American National Standard

ANSI/AAMI/IEC 80001-1:2010

Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities

Association for the Advancement of Medical Instrumentation

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...
Documents
Document Sharing Hub

Objectives and uses of AAMI standards and recommended practices

It is most important that the objectives and potential uses of an AAMI product standard or recommended practice are clearly understood. The objectives of AAMI's technical development program derive from AAMI's overall mission: the advancement of medical instrumentation. Essential to such advancement are (1) a continued increase in the safe and effective application of current technologies to patient care, and (2) the encouragement of new technologies. It is AAMI's view that standards and recommended practices can contribute significantly to the advancement of medical instrumentation, provided that they are drafted with attention to these objectives and provided that arbitrary and restrictive uses are avoided.

A voluntary *standard* for a *medical device* recommends to the manufacturer the information that should be provided with or on the product, basic safety and performance criteria that should be considered in qualifying the device for clinical use, and the measurement techniques that can be used to determine whether the device conforms with the safety and performance criteria and/or to compare the performance characteristics of different products. Some standards emphasize the information that should be provided with the device, including performance characteristics, instructions for use, warnings and precautions, and other data considered important in ensuring the safe and effective use of the device in the clinical environment. Recommending the disclosure of performance characteristics often necessitates the development of specialized test methods to facilitate uniformity in reporting; reaching consensus on these tests can represent a considerable part of committee work. When a drafting committee determines that clinical concerns warrant the establishment of *minimum* safety and performance criteria, referee tests must be provided and the reasons for establishing the criteria must be documented in the rationale.

A *recommended practice* provides guidelines for the use, care, and/or processing of a medical device or system. A recommended practice does not address device performance *per se*, but rather procedures and practices that will help ensure that a device is used safely and effectively and that its performance will be maintained.

Although a device standard is primarily directed to the manufacturer, it may also be of value to the potential purchaser or user of the device as a frame of reference for device evaluation. Similarly, even though a recommended practice is usually oriented towards healthcare professionals, it may be useful to the manufacturer in better understanding the environment in which a medical device will be used. Also, some recommended practices, while not addressing device performance criteria, provide guidelines to industrial personnel on such subjects as sterilization processing, methods of collecting data to establish safety and efficacy, human engineering, and other processing or evaluation techniques; such guidelines may be useful to health care professionals in understanding industrial practices.

In determining whether an AAMI standard or recommended practice is relevant to the specific needs of a potential user of the document, several important concepts must be recognized:

All AAMI standards and recommended practices are *voluntary* (unless, of course, they are adopted by government regulatory or procurement authorities). The application of a standard or recommended practice is solely within the discretion and professional judgment of the user of the document.

Each AAMI standard or recommended practice reflects the collective expertise of a committee of health care professionals and industrial representatives, whose work has been reviewed nationally (and sometimes internationally). As such, the consensus recommendations embodied in a standard or recommended practice are intended to respond to clinical needs and, ultimately, to help ensure patient safety. A standard or recommended practice is limited, however, in the sense that it responds generally to perceived risks and conditions that may not always be relevant to specific situations. A standard or recommended practice is an important *reference* in responsible decision-making, but it should never *replace* responsible decision-making.

Despite periodic review and revision (at least once every five years), a standard or recommended practice is necessarily a static document applied to a dynamic technology. Therefore, a standards user must carefully review the reasons why the document was initially developed and the specific rationale for each of its provisions. This review will reveal whether the document remains relevant to the specific needs of the user.

Particular care should be taken in applying a product standard to existing devices and equipment, and in applying a recommended practice to current procedures and practices. While observed or potential risks with existing equipment typically form the basis for the safety and performance criteria defined in a standard, professional judgment must be used in applying these criteria to existing equipment. No single source of information will serve to identify a particular product as "unsafe". A voluntary standard can be used as one resource, but the ultimate decision as to product safety and efficacy must take into account the specifics of its utilization and, of course, cost-benefit considerations. Similarly, a recommended practice should be analyzed in the context of the specific needs and resources of the individual institution or firm. Again, the rationale accompanying each AAMI standard and recommended practice is an excellent guide to the reasoning and data underlying its provision.

