IEC TR 60601-4-5

Edition 1.0 2021-01

TECHNICAL REPORT

colour inside

Medical electrical equipment –
Part 4-5: Guidance and interpretation – Safety-related technical security specifications

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

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

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

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

IEC online collection - oc.iec.ch

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

Electropedia - www.electropedia.org

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

IEC TR 60601-4-5

Edition 1.0 2021-01

TECHNICAL REPORT

Medical electrical equipment –
Part 4-5: Guidance and interpretation – Safety-related technical security specifications

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 11.040.01

ISBN 978-2-8322-9227-3

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MEDICAL ELECTRICAL EQUIPMENT –

Part 4-5: Guidance and interpretation – Safety-related technical security specifications

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 TR 60601-4-5 has been prepared by subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62: Electrical equipment in medical practice. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft TR	Report on voting
62A/1402/DTR	62A/1417A/RVDTR

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 Technical Report 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.

In this document, the following print types are used:

– TERMS DEFINED IN CLAUSE 3: SMALL CAPITALS;

– COMPLIANCE STATEMENTS IN CLAUSE 4 AND CLAUSE 5: ITALICS.

An asterisk (*) as the first character of a title or at the beginning of a paragraph or table title indicates that there is guidance or rationale related to that item in Annex A.

A list of all parts in the IEC 60601 series, published under the general title *Medical electrical equipment*, can be found on the IEC website.

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

This document provides IT SECURITY specifications for MEDICAL ELECTRICAL EQUIPMENT (ME EQUIPMENT) AND MEDICAL ELECTRICAL SYSTEMS (ME SYSTEMS) connectable to MEDICAL IT-NETWORKS as network components. MEDICAL DEVICE SOFTWARE, although not in the scope of IEC 60601 (all parts), can also make use of this document. The intent of this document is to specify SECURITY capabilities that enable a MEDICAL DEVICE to be more easily integrated into a MEDICAL IT-NETWORK environment at a given SECURITY LEVEL (SL).

ME SYSTEMS placed onto the market as a whole by one legal MANUFACTURER should follow this document as a whole network component of an IT-NETWORK, in the same way as ME EQUIPMENT. ME SYSTEMS configured by the owner of a MEDICAL IT-NETWORK can be treated in the same way as other combinations of medical and nonmedical devices within a MEDICAL IT-NETWORK and are out of the scope of this document but within the scope of standards for MEDICAL IT-NETWORKS (e.g. IEC 80001 (all parts) [7][1]).

This document references already existing SECURITY LEVEL (SL) requirements for components of an IT-NETWORK as listed in IEC 62443-4-2:2019. This document is restricted to the network components which are MEDICAL DEVICES in order to allow the use of additional nonmedical components within the MEDICAL IT-NETWORK complying with IEC 62443 (all parts) [3] or with further appropriate SECURITY standards. This document modifies IEC 62443-4-2:2019 only for specific aspects of MEDICAL DEVICES in MEDICAL IT-NETWORKS. The primary goal of this document is to provide a flexible framework that facilitates addressing current and future vulnerabilities and applying necessary mitigations in a systematic, defendable manner. Each of the proposed COUNTERMEASURES should take into account that requirements regarding the safety and performance of a MEDICAL DEVICE should not be negatively impacted.

The main audience for this document is MEDICAL DEVICE MANUFACTURERS and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

MEDICAL IT-NETWORK integrators, as a further audience, may make use of the SECURITY LEVEL classification for MEDICAL DEVICES, to assist them in the secure integration of MEDICAL DEVICES into their networks. This assistance will be to help MEDICAL IT-NETWORK integrators to identify the realized capability SECURITY LEVEL SL-C of MEDICAL DEVICES and thus to specify appropriate additional SECURITY COUNTERMEASURES in the individual MEDICAL IT-NETWORK they are procuring.

MEDICAL DEVICE MANUFACTURERS should use this document to understand and apply the specifications for specific capability SECURITY LEVEL SL-C of their MEDICAL DEVICES. A MEDICAL DEVICE may not provide the capability itself but may be designed to integrate with a higher-level entity – e.g. a hospital IT-NETWORK or department IT-NETWORK – and thus benefit from that entity's capability. This document should guide MEDICAL DEVICE MANUFACTURERS as to what specifications can be allocated and which specifications need to be native in the MEDICAL DEVICE. MEDICAL DEVICE MANUFACTURERS should provide documentation on how to properly integrate the MEDICAL DEVICE into a MEDICAL IT-NETWORK (see Clause A.2 for typical network connections of MEDICAL DEVICES).

This document should be used to apply and verify appropriate technical SECURITY specifications for MEDICAL DEVICES which thus can easily be integrated into existing or growing MEDICAL IT-NETWORKS and which in some cases are connected to the Internet. This document does not include SECURITY specifications for any additional services installed in a MEDICAL IT-NETWORK.

---

1 Numbers in square brackets refer to the Bibliography.

As defined in IEC TS 62443-1-1:2009 [4], there are a total of seven foundational requirements to be addressed:

– identification and authentication control (IAC);
– use control (UC);
– system integrity (SI);
– data CONFIDENTIALITY (DC);
– restricted data flow (RDF);
– timely response to events (TRE);
– resource availability (RA).

NOTE 1 Data CONFIDENTIALITY includes the unauthorized access to MEDICAL DEVICE data which could be leveraged to cause all many types of HARM. The focus of this document is SAFETY-related SECURITY specifications for MEDICAL DEVICES regarding data CONFIDENTIALITY. However, the listed provisions for SAFETY-related data CONFIDENTIALITY are a good base also for non-SAFETY-related SECURITY aspects.

These seven requirements are used for meeting the capability SECURITY LEVEL SL-C of a MEDICAL DEVICE which may be placed on a MEDICAL IT-NETWORK. Defining SL-C for MEDICAL DEVICES is the goal and objective of this document. The target SECURITY LEVEL SL-T and achieved SECURITY LEVELS (SL-A) for a complete MEDICAL IT-NETWORK or a subset of that network (e.g. a specific ZONE of it) are out of the scope of this document.

A capability SECURITY LEVEL SL-C is defined for COUNTERMEASURES and for inherent SECURITY properties of a MEDICAL DEVICE. It is a measure of the effectiveness strength of the COUNTERMEASURES, which are either separate or integral to a MEDICAL DEVICE, for the addressed SECURITY property and contributes to the achieved SECURITY LEVEL SL-A in the corresponding part of the MEDICAL IT-NETWORK.

COUNTERMEASURES can be:

– technical COUNTERMEASURES (e.g. firewalls, anti-virus software, etc.), or
– administrative COUNTERMEASURES (e.g. policies, and-procedures), or
– physical COUNTERMEASURES (e.g. locked doors, encapsulated printed circuit board, etc.).

The specified "component requirements" (CRs) for MEDICAL DEVICES provided in this document are mainly derived from the IT-NETWORK "system requirements" (SRs) in IEC 62443-3-3 [5] which are in turn derived from the overall foundational requirements defined in IEC TS 62443-1-1:2009 [4]. MEDICAL DEVICE specifications also include a set of "requirement enhancements" (REs). The combination of CRs and REs implemented into a MEDICAL DEVICE will determine the capability SECURITY LEVEL SL-C of the MEDICAL DEVICE.

As this document provides specifications for MEDICAL DEVICES with external data interfaces or with a human interface for processing – e.g. entering, capturing or viewing – CONFIDENTIAL PATIENT DATA, the specifications will be designated as follows:

– MEDICAL DEVICE specifications for ME EQUIPMENT and manufacturer provided by ME SYSTEMS;
– MEDICAL DEVICE SOFTWARE specifications.

The majority of the specifications in this document are the same for these two types and are thus designated simply as a MEDICAL DEVICE specification. When a specification is only applicable to one of the above two types, it is specified as such.

This document refers to both ESSENTIAL PERFORMANCE and ESSENTIAL FUNCTION, which are very distinct. ESSENTIAL FUNCTION is a well-established term for SECURITY aspects and is different from ESSENTIAL PERFORMANCE which is related to safety of one ME EQUIPMENT or ME SYSTEM in NORMAL CONDITION and SINGLE FAULT CONDITION. An ESSENTIAL FUNCTION CONSIDERS, for instance, a successful attack on the MEDICAL IT-NETWORK and its connected MEDICAL DEVICES and supporting systems. This may lead to loss of the MEDICAL IT-NETWORK supporting function and of some functions of the MEDICAL DEVICE itself. In that case, the MEDICAL DEVICE is still responsible for providing a condition sustaining the required minimum functions, including but not limited to BASIC SAFETY and ESSENTIAL PERFORMANCE.

MEDICAL ELECTRICAL EQUIPMENT –

Part 4-5: Guidance and interpretation – Safety-related technical security specifications

1 Scope

This document, which is a Technical Report, provides detailed technical specifications for SECURITY features of MEDICAL DEVICES used in MEDICAL IT-NETWORKS. MEDICAL DEVICES dealt with in this document include MEDICAL ELECTRICAL EQUIPMENT, MEDICAL ELECTRICAL SYSTEMS and MEDICAL DEVICE SOFTWARE. MEDICAL DEVICE SOFTWARE, although not in the scope of IEC 60601 (all parts), can also make use of this document. Based on the seven foundational requirements described in the state-of-the-art document IEC TS 62443-1-1:2009 [4], this document provides specifications for different MEDICAL DEVICE capability SECURITY LEVELS (SL-C). The specified SECURITY capabilities of a MEDICAL DEVICE can be used by various members of the medical community to integrate the device correctly into defined SECURITY ZONES and CONDUITS of a MEDICAL IT-NETWORK with an appropriate MEDICAL IT-NETWORK's target SECURITY LEVEL (SL-T).

This document is applicable to MEDICAL DEVICES with external data interface(s), for example when connected to a MEDICAL IT-NETWORK or when a human interface is used for processing – e.g. entering, capturing or viewing – CONFIDENTIAL DATA.

This document does not apply to other software used on a MEDICAL IT-NETWORK which does not meet the definition of MEDICAL DEVICE SOFTWARE.

NOTE 1 An example of this exclusion is software not incorporated into the MEDICAL DEVICE.

NOTE 2 This document does also not apply to industry protocols such as DICOM and HL7.

This document does not apply to in-vitro diagnostic devices (IVD).

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 60601-1:2005, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*
IEC 60601-1:2005/AMD1:2012
IEC 60601-1:2005/AMD2:2020

IEC 62443-4-2:2019, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60601-1:2005, IEC 60601-1/AMD1:2012 and IEC 60601-1/AMD2:2020 and the following 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 https://www.iso.org/obp

3.1
ASSET
physical or logical object having either a perceived or actual value to the MEDICAL DEVICE or MEDICAL IT-NETWORK

Note 1 to entry: In this specific case, an ASSET is any item that should be protected as part of the MEDICAL DEVICE SECURITY management system.

Note 2 to entry: An ASSET is not limited to the MEDICAL DEVICE alone but can also include the physical ASSETS under its control.

Note 3 to entry: Typically, the RESPONSIBLE ORGANIZATION is an ASSET owner.

[SOURCE: IEC 62443-4-2:2019, 3.1.1, modified – Replacement of "IACS" with "MEDICAL DEVICE or MEDICAL IT-NETWORK" in the definition, replacement of "IACS" with "MEDICAL DEVICE" in Note 2 to entry, and addition of a new Note 3 to entry.]

3.2
AUTHENTICATION
verification of the claimed identity of an entity

Note 1 to entry: AUTHENTICATION is usually a prerequisite to allowing access to resources in a MEDICAL DEVICE.

[SOURCE: IEC 62443-4-2:2019, 3.1.4, modified – Replacement of "control system" with "MEDICAL DEVICE" in Note 1 to entry.]

3.3
AUTHENTICITY
property that an entity is what it claims to be through AUTHENTICATION of origin and verification of INTEGRITY

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.

[SOURCE: IEC 62443-4-2:2019, 3.1.6]

3.4
AVAILABILITY
property of ensuring timely and reliable access to and use of MEDICAL DEVICE information and functionality

[SOURCE: IEC 62443-4-2:2019, 3.1.7, modified – Replacement of "control system" with "MEDICAL DEVICE".]

3.5
COMPENSATING COUNTERMEASURE
COUNTERMEASURE employed in lieu of or in addition to inherent SECURITY capabilities to satisfy one or more SECURITY requirements

Note 1 to entry: Examples include:

– (MEDICAL DEVICE): locked cabinet around a controller that otherwise might be exposed to unauthorized access via its physical data interfaces, or an encapsulated printed circuit board;

– (ZONE level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the MEDICAL IT-NETWORK; and

– (MEDICAL DEVICE): a product supplier's magnetic resonance imaging (MRI) machine cannot meet the access control capabilities from an ASSET owner (i.e. typically the RESPONSIBLE ORGANIZATION), so the product supplier puts a firewall in front of the MRI machine and sells it as a system.

[SOURCE: IEC 62443-4-2:2019, 3.1.9, modified – The example has been formatted as a note to entry. Note 1 to entry has been modified by replacing "component-level" with "MEDICAL DEVICE", "IACS" with "MEDICAL IT-NETWORK", "PLC" with "MRI", by removing "control system" and by adding a second example for the first dash.]

3.6
CONDUIT
logical grouping of communication channels, connecting two or more ZONES that share common SECURITY requirements

Note 1 to entry: A CONDUIT is allowed to traverse a ZONE as long as the SECURITY of the channels contained within the CONDUIT is not impacted by the ZONE.

[SOURCE: IEC 62443-4-2:2019, 3.1.11]

3.7
CONFIDENTIALITY
assurance that information is not disclosed to unauthorized individuals, PROCESSES, or devices

Note 1 to entry: When used in the context of a MEDICAL DEVICE, CONFIDENTIALITY refers to protecting MEDICAL DEVICE data and information from unauthorized access.

[SOURCE: IEC 62443-4-2:2019, 3.1.12, modified – Replacement of "an IACS" with "a MEDICAL DEVICE".]

3.8
CONFIDENTIAL DATA
data to which only a limited number of persons have access and which are meant for restricted use

[SOURCE: ISO 5127:2017, 3.1.10.18, modified – Deletion of Note 1 to entry.]

3.9
COUNTERMEASURE
action, device, procedure or technique that reduces a THREAT, a vulnerability or the consequences of an attack by minimizing the HARM the attack can cause or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: The term "control" is also used to describe this concept in some contexts. The term "COUNTERMEASURE" has been chosen for this document to avoid confusion with the term "control" in the context of "PROCESS control" and "control system".

