Technical Information Report

ANSI/AAMI/IEC TIR80002-1:2009

Medical device software - Part 1: Guidance on the application of ISO 14971 to medical device software

Association for the Advancement of Medical Instrumentation

AVA Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

Medical device software - Part 1: Guidance on the application of ISO 14971 to medical device software

Approved 3 September 2009 by
Association for the Advancement of Medical Instrumentation

Registered 26 October 2009 by
American National Standards Institute

Abstract: Provides information useful for the performance of effective software risk management, as part of the overall risk management process for medical devices containing software. It does this in the context of ISO 14971:2007, Medical devices - Application of risk management to medical devices and in the context of ISO/IEC 62304:2006, Medical device software - Software life cycle processes.

Keywords: risk management, software life cycle, medical device software

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

Published by

Association for the Advancement of Medical Instrumentation
1110 N. Glebe Road, Suite 220
Arlington, VA 22201-4795
www.aami.org

© 2009 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, 1110 N. Glebe Road, Suite 220, Arlington, VA 22201-4795. Phone: (703) 525-4890; Fax: (703) 525-1067.

Printed in the United States of America

ISBN 1-57020-371-7

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

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 might 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 might 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.

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 the content of this document should be sent to AAMI, Attn: Standards Department, 1110 N. Glebe Road, Suite 220, Arlington, VA 22201-4795.

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

Contents

Page

Glossary of equivalent standards vi
Committee representation viii
Background of AAMI adoption of IEC TIR8002-1:2009 x
FOREWORD xi
INTRODUCTION xiii
1 General 1
1.1 Scope 1
1.2 Normative references 2
2 Terms and definitions 2
3 General requirements for RISK MANAGEMENT 3
3.1 RISK MANAGEMENT PROCESS 3
3.2 Management responsibilities 7
3.3 Qualification of personnel 8
3.4 RISK MANAGEMENT plan 10
3.5 RISK MANAGEMENT FILE 12
4 RISK ANALYSIS 14
4.1 RISK ANALYSIS PROCESS 14
4.2 INTENDED USE and identification of characteristics related to the SAFETY of the MEDICAL DEVICE 15
4.3 Identification of HAZARDS 17
4.4 Estimation of the RISK(S) for each HAZARDOUS SITUATION 19
5 RISK EVALUATION 22
6 RISK CONTROL 23
6.1 RISK reduction 23
6.2 RISK CONTROL option analysis 23
6.3 Implementation of RISK CONTROL measure(s) 33
6.4 RESIDUAL RISK EVALUATION 34
6.5 RISK/benefit analysis 34
6.6 RISKS arising from RISK CONTROL measures 35
6.7 Completeness of RISK CONTROL 35
7 Evaluation of overall residual risk acceptability 36
8 Risk management report 37
9 Production and POST-PRODUCTION information 38
Annex A (informative) Discussion of definitions 40
Annex B (informative) Examples of software causes 42
Annex C (informative) Potential software-related pitfalls 52
Annex D (informative) Life-cycle/risk management grid 57

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

Annex E (informative) SAFETY cases 60
Bibliography 61
Index 62
Index of defined terms 63

Figure 1 – Pictorial representation of the relationship of HAZARD, sequence of events, HAZARDOUS SITUATION and HARM – from ISO 14971:2007 Annex E 21
Figure 2 – FTA showing RISK CONTROL measure which prevents incorrect software outputs from causing HARM 25
Figure A.1 – Relationship between sequence of events, HARM and HAZARD 40

Table 1 – Requirements for documentation to be included in the RISK MANAGEMENT FILE in addition to ISO 14971:2007 requirements 13
Table A.1 – Relationship between HAZARDS, foreseeable sequences of events, HAZARDOUS SITUATIONS and the HARM that can occur 41
Table B.1 – Examples of causes by software function area 42
Table B.2 – Examples of software causes that can introduce side-effects 48
Table B.3 – Methods to facilitate assurance that RISK CONTROL methods are likely to perform as intended 51
Table C.1 – Potential software-related pitfalls to avoid 52
Table D.1 – LIFE-CYCLE/RISK MANAGEMENT grid 57

