Technical Information Report

AAMI TIR32:2004/(R)2016

Medical device software risk management

AAMI
Advancing Safety in Healthcare Technology

Medical device software risk management

Approved 23 December 2004 and reaffirmed 26 May 2016 by
Association for the Advancement of Medical Instrumentation

Abstract: This AAMI technical information report provides information useful to performing effective software risk management, a significant part of the overall risk management process for medical devices containing software. It does this in the context of ANSI/AAMI/ISO 14971:2000, *Medical devices—Application of risk management to medical devices*, and in the context of ANSI/AAMI SW68:2001, *Medical device software—Software life cycle processes*.

Keywords: hazard, risk, software

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that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years.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, 1110 N. Glebe Road, Suite 220, Arlington, VA 22201-4795.

Published by

Association for the Advancement of Medical Instrumentation
4301 N. Fairfax Drive, Suite 301
Arlington, VA 22203-1633
www.aami.org

Printed in the United States of America

ISBN 1–57020–233–8

Contents

Glossary of equivalent standards

International Standards adopted in the United States may include normative references to other International Standards. For each International Standard that has been adopted by AAMI (and ANSI), the table below gives the corresponding U.S. designation and level of equivalency to the International Standard.

NOTE—Documents are sorted by international designation.

Other normatively referenced International Standards may be under consideration for U.S. adoption by AAMI; therefore, this list should not be considered exhaustive.

International designation	U.S. designation	Equivalency
IEC 60601-1-2:2001 and Amendment 1:2004	ANSI/AAMI/IEC 60601-1-2:2001 and Amendment 1:2004	Identical
IEC 60601-2-04:2002	ANSI/AAMI DF80:2003	Major technical variations
IEC 60601-2-19:1990 and Amendment 1:1996	ANSI/AAMI II36:2004	Major technical variations
IEC 60601-2-20:1990 and Amendment 1:1996	ANSI/AAMI II51:2004	Major technical variations
IEC 60601-2-21:1994 and Amendment 1:1996	ANSI/AAMI/IEC 60601-2-21 and Amendment 1:2000 (consolidated texts)	Identical
IEC 60601-2-24:1998	ANSI/AAMI ID26:2004	Major technical variations
IEC TR 60878:2003	ANSI/AAMI/IEC TIR60878:2003	Identical
IEC TR 62296:2003	ANSI/AAMI/IEC TIR62296:2003	Identical
ISO 5840:200x[1]	ANSI/AAMI/ISO 5840:2005	Identical
ISO 7198:1998	ANSI/AAMI/ISO 7198:1998/2001/(R)2004	Identical
ISO 7199:1996	ANSI/AAMI/ISO 7199:1996/(R)2002	Identical
ISO 10993-1:2003	ANSI/AAMI/ISO 10993-1:2003	Identical
ISO 10993-2:1992	ANSI/AAMI/ISO 10993-2:1993/(R)2001	Identical
ISO 10993-3:2003	ANSI/AAMI/ISO 10993-3:2003	Identical
ISO 10993-4:2002	ANSI/AAMI/ISO 10993-4:2002	Identical
ISO 10993-5:1999	ANSI/AAMI/ISO 10993-5:1999	Identical
ISO 10993-6:1994	ANSI/AAMI/ISO 10993-6:1995/(R)2001	Identical
ISO 10993-7:1995	ANSI/AAMI/ISO 10993-7:1995/(R)2001	Identical
ISO 10993-9:1999	ANSI/AAMI/ISO 10993-9:1999	Identical
ISO 10993-10:2002	ANSI/AAMI BE78:2002	Minor technical variations
ISO 10993-11:1993	ANSI/AAMI 10993-11:1993	Minor technical variations
ISO 10993-12:2002	ANSI/AAMI/ISO 10993-12:2002	Identical
ISO 10993-13:1998	ANSI/AAMI/ISO 10993-13:1999/(R)2004	Identical
ISO 10993-14:2001	ANSI/AAMI/ISO 10993-14:2001	Identical
ISO 10993-15:2000	ANSI/AAMI/ISO 10993-15:2000	Identical

