Technical Information Report

AAMI TIR57: 2016/(R)2019

Principles for medical device security—Risk management

AAMI
Advancing Safety in Health Technology

Principles for medical device security—Risk management

Approved 5 June 2016 and reaffirmed 3 September 2019 by
AAMI

Abstract: Provides guidance on methods to perform information security risk management for a medical device in the context of the Safety Risk Management process required by ISO 14971. The TIR incorporates the expanded view of risk management from IEC 80001-1 by incorporating the same key properties of Safety, Effectiveness and Data & Systems Security with Annexes that provide process details and illustrative examples.

Keywords: medical device, information security, risk management

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that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years.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, 901 N. Glebe Road, Suite 300, Arlington, VA 22203.

Published by

AAMI
901 N. Glebe Road, Suite 300
Arlington, VA 22203

Printed in the United States of America

ISBN 978-1-57020-612-2

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

Medical Device Security Working Group

The publication of AAMI TIR57 as a new American Technical Information Report was initiated by the AAMI Medical Device Security Working Group.

At the time this document was published, the **AAMI Medical Device Security Working Group** had the following members:

Cochairs:
Ken Hoyme, Adventium Labs
Geoff Pascoe, Deloitte Advisory

Members:
Mike Ahmadi, Synopsys Inc
Pat Baird, Baxter Healthcare Corporation
Andrew Dean, Amgen Inc
Harsh Dharwad, Hospira Worldwide Inc
Sherman Eagles, SoftwareCPR
Scott Eaton, Mindray DS USA Inc
Plamena Entcheva-Dimitrov, Preferred Regulatory Consulting
Charles S. Farlow, Medtronic Inc.
Phil Fisk, Baxter Healthcare Corporation
Brian Fitzgerald, FDA/CDRH
Alan Fryer, Micro Systems Engineering Inc
Kevin Fu, The University of Michigan
Ken Fuchs, Center for Medical Interoperability
Bill Hagestad, Smiths Medical
Ed Heierman, Abbott Laboratories
Mike Jaffe, Cardiorespiratory Consulting LLC
Michelle Jump, Stryker Instruments Division
Joshua Kim, Hill-Rom Holdings
Insup Lee
Yimin Li, St Jude Medical Inc
Dan Lyon, Cigital Inc
Melissa Masters, Battelle Medical Products
Jill McCormick, Department of Veteran Affairs
Mary Beth McDonald, Mary Beth McDonald Consulting
Michael McNeil, Philips Electronics North America
Dale Nordenberg
Andrew O'Keeffe, Draeger Medical Systems Inc
Brodie Pedersen, Logic PD
Arnab Ray
Larry Schwartz, Smiths Medical
Michael Seeberger, Boston Scientific Corporation
Lynette Sherrill, Department of Veteran Affairs
Ferry Tamtoro, Amgen Inc
Tom Vaccaro, Becton Dickinson & Company
Fubin Wu, GessNet
Daidi Zhong, Chongqing University

Alternates:
Tushar Dharampal, St Jude Medical Inc
Leo Espindle, Amgen Inc
Dawn Flakne, Micro Systems Engineering Inc
Elisabeth George, Philips Electronics North America
Roberta Hansen, Abbott Laboratories
Karen Kazak, Baxter Healthcare Corporation
Tara Larson, Medtronic Inc.

Nick Sikorski, Deloitte Advisory
Nikhil Thakur, FDA/CDRH
J.S. Wiley, Draeger Medical Systems Inc

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

This technical information report (TIR) was developed by the Device Security Working Group.

It is widely recognized that there is little existing guidance for conducting cybersecurity risk assessment of medical devices.

The objective of this TIR is to provide guidance on how medical device manufacturers can manage risks from security threats that could impact the confidentiality, integrity, and/or availability of the device or the information processed by the device. Because medical device manufacturers are already familiar with ANSI/AAMI/ISO 14971:2007, this guidance follows the basic structure of that standard.

Suggestions for improving this recommended practice are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

NOTE This foreword does not contain provisions of the AAMI TIR57, *Principles for medical device security– Risk management* (AAMI TIR57:2016), but it does provide important information about the development and intended use of the document.