Documents
Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

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 60601-1:2005	ANSI/AAMI ES60601-1:2005	Major technical variations
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	Major technical variations
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 80601-2-30:2009	ANSI/AAMI/IEC 80601-2-30:2009	Identical (with inclusion)
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 80002-1:2009	ANSI/IEC/TR 80002-1:2009	Identical
ISO 5840:2005	ANSI/AAMI/ISO 5840:2005	Identical
ISO 7198:1998	ANSI/AAMI/ISO 7198:1998/2001/(R)2004	Identical
ISO 7199:2009	ANSI/AAMI/ISO 7199:2009	Identical
ISO 8637:2004	ANSI/AAMI RD16:2007	Major technical variations
ISO 8638:2004	ANSI/AAMI RD17:2007	Major technical variations
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 10993-9:1999	ANSI/AAMI/ISO 10993-9:1999/(R)2005	Identical
ISO 10993-10:2002 and Amendment 1:2006	ANSI/AAMI BE78:2002/(R)2008 ANSI/AAMI BE78:2002/A1:2006/(R)2008	Minor technical variations Identical
ISO 10993-11:2006	ANSI/AAMI/ISO 10993-11:2006	Identical
ISO 10993-12:2007	ANSI/AAMI/ISO 10993-12:2007	Identical
ISO 10993-13:1998	ANSI/AAMI/ISO 10993-13:1999/(R)2004	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 10993-16:1997	ANSI/AAMI/ISO 10993-16:1997/(R)2009	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
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	Identical

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80002-1-2009

International designation	U.S. designation	Equivalency
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	Identical
ISO 11138-1: 2006	ANSI/AAMI/ISO 11138-1:2006	Identical
ISO 11138-2: 2006	ANSI/AAMI/ISO 11138-2:2006	Identical
ISO 11138-3: 2006	ANSI/AAMI/ISO 11138-3:2006	Identical
ISO 11138-4: 2006	ANSI/AAMI/ISO 11138-4:2006	Identical
ISO 11138-5: 2006	ANSI/AAMI/ISO 11138-5:2006	Identical
ISO/TS 11139:2006	ANSI/AAMI/ISO 11139:2006	Identical
ISO 11140-1:2005	ANSI/AAMI/ISO 11140-1:2005	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 11737-1: 2006	ANSI/AAMI/ISO 11737-1:2006	Identical
ISO 11737-2:1998	ANSI/AAMI/ISO 11737-2:1998	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	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 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	Identical
ISO 15223-1:2007 and A1:2008	ANSI/AAMI/ISO 15223-1:2007 and A1:2008	Identical
ISO 15225:2000 and A1:2004	ANSI/AAMI/ISO 15225:2000/(R)2006 and A1:2004/(R)2006	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 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

Full document details: ANSI AAMI IEC TIR80002-1-2009

Committee representation

Association for the Advancement of Medical Instrumentation

Medical Device Software Committee

The adoption of IEC Technical Report 80002-1:2009 as an AAMI Technical Information Report and ANSI Technical Report was initiated by the AAMI Medical Device Software Committee and the AAMI Quality Management Committee. Committee approval of the technical report 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: Michael L. Bendel, Spacelabs Medical
Theresa Dennis, Sterigenics International
Sean Develin, Devrose Systems
Andrew Dunham, PhD, Baxter Healthcare
Sherman Eagles, Software CPR, Winchester, MA
Christine M. Flahive, Chris Flahive Associates, Belle Mead, NJ
Nancy George, Software Quality Management Inc., Towson, MD
Ron Gerner, Abbott Laboratories
Steve Gitelis, Guidant Corporation
Lori Haller, Steris Corporation
James P. Hempel, Tyco Healthcare
Jinhua Huang, GE Healthcare
Sam Jarrell, CerTech
Jeremy Jensen, Boston Scientific Corporation
Marty J. King, Hospira Inc.
Patty Krantz, Medtronic Inc.
Bernie Liebler, Advanced Medical Technology Association (AdvaMed)
Don Lin, PhD, Irvine, CA
Steve Mallory, Welch Allyn Inc.
Angela Mariani, Smiths Medical
Mark Maritch, Datascope Patient Monitoring
Don McAndrews, Respironics
Mary Beth McDonald, St. Jude Medical Inc.
John F. Murray, Jr., U.S. Food and Drug Administration
Geoffrey A. Pascoe, Philips Healthcare
Raj Raghavendran, Johnson & Johnson
Bill Riley, Hill-Rom Company
Harvey Rudolph, PhD, Underwriters Laboratories Inc.
Richard A. Schrenker, Massachusetts General Hospital, Boston, MA
Xianyu Shea, Stryker Instrument Corporation
Carla Sivak, Edwards LifeSciences
Bob Strecker, Draeger Medical Systems Inc.
Stephen Vastagh, National Electrical Manufacturers Association (NEMA)
Ann Vu, Bausch & Lomb Inc.
David W. Walker, Independent Expert
John Walz. Independent Expert
Gregory Whitney, CR Bard