In summary, a standard or recommended practice is truly useful only when it is used in conjunction with other sources of information and policy guidance and in the context of professional experience and judgment.

INTERPRETATIONS OF AAMI STANDARDS AND RECOMMENDED PRACTICES

Requests for interpretations of AAMI standards and recommended practices must be made in writing, to the AAMI Vice President, Standards Policy and Programs. An official interpretation must be approved by letter ballot of the originating committee and subsequently reviewed and approved by the AAMI Standards Board. The interpretation will become official and representation of the Association only upon exhaustion of any appeals and upon publication of notice of interpretation in the "Standards Monitor" section of the *AAMI News*. The Association for the Advancement of Medical Instrumentation disclaims responsibility for any characterization or explanation of a standard or recommended practice which has not been developed and communicated in accordance with this procedure and which is not published, by appropriate notice, as an *official interpretation* in the *AAMI News*.

AVA Documents
Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities

Approved 14 October 2010 by
Association for the Advancement of Medical Instrumentation

Approved 6 October 2010 by
American National Standards Institute, Inc.

Abstract: This standard defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness, and data and system security.

Keywords: medical device, risk management, information technology, interoperability

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

AAMI Standard

This Association for the Advancement of Medical Instrumentation (AAMI) standard implies a consensus of those substantially concerned with its scope and provisions. The existence of an AAMI standard does not in any respect preclude anyone, whether they have approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. AAMI standards are subject to periodic review, and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This AAMI standard may be revised or withdrawn at any time. AAMI procedures require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of publication. Interested parties may obtain current information on all AAMI standards by calling or writing AAMI, or by visiting the AAMI website at www.aami.org.

All AAMI 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.

Published by

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

© 2010 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

This publication is subject to copyright claims of ISO, ANSI, and AAMI. No part of this publication may be reproduced or distributed in any form, including an electronic retrieval system, without the prior written permission of AAMI. All requests pertaining to this document should be submitted to AAMI. It is illegal under federal law (17 U.S.C. § 101, *et seq*.) to make copies of all or any part of this document (whether internally or externally) without the prior written permission of the Association for the Advancement of Medical Instrumentation. Violators risk legal action, including civil and criminal penalties, and damages of $100,000 per offense. For permission regarding the use of all or any part of this document, complete the reprint request form at www.aami.org or contact AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633. Phone: (703) 525-4890; Fax: (703) 525-1067.

Printed in the United States of America

ISBN 1–57020–400-4

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

Contents

Page

Glossary of equivalent standards v
Committee representation vii
Background of AAMI adoption of IEC 80001-1:2010 viii
FOREWORD ix
INTRODUCTION xi
1 Scope 1
2 Terms and definitions 2
3 Roles and responsibilities 7
3.1 General 7
3.2 RESPONSIBLE ORGANIZATION 7
3.3 TOP MANAGEMENT responsibilities 7
3.4 MEDICAL IT-NETWORK RISK MANAGER 9
3.5 MEDICAL DEVICE manufacturer(s) 10
3.6 Providers of other information technology 11
4 Life cycle RISK MANAGEMENT in MEDICAL IT-NETWORKS 12
4.1 Overview 12
4.2 RESPONSIBLE ORGANIZATION RISK MANAGEMENT 14
4.2.1 POLICY FOR RISK MANAGEMENT for incorporating MEDICAL DEVICES 14
4.2.2 RISK MANAGEMENT PROCESS 14
4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation 14
4.3.1 Overview 14
4.3.2 RISK-relevant asset description 15
4.3.3 MEDICAL IT-NETWORK documentation 15
4.3.4 RESPONSIBILITY AGREEMENT 16
4.3.5 RISK MANAGEMENT plan for the MEDICAL IT-NETWORK 17
4.4 MEDICAL IT-NETWORK RISK MANAGEMENT 17
4.4.1 Overview 17
4.4.2 RISK ANALYSIS 18
4.4.3 RISK EVALUATION 18
4.4.4 RISK CONTROL 18
4.4.5 RESIDUAL RISK evaluation and reporting 20
4.5 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT 21
4.5.1 CHANGE-RELEASE MANAGEMENT PROCESS 21
4.5.2 Decision on how to apply RISK MANAGEMENT 21
4.5.3 Go-live 22
4.6 Live network RISK MANAGEMENT 23
4.6.1 Monitoring 23
4.6.2 EVENT MANAGEMENT 23
5 Document control 24
5.1 Document control procedure 24
5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE 24

