IEC TR 80001-2-8

Edition 1.0 2016-05

TECHNICAL REPORT

Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2

IEC TR 80001-2-8:2016-05(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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: csc@iec.ch.

IEC TR 80001-2-8

Edition 1.0 2016-05

TECHNICAL REPORT

Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 11.040.01

ISBN 978-2-8322-3412-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-8, which is a technical report, 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, and ISO technical committee 215: Health informatics. [1)]

---

1) This document contains original material that is © 2013, Dundalk Institute of Technology, Ireland. Permission is granted to ISO and IEC to reproduce and circulate this material, this being without prejudice to the rights of Dundalk Institute of Technology to exploit the original text elsewhere.

It is published as a double logo technical report.

The text of this technical report is based on the following documents of IEC:

Enquiry draft	Report on voting
62A/1018/DTR	62A/1043A/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 14 P-members out of 31 having cast a vote.

This publication has been drafted in accordance with the ISO IEC Directives, Part 2.

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

A list of all parts of the IEC 80001 series, published under the general title *Application of risk management for it-networks incorporating medical devices,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

The IEC 80001-1 standard, the *Application of risk management to IT-networks incorporating medical devices*, provides the roles, responsibilities and activities necessary for RISK MANAGEMENT. IEC TR 80001-2-2, the *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* is a technical report that provides additional guidance in relation to how SECURITY CAPABILITIES might be referenced (disclosed and discussed) in both the RISK MANAGEMENT PROCESS and stakeholder communications and agreements. This technical report provides guidance for the establishment of each of the SECURITY CAPABILITIES presented in IEC TR 80001-2-2.

IEC TR 80001-2-2 contains an informative set of common, descriptive SECURITY CAPABILITIES intended to be the starting point for a security-centric discussion between the vendor and purchaser or among a larger group of stakeholders involved in a MEDICAL DEVICE IT-NETWORK project. Scalability is possible across a range of different sizes of RESPONSIBLE ORGANIZATIONS (henceforth called healthcare delivery organizations – HDOs) as each evaluates RISK using the SECURITY CAPABILITIES and decides what to include or not to include according to their RISK tolerance and available resources. This documentation can be used by HDOs as input to their IEC 80001 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. Other IEC 80001 technical reports will provide step-by-step guidance in the RISK MANAGEMENT PROCESS. IEC TR 80001-2-2 SECURITY CAPABILITIES encourage the disclosure of more detailed SECURITY CONTROLS. This technical report identifies SECURITY CONTROLS from key security standards which aim to provide guidance to a RESPONSIBLE ORGANIZATION when adapting the framework outlined in IEC TR 80001-2-2.

The framework outlined in IEC TR 80001-2-2 requires shared responsibility between HDOs and MEDICAL DEVICE manufacturers (MDMs). Similarly, this guidance applies to both stakeholders, as a shared responsibility, to ensure safe MEDICAL DEVICE IT networks. In order to build a secure MEDICAL DEVICE IT network a joint effort from both stakeholders is required.

A SECURITY CAPABILITY, as defined in IEC TR 80001-2-2, represents a broad category of technical, administrative and/or organizational SECURITY CONTROLS[2)] required to manage RISKS to confidentiality, integrity, availability and accountability of data and systems. This document presents these categories of SECURITY CONTROLS prescribed for a system and the operational environment to establish SECURITY CAPABILITIES to protect the confidentiality, integrity, availability and accountability of data and systems. The SECURITY CONTROLS support the maintenance of confidentiality and the protection from malicious intrusion that might lead to compromises in integrity or system/data availability. The SECURITY CONTROLS for each SECURITY CAPABILITY can be added to as the need arises[3)]. Controls are intended to protect both data and systems but special attention is given to the protection of both PRIVATE DATA and its subset called HEALTH DATA.

In addition to providing a basis for discussing RISK and respective roles and responsibilities toward RISK MANAGEMENT, this report is intended to supply:

a) Health Delivery Organizations (HDOs) with a catalogue of management, operational and administrative SECURITY CONTROLS to maintain the EFFECTIVENESS of a SECURITY CAPABILITY for a MEDICAL DEVICE on a MEDICAL DEVICE IT-NETWORK;

b) MEDICAL DEVICE manufacturers (MDMs) with a catalogue of technical SECURITY CONTROLS for the establishment of each of the 19 SECURITY CAPABILITIES.