Alternates: Aziz Bhai, Hill-Rom Company
Christopher P. Clark, Bausch & Lomb Inc.
Rich Eaton, Medical Imaging & Technology Alliance (MITA)
Kenneth J. Fuchs, Draeger Medical Systems Inc.

Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80002-1-2009

Christopher D. Ganser, CR Bard
Jeff Gilham, Spacelabs Medical Inc.
Steve Hellstrom, Hospira Inc.
Gene Kelly, CerTech
Joshua Kim, Welch Allyn Inc.
Yimin Li, Stryker Medical Division
Don McAndrews, Philips Healthcare
David Michel, Steris Corporation
Dewey Phan, Becton Dickinson
Rodney Rasmussen, Abbott Laboratories
Miguel Rodriguez, Johnson & Johnson
Robert Smith, St. Jude Medical
Donna-Bea Tillman, PhD, U.S. Food and Drug Administration

At the time this document was published, the **AAMI Quality Management Committee** had the following members:

Chair: Charles B. Sidebottom
Carol L. Herman

Members: Leighton W. Hansel, Abbott Laboratories
Carol L. Herman, U.S. Food and Drug Administration
Ed R. Kimmelman, BME, JD, Independent Expert
David Osborn, Philips Healthcare
Harvey Rudolph, PhD, Underwriters Laboratories
Charles B. Sidebottom, PE, Medtronic Inc.
Kimberly A. Trautman, PhD, U.S. Food and Drug Administration
Al Van Houdt, Spacelabs Medical Inc.

Alternates: David J. Geraghty, Spacelabs Medical Inc.
Sherry Leichtweis, Abbott Laboratories
Luann M. Pendy, Medtronic Inc.
Kimberly A. Trautman, U.S. Food and Drug Administration

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

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80002-1-2009

Background on AAMI adoption of IEC/TR 80002-1:2009

The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). 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 80002-1 was developed by a Joint Working Group of Subcommittee (SC) 62A, Common aspects of electrical equipment used in medical practice, of IEC Technical Committee (TC) 62, Electrical equipment in medical practice, and ISO Technical Committee (TC) 210, Quality management and corresponding general aspects for medical devices.

U.S. participation in IEC/SC 62A 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 United States National Committee, which is a committee of the American National Standards Institute (ANSI). AAMI administers the International Secretariat for IEC/SC 62A on behalf of the United States as well as the U.S. Technical Advisory Group and International Secretariat for ISO/TC 210.

AAMI encourages its committees to harmonize their work with international documents as much as possible. The AAMI Medical Device Software Committee, together with the U.S. Technical Advisory Groups for IEC/SC 62A and ISO/TC 210, reviewed IEC/TS 80002-1 to formulate the U.S. position and comments while the document was being developed. As the U.S. Technical Advisory Group for IEC/SC 62A, the lead committee, AdvaMed granted AAMI permission to consider adoption of IEC/TR 80002-1, First Edition, as a new AAMI TIR. Following AAMI procedures, the AAMI Medical Device Software Committee voted to adopt the IEC Technical Report as written.

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 come to light.

Suggestions for improving this technical information report are invited. Comments and suggested revisions should be sent to Standards Department, AAMI, 1110 N. Glebe Road, Suite 220, Arlington, VA 22201-4795.

NOTE—Beginning with the foreword on page xi, this AAMI Technical Information Report is identical to IEC/TR 80002-1:2009.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

MEDICAL DEVICE SOFTWARE –

Part 1: Guidance on the application of ISO 14971 to medical device software

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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 80002-1, 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 210: Quality management and corresponding general aspects for MEDICAL DEVICES.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

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

Enquiry draft	Report on voting
62A/639A/DTR	62A/664/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table. In ISO, the technical report has been approved by 16 P-members out of 17 having cast a vote.