Introduction

Medical device manufacturers are familiar with the requirements of ANSI/AAMI/ISO 14971:2007/(R)2010 *Medical devices — Application of risk management to medical devices*. This standard is an integral part of the safety risk management processes required by many regulatory authorities. ANSI/AAMI/ISO 14971 specifies a process for a manufacturer to identify the hazards associated with medical devices, including *in vitro* diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls (see Clause 1 of ANSI/AAMI/ISO 14971:2007).

NOTE In 2012, the European Committee for Standardization (CEN) adopted EN ISO 14971:2012 as the European harmonized standard, superseding EN ISO 14971:2009. This document does not address content deviations included in Annex ZA of EN ISO 14971:2012. Specifically, the "as far as possible" requirement is not included in the evaluation of security risks. Instead, security risks are to be assessed and controlled to a level that is considered acceptable, taking into account the impact of a threat event and potential vulnerabilities.

Specific clauses of ANSI/AAMI/ISO 14971:2007 define a risk management process consisting of the following elements:

- risk analysis (Clause 4);
- risk evaluation (Clause 5);
- risk control (Clause 6);
- evaluation of overall residual risk acceptability (Clause 7);
- risk management report (Clause 8); and
- production and post-production information (Clause 9).

Figure 1 of ANSI/AAMI/ISO 14971:2007 (see Figure 1) provides a schematic representation of the risk management process. Central to the definition of risk are the concepts of probability of an occurrence of harm and the severity of that harm. Harm is defined in ANSI/AAMI/ISO 14971:2007 as "physical injury or damage to the health of people, or damage to property or the environment".

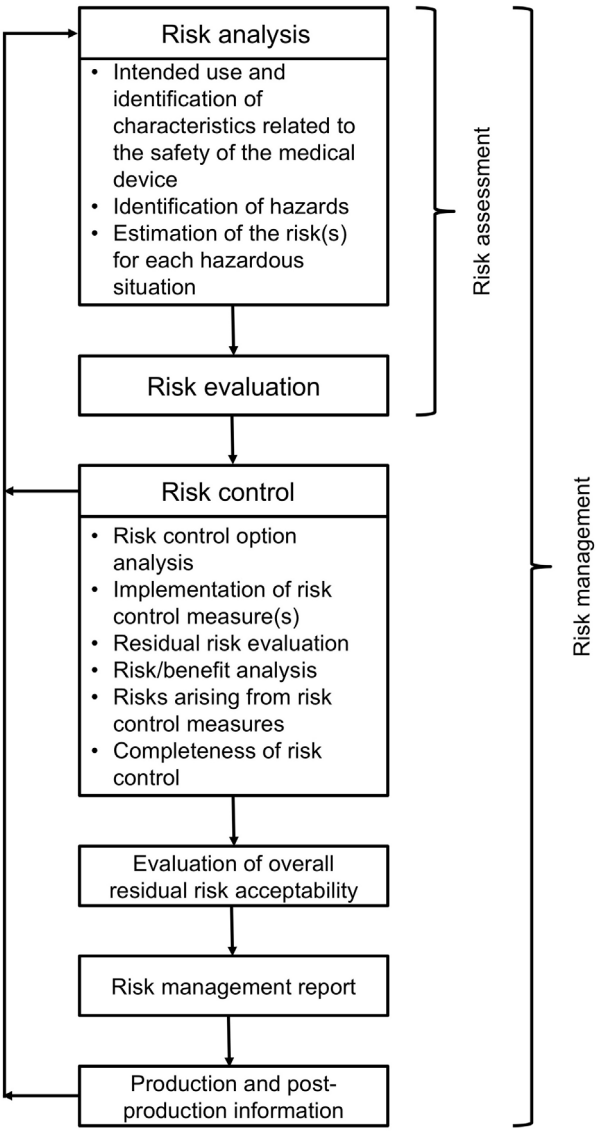

Figure 1 - Schematic representation of the risk management process (ANSI/AAMI/ISO 14971:2007)

The increased use of connected medical devices (i.e., devices directly connected to other systems or devices directly or via a computer network) has created a new source of risk for their safe operation. Security risks are associated with reduction of effectiveness and breach of data and systems security as included in the broader definition of harm in this document. While information security has been considered from the patient data privacy perspective for several years, there is no framework for security risk management for medical devices. This document describes a means of applying the risk management principles presented in ANSI/AAMI/ISO 14971 to the management of security risk.