Documents
Document Sharing Hub

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

Annex A (informative) Rationale 25
Annex B (informative) Overview of RISK MANAGEMENT relationships 29
Annex C (informative) Guidance on field of application 30
Annex D (informative) Relationship with ISO/IEC 20000-2:2005 *Information technology – Service management – Part 2: Code of practice* 32
Bibliography 36

Figure 1 – Illustration of TOP MANAGEMENT responsibilities 9
Figure 2 – Overview of life cycle of MEDICAL IT-NETWORKS including RISK MANAGEMENT 13
Figure B.1 – Overview of roles and relationships 29
Figure D.1 – Service management processes 33

Table A.1 – Relationship between ISO 14971 and IEC 80001-1 27
Table C.1 – IT-NETWORK scenarios that can be encountered in a clinical environment 30
Table D.1 – Relationship between IEC 80001-1 and ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005 34

Documents
Document Sharing Hub

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

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. The code in the US column, "(R)20xx" indicates the year the document was officially reaffirmed by AAMI. E.g., ANSI/AAMI/ISO 10993-4:2002/(R)2009 indicates that 10993-4, originally approved and published in 2002, was reaffirmed without change in 2009.

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 60601-1:2005 Technical Corrigendum 1 and 2	ANSI/AAMI ES60601-1:2005 and ANSI/AAMI ES60601-1:2005/A2:2010 ANSI/AAMI ES60601-1:2005/C1:2009 (amdt)	Major technical variations C1 Identical to Corrigendum 1 & 2
IEC 60601-1-2:2007	ANSI/AAMI/IEC 60601-1-2:2007	Identical
IEC 60601-2-2:2009	ANSI/AAMI/IEC 60601-2-2:2009	Identical
IEC 60601-2-4:2002	ANSI/AAMI DF80:2003/(R)2010	Major technical variations
IEC 60601-2-16:2008	ANSI/AAMI/IEC 60601-2-16:2008	Identical
IEC 60601-2-19:2009	ANSI/AAMI/IEC 60601-2-19:2009	Identical
IEC 60601-2-20:2009	ANSI/AAMI/IEC 60601-2-20:2009	Identical
IEC 60601-2-21:2009	ANSI/AAMI/IEC 60601-2-21:2009	Identical
IEC 60601-2-24:1998	ANSI/AAMI ID26:2004/(R)2009	Major technical variations
IEC 60601-2-47:2001	ANSI/AAMI EC38:2007	Major technical variations
IEC 60601-2-50:2009	ANSI/AAMI/IEC 60601-2-50:2009	Identical
IEC 80001-1:2010	ANSI/AAMI/IEC 80001-1:2010	Identical
IEC 80601-2-30:2009 and Technical Corrigendum 1	ANSI/AAMI/IEC 80601-2-30:2009 and ANSI/AAMI/IEC 80601-2-30:2009/ C1:2009 (amdt) – consolidated text	Identical (with inclusion) C1 Identical to Corrigendum 1
IEC 80601-2-58:2008	ANSI/AAMI/IEC 80601-2-58:2008	Identical
IEC/TR 60878:2009	ANSI/AAMI/IEC TIR60878:2003	Identical
IEC/TR 62296:2009	ANSI/AAMI/IEC TIR62296:2009	Identical
IEC 62304:2006	ANSI/AAMI/IEC 62304:2006	Identical
IEC/TR 62348:2006	ANSI/AAMI/IEC TIR62348:2006	Identical
IEC/TR 62354:2009	ANSI/AAMI/IEC TIR62354:2009	Identical
IEC 62366:2007	ANSI/AAMI/IEC 62377:2007	Identical
IEC/TR 80002-1:2009	ANSI/IEC/TR 80002-1:2009	Identical
ISO 5840:2005	ANSI/AAMI/ISO 5840:2005/(R)2010	Identical
ISO 7198:1998	ANSI/AAMI/ISO 7198:1998/2001/(R)2010	Identical
ISO 7199:2009	ANSI/AAMI/ISO 7199:2009	Identical
ISO 8637:2010	ANSI/AAMI/ISO 8637:2010	Identical
ISO 8638:2010	ANSI/AAMI/ISO 8638:2010	Identical
ISO 10993-1:2009	ANSI/AAMI/ISO 10993-1:2009	Identical
ISO 10993-2:2006	ANSI/AAMI/ISO 10993-2:2006	Identical
ISO 10993-3:2003	ANSI/AAMI/ISO 10993-3:2003/(R)2009	Identical
ISO 10993-4:2002 and Amendment 1:2006	ANSI/AAMI/ISO 10993-4:2002/(R)2009 and Amendment 1:2006/(R)2009	Identical
ISO 10993-5:2009	ANSI/AAMI/ISO 10993-5:2009	Identical
ISO 10993-6:2007	ANSI/AAMI/ISO 10993-6:2007	Identical
ISO 10993-7:2008	ANSI/AAMI/ISO 10993-7:2008	Identical
ISO 10993-9:2009	ANSI/AAMI/ISO 10993-9:2009	Identical
ISO 10993-10:2010	ANSI/AAMI/ISO 10993-10:2010	Identical
ISO 10993-11:2006	ANSI/AAMI/ISO 10993-11:2006	Identical
ISO 10993-12:2007	ANSI/AAMI/ISO 10993-12:2007	Identical
ISO 10993-13:2010	ANSI/AAMI/ISO 10993-13:2010	Identical
ISO 10993-14:2001	ANSI/AAMI/ISO 10993-14:2001/(R)2006	Identical
ISO 10993-15:2000	ANSI/AAMI/ISO 10993-15:2000/(R)2006	Identical
ISO 10993-16:2010	ANSI/AAMI/ISO 10993-16:2010	Identical
ISO 10993-17:2002	ANSI/AAMI/ISO 10993-17:2002/(R)2008	Identical
ISO 10993-18:2005	ANSI/AAMI BE83:2006	Major technical variations
ISO/TS 10993-19:2006	ANSI/AAMI/ISO TIR10993-19:2006	Identical