[1] Currently at FDIS stage

International designation	U.S. designation	Equivalency
ISO 10993-16:1997	ANSI/AAMI/ISO 10993-16:1997/(R)2003	Identical
ISO 10993-17:2002	ANSI/AAMI/ISO 10993-17:2002	Identical
ISO 11134:1994	ANSI/AAMI/ISO 11134:1993	Identical
ISO 11135:1994	ANSI/AAMI/ISO 11135:1994	Identical
ISO 11137:1995 and Amdt 1:2001	ANSI/AAMI/ISO 11137:1994 and A1:2002	Identical
ISO 11138-1:1994	ANSI/AAMI ST59:1999	Major technical variations
ISO 11138-2:1994	ANSI/AAMI ST21:1999	Major technical variations
ISO 11138-3:1995	ANSI/AAMI ST19:1999	Major technical variations
ISO TS 11139:2001	ANSI/AAMI/ISO 11139:2002	Identical
ISO 11140-1:1995 and Technical Corrigendum 1:1998	ANSI/AAMI ST60:1996	Major technical variations
ISO 11140-5:2000	ANSI/AAMI ST66:1999	Major technical variations
ISO 11607:2003	ANSI/AAMI/ISO 11607:2000	Identical
ISO 11737-1:1995	ANSI/AAMI/ISO 11737-1:1995	Identical
ISO 11737-2:1998	ANSI/AAMI/ISO 11737-2:1998	Identical
ISO 11737-3:2004	ANSI/AAMI/ISO 11737-3:2004	Identical
ISO TR 13409:1996	AAMI/ISO TIR13409:1996	Identical
ISO 13485:2003	ANSI/AAMI/ISO 13485:2003	Identical
ISO 13488:1996	ANSI/AAMI/ISO 13488:1996	Identical
ISO 14155-1:2003	ANSI/AAMI/ISO 14155-1:2003	Identical
ISO 14155-2:2003	ANSI/AAMI/ISO 14155-2:2003	Identical
ISO 14160:1998	ANSI/AAMI/ISO 14160:1998	Identical
ISO 14161:2000	ANSI/AAMI/ISO 14161:2000	Identical
ISO 14937:2000	ANSI/AAMI/ISO 14937:2000	Identical
ISO TR 14969:2004	ANSI/AAMI/ISO TIR14969:2004	Identical
ISO 14971:2000 and A1:2003	ANSI/AAMI/ISO 14971:2000 and A1:2003	Identical
ISO 15223:2000, A1:2002, and A2:2004	ANSI/AAMI/ISO 15223:2000, A1:2001, and A2:2004	Identical
ISO 15225:2000 and A1:2004	ANSI/AAMI/ISO 15225:2000 and A1:2004	Identical
ISO 15674:2001	ANSI/AAMI/ISO 15674:2001	Identical
ISO 15675:2001	ANSI/AAMI/ISO 15675:2001	Identical
ISO TS 15843:2000	ANSI/AAMI/ISO TIR15843:2000	Identical
ISO TR 15844:1998	AAMI/ISO TIR15844:1998	Identical
ISO 15882:2003	ANSI/AAMI/ISO 15882:2003	Identical
ISO TR 16142:1999	ANSI/AAMI/ISO TIR16142:2000	Identical
ISO 17664:2004	ANSI/AAMI ST81:2004	Major technical variations
ISO 25539-1:2003	ANSI/AAMI/ISO 25539-1:2003	Identical

Committee representation

Association for the Advancement of Medical Instrumentation

AAMI Medical Device Software Committee

This technical information report was developed by the Software Risk Management Task Group of the AAMI Medical Device Software Committee. Approval of this TIR does not necessarily imply that all committee members voted for its approval.

At the time this document was published, the **AAMI Medical Device Software Committee** had the following members:

