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.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 9
2 Normative references 9
3 Terms and definitions 10
4 Common SECURITY constraints 15
4.1 Overview 15
4.2 * Support of ESSENTIAL FUNCTION 15
4.3 COMPENSATING COUNTERMEASURES 16
4.4 LEAST PRIVILEGE 17
4.5 Data minimization 17
4.6 * Overarching constraints 17
4.6.1 Constraints referenced by the MEDICAL DEVICE specifications 17
4.6.2 Hardware SECURITY 17
4.6.3 * Specific SECURITY features for MEDICAL DEVICES 18
5 SECURITY LEVELS for the different foundational requirements 18
5.1 * Application of SECURITY LEVELS 18
5.2 Modified specifications for SECURITY LEVELS 18
6 Technical description 19
7 Mapping of requirements to capability security levels (SL-C) 21
Annex A (informative) General guidance and rationale 26
A.1 The approach of this document: Type testable MEDICAL DEVICE IT SECURITY properties 26
A.2 Typical network connections of MEDICAL DEVICES covered in this document 32
A.3 Inclusion of ME SYSTEMS 33
A.4 Correlation to existing regulations, standards and technical specifications 34
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] 37
A.6 Documentation of capability SECURITY LEVEL (SL-C) of a MEDICAL DEVICE 37
A.7 Conceptual elements of IEC 62443 (all parts) [3] used for this document 38
A.8 Correlation with IEC TR 80001-2-2 [9] 48
Bibliography 50

Figure 1 – ESSENTIAL FUNCTION 16
Figure A.1 – Illustration with SECURITY LEVELS 27
Figure A.2 – Capability – Target – Achieved 28
Figure A.3 – Wireless point-to-point connection between a portable device (e.g. PATIENT programmer) and an implant 32
Figure A.4 – Connection between a PATIENT's portable device and a doctor's computer 32
Figure A.5 – Connection between a MEDICAL DEVICE and a doctor's computer 32
Figure A.6 – IT-NETWORK in a hospital 33
Figure A.7 – Selection of IT SECURITY related documents 35
Figure A.8 – Example of what a complex IT-NETWORK can consist of 37
Figure A.9 – Comparison of objectives between industrial automation and control systems and general IT-NETWORKS 39

Table 1 – Mapping of single requirements to capability security levels (SL-C) 22
Table A.1 – Exemplary criteria for the selection of appropriate target SECURITY LEVEL SL-T in typical INTENDED USE environments 31
Table A.2 – Exemplary vector of capability SECURITY LEVEL SL-C 38

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*