Documents
Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

International designation	U.S. designation	Equivalency
ISO/TS 10993-20:2006	ANSI/AAMI/ISO TIR10993-20:2006	Identical
ISO 11135-1:2007	ANSI/AAMI/ISO 11135-1:2007	Identical
ISO/TS 11135-2:2008	ANSI/AAMI/ISO TIR11135-2:2008	Identical
ISO 11137-1:2006	ANSI/AAMI/ISO 11137-1:2006/(R)2010	Identical
ISO 11137-2:2006 (2006-08-01 corrected version)	ANSI/AAMI/ISO 11137-2:2006	Identical
ISO 11137-3:2006	ANSI/AAMI/ISO 11137-3:2006/(R)2010	Identical
ISO 11138-1: 2006	ANSI/AAMI/ISO 11138-1:2006/(R)2010	Identical
ISO 11138-2: 2006	ANSI/AAMI/ISO 11138-2:2006/(R)2010	Identical
ISO 11138-3: 2006	ANSI/AAMI/ISO 11138-3:2006/(R)2010	Identical
ISO 11138-4: 2006	ANSI/AAMI/ISO 11138-4:2006/(R)2010	Identical
ISO 11138-5: 2006	ANSI/AAMI/ISO 11138-5:2006/(R)2010	Identical
ISO/TS 11139:2006	ANSI/AAMI/ISO 11139:2006	Identical
ISO 11140-1:2005	ANSI/AAMI/ISO 11140-1:2005/(R)2010	Identical
ISO 11140-3:2007	ANSI/AAMI/ISO 11140-3:2007	Identical
ISO 11140-4:2007	ANSI/AAMI/ISO 11140-4:2007	Identical
ISO 11140-5:2007	ANSI/AAMI/ISO 11140-5:2007	Identical
ISO 11607-1:2006	ANSI/AAMI/ISO 11607-1:2006	Identical
ISO 11607-2:2006	ANSI/AAMI/ISO 11607-2:2006	Identical
ISO 11663:2009	ANSI/AAMI/ISO 11633:2009	Identical
ISO 11737-1: 2006	ANSI/AAMI/ISO 11737-1:2006	Identical
ISO 11737-2:2009	ANSI/AAMI/ISO 11737-2:2009	Identical
ISO 13408-1:2008	ANSI/AAMI/ISO 13408-1:2008	Identical
ISO 13408-2:2003	ANSI/AAMI/ISO 13408-2:2003	Identical
ISO 13408-3:2006	ANSI/AAMI/ISO 13408-3:2006	Identical
ISO 13408-4:2005	ANSI/AAMI/ISO 13408-4:2005	Identical
ISO 13408-5:2006	ANSI/AAMI/ISO 13408-5:2006	Identical
ISO 13408-6:2006	ANSI/AAMI/ISO 13408-6:2006	Identical
ISO 13485:2003	ANSI/AAMI/ISO 13485:2003/(R)2009	Identical
ISO 14155-1:2003	ANSI/AAMI/ISO 14155-1:2003/(R)2008	Identical
ISO 14155-2:2003	ANSI/AAMI/ISO 14155-2:2003/(R)2008	Identical
ISO 14160:1998	ANSI/AAMI/ISO 14160:1998/(R)2008	Identical
ISO 14161:2009	ANSI/AAMI/ISO 14161:2009	Identical
ISO 14708-3:2008	ANSI/AAMI/ISO 14708-3:2008	Identical