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

In this technical report the following print types are used:

- requirements and definitions: in roman type.
- informative material appearing outside of tables, such as notes, examples and references: in smaller type. Normative text of tables is also in a smaller type.
- TERMS USED THROUGHOUT THIS TECHNICAL REPORT THAT HAVE BEEN DEFINED IN CLAUSE 2 AND ALSO GIVEN IN THE INDEX: IN SMALL CAPITALS.

A list of all parts of the IEC 80002 series, published under the general title *Medical device software,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

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 fulfils those intentions without causing any unacceptable RISKS.

It is important to understand that software is not itself a HAZARD, but software may contribute to HAZARDOUS SITUATIONS. Software should always be considered in a SYSTEM perspective and software RISK MANAGEMENT cannot be performed in isolation from the SYSTEM.

Complex software designs can permit complex sequences of events which may contribute to HAZARDOUS SITUATIONS. Much of the TASK of software RISK MANAGEMENT consists of identifying those sequences of events that can lead to a HAZARDOUS SITUATION and identifying points in the sequences of events at which the sequence can be interrupted, preventing HARM or reducing its probability.

Software sequences of events which contribute to HAZARDOUS SITUATIONS may fall into two categories:

a) sequences of events representing unforeseen software responses to inputs (errors in specification of the software);

b) sequences of events arising from incorrect coding (errors in implementation of the software).

These categories are specific to software, arising from the difficulty of correctly specifying and implementing a complex SYSTEM and the difficulty of completely verifying a complex SYSTEM.

Since it is very difficult to estimate the probability of software ANOMALIES that could contribute to HAZARDOUS SITUATIONS, and since software does not fail randomly in use due to wear and tear, the focus of software aspects of RISK ANALYSIS should be on identification of potential software functionality and ANOMALIES that could result in HAZARDOUS SITUATIONS – not on estimating probability. RISKS arising from software ANOMALIES need most often to be evaluated on the SEVERITY of the HARM alone.

RISK MANAGEMENT is always a challenge and becomes even more challenging when software is involved. The following clauses contain additional details regarding the specifics of software and provide guidance for understanding ISO 14971:2007 in a software perspective.

- **Organization of the technical report**

This technical report is organized to follow the structure of ISO 14971:2007 and guidance is provided for each RISK MANAGEMENT activity in relation to software.

There is some intentional REDUNDANCY in the information provided due to the iterative nature of RISK MANAGEMENT activities in the software LIFE-CYCLE.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

Documents
Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80002-1-2009

MEDICAL DEVICE SOFTWARE –

Part 1: Guidance on the application of ISO 14971 to medical device software

1 General

1.1 Scope

This technical report provides guidance for the application of the requirements contained in ISO 14971:2007, *Medical devices— Application of risk management to medical devices* to MEDICAL DEVICE SOFTWARE with reference to IEC 62304:2006, *Medical device software—Software life cycle processes*. It does not add to, or otherwise change, the requirements of ISO 14971:2007 or IEC 62304:2006.

This technical report is aimed at RISK MANAGEMENT practitioners who need to perform RISK MANAGEMENT when software is included in the MEDICAL DEVICE/SYSTEM, and at software engineers who need to understand how to fulfill the requirements for RISK MANAGEMENT addressed in ISO 14971.

ISO 14971, recognized worldwide by regulators, is widely acknowledged as the principal standard to use when performing MEDICAL DEVICE RISK MANAGEMENT. IEC 62304:2006, makes a normative reference to ISO 14971 requiring its use. The content of these two standards provides the foundation for this technical report.

It should be noted that even though ISO 14971 and this technical report focus on MEDICAL DEVICES, this technical report may be used to implement a SAFETY RISK MANAGEMENT PROCESS for all software in the healthcare environment independent of whether it is classified as a MEDICAL DEVICE.

This technical report does not address:

– areas already covered by existing or planned standards, e.g. alarms, usability engineering, networking, etc.;
– production or quality management system software; or
– software development tools.

This technical report is not intended to be used as the basis of regulatory inspection or certification assessment activities.

For the purposes of this technical report, “should” is used to indicate that amongst several possibilities to meet a requirement, one is recommended as being particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. This term is not to be interpreted as indicating requirements.

© 2009 Association for the Advancement of Medical Instrumentation ■ ANSI/AAMI/IEC 80002-1:2009

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

1.2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62304:2006, *Medical device software – Software life cycle processes*

ISO 14971:2007, *Medical devices – Application of risk management to medical devices*

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 14971:2007, IEC 62304:2006 and the following terms and definitions apply.