---

2) For the purpose of consistency throughout this report, the term SECURITY CONTROLS refers to the technical, administrative and organizational controls/safeguards prescribed to establish SECURITY CAPABILITIES.

3) The selection of SECURITY CAPABILITIES and SECURITY CONTROLS will vary due to the diversity of MEDICAL DEVICE products and context in relation to environment and INTENDED USE. Therefore, this technical report is not intended as a “one size fits all” solution.

This report presents the 19 SECURITY CAPABILITIES, their respective "requirement goal" and "user need" (identical to that in IEC TR 80001-2-2) with a corresponding list of SECURITY CONTROLS from a number of security standards. The security standards used for mapping SECURITY CONTROLS to SECURITY CAPABILITIES include[4]:

- NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*

  NIST Special Publication 800-53 covers the steps in the RISK MANAGEMENT Framework that address SECURITY CONTROL selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. This includes selecting an initial set of baseline SECURITY CONTROLS based on a FIPS 199 worst-case impact analysis, tailoring the baseline SECURITY CONTROLS, and supplementing the SECURITY CONTROLS based on an organizational assessment of RISK. The security rules cover 17 areas including access control, incident response, business continuity, and disaster recoverability.

- ISO IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

  This standard defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will fulfil the most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes.

  This standard also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

- ISO IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

  This standard defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets.

  This standard defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

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

  This standard provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels, SL-C (control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.

- ISO IEC 27002:2013*, Information technology – Security techniques – Code of practice for information security controls*

  This standard outlines guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security RISK environment(s). It is designed to be used by organizations that intend to:

---

4) The selection of security standards used in this technical report does not represent an exhaustive list of all potentially useful standards.

1) select controls within the PROCESS of implementing a MEDICAL DEVICE system based on ISO IEC 27001;
2) implement commonly accepted information SECURITY CONTROLS;
3) develop their own information security management guidelines.

- ISO 27799:—[5], *Health informatics – Information security management in health using ISO IEC 27002*

  This standard defines guidelines to support the interpretation and implementation in health informatics of ISO IEC 27002 and is a companion to that standard.

  It specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, HDOs and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.

5) To be published.

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2

1 Scope

This part of IEC 80001, which is a Technical Report, provides guidance to Health Delivery Organizations (HDOs) and MEDICAL DEVICE manufacturers (MDMs) for the application of the framework outlined in IEC TR 80001-2-2. Managing the RISK in connecting MEDICAL DEVICES to IT-NETWORKS requires the disclosure of security-related capabilities and RISKS. IEC TR 80001-2-2 presents a framework for this disclosure and the security dialog that surrounds the IEC 80001-1 RISK MANAGEMENT of IT-NETWORKS. IEC TR 80001-2-2 presents an informative set of common, descriptive security-related capabilities that are useful in terms of gaining an understanding of user needs. This report addresses each of the SECURITY CAPABILITIES and identifies SECURITY CONTROLS for consideration by HDOs and MDMs during RISK MANAGEMENT activities, supplier selection, device selection, device implementation, operation etc.

It is not intended that the security standards referenced herein are exhaustive of all useful standards; rather, the purpose of this technical report is to identify SECURITY CONTROLS, which exist in these particular security standards (listed in the introduction of this technical report), that apply to each of the SECURITY CAPABILITIES.

This report provides guidance to HDOs and MDMs for the selection and implementation of management, operational, administrative and technical SECURITY CONTROLS to protect the confidentiality, integrity, availability and accountability of data and systems during development, operation and disposal.