ISO 14708-4:2008	ANSI/AAMI/ISO 14708-4:2008	Identical
ISO 14708-5:2010	ANSI/AAMI /ISO 14708-5:2010	Identical
ISO 14937:2009	ANSI/AAMI/ISO 14937:2009	Identical
ISO/TR 14969:2004	ANSI/AAMI/ISO TIR14969:2004	Identical
ISO 14971:2007	ANSI/AAMI/ISO 14971:2007/(R)2010	Identical
ISO 15223-1:2007 and A1:2008	ANSI/AAMI/ISO 15223-1:2007 and A1:2008	Identical
ISO 15223-2:2010	ANSI/AAMI/ISO 15223-2:2010	Identical
ISO 15225:2010	ANSI/AAMI/ISO 15225:2010	Identical
ISO 15674:2009	ANSI/AAMI/ISO 15674:2009	Identical
ISO 15675:2009	ANSI/AAMI/ISO 15675:2009	Identical
ISO 15882:2008	ANSI/AAMI/ISO 15882:2008	Identical
ISO 15883-1:2006	ANSI/AAMI ST15883-1:2009	Major technical variations
ISO/TR 16142:2006	ANSI/AAMI/ISO TIR16142:2005	Identical
ISO 17664:2004	ANSI/AAMI ST81:2004	Major technical variations
ISO 17665-1:2006	ANSI/AAMI/ISO 17665-1:2006	Identical (with inclusions)
ISO/TS 17665-2:2009	ANSI/AAMI/ISO TIR17665-2:2009	Identical
ISO 18472:2006	ANSI/AAMI/ISO 18472:2006	Identical
ISO/TS 19218:2005	ANSI/AAMI/ISO 19218:2005	Identical
ISO 22442-1:2007	ANSI/AAMI/ISO 22442-1:2007	Identical
ISO 22442-2:2007	ANSI/AAMI/ISO 22442-2:2007	Identical
ISO 22442-3:2007	ANSI/AAMI/ISO 22442-3:2007	Identical
ISO 25539-1:2003 and A1:2005	ANSI/AAMI/ISO 25539-1:2003/(R)2009 and A1:2005/(R)2009	Identical
ISO 25539-2:2008	ANSI/AAMI/ISO 25539-2:2008	Identical
ISO 27186:2010	ANSI/AAMI/ISO 27186:2010	Identical
ISO 81060-1:2007	ANSI/AAMI/ISO 81060-1:2007	Identical
ISO 81060-2:2009	ANSI/AAMI/ISO 81060-2:2009	Identical

Documents Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

Committee representation

Association for the Advancement of Medical Instrumentation

Information Technology Networks Incorporating Medical Devices Committee

The adoption of IEC 80001-1 as a new American National Standard was initiated by the AAMI Information Technology Networks Incorporating Medical Devices (IT) Committee. U.S. cochairs of the AAMI IT Committee, William Hintz of Medtronic Inc and Richard Schrenker of Massachusettes General Hospital, played an active part in developing the IEC standard.

