

Technical Information Report

ANSI/AAMI/ IEC TIR80001- 2-1:2012

Application of risk
management for IT-networks
incorporating medical
devices — Part 2-1: Step by
step risk management of
medical IT-networks; Practical
applications and examples

Application of risk management for IT-networks incorporating medical devices — Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples

Approved 20 July 2012 by
Association for the Advancement of Medical Instrumentation

Approved 2 September 2012 by
American National Standards Institute, Inc.

Abstract: Step-by-step guide to help in the application of risk management when creating or changing a medical IT-network.

Keywords: medical device, risk management, information technology, interoperability, IT-network

Published by

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

© 2012 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: +1-703-525-4890; Fax: +1-703-525-1067.

Printed in the United States of America

ISBN 1-57020-454-3

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 Technical Report

This AAMI TIR has been registered by the American National Standards Institute as an ANSI Technical Report.

Publication of this ANSI Technical Report has been approved by the accredited standards developer (AAMI). This document is registered as a Technical Report series of publications 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.....	vii
Committee representation.....	x
Background of AAMI adoption of IEC/TR 80001-2-1:2012.....	xi
FOREWORD	xii
INTRODUCTION	xiv
1 Scope	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Prerequisites.....	7
5 Study of terms used in RISK MANAGEMENT	7
5.1 Overview.....	7
5.2 HAZARDS	8
5.3 HAZARDOUS SITUATIONS.....	8
5.4 Foreseeable sequences of events and causes	9
5.5 UNINTENDED CONSEQUENCE	9
5.6 RISK CONTROL measures (mitigations)	10
5.7 Degrees of RISK.....	11
5.8 Checking wording	11
6 The steps	12
6.1 Overview of the steps	12
6.2 A basic example using the 10 steps	12
6.2.1 General.....	12
6.2.2 Initial RISK – Steps 1 – 5 (Figure 2)	12
6.2.3 RISK CONTROL and final RISK – Steps 6 – 10 (Figure 3)	13
7 IEC 80001-1:2010, Subclause 4.4: Step by step	16
7.1 General.....	16
7.2 Application of Subclause 4.4.1: Document all RISK MANAGEMENT elements.....	16
7.3 Note about RISK EVALUATION	16
7.4 The 10-step PROCESS	16
7.4.1 STEP 1: Identify HAZARDS and HAZARDOUS SITUATIONS	16
7.4.2 STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS	17
7.4.3 STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential severities	18
7.4.4 STEP 4: Estimate the probability of UNINTENDED CONSEQUENCE.....	18
7.4.5 STEP 5: Evaluate RISK	19
7.4.6 STEP 6: Identify and document proposed RISK CONTROL measures and re-evaluate RISK (return to Step 3).....	20
7.4.7 STEP 7: Implement RISK CONTROL measures	21
7.4.8 STEP 8: Verify RISK CONTROL measures	21
7.4.9 STEP 9: Evaluate any new RISKS arising from RISK CONTROL.....	22
7.4.10 STEP 10: Evaluate and report overall RESIDUAL RISK	23
7.5 The steps and their relationship to IEC 80001-1 and ISO 14971.....	23