The definition of harm is considered from the perspective of ANSI/AAMI/ISO 14971, as well as from healthcare information technology (IT) standards, such as the ANSI/AAMI/IEC 80001 family. Because a security risk management process that narrowly focuses on the traditional “physical injury or damage” definition may limit the scope of security risk mitigation, this document incorporates the broader considerations that risks include effects outside the traditional scope of patient physical harm and may include “reduction of effectiveness” and “breach of data and systems security” as extended in the ANSI/AAMI/IEC 80001 family of standards. Figure 2 shows the high-level relationship between these two classes of risk.

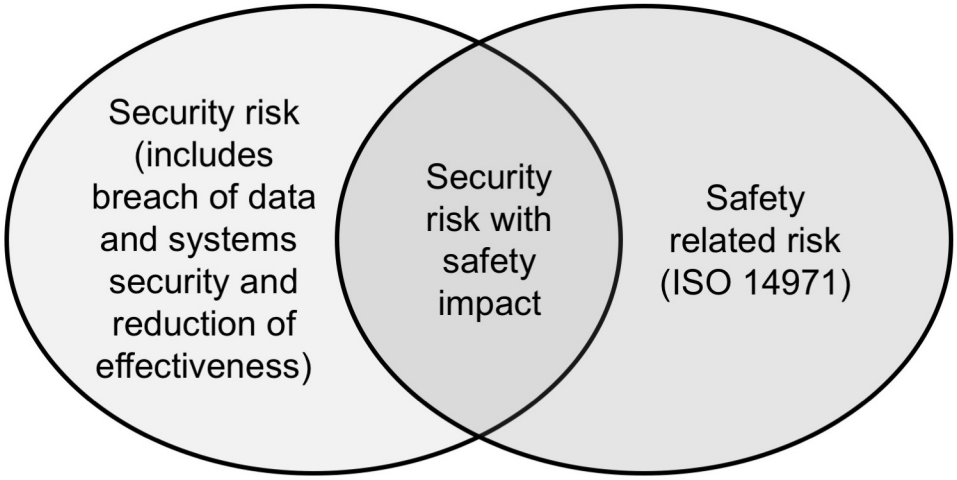

Figure 2 – A Venn diagram showing the relationship between security and safety risks

Considerations for security risk management are mapped to the risk management process steps of ANSI/AAMI/ISO 14971, as well as the security risk management process of NIST SP 800-30 Revision 1 *Guide for Conducting Risk Assessments (see Bibliography [53])*, with a particular emphasis on risk assessment methods. While this TIR utilizes NIST standards as a basis, manufacturers may use other generally accepted alternatives if they are better suited to their development processes.

Supporting annexes contain the following:

- Annex A: Security engineering principles and nomenclature – A high level overview of security engineering principles focused on their application to the medical device domain.
- Annex B: Security risk assessment – A more detailed description of the process for performing security risk assessment for a medical device based on the principles described in NIST SP 800-30 Revision 1 (see Bibliography [53]).
- Annex C: Generating cybersecurity requirements – A discussion on how to create effective, testable requirements for security properties that avoid complexities associated with “shall not” requirements. This is important since mitigating controls for security risks need to be expressed in the requirements for the device so proper verification of effectiveness can be shown.
- Annex D: Questions that can be used to identify medical device security characteristics – A detailed list of questions for manufacturers to assist in exploring security aspects of their devices, organized along the lines of ANSI/AAMI/ISO 80001-2-2:2010.
- Annex E: Security risk examples applied to medical products – A more detailed example of a fictional medical device and analysis of its security risks.
- Annex F: A comparison of terminology between key referenced standards – A comparison of the basic terms of risk management as defined in ANSI/AAMI/ISO 14971:2007, NIST SP 800-30 Revision 1, IEC 80001-1:2010 and this TIR.