Committee approval of this document does not necessarily imply that all committee members voted for its approval.

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

Cochairs

William Hintz, Medtronic Inc.
Richard A. Schrenker, Massachusetts General Hospital (Independent Expert)

Members

Jon Camp, Philips Electronics North America
Todd Cooper, (Independent Expert)
Leanne Cordisco, GE Healthcare
Rebecca K. Crossley, CBET, (Independent Expert)
Conor Curtin, Fresenius Medical Care Renal Therapies Group
Yadin David, EdD CCE PE HCSP, (Independent Expert)
Christina DeMur, Draeger Medical Systems Inc.
Sherman Eagles, SoftwareCPR
Joseph Freitas, CareFusion
Kenneth J. Fuchs, Mindray DS USA Inc.
William Hintz, Medtronic Inc
Yimin Li, Stryker Instruments Division
Marshall Magee, Welch Allyn Inc.
Mary Beth McDonald, St Jude Medical Inc.
Sean Murphy, Lt Col, Air Force Medical Operations Agency SGALE (Independent Expert)
Kenneth Olbrish, (Independent Expert)
Tresia L. O'Shea, Getinge USA
Steven R. Rakitin, (Independent Expert)
Terrie L. Reed, FDA/CDRH
Richard A. Schrenker, Massachusetts General Hospital (Independent Expert)
Rabin Srestha, Spacelabs Medical Inc.
Micheal T. Suelzer, PhD, Baxter Healthcare Corporation
Donna-Bea Tillman, PhD, Microsoft Health Soutions Group

Alternates

Karen S. Delvecchio, GE Healthcare
Brian J. Fitzgerald, Eur Ing MIMM, FDA/CDRH
Xianyu Shea, Stryker Instruments Division
Thomas W. Schultz, Medtronic Inc.
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.

Documents
Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

Background of ANSI/AAMI adoption of IEC 80001-1:2010

As indicated in the foreword to the main body of this document (page ix), the International Electrotechnical Commission (IEC) is a worldwide federation of national standards bodies. The United States is one of the IEC members that took an active role in the development of this standard.

International standard IEC 80001-1:2010 was developed jointly by Sub-Committee IEC/SC 62A, Common aspects of electrical equipment used in medical practice and ISO/TC 215, Health informatics, to define the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security.

U.S. participation in this IEC SC is organized through the U.S. Technical Advisory Group for IEC/SC 62A administered by the Advanced Medical Technology Association (AdvaMed) on behalf of the American National Standards Institute. AAMI administers the International Secretariat for IEC/SC 62A on behalf of the United States, and U.S. experts made a considerable contribution to this International Standard.

AAMI encourages its committees to harmonize their work with International Standards in the area of risk management of information technology as it relates to medical devices. The AAMI Information Technology Networks Incorporating Medical Devices (IT) Committee together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed IEC 80001-1 to formulate the U.S. position and comments while the document was being developed. This close collaboration helped gain widespread U.S. consensus on the document. As the U.S. Technical Advisory Group for IEC/SC 62A, AdvaMed granted AAMI permission to consider adoption of IEC 80001-1 as a new American national Standard. Following AAMI procedures, the AAMI IT Committee voted to adopt the IEC international standard as written.

AAMI and ANSI procedures require that standards be reviewed every five years and, if necessary, revised to reflect technological advances that may have occurred since publication.

AAMI (and ANSI) have adopted other IEC and ISO standards. See the Glossary of Equivalent Standards for a list of IEC and ISO standards adopted by AAMI, which gives the corresponding U.S. designation and the level of equivalency with the IEC and ISO standard.

The concepts incorporated in this standard should not be considered inflexible or static. This standard, like any other, must be reviewed and updated periodically to assimilate progressive technological developments. To remain relevant, it must be modified as technological advances are made and as new data comes to light.