All 19 SECURITY CAPABILITIES are not required in every case and the identified SECURITY CAPABILITIES included in this report should not be considered exhaustive in nature. The selection of SECURITY CAPABILITIES and SECURITY CONTROLS should be based on the RISK EVALUATION and the RISK tolerance with consideration for protection of patient SAFETY, life and health. INTENDED USE, operational environment, network structure and local factors should also determine which SECURITY CAPABILITIES are necessary and which SECURITY CONTROLS most suitably assist in establishing that SECURITY CAPABILITY.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls*[6)]

3 Terms and definitions

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

3.1
DATA AND SYSTEMS SECURITY
operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

[SOURCE: IEC 80001-1:2010, 2.5]

3.2
EFFECTIVENESS
ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, 2.6]

3.3
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEMS SECURITY

[SOURCE: IEC 80001-1:2010, 2.8]

3.4
HAZARD
potential source of HARM

[SOURCE: IEC 80001-1:2010, 2.9]

3.5
HEALTH DATA
PRIVATE DATA that indicates physical or mental health

Note 1 to entry: This term generically defines PRIVATE DATA and it subset, HEALTH DATA, within this report to permit users of this report to adapt it easily to different privacy compliance laws and regulations. For example, in Europe, the requirements might be taken and references changed to “Personal Data” and “Sensitive Data”; in the USA, HEALTH DATA might be changed to “Protected Health Information (PHI)” while making adjustments to text as necessary.

3.6
INTENDED USE
INTENDED PURPOSE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the manufacturer

[SOURCE: IEC 80001-1:2010, 2.10]

---

6) IEC TR 80001-2-2 contains many additional standards, policies and reference materials which are also indispensable for the application of this Technical Report.

3.7
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

[SOURCE: IEC 80001-1:2010, 2.12]

3.8
MEDICAL DEVICE
means any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific 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,
   – disinfection of MEDICAL DEVICES,
   – providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and
b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry: Products which may be considered to be MEDICAL DEVICES in some jurisdictions but for which there is not yet a harmonized approach, are:

– aids for disabled/handicapped people;
– devices for the treatment/diagnosis of diseases and injuries in animals;
– accessories for MEDICAL DEVICES (see Note to entry 3);
– disinfection substances;
– devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a 'parent' MEDICAL DEVICE to enable that MEDICAL DEVICE to achieve its INTENDED PURPOSE should be subject to the same GHTF procedures as apply to the MEDICAL DEVICE itself. For example, an accessory will be classified as though it is a MEDICAL DEVICE in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to MEDICAL DEVICES are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'medical device'.

[SOURCE: IEC 80001-1:2010, 2.14]

3.9
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, 2.16]

3.10
OPERATOR
person handling equipment

[SOURCE: IEC 80001-1:2010, 2.18]

3.11
PRIVATE DATA
any information relating to an identified or identifiable person

3.12
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: IEC 80001-1:2010, 2.19]

3.13
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

[SOURCE: IEC 80001-1:2010, 2.21, modified – The note has been deleted.]

3.14
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

[SOURCE: IEC 80001-1:2010, 2.22, modified – The notes have been deleted.]

3.15
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, 2.23]

3.16
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, 2.24]

3.17
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, 2.25]

3.18
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

[SOURCE: IEC 80001-1:2010, 2.27]

3.19
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring RISK

[SOURCE: IEC 80001-1:2010, 2.28]

3.20
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

[SOURCE: IEC 80001-1:2010, 2.30]

3.21
SECURITY CAPABILITY
broad category of technical, administrative or organizational controls to manage RISKS to confidentiality, integrity, availability and accountability of data and systems

3.22
SECURITY CONTROL
management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[SOURCE: NIST IR 7298]

3.23
VERIFICATION
confirmation through provision of objective evidence that specified requirements have been fulfilled

[SOURCE: IEC 80001-1:2010, 2.32]

4 Guidance for establishing SECURITY CAPABILITIES

4.1 General

This clause presents each of SECURITY CAPABILITIES, as outlined in IEC TR 80001-2-2, with corresponding tables (Tables 1 to 19) of recommended SECURITY CONTROLS from the following standards:

Technical SECURITY CONTROLS:

- NIST SP-800-53;
- ISO IEC 15408-2;
- ISO IEC 15408-3;
- IEC 62443-3-3;

Operational/administrative SECURITY CONTROLS:

- ISO IEC 27002;
- ISO 27799.

For infrastructure and MEDICAL IT NETWORK SECURITY CONTROLS, ISO IEC 27002 and ISO 27799 are grouped together in the below tables as the standards are fully aligned.