[SOURCE: IEC 62443-4-2:2019, 3.1.15]

3.10
*** ESSENTIAL FUNCTION**
CORE FUNCTION
function or capability that is required to maintain BASIC SAFETY, ESSENTIAL PERFORMANCE, a minimum of clinical functionality as specified by the manufacturer, and operational AVAILABILITY for the MEDICAL DEVICE

Note 1 to entry: ESSENTIAL FUNCTIONS include, but are not limited to, the SAFETY instrumented function (BASIC SAFETY and ESSENTIAL PERFORMANCE), the control function and the AVAILABILITY of urgently needed functions and such allowing the OPERATOR to view and manipulate the MEDICAL DEVICE safely with the most urgently needed performance (operational AVAILABILITY). The loss of ESSENTIAL FUNCTION is commonly termed loss of protection, loss of control and loss of view respectively.

Note 2 to entry: The term is derived from IEC 62443-4-2:2019, 3.1.20, and has been refined for the purpose and scope of this document.

3.11
FIRECALL
method established to provide emergency access to a secure MEDICAL DEVICE

Note 1 to entry: In an emergency situation, unprivileged users can gain access to key systems to correct the problem. When a FIRECALL is used, there is usually a review PROCESS to ensure that the access was used properly to correct a problem. These methods generally either provide a one-time use user identifier (ID) or one-time password or other suitable measures.

Note 2 to entry: Also referred to as "break glass" feature.

[SOURCE: IEC 62443-4-2:2019, 3.1.22, modified – Replacement of "control system" with "MEDICAL DEVICE"; addition of the words "or other suitable measures" in Note 1 to entry; addition of Note 2 to entry.]

3.12
INCIDENT
single or a series of unwanted or unexpected information SECURITY events that have a significant probability of compromising business operations and threatening information SECURITY

Note 1 to entry: This definition is based on the term: information SECURITY INCIDENT

[SOURCE: ISO/IEC 27000:2018, 3.31, modified – Deletion of "information security" in the term.]

3.13
INTEGRITY
property of protecting the accuracy and completeness of ASSETS

[SOURCE: IEC 62443-4-2:2019, 3.1.27]

3.14
IT-NETWORK
INFORMATION TECHNOLOGY NETWORK
system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

Note 1 to entry: Adapted from IEC 61907:2009, 3.1.1.

Note 2 to entry: The scope of the MEDICAL IT-NETWORK in this document is defined by the RESPONSIBLE ORGANIZATION based on where the MEDICAL DEVICES in the MEDICAL IT-NETWORK are located and the defined use of the network. It can contain IT infrastructure, home health and non-clinical contexts.

[SOURCE: IEC 80001-1:2010, 2.12, modified – Deletion of the reference to 4.3.3 in Note 2 to entry.]

3.15
LEAST PRIVILEGE
basic principle that holds that users (humans, software PROCESSES or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

Note 1 to entry: LEAST PRIVILEGE is commonly implemented as a set of roles in a MEDICAL DEVICE.

[SOURCE: IEC 62443-4-2:2019, 3.1.28, modified – Replacement of "an IACS" with "a MEDICAL DEVICE" in Note 1 to entry.]

3.16
MEDICAL DEVICE
instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the MANUFACTURER to be used, alone or in combination, for human beings, for one of more of the specific medical purpose(s) of

– diagnosis, prevention, monitoring, treatment or alleviation of disease,
– diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
– investigation, replacement, modification, or support of the anatomy or of a physiological PROCESS,
– supporting or sustaining life,
– control of conception,
– cleaning, disinfection or sterilization of MEDICAL DEVICES,
– providing information by means of in vitro examination of specimens derived from the human body,

and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means

Note 1 to entry: Products which may be considered to be MEDICAL DEVICES in some jurisdictions but not in others include:

– disinfection substances,
– aids for persons with disabilities,
– devices incorporating animal and/or human tissues, and
– devices for in-vitro fertilization or assisted reproductive technologies.

Note 2 to entry: For clarification purposes, in certain regulatory jurisdictions, devices for cosmetic/aesthetic purposes are also considered MEDICAL DEVICES.

Note 3 to entry: For clarification purposes, in certain regulatory jurisdictions, the commerce of devices incorporating human tissues is not allowed.

[SOURCE: IMDRF/GRRP WG/N47:2018, 3.26]

3.17
MEDICAL DEVICE SOFTWARE
software system that has been developed for the purpose of being incorporated into the MEDICAL DEVICE being developed or that is intended for use as a MEDICAL DEVICE

Note 1 to entry: This includes a MEDICAL DEVICE software product, which then is a MEDICAL DEVICE in its own right.

[SOURCE: IEC 62304:2006 and IEC 62304:2006/AMD1:2015, 3.12]

3.18
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE

Note 1 to entry: The MEDICAL IT-NETWORK in its INTENDED USE mainly provides connectivity for MEDICAL DEVICES that are intended to be connected to such an IT-NETWORK. Also non-medical equipment may be connected to the MEDICAL IT-NETWORK, mostly intended to support the MEDICAL DEVICES.

[SOURCE: IEC 80001-1:2010, 2.16, modified – Addition of Note 1 to entry.]

3.19
NON-REPUDIATION
ability to prove the occurrence of a claimed event or action and its originating entities

Note 1 to entry: The purpose of NON-REPUDIATION is to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.

[SOURCE: IEC 62443-4-2:2019, 3.1.32]

3.20
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

Note 1 to entry: The probability of occurrence includes the exposure to a HAZARDOUS SITUATION and the possibility to avoid or limit the HARM.

[SOURCE: ISO/IEC Guide 63:2019, 3.10]

3.21
SAFETY
freedom from unacceptable RISK

[SOURCE: ISO/IEC Guide 63:2019, 3.16]

3.22
SECURITY
CYBERSECURITY
state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction, to a degree that the related risks to AUTHENTICATION, use control, INTEGRITY, data CONFIDENTIALITY, data flow, timely response and AVAILABILITY are maintained at an acceptable level throughout the life cycle

Note 1 to entry: A similar definition of the term is in preparation for ISO 81001-1:— and IEC 81001-5-1:—. In this document, all seven foundational requirements are included (not only three of them).

3.23
SECURITY LEVEL
level corresponding to the required set of COUNTERMEASURES and inherent SECURITY properties of devices and systems for a ZONE or CONDUIT based on assessment of RISK for the ZONE or CONDUIT

[SOURCE: IEC 62443-4-2:2019, 3.1.37]

3.24
THREAT
set of circumstances and associated sequence of events with the potential to adversely affect operations (including mission, functions, image or reputation), ASSETS, MEDICAL DEVICES or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

[SOURCE: IEC 62443-4-2:2019, 3.1.43, modified – Replacement of "control systems" with "MEDICAL DEVICES".]

3.25
ZONE
collection of entities that represents partitioning of a system under consideration on the basis of their functional, logical and physical (including location) relationship

Note 1 to entry: A ZONE has a clear border. The SECURITY policy of a ZONE is typically enforced by a combination of mechanisms both at the ZONE edge and within the ZONE.

[SOURCE: IEC 62443-4-2:2019, 3.1.49]

4 Common SECURITY constraints

4.1 Overview

The SECURITY related RISKS addressed in this document should be controlled by:

– MEDICAL DEVICE SECURITY measures, and/or

– MEDICAL IT-NETWORK SECURITY measures.

Within the scope of this document, only those COUNTERMEASURES are addressed which refer to a MEDICAL DEVICE (i.e. ME EQUIPMENT, MANUFACTURER provided ME SYSTEM, MEDICAL DEVICE SOFTWARE). COUNTERMEASURES which a RESPONSIBLE ORGANIZATION might apply to a MEDICAL IT-NETWORK (including ME SYSTEMS specifically combined by the RESPONSIBLE ORGANISATION) are not within the scope of this document. However, if a MEDICAL DEVICE with external data interfaces requires additional (external) COMPENSATING COUNTERMEASURES, those measures should be addressed in the ACCOMPANYING DOCUMENTS of the MEDICAL DEVICE. Risk assessments according to ISO 14971:2019 [13] are not part of this document; however, they should take into account the technical solutions offered in this document when assessing SECURITY related risks.

Compliance with the specification should be checked by tests and inspections as specified in 4.2 to 4.6, and Clause 5 to Clause 7.

4.2 * Support of ESSENTIAL FUNCTION

BASIC SAFETY and especially ESSENTIAL PERFORMANCE can be affected by THREATS, resulting in hazardous situations or lack of appropriate AVAILABILITY of the MEDICAL DEVICE. BASIC SAFETY, ESSENTIAL PERFORMANCE, a minimum of clinical functionality and operational availability should be maintained during and after an exploitation of a vulnerability (see Figure 1). In this context, the word "maintained" means that the MEDICAL DEVICE goes over to a safe condition either without operating any longer or, for particular MEDICAL DEVICES, operating safely with appropriate, limited functionalities or without clinical function but providing an alarm, if the MEDICAL DEVICE is used under medical supervision.

SECURITY COUNTERMEASURES should not adversely affect the ability to maintain the ESSENTIAL FUNCTION of the MEDICAL DEVICE.

In particular, the following should be applied.

– Access controls (i.e. foundational requirements 1 and 2) should not prevent the operation of ESSENTIAL FUNCTION of MEDICAL DEVICES (see also 4.6.3).

– MEDICAL DEVICES with access controls should implement specific appropriate FIRECALL functions for emergency access to relevant clinical functions or data. If a FIRECALL function is used, this should be made traceable.

– SECURITY COUNTERMEASURES of MEDICAL DEVICES or the connected MEDICAL IT-NETWORK infrastructure that provide boundary protection should not impact the ESSENTIAL FUNCTION of the MEDICAL DEVICE.

– A denial of service (DoS) attack on the MEDICAL DEVICE or on the connected MEDICAL IT-NETWORK should not prevent the MEDICAL DEVICE that implements the SAFETY-related function from performing as indicated in Figure 1.

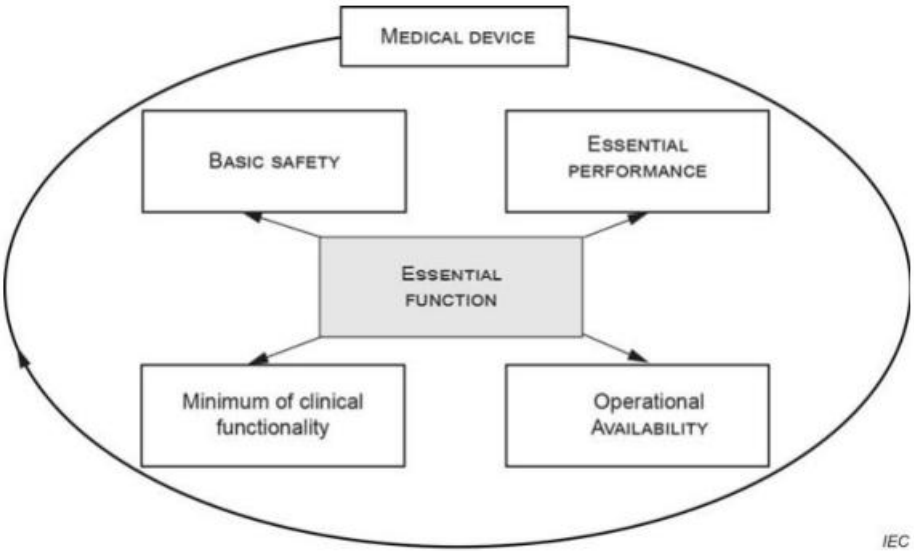


Figure 1 – ESSENTIAL FUNCTION

To determine the required ESSENTIAL FUNCTION, a benefit-risk analysis (between safety and security) should be conducted to determine which functionality can be sacrificed, and which cannot.

NOTE For examples and more guidance, see Annex A.

Compliance with the specification should be checked by inspection of the ESSENTIAL FUNCTION concept in the SECURITY design documents and the correlated test documentation.

4.3 COMPENSATING COUNTERMEASURES

If the target SECURITY LEVEL SL-T for a specific IT-NETWORK or a part of it (e.g. zone) exceeds the capability SECURITY LEVEL SL-C of a MEDICAL DEVICE, COMPENSATING COUNTERMEASURES external to the MEDICAL DEVICE are required unless the responsible organization adjusts their SL-T. In some cases, COMPENSATING COUNTERMEASURES external to the MEDICAL DEVICE are also required as last option to fulfil the intended capability SECURITY LEVEL SL-C. When this is the case, the ACCOMPANYING DOCUMENTS for that MEDICAL DEVICE should describe the appropriate COMPENSATING COUNTERMEASURES to be applied to the connected MEDICAL IT-NETWORK to allow the specification to be met when the MEDICAL DEVICE is integrated into a MEDICAL IT-NETWORK.

Compliance with the specification should be checked by inspection of the ACCOMPANYING DOCUMENTS, focused on the description of appropriate COMPENSATING COUNTERMEASURES, and of the SECURITY design documents.

4.4 LEAST PRIVILEGE

When required and appropriate, MEDICAL DEVICES should provide the capability for the connected MEDICAL IT-NETWORK to enforce the concept of LEAST PRIVILEGE. Individual MEDICAL DEVICES should provide the granularity of permissions and the flexibility of mapping those permissions to roles sufficient to support this. Individual accountability should be available when required.

NOTE The granularity of permissions and assignment is dependent on the type of the MEDICAL DEVICE and is defined in its ACCOMPANYING DOCUMENTS.

Compliance with the specification should be checked by inspection of the role concept and the concept of LEAST PRIVILEGE in the SECURITY design documents and inspection of the ACCOMPANYING DOCUMENTS, focused on the description of granular permissions, and by inspection of test results according to the corresponding parts of Table 1.

4.5 Data minimization

MEDICAL DEVICES should only store and transmit sensitive and person identifiable information (CONFIDENTIAL DATA) that are required, relevant and limited to what is necessary for the purposes for which they are processed. Such data in the MEDICAL DEVICE context should not be held or further used unless this is essential for reasons that are clearly stated by the MANUFACTURER in the ACCOMPANYING DOCUMENTS (e.g. a "flight recorder" or logging function or data needed for standards or regulatory requirements).

Compliance with the specification should be checked by inspection of the CONFIDENTIAL DATA handling concept in the SECURITY design documents, inspection of the ACCOMPANYING DOCUMENTS and by inspection of test results according to the corresponding parts of Table 1.

4.6 * Overarching constraints

4.6.1 Constraints referenced by the MEDICAL DEVICE specifications

The overarching constraints of 4.6.2 and 4.6.3 should be applied.

4.6.2 Hardware SECURITY

Based on a RISK and THREAT analysis, the MEDICAL DEVICE should provide the capability to protect critical ASSETS via hardware mechanisms according to commonly accepted and proven SECURITY practices and specifications (e.g. locks, tokens, SECURITY chips). This protection involves one or more of the following SECURITY objectives: INTEGRITY, timely response, AUTHENTICITY, use control, AVAILABILITY, and restricted data flow.

NOTE 1 When cryptographic capabilities are used for higher SECURITY LEVEL applications and the SECURITY design and implementation of the MEDICAL DEVICE into a MEDICAL IT-NETWORK, a good reference for implementation of the capabilities is ISO/IEC 19790 [14] or FIPS 140-2 [22].