Suggestions for improving this standard are invited. Comments and suggested revisions should be sent to Standards Department, AAMI, 4301 N. Fairfax Dr. Suite 301, Arlington, VA 22203-1633.

NOTE—Beginning with the foreword on page ix, this American National Standard is identical to IEC 80001-1:2010.

© 2010 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC 80001-1:2010

Documents
Document Sharing Hub

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 1: Roles, responsibilities and activities

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.

International Standard IEC 80001-1 has been prepared by a joint working group of 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 standard.

The text of this standard is based on the following documents:

FDIS	Report on voting
62A/703/FDIS	62A/718/RVD

Documents
Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 17 P-members out of 18 having cast a vote.

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

Terms defined in Clause 2 of this standard are printed in SMALL CAPITALS.

For the purposes of this standard:

- "shall" means that compliance with a requirement is mandatory for compliance with this standard;
- "should" means that compliance with a requirement is recommended but is not mandatory for compliance with this standard;
- "may" is used to describe a permissible way to achieve compliance with a requirement; and
- "establish" means to define, document, and implement.

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 web site 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.

IMPORTANT – The 'color inside' logo on the cover page of this publication indicates that it contains colors which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a color printer.

Documents Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

INTRODUCTION

An increasing number of MEDICAL DEVICES are designed to exchange information electronically with other equipment in the user environment, including other MEDICAL DEVICES. Such information is frequently exchanged through an information technology network (IT-NETWORK) that also transfers data of a more general nature.

At the same time, IT-NETWORKS are becoming increasingly vital to the clinical environment and are now required to carry increasingly diverse traffic, ranging from life-critical patient data requiring immediate delivery and response, to general corporate operations data and to email containing potential malicious content (e.g. viruses).

For many jurisdictions, design and production of MEDICAL DEVICES is subject to regulation, and to standards recognized by the regulators. Traditionally, regulators direct their attention to MEDICAL DEVICE manufacturers, by requiring design features and by requiring a documented PROCESS for design and manufacturing. MEDICAL DEVICES cannot be placed on the market in these jurisdictions without evidence that those requirements have been met.

The use of the MEDICAL DEVICES by clinical staff is also subject to regulation. Members of clinical staff have to be appropriately trained and qualified, and are increasingly subject to defined PROCESSES designed to protect patients from unacceptable RISK.

In contrast, the incorporation of MEDICAL DEVICES into IT-NETWORKS in the clinical environment is a less regulated area. IEC 60601-1:2005 [1][1)] requires MEDICAL DEVICE manufacturers to include some information in ACCOMPANYING DOCUMENTS if the MEDICAL DEVICE is intended to be connected to an IT-NETWORK. Standards are also in place covering common information technology activities including planning, design and maintenance of IT-NETWORKS, for instance ISO 20000-1:2005 [9]. However, until the publication of this standard, no standard addressed how MEDICAL DEVICES can be connected to IT-NETWORKS, including general-purpose IT-NETWORKS, to achieve INTEROPERABILITY without compromising the organization and delivery of health care in terms of SAFETY, EFFECTIVENESS, and DATA AND SYSTEM SECURITY.

There remain a number of potential problems associated with the incorporation of MEDICAL DEVICES into IT-NETWORKS, including:

– lack of consideration for RISK from use of IT-NETWORKS during evaluation of clinical RISK;
– lack of support from manufacturers of MEDICAL DEVICES for the incorporation of their products into IT-NETWORKS, (e.g. the unavailability or inadequacy of information provided by the manufacturer to the OPERATOR of the IT-NETWORK);
– incorrect operation or degraded performance (e.g. incompatibility or improper configuration) resulting from combining MEDICAL DEVICES and other equipment on the same IT-NETWORK;
– incorrect operation resulting from combining MEDICAL DEVICE SOFTWARE and other software applications (e.g. open email systems or computer games) in the same IT-NETWORK;
– lack of security controls on many MEDICAL DEVICES; and
– the conflict between the need for strict change control of MEDICAL DEVICES and the need for rapid response to the threat of cyberattack.