NOTE An index of defined terms is found beginning on page 63.

2.1
DIVERSITY
a form of REDUNDANCY in which the redundant elements use different (diverse) components, technologies or methods to reduce the probability that all of the elements fail simultaneously due to a common cause

2.2
REDUNDANCY
provision of multiple components or mechanisms to achieve the same function such that failure of one or more of the components or mechanisms does not prevent the performance of the function

2.3
SAFETY-RELATED SOFTWARE
software that can contribute to a HAZARDOUS SITUATION or software used in the implementation of RISK CONTROL measures

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

3 General requirements for RISK MANAGEMENT

3.1 RISK MANAGEMENT PROCESS

3.1.1 General

Text of ISO 14971:2007

3 General requirements for RISK MANAGEMENT

3.1 RISK MANAGEMENT PROCESS

The MANUFACTURER shall establish, document and maintain throughout the LIFE-CYCLE an ongoing PROCESS for identifying HAZARDS associated with a MEDICAL DEVICE, estimating and evaluating the associated RISKS, controlling these RISKS, and monitoring the effectiveness of the controls. This PROCESS shall include the following elements:

- RISK ANALYSIS;
- RISK EVALUATION;
- RISK CONTROL;
- production and POST-PRODUCTION information.

Where a documented product realization PROCESS exists, such as that described in Clause 7 of ISO 13485:2003 [1][1], it shall incorporate the appropriate parts of the RISK MANAGEMENT PROCESS.

NOTE 1 A documented quality management system PROCESS can be used to deal with SAFETY in a systematic manner, in particular to enable the early identification of HAZARDS and HAZARDOUS SITUATIONS in complex MEDICAL DEVICES and systems.

NOTE 2 A schematic representation of the RISK MANAGEMENT PROCESS is shown in Figure 1. Depending on the specific LIFE-CYCLE phase, individual elements of RISK MANAGEMENT can have varying emphasis. Also, RISK MANAGEMENT activities can be performed iteratively or in multiple steps as appropriate to the MEDICAL DEVICE. Annex B contains a more detailed overview of the steps in the RISK MANAGEMENT PROCESS.

Compliance is checked by inspection of appropriate documents.

---

1) Figures in square brackets refer to the Bibliography.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