A RISK and THREAT analysis should be conducted to determine the level of hardware SECURITY for the MEDICAL DEVICE, and a vulnerability analysis identifying the residual RISKS should be conducted once the hardware SECURITY is selected.

NOTE 2 4.6.2 is not applicable for software which is itself a MEDICAL DEVICE (software as a MEDICAL DEVICE). The ACCOMPANYING DOCUMENTS of such software, however, can define hardware requirements relevant to SECURITY.

Compliance with the specification should be checked by inspection of

– *the hardware bill of materials, comparing it with commonly accepted and proven SECURITY practices and specifications (e.g. locks, tokens, SECURITY chips) with focus on the ASSETS secured by those hardware SECURITY measures,*
– *the corresponding concept in the SECURITY design documents, including residual RISK assessments, and*

– *test results according to the corresponding parts of Table 1.*

4.6.3 * Specific SECURITY features for MEDICAL DEVICES

The MANUFACTURER of a MEDICAL DEVICE should determine, for the design and the ACCOMPANYING DOCUMENTS, the following:

– beside BASIC SAFETY and ESSENTIAL PERFORMANCE, the required product group appropriate ESSENTIAL FUNCTION (e.g. AVAILABILITY in case of ongoing SECURITY attacks on the MEDICAL IT-NETWORK and the connected devices) even with temporarily reduced IT functionality of the MEDICAL DEVICE;

– specific appropriate FIRECALL functions for emergency access to have the possibility to override SECURITY measures and how they are managed (e.g. by logging, information signalling, alarming) in cases of intentional overriding a SECURITY measure due to higher priority SAFETY needs;

– appropriate minimum target SECURITY LEVEL SL-T for all INTENDED USE environments including the network integrations normally existing in these use environments in which the MEDICAL DEVICE is typically used. If SECURITY LEVELS for the use environments are defined by other documents, they should be taken into account and referenced.

NOTE 1 The capability SECURITY LEVEL SL-C of a MEDICAL DEVICE does not necessarily need to be as high as the target SECURITY LEVEL SL-T specified for a certain use environment/ZONE. However, the realized SL-C of a MEDICAL DEVICE is documented in the ACCOMPANYING DOCUMENTS. If the SL-C is lower than a specific SL-T, further suitable COUNTERMEASURES outside of the MEDICAL DEVICE are applicable in the specific use environment/ZONE of the RESPONSIBLE ORGANIZATION so that the achieved SECURITY LEVEL SL-A for the ZONE equals to the SL-T.

NOTE 2 It is expected that future editions of particular standards will specify the issues addressed in 4.6.3 more specifically for their product groups.

Compliance with the specifications should be checked by inspection of the ESSENTIAL FUNCTION concept, of the FIRECALL concept, of the intended use environment concept in the SECURITY design documents, of corresponding test documentation and of the ACCOMPANYING DOCUMENTS.

5 SECURITY LEVELS for the different foundational requirements

5.1 * Application of SECURITY LEVELS

The specifications of this document for SECURITY LEVELS are given in Table 1.

The specifications are based on existing documents for IT SECURITY, like IEC 62443-4-2:2019 and IEC TR 80001-2-2:2012 [9]. They use the terms and wordings as given in IEC 62443-4-2:2019, with some modifications for the purpose of MEDICAL DEVICES: SECURITY LEVELS (SL), foundational requirements (FR), component requirements (CR), software application requirements (SAR), embedded device requirements (EDR), host device requirements (HDR), network device requirements (NDR) and requirement enhancements (RE).

Compliance with the specifications should be checked by inspection of test results according to Table 1, and by inspection of the ACCOMPANYING DOCUMENTS related to the stated capability SECURITY LEVEL (SL-C).

5.2 Modified specifications for SECURITY LEVELS

In addition to the terminology differences explained in Clause 3, the following aspects of Clause 5 to Clause 14 of IEC 62443-4-2:2019 have been modified by this document.

CR 1.2 (RE (1) Unique identification and AUTHENTICATION)

Add: Unique per individual device cryptographically secure communication keys should be used to prevent leveraging the knowledge of one key to access a multitude of devices.

CR 2.1 Authorization enforcement

Add: For applications or PROCESSES running with system privileges, an effective separation of privileges should be in place.

NOTE 1 Further CR like CR 7.7 (least functionality) also contribute to the SECURITY concept.

CR 4.1 (new RE (1) health data de-identification)

Add following RE (1), health data de-identification

The MEDICAL DEVICE should provide the capability (e.g. application software, additional tooling) to directly remove information that allows the identification of a PATIENT by unauthorized persons via the PATIENT's stored health data. This capability, which is exercised before a MEDICAL DEVICE is shipped for repair or disposal, should include the scrubbing of such sensitive health data without the loss of quality and SECURITY forensics information required by the MANUFACTURER.

NOTE 2 Pseudonymisation and use of any manner of PATIENT-identifying keys that are separately accessible only to authorized users permit health data to be re-identified by authorized users only.

This RE (1) should be applicable for capability SECURITY LEVELS SL-C 2, 3 and 4.

CR 5.1 Network segmentation

Add: In cases where standard IT is being used for configuration interfaces, it should be sufficiently protected. The available specifications and technical guidelines should be implemented properly. If, for example, a web interface is being used, the connections should be made available exclusively in encrypted form. Compliance with state-of-the-art minimum requirements on the use of secure point-to-point protocols (e.g. transport layer security) should be ensured, and web servers should operate according to the CYBERSECURITY specifications for secure web server operations.

Compliance with the specifications should be checked by inspection of test results according to the corresponding parts of Table 1, and by inspection of the ACCOMPANYING DOCUMENTS related to the stated capability SECURITY LEVEL (SL-C).

6 Technical description

The following technical description should be supplied to the RESPONSIBLE ORGANIZATION as part of the ACCOMPANYING DOCUMENTS.

a) A specification of target groups which are to be informed about specific technical information related to CYBERSECURITY, including their access privileges/permissions on the device.

b) A technical description for the affected target groups that clearly illustrates how to operate the MEDICAL DEVICE in a technically secure manner. Clinicians/physicians should be provided with the information they need to have meaningful discussion with their PATIENTS about CYBERSECURITY RISKS.

c) Sufficiently detailed, SECURITY concept related, system diagrams for the target groups.

d) A SECURITY concept related CYBERSECURITY bill of material including, but not limited to, a list of commercial, open source, and off-the-shelf software and hardware components. The list should enable the target groups to effectively manage their ASSETS, to understand the potential impact of identified vulnerabilities to the MEDICAL DEVICE (and the connected IT-NETWORK), and to deploy COUNTERMEASURES to maintain the ESSENTIAL FUNCTION of the MEDICAL DEVICE.

e) A specification of the minimum platform requirements for connectable devices including administration workstations, such as hardware properties, operating system versions, middleware and drivers, peripheral devices; additionally for "software as a MEDICAL DEVICE", the minimum platform requirements for installation including the operating system.

f) A description of SECURITY features and functions (including a description of capability SECURITY LEVEL SL-C) that protect the ESSENTIAL FUNCTION, even when the CYBERSECURITY of the MEDICAL DEVICE or the connected MEDICAL IT-NETWORK has been compromised. Documentation of RISKS/THREATS which are covered by the SL-C concept of the MEDICAL DEVICE itself.

g) Information on how hardening of the MEDICAL DEVICE to the greatest possible extent can be achieved, including how to achieve different SECURITY LEVELS for the MEDICAL DEVICE, if the MEDICAL DEVICE is able to be configured to different capability SECURITY LEVELS SL-Cs.

h) A documentation of THREATS that should be considered for the INTENDED USE environment in the context of a CYBERSECURITY assessment or CYBERSECURITY management and a list of services that cannot be secured alone with the mechanisms integrated in the MEDICAL DEVICE (capability SECURITY LEVEL SL-C) in the INTENDED USE environment and thus require additional technical or organisational COMPENSATING COUNTERMEASURES.

i) A documentation of SECURITY related RISKS of using the MEDICAL DEVICE outside the INTENDED USE environment.

j) A list of appropriate, recommended COUNTERMEASURES for the listed THREATS in the INTENDED USE environment to permit secure network connected deployment and servicing (e.g., supporting infrastructure requirements, end point protections such as anti-malware, firewall/firewall rules, application whitelisting, SECURITY event parameters, logging parameters, physical SECURITY detection).

k) Recommendations regarding configurations that ensure secure operations (e.g. a guide for hardening the system). For example:

   – information on changing default passwords and deactivating unnecessary accounts;

   – a checklist to help maintain an overview about the configuration and its SECURITY specific implications;

   – a documentation of the SECURITY specific consequences of possible configuration options/alternatives;

   – an indication of settings which are to be considered critical and whose changes may lead to increased SECURITY RISK;

   – references to further information on SECURITY measures or for secure operations.

l) Advice to target groups to deactivate the applications and unused data ports, especially incoming ports that are not required in their particular scenarios.

m) In case standard IT mechanisms are used in a SECURITY related context, information on how to use these mechanisms in a secure manner and how to protect these mechanisms sufficiently. For example, use of web interfaces exclusively in encrypted form and selection of web servers operating according to the CYBERSECURITY recommendations for secure web server operations.

n) A documentation of all interfaces, access points, network ports and their functions, including a description of the port functionality, the kind of other network components that can be connected, the kind of data/signals that are being transmitted, their protocol types, addressing schemes and the directions including the origin and destinations in which the data/signals flow.

o) A description of how the design enables the device to announce when anomalous conditions (i.e. SECURITY events) are detected. SECURITY event types could be configuration changes, network anomalies, login attempts, or anomalous traffic (e.g. send requests to unknown entities).

p) Where appropriate, instructions for target groups on how to respond upon detection of a CYBERSECURITY vulnerability or an INCIDENT.

q) A description of the operation in an ESSENTIAL FUNCTION mode in case of a presumed or detected attack on the MEDICAL DEVICE or the connected IT-SYSTEM, if such mode requires activities by the OPERATOR or by SERVICE PERSONNEL.

r) A description of how forensic evidence is captured, including but not limited to, any log files kept for a SECURITY event. Log file descriptions should include how and where the log file is located, stored (including storage capacity), recycled, archived, used, and how it could be consumed by automated analysis software (e.g. intrusion detection system).

s) A description of how to backup and restore features and a description of methods for retention and recovery of MEDICAL DEVICE log files and configurations (at least those configurations required for ESSENTIAL FUNCTION) by an authenticated privileged user.

t) A description of the systematic procedures for authorized users to download and install version-identifiable software and firmware from the MANUFACTURER.

u) Information on how to ensure that remote maintenance does not affect the operation of the MEDICAL DEVICE in any way if the remote maintenance during the operation of the MEDICAL DEVICE is allowed/necessary.

v) Information, if known, concerning MEDICAL DEVICE CYBERSECURITY end of support. At the end of support, a MANUFACTURER may no longer be able to reasonably provide SECURITY patches or software updates. If the MEDICAL DEVICE remains in service following the end of support, the CYBERSECURITY RISKS for users can be expected to increase over time.

Compliance with the specifications should be checked by inspecting if the ACCOMPANYING DOCUMENTS are complete and in agreement with the SECURITY design documents.

7 Mapping of requirements to capability security levels (SL-C)

Table 1 indicates which MEDICAL DEVICE SECURITY requirements apply to which foundational requirements (FR) for a given MEDICAL DEVICE capability SECURITY LEVEL SL-C. The MEDICAL DEVICE SECURITY requirements to be met for a given SL-C are denoted by a check mark. The FR, CR, SAR, EDR, HDR, NDR, including RE, used in Table 1 shall be read as specified in IEC 62443-4-2:2019.

NOTE 1 Table 1 has been transferred from IEC 62443-4-2:2019, with modifications applicable for this document as listed in footnotes to table a) b) and c) and specified in 5.2.

NOTE 2 The exemplary vector of capability SECURITY LEVEL SL-C is contained in Annex A.6, Table A.2.

Table 1 – Mapping of single requirements to capability security levels (SL-C)

Component requirements (CR) and requirement enhancements (RE)	SL-C 1	SL-C 2	SL-C 3	SL-C 4
FR 1 – Identification and AUTHENTICATION control (IAC)				
CR 1.1 – Human user identification and AUTHENTICATION	✓	✓	✓	✓
RE (1) Unique identification and AUTHENTICATION		✓	✓	✓
RE (2) Multifactor AUTHENTICATION for all interfaces			✓	✓
CR 1.2 – Software PROCESS and device identification and AUTHENTICATION		✓	✓	✓
RE (1) Unique identification and AUTHENTICATION [a]			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware SECURITY for authenticators			✓	✓
NDR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and AUTHENTICATION		✓	✓	✓
CR 1.7 – Strength of password-based AUTHENTICATION	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users			✓	✓
RE (2) Password lifetime restrictions for all users (human, software PROCESS, or device)				✓
CR 1.8 – Public key infrastructure certificates		✓	✓	✓
CR 1.9 – Strength of public key-based AUTHENTICATION		✓	✓	✓
RE (1) Hardware SECURITY for public key-based AUTHENTICATION			✓	✓
CR 1.10 – Authenticator feedback	✓	✓	✓	✓
CR 1.11 – Unsuccessful login attempts	✓	✓	✓	✓
CR 1.12 – System use notification	✓	✓	✓	✓
NDR 1.13 – Access via untrusted networks	✓	✓	✓	✓
RE (1) Explicit access request approval			✓	✓
CR 1.14 – Strength of symmetric key-based AUTHENTICATION		✓	✓	✓
RE (1) Hardware SECURITY for symmetric key-based AUTHENTICATION			✓	✓
FR 2 – Use control (UC)				
CR 2.1 – Authorization enforcement [a]	✓	✓	✓	✓
RE (1) Authorization enforcement for all users (humans, software PROCESSES and devices)		✓	✓	✓
RE (2) Permission mapping to roles		✓	✓	✓
RE (3) Supervisor override			✓	✓
RE (4) Dual approval				✓
CR 2.2 – Wireless use control	✓	✓	✓	✓
CR 2.3 – Use control for portable and mobile devices [b]				
SAR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code AUTHENTICITY check		✓	✓	✓
EDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code AUTHENTICITY check		✓	✓	✓
HDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code AUTHENTICITY check		✓	✓	✓
NDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code AUTHENTICITY check		✓	✓	✓

Component requirements (CR) and requirement enhancements (RE)	SL-C 1	SL-C 2	SL-C 3	SL-C 4
CR 2.5 – Session lock	✓	✓	✓	✓
CR 2.6 – Remote session termination		✓	✓	✓
CR 2.7 – Concurrent session control			✓	✓
CR 2.8 – Auditable events	✓	✓	✓	✓
CR 2.9 – Audit storage capacity	✓	✓	✓	✓
RE (1) Warn when audit record storage capacity threshold reached			✓	✓
CR 2.10 – Response to audit processing failures	✓	✓	✓	✓
CR 2.11 – Timestamps	✓	✓	✓	✓
RE (1) Time synchronization		✓	✓	✓
RE (2) Protection of time source INTEGRITY				✓
CR 2.12 – NON-REPUDIATION	✓	✓	✓	✓
RE (1) NON-REPUDIATION for all users				✓
EDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
HDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
NDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
FR 3 – System INTEGRITY (SI)				
CR 3.1 – Communication INTEGRITY	✓	✓	✓	✓
RE (1) Communication AUTHENTICATION		✓	✓	✓
SAR 3.2 – Protection from malicious code	✓	✓	✓	✓
EDR 3.2 – Protection from malicious code	✓	✓	✓	✓
HDR 3.2 – Protection from malicious code	✓	✓	✓	✓
RE (1) Report version of code protection		✓	✓	✓
NDR 3.2 – Protection from malicious code	✓	✓	✓	✓
CR 3.3 – SECURITY functionality verification	✓	✓	✓	✓
RE (1) SECURITY functionality verification during normal operation				✓
CR 3.4 – Software and information INTEGRITY	✓	✓	✓	✓
RE (1) AUTHENTICITY of software and information		✓	✓	✓
RE (2) Automated notification of INTEGRITY violations			✓	✓
CR 3.5 – Input validation	✓	✓	✓	✓
CR 3.6 – Deterministic output	✓	✓	✓	✓
CR 3.7 – Error handling	✓	✓	✓	✓
CR 3.8 – Session INTEGRITY		✓	✓	✓
CR 3.9 – Protection of audit information		✓	✓	✓
RE (1) Audit records on write-once media				✓
EDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update AUTHENTICITY and INTEGRITY		✓	✓	✓
HDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update AUTHENTICITY and INTEGRITY		✓	✓	✓
NDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update AUTHENTICITY and INTEGRITY		✓	✓	✓

Component requirements (CR) and requirement enhancements (RE)	SL-C 1	SL-C 2	SL-C 3	SL-C 4
EDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
HDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
NDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
EDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
HDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
NDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
EDR 3.13 – Provisioning ASSET owner roots of trust		✓	✓	✓
HDR 3.13 – Provisioning ASSET owner roots of trust		✓	✓	✓
NDR 3.13 – Provisioning ASSET owner roots of trust		✓	✓	✓
EDR 3.14 – INTEGRITY of the boot PROCESS	✓	✓	✓	✓
RE (1) AUTHENTICITY of the boot PROCESS		✓	✓	✓
HDR 3.14 – INTEGRITY of the boot PROCESS	✓	✓	✓	✓
RE (1) AUTHENTICITY of the boot PROCESS		✓	✓	✓
NDR 3.14 – INTEGRITY of the boot PROCESS	✓	✓	✓	✓
RE (1) AUTHENTICITY of the boot PROCESS		✓	✓	✓
FR 4 – Data CONFIDENTIALITY (DC)				
CR 4.1 – Information CONFIDENTIALITY	✓	✓	✓	✓
RE (1) Health data de-identification [a]		✓	✓	✓
CR 4.2 – Information persistence		✓	✓	✓
RE (1) Erase of shared memory resources			✓	✓
RE (2) Erase verification			✓	✓
CR 4.3 – Use of cryptography	✓	✓	✓	✓
FR 5 – Restricted data flow (RDF)				
CR 5.1 – Network segmentation [a]	✓	✓	✓	✓
NDR 5.2 – ZONE boundary protection	✓	✓	✓	✓
RE (1) Deny all, permit by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
NDR 5.3 – General purpose, person-to-person communication restrictions	✓	✓	✓	✓
CR 5.4 – Application partitioning [b]				
FR 6 – Timely response to events (TRE)				
CR 6.1 – Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
CR 6.2 – Continuous monitoring		✓	✓	✓

Component requirements (CR) and requirement enhancements (RE)	SL-C 1	SL-C 2	SL-C 3	SL-C 4
FR 7 – Resource AVAILABILITY (RA)				
CR 7.1 – Denial of service protection	✓	✓	✓	✓
RE (1) Manage communication load from component		✓	✓	✓
CR 7.2 – Resource management	✓	✓	✓	✓
CR 7.3 – MEDICAL DEVICE backup [c]	✓	✓	✓	✓
RE (1) Backup INTEGRITY verification		✓	✓	✓
CR 7.4 – MEDICAL DEVICE recovery and reconstitution [c]	✓	✓	✓	✓
CR 7.5 – Emergency power [b]				
CR 7.6 – Network and SECURITY configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current SECURITY settings			✓	✓
CR 7.7 – Least functionality	✓	✓	✓	✓
CR 7.8 – MEDICAL DEVICE component inventory [c]		✓	✓	✓

Key

CR: component requirement which is common to all types of MEDICAL DEVICES

EDR: embedded device requirement

HDR: host device requirement

NDR: network device requirement

SAR: software application requirement

[a] For that row, this document includes modified or added requirements, compared to those in IEC 62443-4-2:2019.

[b] That row does not require SECURITY measures for a MEDICAL DEVICE, only IT-NETWORK requirements exist according to IEC 62443-3-3:2013 [5]. The row is included for information only in this document.

[c] The term "control system", related to the "component" in IEC 62443-4-2:2019, has been replaced with "MEDICAL DEVICE" in this document.

Annex A
(informative)

General guidance and rationale

A.1 The approach of this document: Type testable MEDICAL DEVICE IT SECURITY properties

The goal of this document is to provide requirements for type testing regarding SECURITY for a MEDICAL DEVICE. The SECURITY LEVELS defined in this document define the level of resilience to CYBERSECURITY attacks. This document does not define a specific SECURITY LEVEL for a specific device, which is the task of a SECURITY RISK MANAGEMENT PROCESS. By defining a SECURITY LEVEL according to this document, the MANUFACTURER of a MEDICAL DEVICE can describe the level of SECURITY in a standardized way.

When this document is used for type testing, the tester simply verifies the MANUFACTURER'S claims for a certain SECURITY LEVEL as illustrated in Figure A.1. It is up to the MANUFACTURER to declare the SECURITY LEVEL implemented in the MEDICAL DEVICE, with any limitations and extensions. The type test does not evaluate if the declared capability SECURITY LEVEL SL-C makes the device fit for purpose in a given INTENDED USE environment. That is up to the SECURITY RISK MANAGEMENT PROCESS to evaluate.

A SECURITY RISK MANAGEMENT PROCESS would typically evaluate the impact on SAFETY, exposure to THREATS, significance of vulnerabilities and value of the ASSETS of a MEDICAL DEVICE. This analysis would then result in the requirement for a certain SECURITY LEVEL. The COUNTERMEASURES defined by a certain SECURITY LEVEL are then evaluated in the SECURITY RISK MANAGEMENT PROCESS, and the residual RISK is then evaluated. This document is a tool to define suitable COUNTERMEASURES for a chosen SECURITY LEVEL.

MEDICAL DEVICE MANUFACTURERS and network operators (RESPONSIBLE ORGANIZATIONS) have shared responsibility for RISK MANAGEMENT but different and complementary roles to play and different processes to apply (for further information, see IEC 80001-1:2010 and ISO 81001-1[2]). IEC 60601 (all parts) focus on the role of the MANUFACTURER.

---

2 Under preparation. Stage at the time of publication: ISO/FDIS 81001-1:2020.

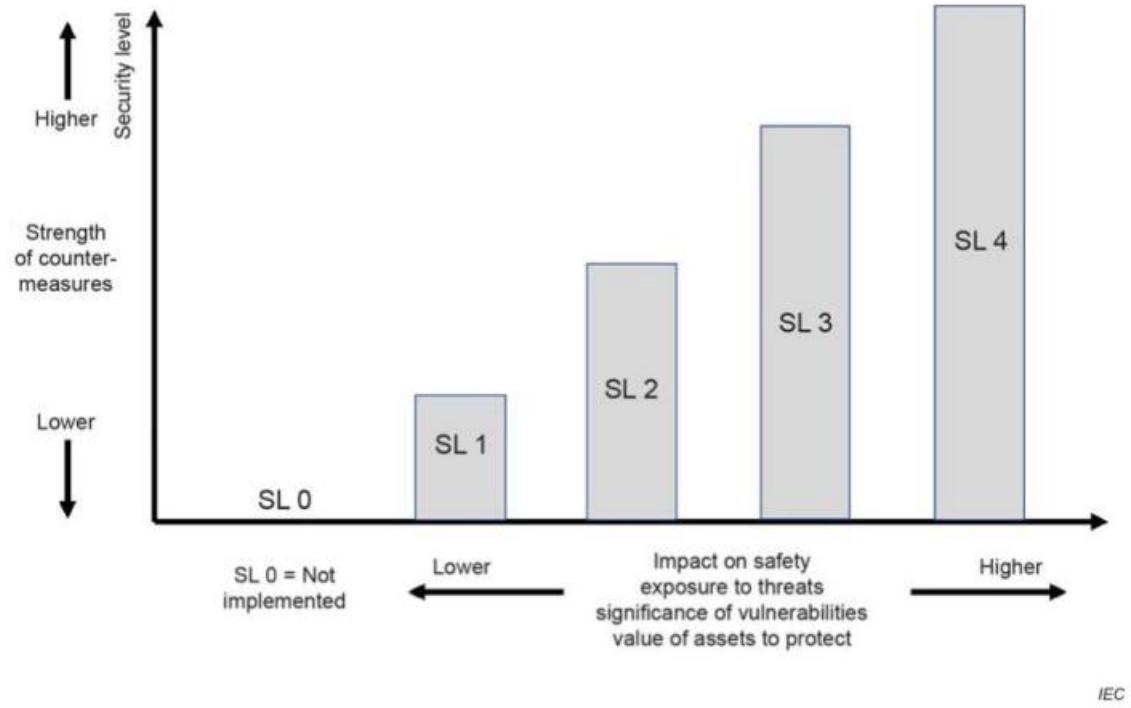


Figure A.1 – Illustration with SECURITY LEVELS

SECURITY LEVELS (SL) have to do with different aspects of the SECURITY life cycle as illustrated in Figure A.2.

– The target SECURITY LEVEL (SL-T) is the desired level of SECURITY for a particular MEDICAL IT-NETWORK or a specified ZONE of it. It is usually determined by performing a RISK assessment on a MEDICAL IT-NETWORK and determining that it shall have a particular level of SECURITY to ensure its correct operation. A system integrator specifies the SL-T for each ZONE of the MEDICAL IT-NETWORK. "Requirements specification" is a metaphor for this.

– The capability SECURITY LEVEL (SL-C) is the SECURITY LEVEL that a MEDICAL DEVICE or other components of a MEDICAL IT-NETWORK can provide when properly configured. This level states that a particular MEDICAL DEVICE or other component of the MEDICAL IT-NETWORK is capable (or not) of meeting the required target SECURITY LEVEL SL-T natively without additional COMPENSATING COUNTERMEASURES when properly configured and integrated. A MANUFACTURER declares and verifies the MEDICAL DEVICE's SL-C. "Datasheet and test report" is a metaphor for this.

– An achieved SECURITY LEVEL (SL-A) is the actual level of SECURITY for a particular MEDICAL IT-NETWORK or a specified ZONE of it. It is measured after a MEDICAL IT-NETWORK's design is available or when a MEDICAL IT-NETWORK is in place. It is used to establish that a SECURITY system or a specified ZONE is meeting the goals that were originally set out in the target SECURITY LEVEL SL-T. A system integrator (or someone else) evaluates the SL-A after integration of MEDICAL DEVICES or other components into a MEDICAL IT-NETWORK. "Integration test result" is a metaphor for this.

For more information on the use of SECURITY LEVELS, see IEC 62443-3-3:2013 [5], Clause A.2.

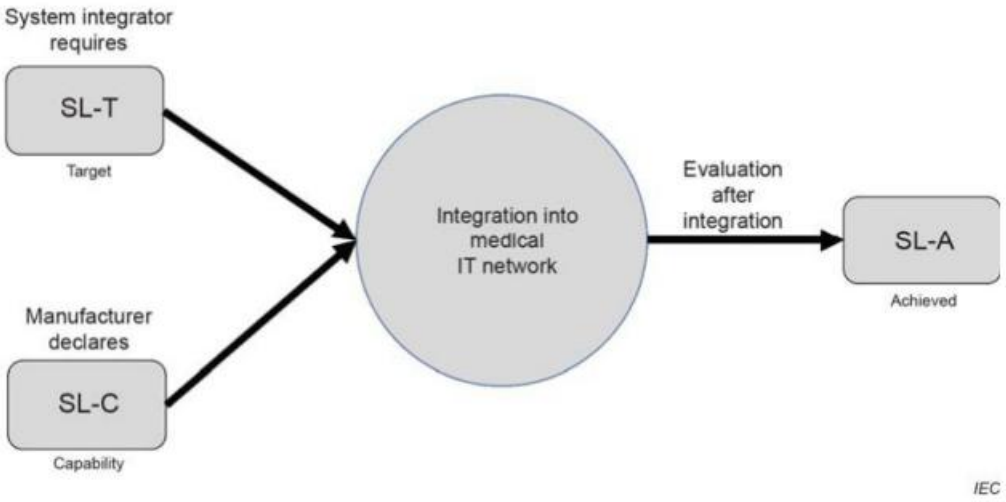


Figure A.2 – Capability – Target – Achieved

The manufacturer should specify target SECURITY LEVEL SL-T for the use environment (ZONE) or use environments (ZONES) in which the MEDICAL DEVICE is typically operated. This is used as a basis to specify an appropriate capability SECURITY LEVEL SL-C for the MEDICAL DEVICE. However, there is no need to mandatorily achieve an SL-C being identical or higher than the SL-T. Also, a lower SL-C for a MEDICAL DEVICE can be accepted provided it is listed in the ACCOMPANYING DOCUMENTS. The RESPONSIBLE ORGANIZATION (e.g. hospital IT manager or clinical engineer) can then manage that the achieved SECURITY LEVEL SL-A for the complete ZONE, including further COMPENSATING COUNTERMEASURES external to the MEDICAL DEVICE, complies with the required SL-T.

If a MEDICAL DEVICE is used outside professional healthcare environments, a capability SECURITY LEVEL SL-C complying with the target SECURITY LEVEL SL-T is typically appropriate.

An explanation of security levels and their use is given in A.2.1 of IEC 62443-3-3:2013 [5]:

"*The following is an excerpt from 5.11.1 of IEC TS 62443-1-1:2009 [4] that provides a good explanation of what SECURITY LEVELS are and how they can be used.*

> *SECURITY LEVELS provide a qualitative approach to addressing SECURITY for a ZONE. As a qualitative method, SECURITY LEVEL definition has applicability for comparing and managing the SECURITY of ZONES within an organization. As more data becomes available and the mathematical representations of RISK, THREATS, and SECURITY INCIDENTS are developed, this concept will move to a quantitative approach for selection and verification of SECURITY LEVELS (SL). It will have applicability to both end user companies, and vendors of IACS [3] and SECURITY products. It will be used to select IACS devices and COUNTERMEASURES to be used within a ZONE and to identify and compare SECURITY of ZONES in different organizations across industry segments.*

---

3 In this document, industrial automation and control system (IACS) is replaced in accordance with Clause 3. See also last paragraph at the end of A.1.

In the first phase of development, the IEC 62443 series [3] of standards tends to use qualitative SECURITY LEVELS, using terms such as "low", "medium", and "high". The ASSET owner will be required to come up with their own definition of what those classifications mean for their particular application. The long-term goal for the IEC 62443 series [3] is to move as many of the SECURITY LEVELS and requirements to quantitative descriptions, requirements and metrics as possible to establish repeatable applications of the standard across multiple companies and industries. Achieving this goal will take time, since more experience in applying the standards and data on industrial SECURITY systems will need to be acquired to justify the quantitative approach.

When mapping requirements to the different SECURITY LEVELS, standard developers need some frame of reference describing what the different SECURITY LEVELS mean and how they differ from each other. The goal of this annex is to propose such a frame of reference."

The following are rationales for specific clauses and subclauses in this particular standard, with clause and subclause numbers parallel to those in the body of the document. The numbering is, therefore, not consecutive.

Definition 3.10 – ESSENTIAL FUNCTION

Though BASIC SAFETY and ESSENTIAL PERFORMANCE are the core concept for the design of a secure MEDICAL DEVICE, it is recognized that only meeting BASIC SAFETY and ESSENTIAL PERFORMANCE requirements is sometimes not sufficient for such a design. Under the area of AVAILABILITY, special considerations shall be applied by a MEDICAL DEVICE MANUFACTURER.

For example, if an INTENDED USE environment/ZONE in which a MEDICAL DEVICE typically operates is attacked, resulting in the introduction of malicious code, or if the MEDICAL DEVICE itself is affected by a cyber-attack, suitable COUNTERMEASURES should be in place to allow the affected RESPONSIBLE ORGANIZATION to continue to provide some level of medical care for acute injuries or diseases. If one only considered BASIC SAFETY and ESSENTIAL PERFORMANCE, these could often be met by terminating clinical functionality in a safe manner (e.g. providing alarm, implementing safe shutdown method).

The definition of ESSENTIAL FUNCTION has been modified to clearly state that for MEDICAL DEVICES additional capability may be needed in such cases. This, minimum clinical functionality and operational AVAILABILITY, is required to ensure the RESPONSIBLE ORGANIZATION can continue to provide a level of medical care even in cases of successful attacks. An example of such a minimum clinical functionality is, for a MEDICAL DEVICE, to fall back to a mode isolated from the compromised IT-NETWORK with some minimum performance required for the ongoing provision of healthcare.

As a SECURITY related update of hardware or software may require weeks or even months to validate SECURITY, safety and clinical performance, the RESPONSIBLE ORGANISATION in many cases needs such an ongoing ESSENTIAL FUNCTION of MEDICAL DEVICES in that interim period.

Subclause 4.2 – Support of ESSENTIAL FUNCTION

For the benefit-risk analysis (between safety and security), this subclause explains the risk of losing confidentiality in parts or totally when supporting an important clinical function after a successful attack on the IT-NETWORK or the MEDICAL DEVICE. As an example, when a ransomware attack infects the MEDICAL IT-NETWORK, the IT department might mitigate the fast spreading of malware by terminating all MEDICAL IT-NETWORK connections. If the MEDICAL DEVICE is configured to use network-based authentication services, then the MEDICAL DEVICE is not accessible anymore. Depending on the INTENDED USE, BASIC SAFETY, ESSENTIAL PERFORMANCE and additional considerations, a benefit-risk analysis could determine to disable access controls and grant access without login credentials in such cases, either by OPERATOR intervention or even automatically.

Such an analysis should consider whether it is normal operation to store and maintain PATIENT data on the MEDICAL DEVICE; then, disabling of access controls might be inappropriate and a fallback scenario, like cached credentials or a FIRECALL functionality, could be more appropriate for implementation. This could be for the purpose of being able to use the MEDICAL DEVICE, especially, for example, for life sustaining purposes or for the purpose of accessing PATIENT information stored on the MEDICAL DEVICE, whatever is more important for its use in the clinical setting. Special care should be taken for resolution of situations in which safety aspects can only be ensured in taking into account an ongoing data privacy leak.

Traceability in case of making use of a FIRECALL function means that specific means are available, for example event logging, notification, alarming, depending on the kind of medical device, the use environment and the potential harm.

Subclause 4.6 – Overarching constraints

All of the MEDICAL DEVICES defined in this document are assumed to be developed and supported following a secure software development PROCESS, for example as described in IEC 81001-5-1[4] [10] or in IEC 62443-4-1 [6].

Subclause 4.6.3 – Specific SECURITY features for MEDICAL DEVICES

Examples (particular standards can come to different results and can also differentiate between diverse INTENDED USE environments/ZONES).

– An Internet-linked implantable cardioverter modem usable in home environments might operate in a use environment/ZONE with a target SECURITY LEVEL SL-T of 4.
– A diagnostic workstation used in a large clinic network might operate in a use environment/ZONE with a target SECURITY LEVEL SL-T of 3 if the clinical network is not separated from the public network or an SL-T of 2 if the clinical network is separated from the public network.
– A dialysis machine used in an in-centre dialysis clinic with its own clinic network might operate in a use environment/ZONE with a target SECURITY LEVEL SL-T of 2.
– An anaesthesia workstation usable in operating rooms with a separated clinical intensive care network might operate in a use environment/ZONE with a target SECURITY LEVEL SL-T of 1.

Table A.1 lists exemplary criteria for the selection of an appropriate target SECURITY LEVEL SL-T in typical INTENDED USE environments.

4 Under preparation. Stage at the time of publication: IEC/CCDV 81001-5-1:2020.

Table A.1 – Exemplary criteria for the selection of appropriate target SECURITY LEVEL SL-T in typical INTENDED USE environments

Aspects of vulnerability	Exemplary factors to consider	Comment/Examples
ASSETS regarding safety		
Consequence of loss of BASIC SAFETY and ESSENTIAL PERFORMANCE	The level of HARM, as light injury, serious injury or death to the PATIENT, OPERATOR or bystanders	Range: From simple diagnostic measurement that can easily be repeated (low SL-T) up to life-supporting functions (high SL-T)
ASSETS regarding information SECURITY (foundational requirements 1 to 7)		
PATIENT data	Is there any PATIENT data stored? Single PATIENT or many PATIENTS?	From no PATIENT data stored (low SL-T) up to critical multiple PATIENT data stored (high SL-T)
Indirect access to other ASSETS	Value of ASSETS, where access is controlled by the device	From no access to other ASSETS in A MEDICAL IT-NETWORK (low SL-T) up to access to critical ASSETS (high SL-T)
INTENDED USE environment		
User profile	Used by PATIENTS or used by SECURITY-instructed healthcare professionals only?	From use by trained and SECURITY-instructed professionals only (low SL-T) up to use by lay OPERATORS (high SL-T)
Physical environment	Is access controlled in a professional environment or only by PATIENTS in their homes?	From professionally controlled areas (low SL-T) up to public areas (high SL-T)
Size of attack surface		
Number of, and accessibility of ports on the device	Are there no external or accessible internal ports? Or do several accessible interfaces exist, including wireless interfaces?	From no external/accessible ports (low SL-T) up to many and publicly accessible ports (high SL-T)
Impact on public health		
Number of impacted devices	Are very few devices placed in the market and therefore not a preferred target of attackers or is their placement widespread?	From very small installed base with low value ASSETS (low SL-T) to big number of devices with valuable ASSETS (high SL-T)

Subclause 5.1 – Application of SECURITY LEVELS

In principle, the terms and wordings of Clause 5 to Clause 14 of IEC 62443-4-2:2019 have been used in this document, especially in Table 1, with the corresponding modification (see Clause 3).

Clause 12 of IEC 62443-4-2:2019 has been used for MEDICAL DEVICE SOFTWARE while Clause 13 of IEC 62443-4-2:2019 has been used for MEDICAL DEVICES with embedded software.

For data CONFIDENTIALITY, different and diverging national requirements and sometimes even different approval responsibilities within one country exist. The scope of this document is restricted to SAFETY-related SECURITY specifications for MEDICAL DEVICES. However, the listed provisions in Table 1, making use of Clause 8 of IEC 62443-4-2:2019 for SAFETY-related data CONFIDENTIALITY, are a good base also for non-SAFETY-related SECURITY aspects.

Clause 15 of IEC 62443-4-2:2019, which refers to network device requirements, has not been used as the scope of this document intentionally applies only to MEDICAL DEVICES so that they can be more securely integrated into a MEDICAL IT-NETWORK. The scope of this document does not include SECURITY management for the overall MEDICAL IT-NETWORK. Further nonmedical equipment and systems within the MEDICAL IT-NETWORK may follow Clause 15 or further clauses of IEC 62443-4-2:2019, or even other SECURITY standards, but are out of the focus and scope of this document.

When reading the acronym "IACS" in IEC 62443-4-2:2019 in the context of this document, it should be read as MEDICAL IT-NETWORK. When reading the acronym "IACS components" in IEC 62443-4-2:2019 in the context of this document, it should be read as MEDICAL DEVICE. When reading the acronym "control system" in IEC 62443-4-2:2019, in the context of this document, it should be read as MEDICAL DEVICE.

A.2 Typical network connections of MEDICAL DEVICES covered in this document

The following Figure A.3 to Figure A.6 illustrate typical situations in which the data interface of a MEDICAL DEVICE is connected to IT-NETWORKS.

Figure A.3 – Wireless point-to-point connection between a portable device (e.g. PATIENT programmer) and an implant

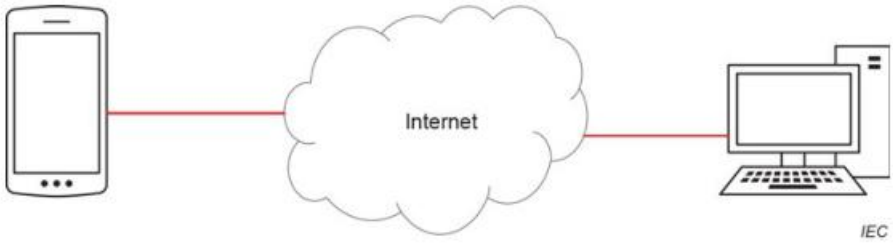


Figure A.4 – Connection between a PATIENT's portable device and a doctor's computer

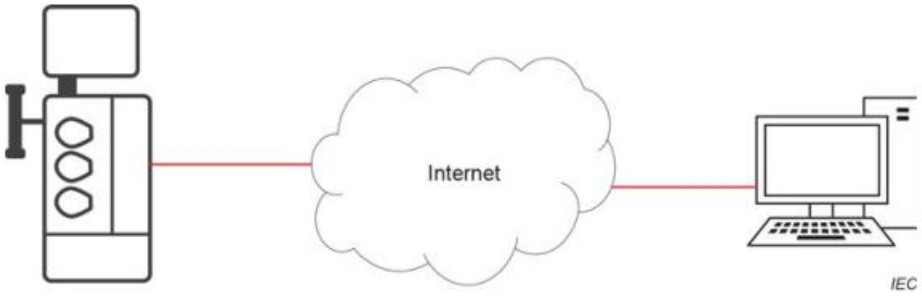
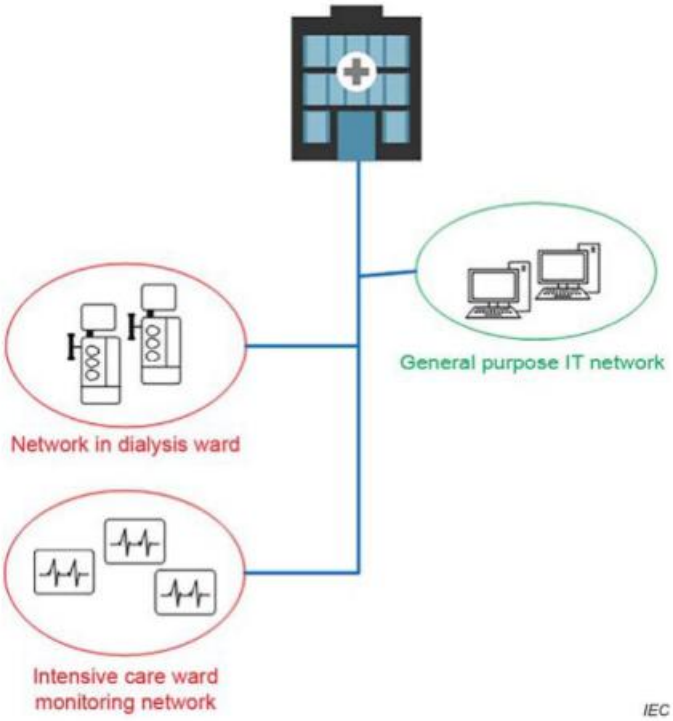


Figure A.5 – Connection between a MEDICAL DEVICE and a doctor's computer



Each of the bubbles can represent one ZONE or can, by itself, consist of separate ZONES. The red bubbles are typically representing a different ZONE than the green bubble.

Figure A.6 – IT-NETWORK in a hospital

A.3 Inclusion of ME SYSTEMS

This document is based on a SECURITY concept with clear but distributed responsibilities.

It is the responsibility of a MEDICAL DEVICE MANUFACTURER to achieve and maintain a self-declared capability SECURITY LEVEL SL-C with the design of the MEDICAL DEVICE.

To complement this, it is the responsibility of the individual MEDICAL IT-NETWORK's owner (e.g. in a hospital or a doctor's office) to determine the ZONES and CONDUITS of that MEDICAL IT-NETWORK and their needed target SECURITY LEVEL SL-T, as well as to verify the achieved SECURITY LEVEL SL-A. The latter may make use of the information about capability SECURITY LEVEL SL-C provided by the MEDICAL DEVICE MANUFACTURER.

Due to that distributed responsibility, the IEC 60601-1 term of ME SYSTEMS has to be used carefully (and has intentionally been used carefully within this document). Literally, every MEDICAL IT-NETWORK in terms of IEC 80001-1:2010 [8] can also be read as being an ME SYSTEM in terms of IEC 60601-1.

NOTE IEC 80001-1:2010 [8], definition 2.16: "an IT-NETWORK that incorporates at least one MEDICAL DEVICE". IEC 60601-1, definition 3.64: "combination, as specified by its MANUFACTURER, of items of equipment, at least one of which is ME EQUIPMENT to be inter-connected by functional connection or by use of a multiple socket-outlet".

