IEC TR 80001-2-9

Edition 1.0 2017-01

TECHNICAL REPORT

Application of risk management for it-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

IEC TR 80001-2-9:2017-01(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 It also gives information on projects, replaced and withdrawn publications.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 16 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 80001-2-9

Edition 1.0 2017-01

TECHNICAL REPORT

Application of risk management for it-networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 11.040.01, 35.240.80

ISBN 978-2-8322-3907-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

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 TR 80001-2-9, 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.

It is published as a double logo technical report.

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

Enquiry draft	Report on voting
62A/1097/DTR	62A/1128/RVDTR

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.

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

Terms defined in Clause 3 of this standard are printed in SMALL CAPITALS.

A list of all parts of the 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 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.

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

INTRODUCTION

This document outlines a process for supporting CONFIDENCE in the use of the 80001 series by developing security ASSURANCE cases (henceforth SECURITY CASEs) to complement a security RISK MANAGEMENT process. IEC 80001-1 provides the roles, responsibilities and activities necessary for RISK MANAGEMENT.

IEC TR 80001-2-2 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 phases. 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, intended use and available resources. This information may be used by HDOs as input to their IEC 80001-1 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. IEC TR 80001-2-1 provides step-by-step guidance in the RISK MANAGEMENT PROCESS. IEC TR 80001-2-2 SECURITY CAPABILITIES encourages the disclosure of more detailed SECURITY CONTROLS.

IEC TR 80001-2-8 identifies SECURITY CONTROLS from key security standards which aim to provide guidance to HDOs, MEDICAL DEVICE manufacturers (MDMs) when adapting the framework outlined in IEC TR 80001-2-2 and establishing each of the SECURITY CAPABILITIES presented here. A SECURITY CAPABILITY, as defined in IEC TR 80001-2-2, represents a broad category of technical, administrative and/or organizational SECURITY CONTROLS[1)] required to manage RISKS to confidentiality, integrity, availability and accountability of data and systems. IEC TR 80001-2-8 presents these categories of SECURITY CONTROLS prescribed for a system to establish SECURITY CAPABILITIES to support the maintenance of confidentiality and the protection from intentional or unintentional intrusion that may lead to compromises in integrity or system/data availability. IEC TR 80001-2-8 provides HDOs and MDMs with a catalogue of technical, management, operational and administrative controls. IEC TR 80001-2-8 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.

This document integrates the information and guidance contained in IEC TR 80001-2-2 and IEC TR 80001-2-8 together to provide guidance to HDOs and MDMs for identifying, developing, interpreting, updating and maintaining security ASSURANCE cases. Although other means of establishing CONFIDENCE in a particular property (e.g. security) exist, this document provides one such way in assuring CONFIDENCE in the establishment of IEC TR 80001-2-2 SECURITY CAPABILITIES through the use of SECURITY CASES. The purpose of the SECURITY CASE is to provide CONFIDENCE in the establishment of the IEC TR 80001-2-2 SECURITY CAPABILITIES for networked MEDICAL DEVICES. This is achieved by applying a SECURITY PATTERN to each of the 19 SECURITY CAPABILITIES. The objectives of the SECURITY PATTERN are as follows:

– to reduce the time required to develop the SECURITY CASE by providing a repeatable and systematic step-by-step, RISK based blue-print;

– provide a means to re-use components of the SECURITY PATTERN either within a SECURITY CASE or from one SECURITY CASE to another;

– to reduce the complexity often associated with the development of SECURITY CASES;

– provide a visible traceability matrix linking the SECURITY CONTROLS to the security threats and vulnerabilities identified during RISK MANAGEMENT;

---

1) For the purpose of consistency throughout this document, the terms SECURITY CONTROLS refer to the technical, management, administrative and organizational controls/safeguards prescribed to establish SECURITY CAPABILITIES.

– reduce the likelihood of missing a step in the ARGUMENT;
– improve the readability of the SECURITY CASE;
– provide CONFIDENCE regarding the integrity of the EVIDENCE collected based on the information presented in the ARGUMENT.

The process of developing the SECURITY CASE is not intended to replace a RISK MANAGEMENT process nor does it generate new processes, rather, the SECURITY CASE should complement the RISK MANAGEMENT process with a reference to, or, inclusion of the following supporting documentation by MDMs and HDOs:

– information regarding the intended use of the MEDICAL DEVICE, operational environment, network structure, interfaces, boundaries etc.;
– information regarding system description, security objectives and assets to be protected;
– justification for selection of SECURITY CAPABILITIES;
– justification for non-selection of SECURITY CAPABILITIES;
– assets being protected by specific SECURITY CAPABILITY;
– RISK acceptability criteria policy;
– all identified unacceptable threats/vulnerabilities;
– threat / vulnerability / RISK log;
– impact / threat scenario / consequence information;
– reference to source for selection of SECURITY CONTROLS (e.g. IEC TR 80001-2-8 tables).