While safety risk involves evaluating the probability and severity of a hazard leading to harm, security risk is based on an assessment of the likelihood that a threat will successfully exploit a device vulnerability, an event that could lead to an adverse impact due to a compromise of system confidentiality, integrity, and/or availability. This loosely parallels the concepts of probability and severity described in ANSI/AAMI/ISO 14971. Organizations should exercise caution when attempting to quantify likelihood of a future adverse impact in traditional probabilistic terms. Instead, they should focus on the skills and motivations of an attacker, and whether the effort required to exploit a vulnerability is less than the perceived gain the attacker will achieve by compromising the system (see B.2.1.1).

Security is an emergent property of a system. As such, the security of a device needs to be considered in the context of the broader system. This document directs manufacturers to understand, evaluate, and document the operating environment of a device so security risks are evaluated in their operational context. It is recognized that the manufacturer cannot ensure aspects of this operating environment that are outside the manufacturer’s control. However, it is incumbent on the manufacturer to understand the methods that Health Delivery Organizations (HDOs)

use to manage the risks of networked medical devices as specified in ANSI/AAMI/ISO 80001-1, as well as the methods used to communicate cybersecurity needs, risks, and controls as documented in ANSI/AAMI/ISO 80001-2-2. Manufacturers should understand the concept of a Responsibility Agreement[1] that may be negotiated with the purchasing HDO, and be prepared to communicate any specific security expectations of the network that the device is connected to through methods such as the HIMSS/NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2). Manufacturers should also recognize that a poorly secured and updated device could be a source of security vulnerability to other computing systems and other devices to which the device is connected, directly or on a shared network. Such a device can be used as a "pivot" to attack other systems and devices. A reasonable expectation of organizations deploying the device is that such risks have been considered and appropriately mitigated.

As a result, this document uses the broader definition of risk as used in the ANSI/AAMI/IEC 80001 family of standards. Manufacturers that follow the recommendations of this report should consider those risks that come from outside the device, mitigate those that are feasible, and document the expectations of the organization that becomes responsible for integrating the device into a broader network.

The framework described in this document is presented as a companion process to the safety risk management requirements of ANSI/AAMI/ISO 14971. This is similar to the risk management approach documented in ANSI/AAMI/IEC 62366-1:2015 for usability engineering. The key to successful integration of a device security risk management process into the larger risk management process is to bring together personnel with expertise in traditional device development, human factors, and cybersecurity product development. This collaboration will be essential to the ultimate goal of developing secure medical devices.

[1] Responsibility Agreements are described in ANSI/AAMI/ISO 80001-1.

Principles for medical device security – Risk management

1 Scope

This TIR provides guidance for addressing information security within the risk management framework defined by ANSI/AAMI/ISO 14971.

This guidance is intended to assist manufacturers and other users of the standard in the following:

- identifying threats, vulnerabilities, and assets associated with medical devices;
- estimating and evaluating associated security risks;
- controlling security risks; and
- monitoring effectiveness of the risk controls.

This document is based on an application of ANSI/AAMI/ISO 14971 with an expanded consideration of the possible impacts that a security compromise can have on the medical device, people, the environment, the manufacturer, and the information processed and stored by the device. This report also incorporates several principles from NIST SP 800-30 Revision 1 (see Bibliography [53]), a security risk management process developed for traditional IT systems.

The guidance provided by this document is applicable to all stages of the life-cycle of a medical device.

2 Terms and definitions

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

2.1
asset
person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value

[SOURCE: NICCS Glossary of Common Cybersecurity Terminology – As accessed on June 15, 2015.]

2.2
authentication
verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

[SOURCE: SP 800-53; SP 800-53A; SP 800-27; FIPS 200; SP 800-30]

2.3
authenticity
property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator (see Authentication)

[SOURCE: SP 800-53; SP 800-53A; CNSSI-4009; SP 800-39]

2.4
authorization
access privileges granted to a user, program, or process, or the act of granting those privileges

[SOURCE: CNSSI-4009]

