Technical Information Report

AAMI/IEC TIR80001-2-8: 2016

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 80001-2-2

AAMI
Advancing Safety in Healthcare Technology

A Technical Report prepared by AAMI and registered with ANSI

AAMI/IEC TR80001-2-8:2016

Advancing Safety in Healthcare Technology

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 80001-2-2

Approved 18 November 2016 by
AAMI

Registered 30 December 2016 by
American National Standards Institute, Inc.

Abstract: This technical report provides guidance for the application of the framework outlined in AAMI/IEC 80001-2-2. Managing the RISK in connecting MEDICAL DEVICES to IT-networks requires the disclosure of security-related capabilities and RISKS. AAMI/IEC 80001-2-2 presents a framework for this disclosure and the security dialog that surrounds the AAMI/IEC 80001-1 RISK MANAGEMENT of IT-networks. AAMI/IEC 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 all stakeholders during RISK MANAGEMENT activities, supplier selection, device selection etc.

Keywords: medical device, security, IT networks

Published by

AAMI
4301 N Fairfax Drive, Suite 301
Arlington, VA 22203-1633

Printed in the United States of America

ISBN 978-1-57020-615-3

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years. For a TIR, AAMI consults with a technical committee about five years after the publication date (and periodically thereafter) for guidance on whether the document is still useful—that is, to check that the information is relevant or of historical value. If the information is not useful, the TIR is removed from circulation.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are voluntary, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

ANSI Registration

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

Contents

Page

Glossary of equivalent standards

International Standards or Technical Reports adopted in the United States may include normative references to other International Standards. AAMI maintains a current list of each International Standard that has been adopted by AAMI (and ANSI). Available on the AAMI website at the address below, this list gives the corresponding U.S. designation and level of equivalency to the International Standard.

www.aami.org/standards/glossary.pdf

Committee representation

Association for the Advancement of Medical Instrumentation
Information Technology Networks Work Group

The publication of AAMI/IEC TR 80001-2-8 as a new American National Technical Report was initiated by the AAMI Information Technology Networks Work Group who provides US comments to the 80001 series via the International Organization for Standardization (ISO) ISO/TC215 – IEC/SC62A JWG7 committee.

At the time this document was published, the **AAMI Information Technology Networks** had the following members:

Cochair: Bill Hintz, Medtronic Inc WHQ Campus

Members: John Collins, American Hospital Association - Washington, DC
Todd Cooper, Center for Medical Interoperability
Becky Crossley, Susquehanna Health
Conor Curtin, Fresenius Medical Care - Waltham, MA
Yadin David, Biomedical Engineering Consultants LLC
Richard DeLaCruz, Silver Lake Group Inc
Sherman Eagles, SoftwareCPR
Scott Eaton, Mindray DS USA Inc
Kurt Elliason, Smiths Medical
Jim Gabalski, Getinge USA
George Gray, Ivenix Inc
Thomas Grobaski, Belimed Inc
Catherine Li, FDA/CDRH
Yimin Li, St Jude Medical Inc
Jared Mauldin, Integrated Medical Systems
Mary Beth McDonald, Mary Beth McDonald Consulting
Dave Osborn, Philips Electronics North America
Geoff Pascoe
Steven Rakitin, Software Quality Consulting
Rick Schrenker, Massachusetts General Hospital
Neal Seidl, GE Healthcare - Waukesha, WI
Xianyu Shea, Stryker Medical Division
Ray Silkaitis, Amgen Inc
Bob Steuer, Spacelabs Healthcare
Donna-Bea Tillman, Biologics Consulting Group
J.S. Wiley, Draeger Medical Systems Inc
Daidi Zhong, Chongqing University

Alternates: Cheryl Carey, Medical Imaging & Technology Alliance a Division of NEMA
James Dundon, Spacelabs Healthcare
Brian Fitzgerald, FDA/CDRH
Rich Gardner, GE Healthcare
Andrew Northup, Medical Imaging & Technology Alliance a Division of NEMA
Phil Raymond, Philips Electronics North America
Thomas Schultz, Medtronic Inc WHQ Campus
Ferry Tamtoro, Amgen Inc
Chandresh Thakur, CareFusion
Fei Wang, Fresenius Medical Care

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

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]

It is published as a double logo technical report.

[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.

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.

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

[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.

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:

  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.

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

- 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.

[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.