options énumérées en 13.2.

14 Module K: IEC 61162-1 ou IEC 61162-2 en tant qu'interface

Ce module s'applique tant pendant le fonctionnement normal qu'en mode entretien.

Les interfaces conformes à l'IEC 61162-1 ou à l'IEC 61162-2 sont câblées d'un matériel à l'autre. Les normes de matériel existantes traitent déjà des questions telles que la protection de la configuration des paramètres, etc. qui peut être vulnérable en cas de menace informatique.

NOTE Un exemple de protection de configuration des paramètres est l'AIS de type Classe A de l'IEC 61993-2:2018.

Les exigences de vérification de somme de contrôle et de traitement des sentences mal formées sont intégralement spécifiées dans les normes de matériel existantes et dans l'IEC 61162-1.

Les exigences de conversion du trafic entre une interface IEC 61162-1 ou IEC 61162-2 et une interface IEC 61162-450 sont spécifiées dans le module L.

15 Module L: IEC 61162-450 en tant qu'interface

15.1 Généralités

Ce module s'applique pendant le fonctionnement normal.

Le module A et le module B s'appliquent pour tout fichier reçu par l'intermédiaire de cette interface.

Le module D s'applique pour la protection contre les programmes malveillants et la prévention des intrusions.

15.2 Sentences IEC 61162-1

Une instruction non autorisée d'exécution d'une action ou de définition d'un paramètre de configuration du fabricant est un exemple de menace externe liée aux interfaces IEC 61162-450 et aux sentences IEC 61162-1 réparties dans le réseau local (LAN). Les exigences relatives à cette question sont couvertes par le module H.

Les exigences en matière de vérification de somme de contrôle ou de traitement des sentences mal formées sont couvertes par le module K.

Les exigences en matière d'authentification et d'identification sont intégralement spécifiées dans l'IEC 61162-450.

L'authentification peut être utilisée, comme décrit dans pour le paramètre de bloc TAG "Authentification générale – a" de l'IEC 61162-450.

15.3 IEC 61162-450 utilisé pour le transfert de fichier

Le paragraphe 15.3 s'applique tant au transfert de fichier binaire IEC 61162-450 qu'à tous les transferts de fichier reposant sur ONF (voir l'IEC 61162-450).

Pour le transfert des fichiers de données, le module A s'applique. L'enregistrement ou la consignation des fichiers de données (par VDR, par exemple) n'est pas limité(e).

Pour le transfert des fichiers exécutables, le module B s'applique.

16 Module M: Autres interfaces

Ce module s'applique pendant le fonctionnement normal.

Ce module s'applique à toute interface autre que celles mentionnées dans le module J, le module K ou le module L, telle que Firewire, Thunderbolt, Small Computer System Interface (SCSI), etc., y compris les interfaces sans fil comme Bluetooth®[4], Wi-Fi®[5], Near Field Communication (NFC – communication en champ proche), etc. qui ne font pas partie du module J, du module K ou du module L.

NOTE Wi-Fi est une famille de technologies de réseau sans fil reposant sur la famille de normes IEEE 802.11.

Tous les modules pertinents du présent document s'appliquent lorsqu'une interface offre une fonctionnalité applicable.

17 Module N: Entretien du logiciel

17.1 Généralités

Ce module s'applique tant pendant le fonctionnement normal qu'en mode entretien.

NOTE 1 Le matériel peut changer dans la norme de construction pendant son cycle de vie. Par exemple, une nouvelle caractéristique peut être ajoutée, une caractéristique existante peut être modifiée ou des erreurs de conception (souvent appelées bogues) peuvent être corrigées. Le certificat d'agrément de type est valable pour une version identifiée du produit. Par conséquent, un nouvel essai de conformité et un nouveau certificat peuvent être exigés en cas de modification du logiciel.

NOTE 2 Les lois locales en matière d'évaluation de conformité (au sein de l'Union européenne, par exemple) peuvent exiger de signaler toutes les modifications à l'autorité d'évaluation de la conformité.

Les mises à jour de logiciels relatives à la sécurité représentent une part importante de la protection d'un système contre des attaques, même si les correctifs et nouvelles fonctionnalités sont souvent des éléments importants dans l'entretien du matériel. Toutefois, il est important de vérifier que les modifications apportées au logiciel ne compromettent pas la fonctionnalité prévue du matériel ou sur sa conformité aux règlements en vigueur, avant le déploiement.

L'entretien du logiciel peut être réalisé par:

– des personnes autorisées proches du matériel, en mode entretien;
– l'équipe en fonctionnement normal, si des moyens semi-automatisés sont prévus;
– des personnes autorisées éloignées du matériel en mode entretien pour l'accès à distance (voir l'Article 18).

Le mode entretien est destiné à être disponible uniquement au personnel autorisé par le fabricant.

---

4 Bluetooth est le nom commercial d'un produit fourni par Bluetooth SIG, Inc. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il est démontré qu'ils conduisent aux mêmes résultats.

5 Wi-Fi est le nom commercial d'un produit fourni par la Wi-Fi Alliance. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il est démontré qu'ils conduisent aux mêmes résultats.