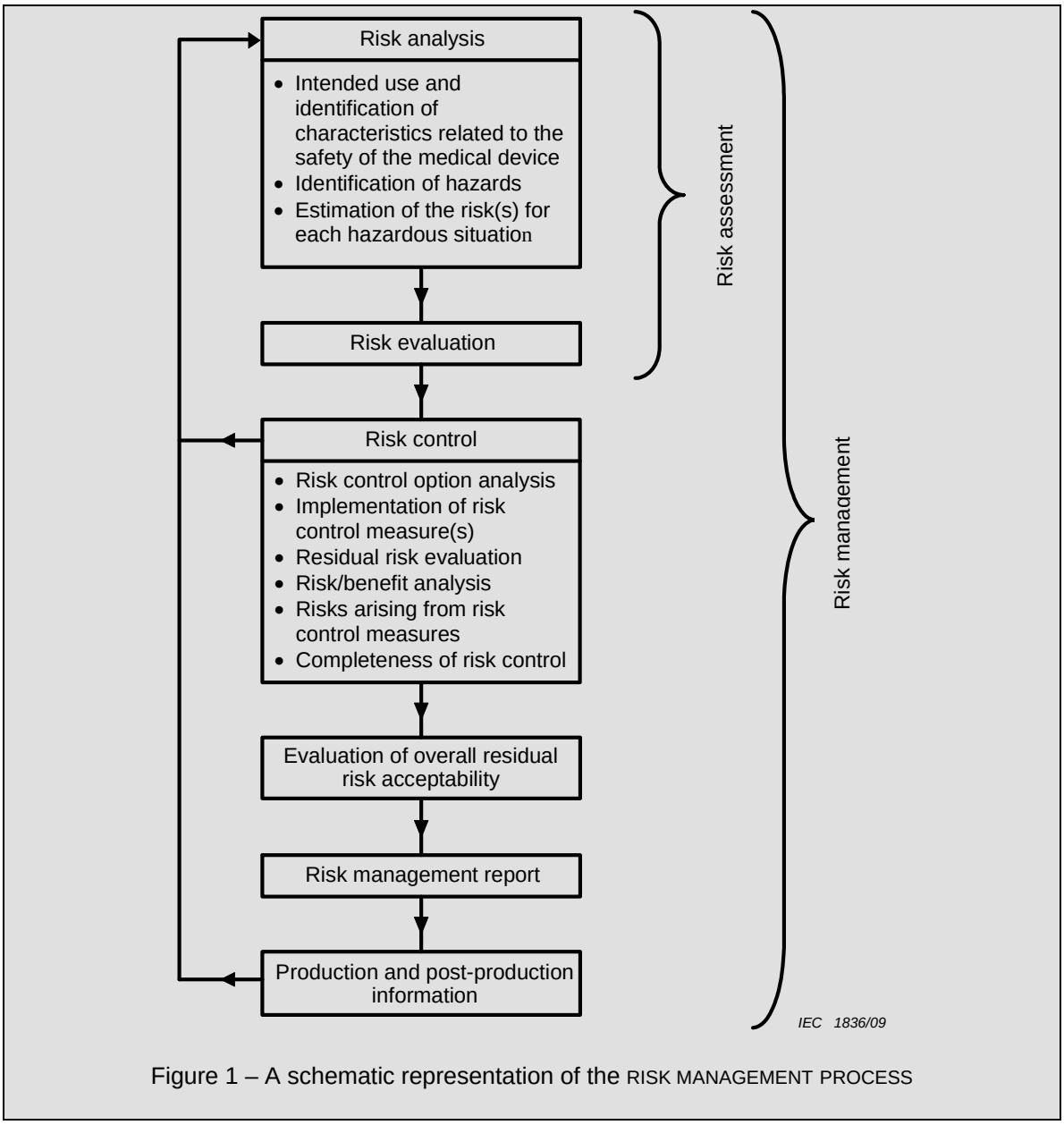

Figure 1 – A schematic representation of the RISK MANAGEMENT PROCESS

SAFETY is a property of the SYSTEM (in this case the whole MEDICAL DEVICE), which can include software. RISK MANAGEMENT should be performed on the SYSTEM comprising the software and its whole hardware environment. Software RISK MANAGEMENT activities should not be conducted in isolation from the SYSTEM.

While software aspects of RISK MANAGEMENT can not be effectively performed in isolation from overall MEDICAL DEVICE RISK MANAGEMENT, there are activities that may be best performed by software engineers as an integral part of the software LIFE-CYCLE. There are also elements of software that require more focus and different explanation than that provided in ISO 14971:2007 for overall MEDICAL DEVICE RISK MANAGEMENT. It is important to stress that even the software aspects of RISK MANAGEMENT need to focus on the MEDICAL DEVICE RISK in order to be effective.

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80002-1-2009

NOTE 1 Software aspects of RISK MANAGEMENT can not be effectively performed in isolation from overall MEDICAL DEVICE RISK MANAGEMENT because of the interdependence of hardware failures, software failures, and hardware and software RISK CONTROL measures.

NOTE 2 For instance all software failures are systematic not random (as many types of hardware failures/breakdowns are) and their probability can not be accurately estimated. Therefore, the way in which the probability component of RISK is applied to software is quite different. See 4.4.3.

There are many opportunities for software engineers to contribute to the overall SAFETY of the MEDICAL DEVICE during the early stages of MEDICAL DEVICE design. The role of software in the SAFETY of the MEDICAL DEVICE should be considered before the SYSTEM design is finalized.

By participating in the MEDICAL DEVICE design PROCESS, the software engineer can contribute to SAFETY-related decisions concerning software-related RISKS as the design evolves. Such decisions should include but not be limited to:

- the provision of adequate hardware resources to support the software;
- the partitioning of functions between hardware and software;
- the intended use of the whole MEDICAL DEVICE and the intended use of the software user interfaces;
- the avoidance of unnecessarily complex software.

3.1.2 Iteration

Typical software development LIFE-CYCLES often use iteration. The use of iteration allows:

- investigation of the feasibility of different software designs;
- development of different SOFTWARE ITEMS at different times;
- staged delivery of different VERSIONS of the software;
- correction of errors made during the software development PROCESS.