8	Practical examples	25
8.1	General.....	25
8.2	Example 1: Wireless PATIENT monitoring during PATIENT transport	25
8.2.1	Full description of context	25
8.2.2	Description of network under analysis	25
8.2.3	The 10 Steps.....	25
8.3	Example 2: Remote ICU / Distance medicine	28
8.3.1	Full description of context	28
8.3.2	Description of network under analysis	28
8.3.3	The 10 Steps.....	28
8.4	Example 3: Post Anesthesia Care Unit (PACU)	31
8.4.1	Full description of context	31
8.4.2	Description of network under analysis	31
8.4.3	The 10 Steps.....	32
8.5	Example 4: Ultrasound – Operating system (OS) vulnerability	37
8.5.1	Full description of context	37
8.5.2	Description of network under analysis	37
8.5.3	The 10 Steps.....	37
	Annex A (informative) Common HAZARDS, HAZARDOUS SITUATIONS, and causes to consider in MEDICAL IT-NETWORKS	41
	Annex B (informative) List of questions to consider when identifying HAZARDS of the MEDICAL IT-NETWORK	46
	Annex C (informative) Layers of MEDICAL IT-NETWORKS where errors can be found	47
	Annex D (informative) Probability, severity, and RISK acceptability scales used in the examples in this technical report	50
	Annex E (informative) MONITORING RISK mitigation effectiveness	53
	Annex F (informative) RISK ANALYZING small changes in a MEDICAL IT-NETWORK	56
	Annex G (informative) Example of Change Window Form	57
	Annex H (informative) Template for examples	58
	Bibliography	60
	Figure 1 – Basic flow of concepts from HAZARD to HAZARDOUS SITUATION to UNINTENDED CONSEQUENCE	8
	Figure 2 – Steps 1 – 5: HAZARD identification through RISK EVALUATION	13
	Figure 3 – Steps 6 – 10: RISK CONTROL measures through overall RESIDUAL RISK	14
	Figure 4 – Sample summary RISK ASSESSMENT register format	15
	Figure 5 – Relation of cause to HARM.....	19
	Figure 6 – Schematic of the post anesthesia care unit (PACU)	32
	Figure 7 – Example of the use of color coding cables	35
	Figure 8 – Sample summary RISK ASSESSMENT register for the PACU example.....	36
	Figure D.1 – Application of STEPs 5 and 6 with 3 levels of RISK acceptability	52
	Figure F.1 – Overview of RISK ANALYZING small changes in a MEDICAL IT-NETWORK	56

Table 1 – Relationship of KEY PROPERTIES, SAFETY, EFFECTIVENESS and DATA AND SYSTEMS SECURITY with associated UNINTENDED CONSEQUENCE as used in this technical report	10
Table 2 – Methods for checking accurate and appropriate wording of causes, HAZARDOUS SITUATIONS, and UNINTENDED CONSEQUENCES	11
Table 3 – Relationship between this technical report, IEC 80001-1:2010 and ISO 14971:2007	24
Table A.1 – HAZARDS related to potential required network characteristics	43
Table A.2 – Relationship between HAZARDS, foreseeable sequences, and causes	44
Table A.3 – Relationship between HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS	45
Table C.1 – Layers of a MEDICAL IT-NETWORK	47
Table C.2 – Example of the layers of a MEDICAL IT-NETWORK	49
Table D.1 – Probability scales used in the examples in this technical report	50
Table D.2 – Severity scales	50
Table D.3 – RISK level matrix	51

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 IEC 60601-1:2005/A1:2012 IEC Technical Corrigendum 1 and 2	ANSI/AAMI ES60601-1:2005/(R)2012 ANSI/AAMI ES60601-1:2005/A1:2012 ANSI/AAMI ES60601-1:2005/C1:2009/(R)2012 (amdt) ANSI/AAMI ES60601-1:2005/A2:2010/(R)2012	Major technical variations A1 identical C1 identical to Corrigendum 1 & 2 A2 applies to AAMI, only
IEC 60601-1-11:2010	ANSI/AAMI HA60601-1-11:2011	Major technical variations
IEC 60601-1-2:2007	ANSI/AAMI/IEC 60601-1-2:2007/(R)2012	Identical
IEC 60601-2-2:2009	ANSI/AAMI/IEC 60601-2-2:2009	Identical
IEC 60601-2-4:2010	ANSI/AAMI/IEC 60601-2-4:2010	Identical
IEC 60601-2-16:2012	ANSI/AAMI/IEC 60601-2-16:2012	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 60601-2-25:2011	ANSI/AAMI/IEC 60601-2-25:2011	Identical
IEC 60601-2-27:2011	ANSI/AAMI/IEC 60601-2-27:2011	Identical
IEC 60601-2-47:2012	ANSI/AAMI/IEC 60601-2-47:2012	Identical
IEC 60601-2-50:2009	ANSI/AAMI/IEC 60601-2-50:2009	Identical
IEC/TR 60878:2009	ANSI/AAMI/IEC TIR60878:2003	Identical
IEC/TR 61289:2011	ANSI/AAMI/IEC TIR61289:2011	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 62366:2007	Identical
IEC 80001-1:2010	ANSI/AAMI/IEC 80001-1:2010	Identical
IEC/TR 80001-2-1:2012	ANSI/AAMI/IEC 80001-2-1:2012	Identical
IEC/TR 80001-2-2:2012	ANSI/AAMI/IEC 80001-2-2:2012	Identical
IEC/TR 80001-2-3:2012	ANSI/AAMI/IEC 80001-2-3:2012	Identical
IEC/TR 80002-1:2009	ANSI/IEC/TR 80002-1:2009	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
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 and Amendment 1:2012	ANSI/AAMI/ISO 7199:2009 and Amendment 1:2012	Identical
ISO 8637:2010	ANSI/AAMI/ISO 8637:2010	Identical
ISO 8638:2010	ANSI/AAMI/ISO 8638:2010	Identical

International designation	U.S. designation	Equivalency
ISO 10993-1:2009	ANSI/AAMI/ISO 10993-1:2009	Identical
ISO 10993-2:2006	ANSI/AAMI/ISO 10993-2:2006/(R)2010	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/(R)2010	Identical
ISO 10993-7:2008	ANSI/AAMI/ISO 10993-7:2008/(R)2012	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/(R)2010	Identical
ISO 10993-12:2012	ANSI/AAMI/ISO 10993-12:2012	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/(R)2011	Major technical variations
ISO/TS 10993-19:2006	ANSI/AAMI/ISO TIR10993-19:2006	Identical
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 11137-2:2012	ANSI/AAMI/ISO 11137-2:2012	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/(R)2012	Identical
ISO 11140-4:2007	ANSI/AAMI/ISO 11140-4:2007/(R)2012	Identical
ISO 11140-5:2007	ANSI/AAMI/ISO 11140-5:2007/(R)2012	Identical
ISO 11607-1:2006	ANSI/AAMI/ISO 11607-1:2006/(R)2010	Identical
ISO 11607-2:2006	ANSI/AAMI/ISO 11607-2:2006/(R)2010	Identical
ISO 11658:2012	ANSI/AAMI/ISO 11658:2012	Identical
ISO 11663:2009	ANSI/AAMI/ISO 11663:2009	Identical
ISO 11737-1:2006	ANSI/AAMI/ISO 11737-1:2006	Identical
ISO 11737-2:2009	ANSI/AAMI/ISO 11737-2:2009	Identical
ISO/TS 12417:2011	ANSI/AAMI/ISO TIR12417:2011	Identical
ISO 13022:2012	ANSI/AAMI/ISO 13022:2012	Identical
ISO 13408-1:2008	ANSI/AAMI/ISO 13408-1:2008/(R)2011	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

International designation	U.S. designation	Equivalency
ISO 13408-7:2012	ANSI/AAMI/ISO 13408-7:2012	Identical
ISO 13485:2003	ANSI/AAMI/ISO 13485:2003/(R)2009	Identical
ISO 13958:2009	ANSI/AAMI/ISO 13958:2009	Identical
ISO 13959:2009	ANSI/AAMI/ISO 13959:2009	Identical
ISO 14155:2011	ANSI/AAMI/ISO 14155:2011	Identical
ISO 14160:2011	ANSI/AAMI/ISO 14160:2011	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 15223-1:2012	ANSI/AAMI/ISO 15223-1:2012	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 and A2:2012	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/(R)2010	Identical
ISO/TS 19218-1:2011	ANSI/AAMI/ISO TIR19218:2011	Identical
ISO 20857:2010	ANSI/AAMI/ISO 20857:2010	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/TR 22442-4:2010	ANSI/AAMI/ISO TIR22442-4:2010	Identical
ISO 23500:2011	ANSI/AAMI/ISO 23500:2011	Identical
ISO/TS 23810:2012	ANSI/AAMI/ISO TIR23810:2012	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 25539-3:2011	ANSI/AAMI/ISO 25539-3:2011	Identical
ISO 26722:2009	ANSI/AAMI/ISO 26722:2009	Identical
ISO 27185:2012	ANSI/AAMI/ISO 27185:2012	Identical
ISO 27186:2010	ANSI/AAMI/ISO 27186:2010	Identical
ISO 80369-1:2010	ANSI/AAMI/ISO 80369-1:2010	Identical
ISO 81060-1:2007	ANSI/AAMI/ISO 81060-1:2007	Identical
ISO 81060-2:2009	ANSI/AAMI/ISO 81060-2:2009	Identical

Committee representation

Association for the Advancement of Medical Instrumentation

Information Technology Working Group

The adoption of IEC/TR 80001-2-1 as a new AAMI/IEC Technical Information Report was initiated by the AAMI Information Technology Working Group. U.S. cochair of AAMI/SM/WG 02, William Hintz of Medtronic, Inc. and Richard Schrenker of Massachusetts General Hospital, played an active part in developing the IEC Technical Report.

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

Cochairs: William Hintz, Medtronic Inc. WHQ Campus
Richard A. Schrenker, Massachusetts General Hospital

Members: John T. Collins, MSEE, American Society for Healthcare Engineering
Todd Cooper, 80001 Experts (Independent Expert)
Rebecca K. Crossley, CBET, Susquehanna Health System (Independent Expert)
Conor Curtin, Fresenius Medical Care Renal Therapies Group
Yadin David, EdD CCE PE HCSP, Biomedical Engineering Consultants LLC (Independent Expert)
Karen S. Delvecchio, GE Healthcare
Christina DeMur, Draeger Medical Systems Inc.
Sherman Eagles, SoftwareCPR
Donald J. Fournier, Draeger Medical Systems Inc.
Joseph Freitas, CareFusion
Kenneth J. Fuchs, Mindray DS USA Inc.
George W. Gray, Fluidnet Corporation
Thomas Grobaski, Belimed Inc
William Hintz, Medtronic Inc. WHQ Campus
Yimin Li, Stryker Instruments Division
Marshall Magee, Welch Allyn Inc.
Jared Mauldin, Integrated Medical Systems
Mary Beth McDonald, St Jude Medical Inc.
Tresia L. O'Shea, Getinge USA
Geoffrey A. Pascoe, MSCCS BEE GSEC, (Independent Expert)
Steven R. Rakitin, Software Quality Consulting (Independent Expert)
Terrie L. Reed, MSIE, FDA/CDRH
Richard A. Schrenker, Massachusetts General Hospital
Bob Steurer, Spacelabs Medical Inc.
Micheal T. Suelzer, PhD, Baxter Healthcare Corporation
Donna-Bea Tillman, PhD, (Independent Expert)
Daidi Zhong, PhD, Chongqing University (Independent Expert)

Alternates: James Dundon, Spacelabs Medical Inc.
Brian J. Fitzgerald, Eur Ing MIMM, FDA/CDRH
Thomas W. Schultz, Medtronic Inc WHQ Campus
Xianyu Shea, Stryker Instruments Division
Fei Wang, Fresenius Medical Care Renal Therapies Group

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.

Background of ANSI/AAMI adoption of IEC/TR 80001-2-1:2012

As indicated in the foreword to the main body of this document (page xii), 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 technical report.

International technical report IEC/TR 80001-2-1:2012 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 Technical Report.

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 Working Group together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed IEC/TR 80001-2-1 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/TR 80001-2-1 as a new AAMI Technical Information Report. Following AAMI procedures, the AAMI Information Technology Working Group voted to adopt the IEC technical report as written.

AAMI (and ANSI) have adopted other IEC and ISO documents. 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 technical information report should not be considered inflexible or static. This technical information report, 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.

As used within the context of this document, "should" indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action should be avoided but is not prohibited. "May" is used to indicate that a course of action is permissible within the limits of the technical information report. "Can" is used as a statement of possibility and capability. Finally, "must" is used only to describe "unavoidable" situations, including those mandated by government regulation.

NOTE—This technical information report is not a standard and the material contained herein is not normative in nature. The committee has in a few places used the term "shall" based on their knowledge of requirements contained in relevant standards and/or regulatory requirements.

Suggestions for improving this document 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 IEC foreword on page xii, this AAMI Technical Information Report is identical to IEC/TR 80001-2-1:2012.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

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 cooperation 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 80001-2-1, which is a technical report, 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.

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

Enquiry draft	Report on voting
62A/782/DTR	62A/803/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.

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.

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.

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

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.

INTRODUCTION

This technical report is a step-by-step guide to help in the application of RISK MANAGEMENT when creating or changing a MEDICAL IT-NETWORK. It provides easy to apply steps, examples, and information helping in the identification and control of RISKS. All relevant requirements in IEC 80001-1:2010 are addressed and links to other clauses and subclauses of IEC 80001-1 are addressed where appropriate (e.g. handover to release management and monitoring).

This technical report focuses on practical RISK MANAGEMENT. It is not intended to provide a full outline or explanation of all requirements that are satisfactorily covered by IEC 80001-1.

This step-by-step guidance follows a 10-step PROCESS that follows subclause 4.4 of IEC 80001-1:2010, which *specifically* addresses RISK ANALYSIS, RISK EVALUATION and RISK CONTROL. These activities are embedded within the full life cycle RISK MANAGEMENT PROCESS. They can never be the first step, as RISK MANAGEMENT follows the general PROCESS model which sets planning before any action.

For the purpose of this technical report, “prerequisites” as stated in subclause 1.3 are considered to be in place before execution of the 10 steps. Also, it is well understood that all steps outlined in this technical report should have been performed before any new MEDICAL IT-NETWORK can go live or before proceeding with a change to an existing MEDICAL IT-NETWORK. It is emphasized that subclause 4.5 of IEC 80001-1:2010 “CHANGE RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT” explicitly includes and applies to new MEDICAL IT-NETWORKS, as well as changes to existing networks.

This technical report will be useful to those responsible for or part of a team executing RISK MANAGEMENT when changing or creating (as the ultimate change) a MEDICAL IT-NETWORK. MEDICAL DEVICES in the context of IEC 80001 refer to those MEDICAL DEVICES that connect to a network.

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

Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

1 Scope

This technical report provides step-by-step information to aid RESPONSIBLE ORGANIZATIONS in implementation of the RISK MANAGEMENT PROCESS required by IEC 80001-1. Specifically, it details the steps involved in executing subclause 4.4 of IEC 80001-1:2010 and provides guidance in the form of a study of RISK MANAGEMENT terms, RISK MANAGEMENT steps, an explanation of each step, step-by-step examples, templates, and lists of HAZARDS and causes to consider.

The steps outlined within this technical report are considered to be universally applicable. Application of these steps can be scaled as described within this document.

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*

3 Terms and definitions

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

3.1

CHANGE PERMIT

an outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT activities subject to specified constraints

[SOURCE: IEC 80001-1:2010, definition 2.3]

3.2

CHANGE RELEASE MANAGEMENT

PROCESS that ensures that all changes to the IT-NETWORK are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with CONFIGURATION MANAGEMENT

[SOURCE: IEC 80001-1:2010, definition 2.2]

3.3

CONFIGURATION MANAGEMENT

PROCESS that ensures that configuration information of components and the IT-NETWORK are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the IT-NETWORK

[SOURCE: IEC 80001-1:2010, definition 2.4]

3.4

DATA AND SYSTEMS SECURITY

operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

[SOURCE: IEC 80001-1:2010, definition 2.5, modified – two notes integral to understanding the scope of the definition in the original document have been deleted.]

3.5

EFFECTIVENESS

ability to produce the intended result for the PATIENT and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, definition 2.6]

3.6

ELECTROMAGNETIC INTERFERENCE

EMI

any electromagnetic phenomenon that may degrade the performance of a device, equipment, or system

[SOURCE: IEC 60601-1-2:2007, definition 3.5, modified – the term has been changed, an abbreviation added and the note to the original definition removed.]