Cochairs: Sherman Eagles
John F. Murray, Jr.
Secretary: Nancy George
Members: Robert G. Britain, National Electrical Manufacturers Association (NEMA)
Warren P. Dickinson, Ion Beam Applications
Sherman Eagles, Medtronic Inc.
Christine M. Flahive, Christine M. Flahive Associates
John J. Flynn, Hill-Rom Company
Richard C. Fries, Instrumentarium USA Inc.
Larry A. Fry, Draeger Medical
Nancy George, Software Quality Management Inc.
Larry Gillum, Cardinal Health Medical Products and Services Group
Steven Gitelis, Guidant Corp.
Lori Haller, STERIS Corp.
James P. Hempel, Tyco Healthcare/US Surgical
Neil Holland, Abbott Laboratories
David R. Jones, Philips Medical Systems
Christopher Keegan, Welch Allyn Inc.
Charlie D. King, Siemens Medical Systems
Alan Kusinitz, SoftwareCPR
Bernie Liebler, Advanced Medical Technology Association (AdvaMed)
Mary Beth McDonald, St. Jude Medica
E. Paul Morozoff, Spacelabs Medic Inc
Paul Mueller, Bausch & Lomb Inc
John F. Murray, Jr., U.S. Food and Drug Administration
Harvey Rudolph, PhD, Underwriters Laboratories Inc.
Carla Sivak, Mitek/Johnson & Johnson
Christine Strysik, Baxter Healthcare Corp.
Steven D. Walter, Becton Dickinson
Gregory Whitney, CR Bard
Alternates: Christopher P. Clark, Bausch & Lomb Inc.
Brian J. Fitzgerald, U.S. Food and Drug Administration
Christopher D. Hanser, CR Bard
Florentin Kilpo, Medtronic Physio-Control
Gretel Lumley, Philips Medical Systems
David McCall, STERIS Corp.
Henri Mertz, Becton Dickinson
Carl Pantiskas, Spacelabs Medical Inc.
Raj G. Raghavendran, Ethicon Endo-Surgery/Johnson & Johnson
Robert Smith, St. Jude Medical
Fayez Sweiss, Abbott Laboratories
Donna Bea Tillman, PhD, U.S. Food and Drug Administration
Stephen Vastagh, National Electrical Manufacturers Association (NEMA)

The AAMI Medical Device Software Committee gratefully acknowledges the work of its **Software Risk Management Task Group**. At the time this document was published, the task group had the following members:

Cochairs: Paul L. Jones
Alan Kusinitz
Secretary: Annette M. Hillring
Members: Sherman Eagles, Medtronic Inc.
Lucille Ferus, SoftwareCPR
Stan Hamilton, SoftwareCPR
Annette M. Hillring, Johnson & Johnson
Paul L. Jones, U.S. Food and Drug Administration
Alan Kusinitz, SoftwareCPR
Eric Linner, Baxter Healthcare Corp.
John F. Murray, Jr., U.S. Food and Drug Administration
Brian Pate, GE Healthcare
Raj G. Raghavendran, Ethicon Endo-Surgery/Johnson & Johnson
Yves Theriault, STERIS Corp.

The AAMI Medical Device Software Committee and its Software Risk Management Task Group would like to thank the following individuals for their invaluable contribution to the development of this TIR:

Sean M. Beatty, High Impact Services Inc.
Doug Lichorwic, Northrup Grumman
David Vogel, Intertech Engineering Associates, Inc.

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

Foreword

Effective software risk management is a significant part of the overall risk management process for medical devices containing software. This technical information report (TIR) provides information useful to performing effective software risk management. It does this in the context of ANSI/AAMI/ISO 14971:2000, *Medical devices—Application of risk management to medical devices*, and in the context of ANSI/AAMI SW68:2001, *Medical device software—Software life cycle processes*.

Introduction

Software is often an integral part of medical device technology. Establishing the safety and effectiveness of a medical device containing software requires knowledge of what the software is intended to do and demonstration that the implementation of the software fulfills those intentions without causing any unacceptable risks.

Accidents are often preceded by a belief that they cannot happen. People often believe that software is designed to work properly and that testing ensures that it will work properly, despite a general recognition that neither quality nor safety can be "tested into" software. The fact is that most software testing does little more than exercise a small sampling of the software logic in all but the simplest of programs.

Ignoring the possibility of defects in software can lead to the release of medical device software that can fail in ways that affect device safety and effectiveness. This report is predicated on the notion that, as part of the software development process and general device risk management process, specific focus is required on

— identifying software's relationship to potential device hazards, both in terms of intended software functionality and the effects of potential software defects;

— identifying adequate risk control measures in terms of software and nonsoftware design; and

— verifying the implementation and effectiveness of risk control measures.

The cost of diligence in this regard is inconsequential compared to the cost of an accident in any way one would like to define cost (e.g., human, financial, legal, or regulatory exposure).

Many standards have taken the approach of having separate "safety" and "performance" standards for medical electrical equipment. This approach was a natural extension of the historical approach taken at the national and international level with other electrical equipment standards (e.g., those for consumer electronics), where basic physical safety is regulated through mandatory standards but other "performance" specifications are regulated by market pressure. In this context, one could say, "The ability of an electric kettle to boil water is not critical to its safe use!"