IEC 62304:2006 requires iteration of RISK MANAGEMENT activities and coordination with SYSTEM design activities throughout the software LIFE-CYCLE. For example, during software development, Subclause 5.2.4 of IEC 62304:2006 requires the re-evaluation of the MEDICAL DEVICE RISK ASSESSMENT when software requirements are established. This re-evaluation may cause an update to SYSTEM requirement specifications and the MEDICAL DEVICE RISK ASSESSMENT. RISK EVALUATION should be repeated at all stages from requirements via ARCHITECTURE and design to the implementation of software.

ISO 14971 does not prescribe a design and development PROCESS, and it generally only requires RISK MANAGEMENT steps to be done before and after (not during) the implementation of the design (including RISK CONTROL measures). For example, when a RISK CONTROL measure has been implemented, ISO 14971 requires that it be reviewed to ensure that it has not caused any further HAZARDS and HAZARDOUS SITUATIONS. This should not be interpreted as an instruction to perform this review only after the implementation is complete—it is advantageous to address any further HAZARDS as soon as they become apparent. This implies iteration within the implementation of the RISK CONTROL measure.

It is important that all DELIVERABLES are kept consistent at all times. Iteration is a threat to the consistency of DELIVERABLES. It is therefore important that rigorous configuration management be used to ensure that all effects of a change are identified and all relevant DELIVERABLES are updated after a change. This is particularly important if software is involved, since software can be changed rapidly and an apparently small change can have unexpected side effects. All information related to the software needs to be up to date in order to avoid miscommunication

Documents Document Sharing Hub
Full document details: ANSI AAMI IEC TIR80002-1-2009

between engineers. Proposals for software changes are examined for side-effects, especially side-effects which affect SAFETY. This may lead to repetition of parts of the RISK MANAGEMENT PROCESS.

3.1.3 Pro-active or reactive design approach to SAFETY

RISK MANAGEMENT should begin early with substantial input to the MEDICAL DEVICE specification, taking SAFETY into consideration in early design phases, i.e. a pro-active design approach is preferable to a reactive design approach. With a pro-active approach, SAFETY is considered along with other customer needs and captured as early SAFETY requirements. While a reactive approach is sometimes unavoidable (for example when a legacy product is updated), the proactive approach is usually the most effective, quickest and cheapest way to achieve a safe MEDICAL DEVICE.

The advantages of a pro-active SAFETY design are:

– from the outset the SYSTEM specification not only includes what the MEDICAL DEVICE should do but also identifies the SYSTEM behaviors that should be avoided in order to reduce the RISK;

– from the outset a SYSTEM ARCHITECTURE can be planned that can be demonstrated to provide the desired features while avoiding or preventing unsafe states;

– as the ARCHITECTURE is elaborated into a full design, RISK CONTROL measures can be developed while avoiding rework;

– the choice of SAFETY approaches and RISK CONTROL measures can be made early (for example, inherent SAFETY by design can be maximized and information for SAFETY minimized).

3.1.4 Characteristics of safe SYSTEMS incorporating software

Highly desirable characteristics of safe SYSTEMS include:

– the use of simple hardware SAFETY mechanisms to avoid excessive demands on SAFETY-RELATED SOFTWARE ITEMS;

– the use of only very simple SAFETY-RELATED SOFTWARE ITEMS;

– the distribution of SAFETY-RELATED SOFTWARE ITEMS between a number of independent processors;

– sufficient hardware to run all SAFETY-RELATED SOFTWARE when needed and without contention;

– the use of a deterministic design of software timing;

– the appropriate handling of failure conditions, for example

  - warning the user of failures and to allow opportunities for informed intervention;
  - providing reduced functionality in failure conditions;
  - shutting down safely when possible in failure conditions;
  - recovering quickly from failures;

– the means of preventing software code from being modified in its execution environment either through self-modification or as the result of data input;

– the means of detecting and/or preventing corruption of SAFETY-related data.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

3.2 Management responsibilities

Text of ISO 14971:2007

3.2 Management responsibilities

TOP MANAGEMENT shall provide evidence of its commitment to the RISK MANAGEMENT PROCESS by:
- ensuring the provision of adequate resources

and
- ensuring the assignment of qualified personnel (see 3.3) for RISK MANAGEMENT.

TOP MANAGEMENT shall:

- define and document the policy for determining criteria for RISK acceptability; this policy shall ensure that criteria are based upon applicable national or regional regulations and relevant International Standards, and take into account available information such as the generally accepted state of the art and known stakeholder concerns;
- review the suitability of the RISK MANAGEMENT PROCESS at planned intervals to ensure continuing effectiveness of the RISK MANAGEMENT PROCESS and document any decisions and actions taken; if the MANUFACTURER has a quality management system in place, this review may be part of the quality management system review.