When these problems manifest themselves, unintended consequences frequently follow.

---

1) Numbers in square brackets refer to the Bibliography.

Documents
Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

This standard is addressed to RESPONSIBLE ORGANIZATIONS, to manufacturers of MEDICAL DEVICES, and to providers of other information technology.

This standard adopts the following principles as a basis for its normative and informative sections:

– The incorporation or removal of a MEDICAL DEVICE or other components in an IT-NETWORK is a task which requires design of the action; this might be out of the control of the manufacturer of the MEDICAL DEVICE.

– RISK MANAGEMENT should be used before the incorporation of a MEDICAL DEVICE into an IT-NETWORK takes place, and for any changes during the entire life cycle of the resulting MEDICAL IT-NETWORK, to avoid unacceptable RISKS, including possible RISK to patients, resulting from the incorporation of the MEDICAL DEVICE into the IT-NETWORK. Many things are part of a RISK decision, such as liability, cost, or impact on mission. These should be considered in determining acceptable RISK in addition to the requirements described in this standard.

– Aspects of removal, maintenance, change or modification of equipment, items or components should be addressed adequately in addition to the incorporation of MEDICAL DEVICES.

– The manufacturer of the MEDICAL DEVICE is responsible for RISK MANAGEMENT of the MEDICAL DEVICE during the design, implementation, and manufacturing of the MEDICAL DEVICE. This standard does not cover the RISK MANAGEMENT PROCESS for the MEDICAL DEVICE.

– The manufacturer of a MEDICAL DEVICE intended to be incorporated into an IT-NETWORK might need to provide information about the MEDICAL DEVICE that is necessary to allow the RESPONSIBLE ORGANIZATION to manage RISK according to this standard. This information can include, as part of the ACCOMPANYING DOCUMENTS, instructions specifically addressed to the person who incorporates a MEDICAL DEVICE into an IT-NETWORK.

– Such ACCOMPANYING DOCUMENTS should convey instructions about how to incorporate the MEDICAL DEVICE into the IT-NETWORK, how the MEDICAL DEVICE transfers information over the IT-NETWORK, and the minimum IT-NETWORK characteristics necessary to enable the INTENDED USE of the MEDICAL DEVICE when it is incorporated into the IT-NETWORK. The ACCOMPANYING DOCUMENTS should warn of possible hazardous situations associated with failure or disruptions of the IT-NETWORK, and the misuse of the IT-NETWORK connection or of the information that is transferred over the IT-NETWORK.

– RESPONSIBILITY AGREEMENTS can establish roles and responsibilities among those engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK, all aspects of the life cycle of the resulting MEDICAL IT-NETWORK and all activities that form part of that life cycle.

– The RESPONSIBLE ORGANIZATION is required to appoint people to certain roles defined in this standard. This standard defines the responsibilities of those roles. The most important of those roles is the MEDICAL IT-NETWORK RISK MANAGER. This role can be assigned to someone within the RESPONSIBLE ORGANIZATION or to an external contractor.

– The MEDICAL IT-NETWORK RISK MANAGER is responsible for ensuring that RISK MANAGEMENT is included during the PROCESSES of:

  - planning and design of new incorporations of MEDICAL DEVICES or changes to such incorporations;
  - putting the MEDICAL IT-NETWORK into use and the consequent use of the MEDICAL IT-NETWORK; and
  - CHANGE-RELEASE MANAGEMENT and change management of the IT-NETWORK during the IT-NETWORK'S entire life cycle.

© 2010 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC 80001-1:2010
Documents Document Sharing Hub

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

– RISK MANAGEMENT should be applied to address the following KEY PROPERTIES appropriate for the IT-NETWORK incorporating a MEDICAL DEVICE:

- SAFETY (freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment);
- EFFECTIVENESS (ability to produce the intended result for the patient and the RESPONSIBLE ORGANIZATION); and
- DATA AND SYSTEM SECURITY (an operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability).

Documents
Document Sharing Hub
AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...

© 2010 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC 80001-1:2010

Documents
Document Sharing Hub

AAMI
Single user license only. Copying, networking, and distribution prohibited.
Full document details: ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsi...