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 It also gives information on projects, replaced and withdrawn publications.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

colour inside

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]