The above information becomes part of, and remains with the SECURITY CASE from concept phase through to development, operation and retirement. Supporting information such as this can aid in better design choices, better maintenance during operation and more efficient and informative feedback practices.

This document is not intended to provide exhaustive guidance for the application of a RISK MANAGEMENT process nor does it mandate the use of any particular RISK MANAGEMENT process however IEC 80001-1 provides guidance on how to carry out RISK MANAGEMENT for medical IT-networks. Similarly, ISO 14971 provides guidance for the process of conducting RISK MANAGEMENT for MEDICAL DEVICES**.** For RISK MANAGEMENT processes such as RISK/benefit analysis, which is not covered in this document, HDOs refer to IEC 80001-1:2010, 4.4.5 and MDMs refer to ISO 14971,6.5.

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

Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities

1 Scope

This part of 80001 establishes a SECURITY CASE framework and provides guidance to health care delivery organizations (HDO) and MEDICAL DEVICE MANUFACTURERS (MDM) for identifying, developing, interpreting, updating and maintaining SECURITY CASES for networked MEDICAL DEVICES. Use of this part of 80001 is intended to be one of the possible means to bridge the gap between MDMs and HDOs in providing adequate information to support the HDOs RISK MANAGEMENT of IT-NETWORKS. This document leverages the requirements set out in ISO/IEC 15026-2 for the development of ASSURANCE cases[2]. It is not intended that this SECURITY CASE framework will replace a RISK MANAGEMENT strategy, rather, the intention is to complement RISK MANAGEMENT and in turn provide a greater level of ASSURANCE for a MEDICAL DEVICE by:

– mapping specific RISK MANAGEMENT steps to each of the IEC TR 80001-2-2 SECURITY CAPABILITIES, identifying associated threats and vulnerabilities and presenting them in the format of a SECURITY CASE with the inclusion of a re-useable SECURITY PATTERN;
– providing guidance for the selection of appropriate SECURITY CONTROLS to establish SECURITY CAPABILITIES and presenting them as part of the SECURITY CASE pattern (IEC TR 80001-2-8 provides examples of such SECURITY CONTROLS);
– providing EVIDENCE to support the implementation of a SECURITY CONTROL, hence providing CONFIDENCE in the establishment of each of the SECURITY CAPABILITIES.

The purpose of developing the SECURITY CASE is to demonstrate CONFIDENCE in the establishment of IEC TR 80001-2-2 SECURITY CAPABILITIES. The quality of artifacts gathered and documented during the development of the SECURITY CASE is agreed and documented as part of a RESPONSIBILITY AGREEMENT between the relevant stakeholders. This document provides guidance for one such methodology, through the use of a specific SECURITY PATTERN, to develop and interpret SECURITY CASES in a systematic manner.

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 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*[3]

---

2) These requirements are adapted for networked MEDICAL DEVICES where the sole critical property is “security” and where the CLAIM relates to the establishment of the IEC TR 80001-2-2 SECURITY CAPABILITIES with the inclusion of a specific security ARGUMENT PATTERN.

3) IEC TR 80001-2-2 contains many additional standards, policies and reference materials which are also indispensible for the application of this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

3.1.1
ASSURANCE
grounds for justified CONFIDENCE that a CLAIM has been or will be achieved

[SOURCE: ISO/IEC 15026-1:2013, 3.1.1]

3.1.2
ARGUMENT
connected series of CLAIMS intended to establish an overall CLAIM

[SOURCE: GSN Community Standard Version 1:2011, 0.3]

3.1.3
CLAIM
proposition being asserted by the author that is a true or false statement

[SOURCE: GSN Community Standard Version 1:2011, Glossary]

3.1.4
CONFIDENCE
quality or state of being certain that the ASSURANCE case is appropriately and effectively structured, and correct

[SOURCE: Definition by: Grigorova, S., & Maibaum, T. S. E. (2013, November). Taking a page from the law books: Considering evidence weight in evaluating assurance case confidence. In *Software Reliability Engineering Workshops (ISSREW), 2013 IEEE International Symposium on* (pp. 387-390). IEEE. Definition: page 388]

3.1.5
EVIDENCE
information or objective artefacts being offered in support of one or more CLAIMS

[SOURCE: GSN Community Standard Version 1:2011, Glossary]

3.1.6
MEDICAL DEVICE
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 can 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 can 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]

3.1.7
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

Note 1 to entry This agreement can be a legal document, e.g. a contract.

[SOURCE: IEC 80001-1:2010, 2.21]

3.1.8
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry The accountable entity can be, for example, a hospital, a private clinician or a telehealth organization.

Note 2 to entry Adapted from IEC 60601-1:2005, 3.101.

[SOURCE: IEC 80001-1:2010, 2.22]

3.1.9
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

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