While this interpretation of a MEDICAL IT-NETWORK being an ME SYSTEM is possible though not shared unanimously, it is not helpful for this document. This document focuses on the capability SECURITY LEVEL SL-C of MEDICAL DEVICES in terms of ME EQUIPMENT or "classical" ME SYSTEMS as a combination of a ME EQUIPMENT with a small number of (some few) further medical or nonmedical equipment placed onto the market by one MANUFACTURER. It should be allowed for the MANUFACTURER to design, verify and declare SL-C for such an ME SYSTEM in total as if it was a ME EQUIPMENT. So, MEDICAL DEVICE is intended to include those ME SYSTEMS placed onto the market by one MANUFACTURER, but for the complete MEDICAL IT-NETWORK, the responsibility remains at the local owner of the MEDICAL IT-NETWORK.

For integration of a MEDICAL DEVICE as a component with certain capability SECURITY LEVEL SL-C into a MEDICAL IT-NETWORK, a target SECURITY LEVEL SL-T for the MEDICAL IT-NETWORK or certain ASSETS of it should be assigned to an INTENDED USE environment/ZONE. An SL-T may also be assigned to a CONDUIT. SL-T for a ZONE and CONDUIT is determined during RISK assessment for the MEDICAL IT-NETWORK according to IEC 80001-1:2010 [8]. It is not required to assign an SL-T to CONDUITS as long as the SECURITY properties associated with the CONDUIT are taken into consideration during RISK assessment of the ZONES which use the CONDUIT under consideration.

The RISK assessment for the MEDICAL IT-NETWORK according to IEC 80001-1:2010 [8] should take into consideration the likelihood and consequences of SECURITY of a ZONE or CONDUIT being compromised. That RISK assessment may be qualitative, semi-quantitative, or quantitative. The target SECURITY LEVEL SL-T determines the required effectiveness of COUNTERMEASURES, devices including MEDICAL DEVICES that shall be in place to prevent SECURITY of the ZONE or CONDUIT from being compromised.

The factors that influence the determination of target SECURITY LEVEL SL-T for a ZONE and CONDUIT are:

– the network architecture with the defined ZONE boundaries and CONDUITS,
– the SL-T of the ZONES with which the ZONE under consideration will communicate,
– the SL-T of CONDUIT, if assigned, used for communication by the ZONE, and
– the physical access to devices and systems within the ZONE.

Within a ZONE, determining the target SECURITY LEVEL SL-T should be based on layers of SECURITY and their impact on the whole.

Examples of SECURITY properties that may be addressed by a COMPENSATING COUNTERMEASURE external of or integral to a MEDICAL DEVICE are given below:

– proving peer entity AUTHENTICITY;
– preserving AUTHENTICITY and INTEGRITY of messages;
– preserving CONFIDENTIALITY of messages/information/communication;
– ensuring accountability (NON-REPUDIATION);
– enforcing access control policies;
– preventing denial-of-service attacks;
– maintaining platform trustworthiness;
– detecting tampering;
– monitoring SECURITY status.

A.4 Correlation to existing regulations, standards and technical specifications

The sheer number of CYBERSECURITY frameworks, standards and guidance documents may seem overwhelming to the MEDICAL DEVICE MANUFACTURER. Figure A.7 shows an overview of the most commonly used frameworks, standards and guidance used for MEDICAL DEVICES.

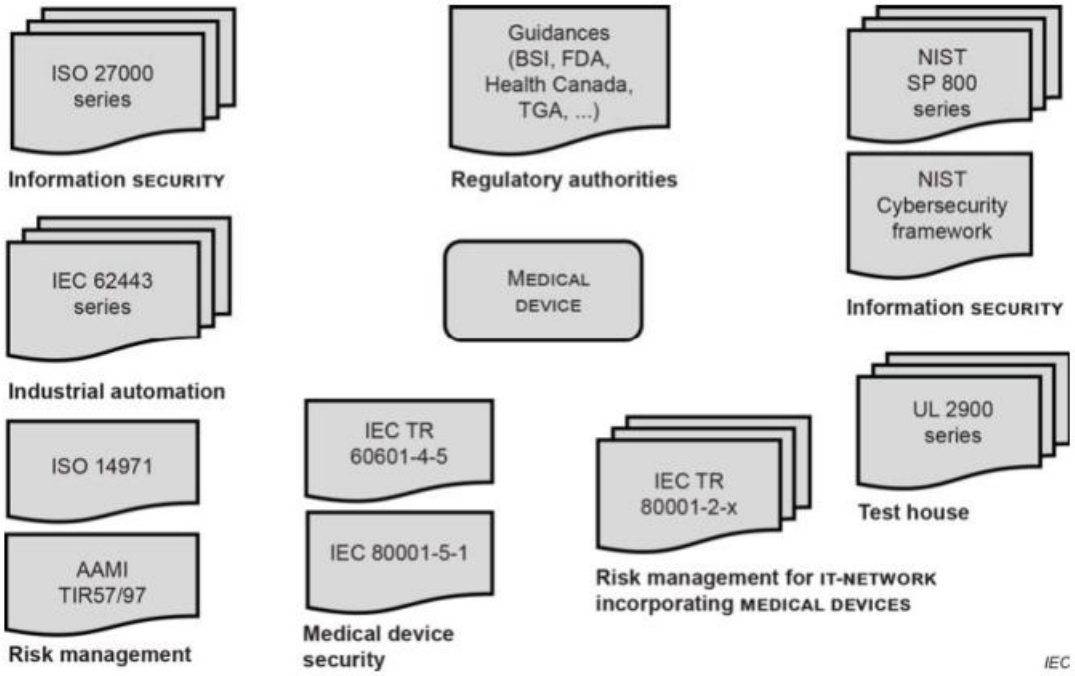


Figure A.7 – Selection of IT SECURITY related documents

– The NIST (National Institute of Standards and Technology) Cybersecurity Framework and special publications [24] are designed to support everything from small IT-NETWORKS to large systems that are critical for national SECURITY.

– ISO/IEC 27000:2018 [15], together with its correlated standards, is a information SECURITY standard for IT-NETWORKS in general, which includes optional standards for a management system. This standard, together with its correlated standards, includes sector-specific adaptations, one of which is for the medical sector.

– IEC 62443 (all parts) [3] is a series of SECURITY standards for industrial automation control systems (IACS)[5]. Since IACS are used in important systems such as electrical power distribution, water distribution and critical industries, this series was developed to assist in designing these systems to enable a very high level of protection against SECURITY related disturbances.

– The IEC 80001-2 [26] and ISO 80001-2 series [7] of technical reports addresses the needs of HDO's (health delivery organizations), but some of these reports are also useful for device MANUFACTURERS. One of these is IEC TR 80001-2-2:2012 [9], which describes the disclosure of some SECURITY capabilities and is cross-referenced in this document.

– Described as the Underwriter Laboratories (UL) Cybersecurity Assurance Program, the test house, UL, published the general standard UL 2900-1 [25] for software CYBERSECURITY in network-connected products and a particular standard, ANSI/CAN/UL 2900-2-1 [19], for healthcare systems. These standards contain mainly PROCESS requirements and some specific product requirements, which can be incorporated by a MANUFACTURER. These standards should be viewed as containing a set of verifiable product and PROCESS requirements rather than a complete SECURITY framework.

– In addition to the frameworks listed above, there are CYBERSECURITY guidance documents published by regulatory authorities like the U.S. FDA [21] and the German BSI [20]. These guidance documents contain a mix of concrete technical and organizational implementation requirements.

---

5 In this document, industrial automation and control system (IACS) is replaced in accordance with Clause 3. See also last paragraph of Clause A.1.

– A further addition to the list above are the technical reports TIR57:2016 [17] and TIR97:2019 [18], published by AAMI. These reports define a SECURITY RISK MANAGEMENT PROCESS modelled on ISO 14971:2019 [13] and build heavily on the NIST Cybersecurity Framework and Special Publications [24].

– ISO 14971:2019 [13] is the base standard for RISK MANAGEMENT for MEDICAL DEVICES.

– A future standard for the SECURITY life cycle activities is IEC 81001-5-1 [10], which uses the same structure as IEC 62304:2006 and IEC 62304/AMD1:2015 [2]. This standard integrates with this document.

There are two philosophies that can be identified in the different SECURITY frameworks, standards and technical reports. One is an open-ended approach, which starts with a RISK analysis (identification and evaluation) and then selects RISK control measures (e.g. COUNTERMEASURES) based on the RISK. This is typical of, for example, ISO/IEC 27000:2018 [15], NIST [24], ISO 14971:2019 [13] and AAMI TIR57:2016 [17] or AAMI TIR97:2019 [18]. The other approach is to start by selecting a level of SECURITY based on a general RISK assessment (or specific device-related criteria) and then choose one of several pre-defined SECURITY LEVELS. This is how IEC 62443 (all parts) [3] is designed.

The future standard IEC 81001-5-1 [10] and this document will adapt a hybrid philosophy. RISK identification and evaluation is done with an ISO 14971:2019 [13] mind-set, which also has to include the impact on SAFETY. The level of RISK, both SAFETY and SECURITY, will define which SECURITY LEVEL from IEC 62443 (all parts) [3] should be chosen for a specific MEDICAL DEVICE. This is the responsibility of the MEDICAL DEVICE MANUFACTURER and the writers of particular standards. The selected SECURITY LEVEL then defines a pre-set number of COUNTERMEASURES, which will determine the residual SECURITY related RISK of the MEDICAL DEVICE. Note that the IEC 62443 [3] SECURITY capabilities cannot be adapted blindly to a MEDICAL DEVICE. As an example, all user password-related capabilities may not be applicable to MEDICAL DEVICES in an intensive care unit. The combination of physical access control (e.g. only medical staff are allowed) and the need to operate MEDICAL DEVICES without any delay in critical situations will override the requirements for OPERATOR password SECURITY.

A review of the frameworks mentioned above shows that many of the technical and organizational implementation requirements refer back to ISO/IEC 27000:2018 [15] and IEC 62443 (all parts) [3]. IEC 62443 (all parts) [3], and specifically IEC 62443-4-2:2019, was chosen as the basis for this document. The main reasons for this are:

– IEC 62443 (all parts) [3] can be considered as state of the art regarding SECURITY requirements.

– IEC 62443 (all parts) [3] is the only one of the listed open frameworks that has a tiered structure for requirements (SL1 to SL4). This makes it easier for MEDICAL DEVICE MANUFACTURERS to declare/describe their SECURITY capabilities and for system integrators to specify requirements on MEDICAL DEVICES.

– Most of the IEC 62443 [3] SECURITY capabilities can be applied directly on MEDICAL DEVICE SECURITY.

It should be noted, however, that some adaptations have been necessary when implementing IEC 62443-4-2:2019 due to the fact that an industrial automation and control system cannot always be compared to a MEDICAL DEVICE. The adaptations to IEC 62443-4-2:2019 are described in this document.

A.5 Concept of ZONES and CONDUITS with specified target SECURITY LEVELS (SL-T) within an IT-NETWORK as specified by IEC 62443 (all parts) [3]

Figure A.8, which is extracted from Figure 7 of IEC TS 62443-1-1:2009 [4], gives an example of what a complex IT-NETWORK can consist of, and how it could be segregated into different use environments/ZONES at the same SECURITY LEVEL. It also shows CONDUITS that may connect or even cross such ZONES. In the medical field, the components of a MEDICAL IT-NETWORK may be MEDICAL DEVICES and/or nonmedical equipment. MEDICAL DEVICES as "components" of such a MEDICAL IT-NETWORK are in the focus of this document.

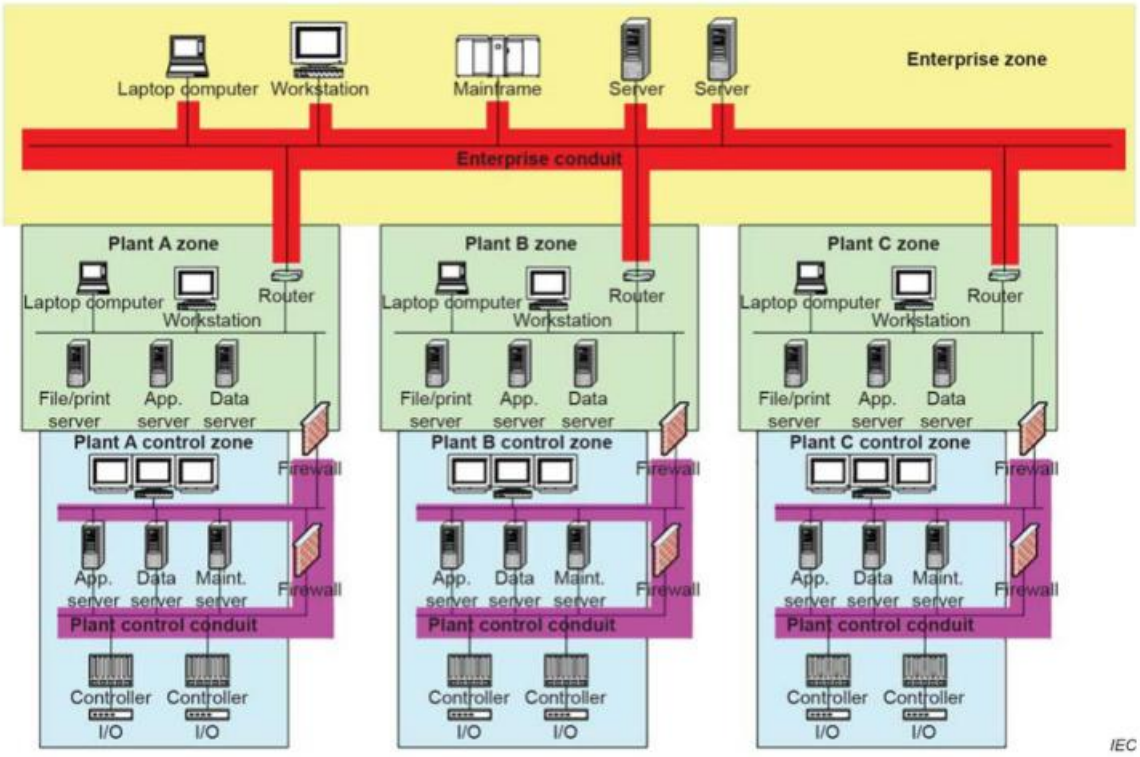


Figure A.8 – Example of what a complex IT-NETWORK can consist of

A.6 Documentation of capability SECURITY LEVEL (SL-C) of a MEDICAL DEVICE

One single capability SECURITY LEVEL SL-C of 0 to 4 should usually be assigned to a MEDICAL DEVICE in general, so the MEDICAL DEVICE follows all technical requirements (CR) and their requirement enhancements (RE) for the corresponding SL-C.