NOTE The documents can be incorporated within the documents produced by the MANUFACTURER'S quality management system and these documents can be referenced in the RISK MANAGEMENT FILE.

Compliance is checked by inspection of the appropriate documents.

Both ISO 14971:2007 and IEC 62304:2006 assume that a quality management system is in place. The RISK MANAGEMENT requirements for TOP MANAGEMENT are listed in Subclause 3.2 of ISO 14971:2007.

NOTE Subclause 3.1 of ISO 14971:2007 states that RISK MANAGEMENT can be an integral part of a quality management system and Subclause 4.1 of IEC 62304:2006 states that the demonstration of the MANUFACTURER'S ability to consistently meet customer requirements and applicable regulatory requirements can be by the use of a quality management system that complies with ISO 13485 or a quality management system required by national regulation. IEC 62304:2006 also provides guidance on the provisions of Subclause 4.1 in Annex B.4, stating that it is necessary to establish RISK MANAGEMENT as an integral part of a quality management system as an overall framework for the application of appropriate software engineering methods and techniques.

TOP MANAGEMENT is responsible for putting in place the necessary organizational structure, adequate resources, accountability, and training (see 3.3) for an effective RISK MANAGEMENT PROCESS as well as for the safe design and maintenance of MEDICAL DEVICE SOFTWARE.

A MANUFACTURER may consider outsourcing software development or maintenance PROCESS activities (e.g. design, implementation, testing, or maintenance). In these situations, TOP MANAGEMENT is still fully responsible for ensuring that appropriate RISK MANAGEMENT activities occur for outsourced software development or maintenance PROCESSES activities and also ensuring that RISK CONTROL measures are appropriately applied.

When software development is outsourced, MANUFACTURERS should ensure by suitable contractual agreements that they will have sufficient control of the software and its design to ensure the performance of all RISK MANAGEMENT required by ISO 14971, during the whole LIFE-CYCLE of the MEDICAL DEVICE, including the correction of software ANOMALIES after the software has been released.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009

The MANUFACTURER should consider setting performance requirements on suppliers (see Subclause 7.4 of ISO 13485 [1] for supplier control), such as requiring the supplier to demonstrate:

– effective RISK MANAGEMENT by compliance to ISO 14971;

– effective software engineering practices by compliance to IEC 62304;

– ability to provide MEDICAL DEVICE SOFTWARE that consistently meets customer requirements and applicable regulatory requirements.

If there are RISK CONTROL measures applied to outsourced PROCESSES or products, the RISK CONTROL measures and their importance should be documented and clearly communicated to the supplier within a contractual agreement.

3.3 Qualification of personnel

3.3.1 General

Text of ISO 14971:2007

3.3 Qualification of personnel

Persons performing RISK MANAGEMENT tasks shall have the knowledge and experience appropriate to the tasks assigned to them. These shall include, where appropriate, knowledge and experience of the particular MEDICAL DEVICE (or similar MEDICAL DEVICES) and its use, the technologies involved or RISK MANAGEMENT techniques. Appropriate qualification RECORDS shall be maintained.

NOTE RISK MANAGEMENT tasks can be performed by representatives of several functions, each contributing their specialist knowledge.

Compliance is checked by inspection of the appropriate RECORDS.

Team members involved in the development and maintenance of the SOFTWARE SYSTEM should have the knowledge and experience appropriate to the TASKS assigned to them. It is fundamental that the person assigned to TASKS with RISK MANAGEMENT implications has the required knowledge of RISK MANAGEMENT. The involvement of a multidisciplinary team, including clinical experts (such as clinical support and technical service experts, and experts on other relevant subjects), software engineers, SYSTEM designers, experts on usability/human factors engineering, and domain experts, and the degree and type of their interaction with the software engineering and test staff should also be considered with respect to RISK MANAGEMENT.

This may require the development of a training program for the individuals to ensure full understanding of the required activities.

Also, the qualification of the member in the RISK MANAGEMENT team with respect to software should be considered and may require special training.

The following subclauses should provide an overview of the field of required knowledge which should be considered.

Documents Document Sharing Hub

Full document details: ANSI AAMI IEC TIR80002-1-2009