This is not the situation with medical devices. Responsible organizations must depend on standards to ensure effectiveness as well as basic safety. The accuracy with which the equipment controls the delivery of energy or therapeutic substances to the patient is of concern because a lack of effectiveness can become a safety issue. Likewise, the manner in which medical device software processes and displays physiological or diagnostic data is of concern because it can affect patient management. Medical authorities are equally concerned about the ability of the equipment to prevent hazards and to perform clinical functions effectively. An increasing amount of the clinical functionality of many medical devices is controlled by a software subsystem of the medical device.

Thus, it is sometimes difficult to make clear distinctions between safety and effectiveness. As such, where this report uses the term "safety," it is intended to include effectiveness in cases where the lack of effectiveness can be a safety issue.

The benefit derived by the patient must always be considered along with the risk in using a medical device. This implies that the need for protection from risk caused by the medical device differs depending on the risk to the patient of not receiving treatment, and these varying needs must be considered as part of the overall risk evaluation of the device.

Many standards and publications—national, international, and sector specific—address risk management, and others address software life cycle development processes. However, none of these documents address software system safety design issues in the context of medical device systems. Additionally, software-related aspects of medical device risk management need to be explained in software terms with software examples. The AAMI Medical Device Software Committee recognizes a need for this information and is addressing the issue by way of this technical information report.

Medical device software risk management

1 Scope

This technical information report (TIR) should be regarded as a reference for developing safe software systems to be used in medical devices. The information that it contains provides a framework within which experience, insight, and judgment are applied systematically to reduce medical device risks. The TIR does this in the context of ANSI/AAMI/ISO 14971:2000, *Medical devices—Application of risk management to medical devices*, and in the context of ANSI/AAMI SW68:2001, *Medical device software—Software life cycle processes*.

For readers to understand the scope of this document, it is important to understand the distinction between software safety and software reliability. The National Institute of Science and Technology information report [NISTIR 5589] on software hazard analysis states this distinction quite clearly:

> Software safety should not be confused with software reliability. Reliability is the ability of a system to perform its required functions under stated conditions for a specified period of time [IEEE610]. Safety is the probability that conditions (hazards) that can lead to a mishap do not occur, whether or not the intended function is performed [LEVESON86]. Reliability is interested in all possible software errors, while safety is concerned only with those errors that cause actual system hazards [LEVESON86]. . . . Software safety and software reliability are part of software quality. Quality is the degree to which a system meets specified requirements, and customer or user needs or expectations [IEEE610].

Many of the same techniques used to ensure software reliability and quality are relevant for ensuring software safety. This report does not discuss general aspects of software quality assurance.

1.1 Purpose

The goal of this TIR is to be a technical reference on risk management for medical devices. It is intended primarily for software engineers, software quality assurance personnel, and those responsible for medical device risk management. Others involved in medical device product development, quality assurance, regulatory affairs, and auditing may also find this document useful.

The report attempts to clarify process relationships outlined in ANSI/AAMI SW68:2001, *Medical device software—Software life cycle processes*, and ANSI/AAMI/ISO 14971:2000, *Medical devices—Application of risk management to medical devices*, in the context of software system safety, keeping in mind the varied interests of the audience.

Understanding the terminology and its proper context is key to understanding the associated processes. This report attempts to clarify some of those subtleties by looking at the components of risk management, and by using precise language to identify how those components relate to each other. For example, ISO definitions such as *hazard*, *harm*, and *safety* are clarified through use of additional terms and examples from a software perspective.

The report provides guidance for those new to the concepts of software system safety in the medical device industry and as an aide-memoire for medical device and software designers more familiar with the topic.

The first objective of this report is to provide those working “down in the trenches” with some insight into safety considerations when using software in a medical device. A second objective is to help risk managers understand the implications for risk management posed by the presence of software in the system. All too often, those charged with the responsibility for developing software and those charged with the responsibility of managing risk operate independently of each other. It is a goal of this report to help bridge this divide by fostering communication and a shared understanding of the relationship between software engineering and risk management.

1.2 Field of application

This TIR contains information applicable to risk management for the entire array of medical device software, including:

— Embedded software systems (e.g., glucose meter firmware)

— Stand-alone software systems (e.g., dosage calculations programs)