However, such a unique capability SECURITY LEVEL SL-C for the whole MEDICAL DEVICE in some cases may not be suitable or necessary, and it is also possible to assign individual SL-C for each foundational requirement (1 to 7). In such cases, a vector should be used to describe the mapping between the implemented capabilities SECURITY LEVELS and the seven foundational requirements.

NOTE 1 See also IEC 62443-3-3:2013 [5], A.3.3, related to the security level vector format.

NOTE 2 For clarity in communication, the full vector format is used if no unique capability SECURITY LEVEL SL-C is applied, for example even if only one single foundational requirement has an SL-C that is higher than "0".

SL-Vector: SL-C (MEDICAL DEVICE) = { IAC UC SI DC RDF TRE RA }

where

IAC is the identification and AUTHENTICATION control;

UC is the use control;

SI is the system INTEGRITY;

DC is the data CONFIDENTIALITY;

RDF is the restricted data flow;

TRE is the timely response to events;

RA is the resource AVAILABILITY-

Numerical value (0 to 4) representing the capability SECURITY LEVEL SL-C of each of the seven foundational requirements

EXAMPLE **SL-C (Example MEDICAL DEVICE) = { 3 3 2 0 2 1 1 }** which decomposes as shown in Table A.2.

Table A.2 – Exemplary vector of capability SECURITY LEVEL SL-C

FOUNDATIONAL REQUIREMENT	SECURITY LEVEL
Identification and AUTHENTICATION control (IAC)	SL-C 3
Use control (UC)	SL-C 3
System INTEGRITY (SI)	SL-C 2
Data CONFIDENTIALITY (DC)	SL-C 0
Restricted data flow (RDF)	SL-C 2
Timely response to events (TRE)	SL-C 1
Resource AVAILABILITY (RA)	SL-C 1

A.7 Conceptual elements of IEC 62443 (all parts) [3] used for this document

IEC TS 62443-1-1:2009 [4]

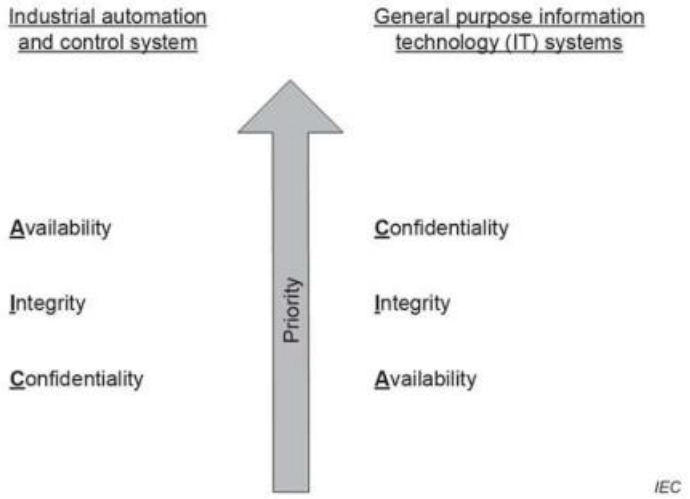
Subclause 5.2 of IEC TS 62443-1-1:2009 [4] – Security objectives

"Information security has traditionally focused on achieving three objectives, confidentiality, integrity, and availability, which are often abbreviated by the acronym CIA. An information technology security strategy for typical back office or business systems may place the primary focus on confidentiality and the necessary access controls required to achieve it. Integrity might fall to the second priority, with availability as the lowest.

In the industrial automation and control systems' environment, the general priority of these objectives is often different. Security in these systems is primarily concerned with maintaining the availability of all systems' components. There are inherent risks associated with industrial machinery that is controlled, monitored, or otherwise affected by industrial automation and control systems. Therefore, integrity is often second in importance. Usually confidentiality is of lesser importance, because often the data is raw in form and need to be analysed within context to have any value.

The facet of time responsiveness is significant. Control systems can have requirements of system responsiveness in the one millisecond range, whereas traditional business systems are able to successfully operate with single or multiple second response times.

In some situations, the priorities are completely inverted, as shown in Figure A.9.



SOURCE: IEC TS 62443-1-1:2009 [4], Figure 1

Figure A.9 – Comparison of objectives between industrial automation and control systems and general IT-NETWORKS

Depending on the circumstances, the integrity of the system could also have the highest priority. Certain operational requirements will cause individual components or the systems as a whole to have different priorities for the objectives (i.e. integrity or availability concerns may outweigh confidentiality or vice versa). This may in turn lead an organization to deploy different countermeasures to achieve these security objectives."

Subclause 5.3 of IEC TS 62443-1-1:2009 [4] – Foundational requirements

"The simple CIA model shown in Figure 1 (of IEC TS 62443-1-1:2009 [4]) *is not adequate for a full understanding of the requirements for security in IACS[6]. Although it is beyond the scope of this technical specification to describe an exhaustive list of detailed requirements, there are several basic and foundational requirements that have been identified for industrial automation security. These are the following requirements:*

a) *Access Control (AC): control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.*

b) *Use Control (UC): control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.*

c) *Data Integrity (DI): ensure the integrity of data on selected communication channels to protect against unauthorized changes.*

d) *Data Confidentiality (DC): ensure the confidentiality of data on selected communication channels to protect against eavesdropping.*

e) *Restrict Data Flow (RDF): restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.*

---

6 In this document, industrial automation and control system (IACS) is replaced in accordance with Clause 3. See also last paragraph of Clause A.1.

f) Timely Response to Event (TRE): respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission-critical or safety-critical situations.

g) Resource Availability (RA): ensure the availability of all network resources to protect against denial of service attacks."

Subclause 5.6.6 of IEC TS 62443-1-1:2009 [4] – Countermeasures

"Countermeasures are actions taken, or provisions made for the purpose of reducing risk to an acceptable level or to meet security policies. They do not typically eliminate risk. The nature of the countermeasures employed depends on the nature of the threat being addressed.

There are several possible countermeasures to address external threats. Examples include the following:

a) authentication of users and/or computers;

b) access controls;

c) intrusion detection;

d) encryption;

e) digital signatures;

f) resource isolation or segregation;

g) scanning for malicious software;

h) system activity monitoring;

i) physical security."

Subclause 5.9 of IEC TS 62443-1-1:2009 [4] – Security zones

Subclause 5.9.1 of IEC TS 62443-1-1:2009 [4] – General

"Every situation has a different acceptable level of security. For large or complex systems, it may not be practical or necessary to apply the same level of security to all components. Differences can be addressed by using the concept of a security zone, or area under protection. A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements. This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone. There can also be zones within zones, or subzones, that provide layered security, giving defense in depth and addressing multiple levels of security requirements. Defense in depth can also be accomplished by assigning different properties to security zones.

A security zone has a border, which is the boundary between included and excluded elements. The concept of a zone also implies the need to access the assets in a zone from both within and without. This defines the communication and access required to allow information and people to move within and between the security zones. Zones may be considered to be trusted or untrusted.

Security zones can be defined in either a physical sense (a physical zone) or in a logical manner (virtual zone). Physical zones are defined by grouping assets by physical location. In this type of zone, it is easy to determine which assets are within each zone. Virtual zones are defined by grouping assets, or parts of physical assets, into security zones based on functionality or other characteristics, rather than the actual location of the assets."

Subclause 5.10 of IEC TS 62443-1-1:2009 [4] – Conduits

Subclause 5.10.1 of IEC TS 62443-1-1:2009 [4] – General

"Information needs to flow into, out of, and within a security zone. Even in a non-networked system, some communication exists (e.g. intermittent connection of programming devices to create and maintain the systems). To cover the security aspects of communication and to provide a construct to encompass the unique requirements of communications, this document is defining a special type of security zone: a communications' conduit.

A conduit is a particular type of security zone that groups communications that can be logically organized into a grouping of information flows within and also external to a zone. It can be a single service (e.g. a single Ethernet network) or can be made up of multiple data carriers (e.g. multiple network cables and direct physical accesses). As with zones, it can be made of both physical and logical constructs. Conduits may connect entities within a zone or may connect different zones.

As with zones, conduits may be either trusted or untrusted. Conduits that do not cross zone boundaries are typically trusted by the communicating processes within the zone. Trusted conduits crossing zone boundaries need to use an end-to-end secure process.

Untrusted conduits are those that are not at the same level of security as the zone endpoint. In this case the actual communication security becomes the responsibility of the individual channel."

Subclause 5.11 of IEC TS 62443-1-1:2009 [4] – Security levels

Subclause 5.11.1 of IEC TS 62443-1-1:2009 [4] – General

"The security level concept has been created to focus thinking about security on a zone basis rather than on an individual device basis or a system basis. Often an IACS[7] consists of devices and systems from multiple vendors, all functioning together to provide the integrated automation functions for the industrial operation. Just as the functional capabilities of the individual devices contribute to the capability of the IACS, the security capabilities of the individual devices and implemented countermeasures need to function with each other to achieve a desired level of security for a zone. Security levels provide a frame of reference for making decisions on the use of countermeasures and devices with differing inherent security capabilities.

Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of security levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.

Each organization using the security level method should establish a definition of what each level represents and how to measure the level of security for the zone. This definition or characterization should be used consistently across the organization. The security level may be used to identify a comprehensive layered defense-in-depth strategy for a zone that includes hardware and software-based technical countermeasures along with administrative-type countermeasures.

---

7 In this document, industrial automation and control system (IACS) is replaced in accordance with Clause 3. See also last paragraph of Clause A.1.

Security level corresponds to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit. The security level method provides the ability to categorize risk for a zone or conduit. It also helps define the required effectiveness of countermeasures used to prevent unauthorized electronic intervention that can read or impact the normal functioning of devices and systems within the zone or conduit. Security level is a property of a zone and conduit rather than of a device, system, or any part of a system."

Subclause 5.11.2 of IEC TS 62443-1-1:2009 [4] – Types of security levels

Subclause 5.11.2.1 of IEC TS 62443-1-1:2009 [4] – General

"Three different types of security levels can be defined as follows:

a) SL(target) – target security level for a zone or conduit;

b) SL(achieved) – achieved security level of a zone or conduit;

c) SL(capability) – security level capability of countermeasures associated with a zone or conduit or inherent security level capability of devices or systems within a zone or conduit."

Subclause 5.11.2.2 of IEC TS 62443-1-1:2009 [4] – SL(target) – target security level

"A target security level should be assigned to a zone. A target security level may be assigned to a conduit. SL(target) for a zone and conduit is determined during risk assessment. It is not required to assign a target security level to conduits as long as the security properties associated with the conduit are taken into consideration during risk assessment of the zones which use the conduit under consideration. Risk assessment should take into consideration the likelihood and consequences of security of a zone or conduit being compromised. Risk assessment may be qualitative, semi-quantitative, or quantitative. SL(target) determines the required effectiveness of countermeasures, devices, and systems that need to be in place to prevent security of the zone or conduit from being compromised.

Countermeasures can be:

a) technical countermeasures (e.g. firewalls, anti-virus software);

b) administrative countermeasures (policies and procedures);

c) physical countermeasures (e.g. locked doors).

Factors that influence the determination of SL(target) for a zone and conduit are:

d) network architecture with defined zone boundaries and conduits;

e) SL(target) of the zones with which the zone under consideration will communicate;

f) SL(target) of conduit, if assigned, used for communication by the zone;

g) physical access to devices and systems within the zone.

Within the zone, computing the target security level should be based on layers of security and their impact on the whole."

Subclause 5.11.2.3 of IEC TS 62443-1-1:2009 [4] – SL(achieved) – achieved security level

"SL(achieved) of a zone or conduit depends on inherent security properties of devices and systems within the zone or conduit and/or properties of countermeasures that are in place to prevent the security of the zone or conduit from being compromised. SL(achieved) is a function of time and decreases with time due to degradation of countermeasures, new vulnerabilities, adjusted threats or attack methods, breach in security layers, and inherent security properties of devices and systems until they are reviewed, updated, or upgraded.

The objective is to ensure that at any given time SL(achieved) of a zone or conduit is greater than or equal to the SL(target) for the zone or conduit."

Subclause 5.11.2.4 of IEC TS 62443-1-1:2009 [4] – SL(capability) – security level capability of countermeasures, devices or systems

"SL(capability) is defined for countermeasures and inherent security properties of devices and systems within a zone or conduit that contribute to the security of a zone or conduit. It is a measure of the effectiveness of the countermeasure, device, or system for the security property that they address.

Examples of security properties that may be addressed by a countermeasure, device or system are given below:

a) proving peer entity authenticity;

b) preserving authenticity and integrity of messages;

c) preserving confidentiality of messages/information/communication;

d) ensuring accountability (non-repudiation);

e) enforcing access control policies;

f) preventing denial-of-service attacks;

g) maintaining platform trustworthiness;

h) detecting tampering;

i) monitoring security status.

SL(capability) of a countermeasure, device or system within a zone or conduit contributes to the SL(achieved) based on the relevant security properties addressed by countermeasures, devices or systems for that zone or conduit."

IEC 62443-3-3:2013 [5]

Subclause 3.3 of IEC 62443-3-3:2013 [5] – Conventions

"This standard expands the seven foundational requirements defined in IEC TS 62443-1-1:2009 [4] into a series of SRs. Each SR has a baseline requirement and zero or more requirement enhancements (REs) to strengthen security. To provide clarity to the reader, rationale and supplemental guidance is provided for each baseline requirement and notes for any associated REs as is deemed necessary. The baseline requirement and REs, if present, are then mapped to the control system capability security level, SL-C (foundational requirement, control system) 1 to 4.

All seven foundational requirements have a defined a set of four security levels. The control system capability level 0 for a particular foundational requirement is implicitly defined as no requirements. For example, the purpose statement for Clause 8 (of IEC 62443-3-3:2013 [5]), *foundational requirement 4 – data confidentiality, is:*

> *Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.*

The associated four security levels are defined as:

- *SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.*
- *SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.*

- *SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS[8] specific skills and moderate motivation.*
- *SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.*

The individual SR and RE assignments are thus based on an incremental increase in overall control system security for that particular foundational requirement.

The SL-C (control system), used throughout this document, signifies a capability required to meet a given security level rating for a given foundational requirement. A complete description of the security level vector concept can be found in Annex A (of IEC 62443-3-3:2013 [5])*."*

Clause A.2 of IEC 62443-3-3:2013 [5] – Security levels

Subclause A.2.1 of IEC 62443-3-3:2013 [5] – Definition

"The following is an excerpt from 5.11.1 of IEC TS 62443-1-1:2009 [4] that provides a good explanation of what security levels are and how they can be used.