3.7

EVENT MANAGEMENT

PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner

[SOURCE: IEC 80001-1:2010, definition 2.7]

3.8

HARM

physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEMS SECURITY

[SOURCE: IEC 80001-1:2010, definition 2.8]

3.9

HAZARD

potential source of HARM

[SOURCE: IEC 80001-1:2010, definition 2.9]

3.10

HAZARDOUS SITUATION

circumstance in which people, property, or the environment are exposed to one or more HAZARD(s)

[SOURCE: ISO 14971:2007, definition 2.4]

3.11

HEALTH DATA

PRIVATE DATA that indicates physical or mental health

Note 1 to entry: This generically defines PRIVATE DATA and its subset, HEALTH DATA, within this document to permit users of this document to adapt it easily to different privacy compliance laws and regulations. For example, in Europe, the requirements might be taken and references changed to "Personal Data" and "Sensitive Data"; in the USA, HEALTH DATA might be changed to "Protected Health Information (PHI)" while making adjustments to text as necessary.

[SOURCE: IEC 80001-2-2:2012, definition 3.7]

3.12

INTENDED USE

use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the MANUFACTURER

[SOURCE: IEC 80001-1:2010, definition 2.10]

3.13

INTEROPERABILITY

property permitting diverse systems or components to work together for a specified purpose

[SOURCE: IEC 80001-1:2010, definition 2.11]

3.14

INFORMATION TECHNOLOGY

IT

technology (computer systems, networks, software) used to PROCESS, store, acquire and distribute information

3.15

IT-NETWORK

INFORMATION TECHNOLOGY NETWORK

system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

[SOURCE: IEC 80001-1:2010, definition 2.12, modified – the two notes to the original definition have not been retained.]

3.16

KEY PROPERTIES

three RISK managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

[SOURCE: IEC 80001-1:2010, definition 2.13]

3.17

LOCAL AREA NETWORK

LAN

computer network covering a small physical area, such as a home or office, or small group of buildings, such as a school or an airport

3.18

MANUFACTURER

natural or legal person with responsibility for the design, manufacture, packaging, or labeling of a MEDICAL DEVICE, assembling a system, or adapting a medical device before it is placed on the market or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party

[SOURCE: ISO 14971:2007, definition 2.8, modified – Note 1 to the original definition, which provides pertinent information, has not been retained.]

3.19

MEDICAL DEVICE

any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

- a) intended by the MANUFACTURER to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
 - diagnosis, prevention, monitoring, treatment or alleviation of disease,
 - diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
 - investigation, replacement, modification, or support of the anatomy or of a physiological PROCESS,
 - supporting or sustaining life,
 - control of conception,
 - disinfection of MEDICAL DEVICES,
 - providing information for medical or diagnostic purposes by means of *in vitro* examination of specimens derived from the human body; and
- b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry: Products which may be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:

- aids for disabled/handicapped people;
- devices for the treatment/diagnosis of diseases and injuries in animals;
- accessories for medical devices (see Note 3 to entry);
- disinfection substances;
- devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by MANUFACTURERS to be used together with a “parent” medical device to enable that medical device to achieve its intended purpose should be subject to the same GHTF procedures as apply to the medical device itself. For example, an accessory will be classified as though it is a medical device in its own right. This may result in the accessory having a different classification than the “parent” device.

Note 4 to entry: Components to medical devices are generally controlled through the MANUFACTURER’S quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a “medical device”.

[SOURCE: IEC 80001-1:2010, definition 2.14]

3.20

MEDICAL IT-NETWORK

IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, definition 2.16]

3.21

MONITORING

ongoing review of all RISK MANAGEMENT activities and RISK CONTROL options that were put in place to achieve acceptable RISK in the use of MEDICAL IT-NETWORK(S).

3.22

OPERATOR

person handling equipment

[SOURCE: IEC 80001-1:2010, definition 2.18]

3.23

PATIENT

individual awaiting or under medical care and treatment

3.24

PROCESS

set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: IEC 80001-1:2010, definition 2.19]

3.25

QUALITY OF SERVICE

QoS

the capability or means of providing differentiated levels of networking performance in terms of traffic engineering (packet delay, loss, jitter, bit rate) to different data flows.

3.26

RESIDUAL RISK

RISK remaining after RISK CONTROL measures have been taken

[SOURCE: IEC 80001-1:2010, definition 2.20]

3.27

RESPONSIBILITY AGREEMENT

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

[SOURCE: IEC 80001-1:2010, definition 2.21, modified – a note to the original definition, containing examples, has not been retained.]