> *Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of security levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.*

In the first phase of development, the IEC 62443 series [3] of standards tends to use qualitative Security Levels, using terms such as "low", "medium", and "high". The asset owner will be required to come up with their own definition of what those classifications mean for their particular application. The long-term goal for the IEC 62443 series [3] is to move as many of the security levels and requirements to quantitative descriptions, requirements and metrics as possible to establish repeatable applications of the standard across multiple companies and industries. Achieving this goal will take time, since more experience in applying the standards and data on industrial security systems will need to be acquired to justify the quantitative approach.

When mapping requirements to the different security levels, standard developers need some frame of reference describing what the different security levels mean and how they differ from each other. The goal of this annex is to propose such a frame of reference."

Subclause A.2.2 of IEC 62443-3-3:2013 [5] – Types of security levels

"Security Levels have been broken down into three different types: target, achieved and capability. These types, while they all are related have to do with different aspects of the security life cycle.

- ***Target Security Levels (SL-T)** are the desired level of security for a particular system. This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.*

---

8 In this document, industrial automation and control system (IACS) is replaced in accordance with Clause 3. See also last paragraph of Clause A.1.

- ***Achieved Security Levels (SL-A)*** *are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target security levels.*
- ***Capability Security Levels (SL-C)*** *are the security levels that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the target security levels natively without additional compensating countermeasures when properly configured and integrated."*

Clause A.3 of IEC 62443-3-3:2013 [5] – Security levels vector

Subclause A.3.1 of IEC 62443-3-3:2013 [5] – Foundational requirements

"Security levels are based on the seven foundational requirements for security as defined in IEC TS 62443-1-1:2009 [4]:

1) identification and authentication control (IAC),

2) use control (UC),

3) system integrity (SI),

4) data confidentiality (DC),

5) restricted data flow (RDF),

6) timely response to events (TRE), and

7) resource availability (RA).

Instead of compressing security levels down to a single number, it is possible to use a vector of security levels that uses the seven foundational requirements above instead of a single protection factor. This vector of security levels allows definable separations between security levels for the different foundational requirements using language. This language can be based on the additional consequences associated with security systems or different attacks against the security objectives addressed by the foundational requirements. The language used in the security level definitions can contain practical explanations of how one system is more secure than another without having to relate everything to HSE (health, safety and environmental) consequences."

Subclause A.3.2 of IEC 62443-3-3:2013 [5] – Level definitions

Subclause A.3.2.1 of IEC 62443-3-3:2013 [5] – Overview

"The IEC 62443 series [3] define security levels in terms of five different levels (0, 1, 2, 3 and 4), each with an increasing level of security. The current model for defining security levels depends on protecting an increasingly more complex threat and differs slightly depending on what type of security level it is applied. For SL-C, this means that a particular component or system is capable of being configured by an asset owner or system integrator to protect against an increasingly complex type of threat. For SL-T, this means that the asset owner or system integrator has determined through a risk assessment that they need to protect this particular zone, system or component against this level of threat. For SL-A, this means that the asset owner, system integrator, product supplier and/or any combination of these has configured the zone, system or component to meet the particular security requirements defined for that SL.

The language used for each of the security levels uses terms like casual, coincidental, simple, sophisticated and extended. This language is intentionally vague to allow the same basic language to be used for all of the documents in the IEC 62443 series [3]. Each of the individual documents in the series will define the requirements for the security levels that apply to their particular purpose.

While the requirements for each of the security levels will be different throughout the IEC 62443 series [3], there need to be a general understanding of what each of the security levels should protect against. The following sections will provide some guidance on how to differentiate between the security levels."

Subclause A.3.2.2 of IEC 62443-3-3:2013 [5] – SL 0: No specific requirements or security protection necessary

"Security level 0 has multiple meanings depending on the situation in which it is applied. In defining SL-C it would mean that the component or system fails to meet some of the security level 1 requirements for that particular foundational requirement. This would most likely be for components or systems that would be part of a larger zone where other components or systems would provide compensating countermeasures. In defining SL-T for a particular zone it means that the asset owner has determined that the results of their risk analysis indicate that less than the full security level 1 specific requirements are necessary for that particular foundational requirement on that component or system. This would more likely happen for individual components within a system or zone that do not contribute in any way to the foundational requirement specific requirements. In defining SL-A it would mean that the particular zone fails to meet some of the security level 1 requirements for that particular foundational requirement."

Subclause A.3.2.3 of IEC 62443-3-3:2013 [5] – SL 1: Protection against casual or coincidental violation

"Casual or coincidental violations of security are usually through the lax application of security policies. These can be caused by well-meaning employees just as easily as they can be by an outsider threat. Many of these violations will be security program related and will be handled by enforcing policies and procedures.

Using Figure A.1 (of IEC 62443-3-3:2013 [5])*, a simple example would be an operator able to change a set point on the engineering station in the BPCS zone to a value outside certain conditions determined by the engineering staff. The system did not enforce the proper authentication and use control restrictions to disallow the change by the operator. Also using Figure A.1* (of IEC 62443-3-3:2013 [5])*, another example would be a password being sent in clear text over the conduit between the BPCS zone and the DMZ zone, allowing a network engineer to view the password while troubleshooting the system. The system did not enforce proper data confidentiality to protect the password. Using Figure A.2* (of IEC 62443-3-3:2013 [5])*, a third example would be an engineer that means to access the PLC in industrial network number 1 but actually accesses the PLC in industrial network number 2. The system did not enforce the proper restriction of data flow preventing the engineer from accessing the wrong system."*

Subclause A.3.2.4 of IEC 62443-3-3:2013 [5] – SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation

"Simple means do not require much knowledge on the part of the attacker. The attacker does not need detailed knowledge of security, the domain or the particular system under attack. These attack vectors are well known and there may be automated tools for aiding the attacker. They are also designed to attack a wide range of systems instead of targeting a specific system, so an attacker does not need a significant level of motivation or resources at hand.

Using Figure A.1 (of IEC 62443-3-3:2013 [5]), *an example would be a virus that infects the maintenance workstation in the Plant DMZ zone spreading to the BPCS engineering workstation since they both use the same general purpose operating system. Using Figure A.2* (of IEC 62443-3-3:2013 [5]), *another example would be an attacker compromising a web server in the enterprise network by an exploit downloaded from the Internet for a publicly known vulnerability in the general purpose operating system of the web server. The attacker uses the web server as a pivot point in an attack against other systems in the enterprise network as well as the industrial network. Also using Figure A.2* (of IEC 62443-3-3:2013 [5]), *a third example would be an operator that views a website on the HMI located in industrial network number 1 which downloads a Trojan that opens a hole in the routers and firewalls to the Internet."*

Subclause A.3.2.5 of IEC 62443-3-3:2013 [5] – SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS[9] specific skills and moderate motivation

"Sophisticated means require advanced security knowledge, advanced domain knowledge, advanced knowledge of the target system or any combination of these. An attacker going after a security level 3 system will likely be using attack vectors that have been customized for the specific target system. The attacker may use exploits in operating systems that are not well known, weaknesses in industrial protocols, specific information about a particular target to violate the security of the system or other means that require a greater motivation as well as skill and knowledge set than are required for security level 1 or 2.

An example of sophisticated means could be password or key cracking tools based on hash tables. These tools are available for download, but applying them takes knowledge of the system (such as the hash of a password to crack). Using Figure A.1 (of IEC 62443-3-3:2013 [5]), *another example would be an attacker that gains access to the FS-PLC through the serial conduit after gaining access to the control PLC through a vulnerability in the Ethernet controller. Using Figure A.2* (of IEC 62443-3-3:2013 [5]), *a third example would be an attacker that gains access to the data historian by using a brute-force attack through the industrial/enterprise DMZ firewall initiated from the enterprise wireless network."*

Subclause A.3.2.6 of IEC 62443-3-3:2013 [5] – SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

"Security level 3 and security level 4 are very similar in that they both involve sophisticated means used to violate the security requirements of the system. The difference comes from the attacker being even more motivated and having extended resources at their disposal. These may involve high-performance computing resources, large numbers of computers or extended periods of time.

An example of sophisticated means with extended resources would be using super computers or computer clusters to conduct brute-force password cracking using large hash tables. Another example would be a botnet used to attack a system using multiple attack vectors at once. A third example would be an organized crime organization that has the motivation and resources to spend weeks attempting to analyse a system and develop custom "zero-day" exploits."

Subclause A.3.3 of IEC 62443-3-3:2013 [5] – Security level vector format

"A vector can be used to describe the security requirements for a zone, conduit, component or system better than a single number. This vector may contain either a specific security level requirement or a zero value for each of the foundational requirements (see A.3.1 of IEC 62443-3-3:2013 [5]*).*

---

9 In this document, industrial automation and control system (IACS) is replaced in accordance with Clause 3. See also last paragraph of Clause A.1.

FORMAT → SL-?([Foundational Requirement,]domain) = { IAC UC SI DC RDF TRE RA }

where

SL-? = (Required) The Security Level type (see A.2.2 of IEC 62443-3-3:2013 [5]*). The possible formats are:*

- *SL-T = Target SL*
- *SL-A = Achieved SL*
- *SL-C = Capability SL*

[Foundational Requirement,] = (Optional) Field indicating the foundational requirement that the security level value applies. The foundational requirements are written out in abbreviated form instead of numerical form to aid in readability.

domain = (Required) The applicable domain that the security level applies. Domains can refer to zones, control systems, subsystems or components. Some examples of different domains from Figure A.1 (of IEC 62443-3-3:2013 [5])*, are SIS zone, BPCS zone, BPCS HMI, Plant DMZ domain controller, Plant DMZ to control centre conduit and SIS to BPCS serial conduit. In this particular standard, all requirements refer to a control system, so the domain term is not used as it would be by other documents in the IEC 62443 series* [3].

EXAMPLE 1 → SL-T(BPCS zone) = { 2 2 0 1 3 1 3 }

EXAMPLE 2 → SL-C (SIS Engineering Workstation) = { 3 3 2 3 0 0 1 }

EXAMPLE 3 → SL-C (RA, FS-PLC) = 4

NOTE The last example specifies only the RA component of a 7-dimension SL-C."

A.8 Correlation with IEC TR 80001-2-2 [9]

IEC TR 80001-2-2:2012 [9], which deals with RISK MANAGEMENT for IT-NETWORKS incorporating MEDICAL DEVICES and especially with disclosure and communication of MEDICAL DEVICE SECURITY needs, RISKS and controls, has shown up the need for communication between MANUFACTURERS of MEDICAL DEVICES and the RESPONSIBLE ORGANIZATION that might want to integrate the MEDICAL DEVICE with its data interfaces into an IT-NETWORK. In determining this need, IEC TR 80001-2-2:2012 [9] has already started with some communication of SECURITY related device properties that are similar to capabilities in the meaning of this document. However, that has not been the focus of that document, and the concept of reproducible and testable SECURITY LEVELS has successfully been evaluated in IEC 62443 (all parts) [3]. This document makes use of that concept and completes it with MEDICAL DEVICE specific specifications, including MEDICAL DEVICE group specific FIRECALL functions and ESSENTIAL FUNCTION.

A comparison of the SECURITY properties listed in IEC TR 80001-2-2:2012 [9] with the capabilities used in IEC 62443-4-2:2019 and in this document came to the following result.

All of the properties listed in Table C.1 of IEC TR 80001-2-2:2012 [9] are covered in IEC 62443-4-2:2019 and also in this document, except of the PROCESS element RDMP in Table C.1 of IEC TR 80001-2-2:2012 [9], and the medical application specific element DIDT (generally covered in CR 4.1 and CR 4.2 of IEC 62443-4-2:2019, but not health data specific).

On the other hand, the following MEDICAL DEVICE specific capabilities (CR, SAR, EDR, HDR) are not addressed in IEC TR 80001-2-2:2012 [9]: CR 1.3, CR 1.4, CR 1.7, CR 1.8, CR 1.9, CR 1.10, CR 1.11, CR 1.12, CR 1.14, CR 2.2, SAR/EDR/HDR 2.4, CR 2.7, CR 2.9, CR 2.10, CR 2.12, EDR/HDR 2.13, CR 3.3, CR 3.5, CR 3.6, CR 3.7, CR 3.8, EDR/HDR 3.10, EDR/HDR 3.11, EDR/HDR 3.12, EDR/HDR 3.13, EDR/HDR 3.14, CR 5.1, CR 7.1, CR 7.2, CR 7.5, CR 7.8.

Also, diverse NDR are not addressed in Table C.1 of IEC TR 80001-2-2:2012 [9]: NDR 1.6, NDR 1.13, NDR 2.4, NDR 2.13, NDR 3.10, NDR 3.11, NDR 3.12, NDR 3.13, NDR 3.14, NDR 5.2, NDR 5.3.

NOTE As a conclusion, a test report that demonstrates compliance to the specifications of this document also demonstrates compliance to the product related specifications of IEC TR 80001-2-2:2012 [9]. PROCESS related specifications of IEC TR 80001-2-2:2012 [9] are covered elsewhere.

Bibliography

[1] IEC 61907:2009, *Communication network dependability engineering*

[2] IEC 62304:2006, *Medical device software – Software life cycle processes*
IEC 62304:2006/AMD1:2015

[3] IEC 62443 (all parts), *Security for industrial automation and control systems*

[4] IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[5] IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

[6] IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

[7] ISO 80001-2 (all parts), *Application of risk management for IT-networks incorporating medical devices – Application guidance*

[8] IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities*

[9] IEC TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*

[10] IEC 81001-5-1:—, *Health software and health IT systems safety, effectiveness and security – Part 5: Security – Part 5-1: Activities in the product life cycle* [10]

[11] ISO 5127:2017, *Information and documentation – Foundation and vocabulary*

[12] ISO IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[13] ISO 14971:2019, *Medical devices – Application of risk management to medical devices*

[14] ISO/IEC 19790, *Information technology – Security techniques – Security requirements for cryptographic modules*

[15] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[16] ISO 81001-1:—, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts* [11]

[17] AAMI TIR57:2016, *Principles for medical device security – Risk management*

[18] AAMI TIR97:2019, *Principles for medical device security – Postmarket risk management for device manufacturers*

---

[10] Under preparation. Stage at the time of publication: IEC/CCDV 81001-5-1:2020.

[11] Under preparation. Stage at the time of publication: ISO/FDIS 81001-1:2020.

[19] ANSI/CAN/UL 2900-2-1, *ANSI/CAN/UL Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems*

[20] BSI Recommendation: Manufacturers, 2018, *Cyber Security Requirements for Network-Connected Medical Devices*

[21] FDA Draft Guidance, 2018, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff*

[22] FIPS 140-2, *Security Requirements for Cryptographic Modules*

[23] IMDRF/GRRP WG/N47:2018, *Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices*

[24] NIST Cybersecurity Framework and special publications,
https://www.nist.gov/cyberframework,
https://www.nist.gov/mml/csd/nist-special-publications-sp

[25] UL 2900-1, *Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*

[26] IEC 80001-2 (all parts), *Application of risk management for IT-networks incorporating medical devices – Application guidance*

_____