3.28

RESPONSIBLE ORGANIZATION

RO

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

[SOURCE: IEC 80001-1:2010, definition 2.22, modified – a note to the original definition, containing examples, has not been retained.]

3.29

RISK

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

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

3.30

RISK ANALYSIS

systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, definition 2.24]

3.31

RISK ASSESSMENT

overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, definition 2.25]

3.32

RISK CONTROL

PROCESS in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[SOURCE: IEC 80001-1:2010, definition 2.26]

3.33

RISK EVALUATION

PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

[SOURCE: IEC 80001-1:2010, definition 2.27]

3.34

RISK MANAGEMENT

systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and MONITORING RISK

[SOURCE: IEC 80001-1:2010, definition 2.28]

3.35

RISK MANAGEMENT FILE

set of records and other documents that are produced by RISK MANAGEMENT

[SOURCE: IEC 80001-1:2010, definition 2.29]

3.36

SAFETY

freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

[SOURCE: IEC 80001-1:2010, definition 2.30]

3.37

TOP MANAGEMENT

person or group of people who direct(s) and control(s) the RESPONSIBLE ORGANIZATION accountable for a MEDICAL IT-NETWORK at the highest level

[SOURCE: IEC 80001-1:2010, definition 2.31]

3.38

UNINTENDED CONSEQUENCE

UC

unwanted and negative outcome of an event that results in one or more degraded KEY PROPERTIES

3.39

VERIFICATION

confirmation through provision of objective evidence that specified requirements have been fulfilled

Note 1 to entry: The term “verified” is used to designate the corresponding status.

Note 2 to entry: Confirmation can comprise activities such as:

- performing alternative calculations;
- comparing a new design specification with a similar proven design specification;

- undertaking tests and demonstrations; and
- reviewing documents prior to issue.

Note 3 to entry: In design and development, VERIFICATION concerns the PROCESS of examining the result of a given activity to determine conformity with the stated requirement for that activity.

[SOURCE: IEC 80001-1:2010, definition 2.32]

4 Prerequisites

Before beginning the steps outlined within this technical report, the requirements in subclauses 3.1 to 4.3 of IEC 80001-1:2010 need to be completed. Additionally, the RESPONSIBLE ORGANIZATION (RO) must be prepared to meet the requirements in subclauses 4.5 through 5.2. For example, the RISK MANAGEMENT policy and PROCESSES are in place; the RISK MANAGEMENT plan is complete; any required RESPONSIBILITY AGREEMENTS are in place; probability, severity, and RISK acceptability scales are defined.

For RISK MANAGEMENT of any system to proceed, the system must be defined. In the case of MEDICAL IT-NETWORKS, the network under analysis must be well defined and can already contain some existing controls. This will be important in Steps 3 and 4. For new MEDICAL IT-NETWORKS, this can be a preliminary design.

In addition to defining the system under analysis, fundamental information regarding RO specific use, needs, and concerns are needed in order to complete the RISK estimation. This is referred to as “context” of use and includes information such as:

- acuity of PATIENTS;
- clinical workflow;
- clinical staffing and competencies;
- INTENDED USE/clinical or business use case; and
- clinical and business criticality of the systems/applications using the network.

The steps described in this report will generally be executed by a team of individuals within the RESPONSIBLE ORGANIZATION. It is recommended to have representation from multiple departments, including IT, biomedical engineering, clinical, and RISK MANAGEMENT. The makeup of the team should align with existing structures within the organization.

5 Study of terms used in RISK MANAGEMENT

5.1 Overview

RISK MANAGEMENT is a very large field of study. This technical report provides an introduction to this subject with examples that can be undertaken with minimal knowledge. It provides step by step instructions for undertaking a RISK ASSESSMENT PROCESS.

IEC 80001-1 provides a RISK MANAGEMENT philosophy. As there are several RISK MANAGEMENT philosophies available, this one might or might not be completely in line with RISK MANAGEMENT approaches and techniques already in place at the RO. The RO should consider taking appropriate steps to reconcile the differences in methodology and terminology.

Figure 1 shows the basic flow of concepts from HAZARD to HAZARDOUS SITUATION to UNINTENDED CONSEQUENCE.