IEC/TR 80002-1

Edition 1.0 2009-09

TECHNICAL REPORT

colour inside

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

IEC/TR 80002-1:2009(E)

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

IEC/TR 80002-1

Edition 1.0 2009-09

TECHNICAL REPORT

colour inside

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XB

ICS 11.040.01

ISBN 2-8318-1061-9

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 General 7
1.1 Scope 7
1.2 Normative references 7
2 Terms and definitions 8
3 General requirements for RISK MANAGEMENT 8
3.1 RISK MANAGEMENT PROCESS 8
3.2 Management responsibilities 11
3.3 Qualification of personnel 13
3.4 RISK MANAGEMENT plan 14
3.5 RISK MANAGEMENT FILE 16
4 RISK ANALYSIS 17
4.1 RISK ANALYSIS PROCESS 17
4.2 INTENDED USE and identification of characteristics related to the SAFETY of the MEDICAL DEVICE 18
4.3 Identification of HAZARDS 20
4.4 Estimation of the RISK(S) for each HAZARDOUS SITUATION 22
5 RISK EVALUATION 25
6 RISK CONTROL 26
6.1 RISK reduction 26
6.2 RISK CONTROL option analysis 26
6.3 Implementation of RISK CONTROL measure(s) 35
6.4 RESIDUAL RISK EVALUATION 36
6.5 RISK/benefit analysis 36
6.6 RISKS arising from RISK CONTROL measures 37
6.7 Completeness of RISK CONTROL 37
7 Evaluation of overall residual risk acceptability 38
8 Risk management report 38
9 Production and POST-PRODUCTION information 39
Annex A (informative) Discussion of definitions 41
Annex B (informative) Examples of software causes 43
Annex C (informative) Potential software-related pitfalls 53
Annex D (informative) Life-cycle/risk management grid 57
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 24
Figure 2 – FTA showing RISK CONTROL measure which prevents incorrect software outputs from causing HARM 28
Figure A.1 – Relationship between sequence of events, HARM and HAZARD 41

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

Table 1 – Requirements for documentation to be included in the RISK MANAGEMENT FILE in addition to ISO 14971:2007 requirements 17
Table A.1 – Relationship between HAZARDS, foreseeable sequences of events, HAZARDOUS SITUATIONS and the HARM that can occur 42
Table B.1 – Examples of causes by software function area 43
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 52
Table C.1 – Potential software-related pitfalls to avoid 53
Table D.1 – LIFE-CYCLE/RISK MANAGEMENT grid 57

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08f6f2308-d135-4462-9c47-31044c59470/iec-tr-80002-1-2009

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.

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 fulfil 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/0f1f6225-8b12-44b2-9c47-310d4a594706/iec-tr-80002-1-2009

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.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3 General requirements for RISK MANAGEMENT

3.1 RISK MANAGEMENT PROCESS

3.1.1 General

IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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.

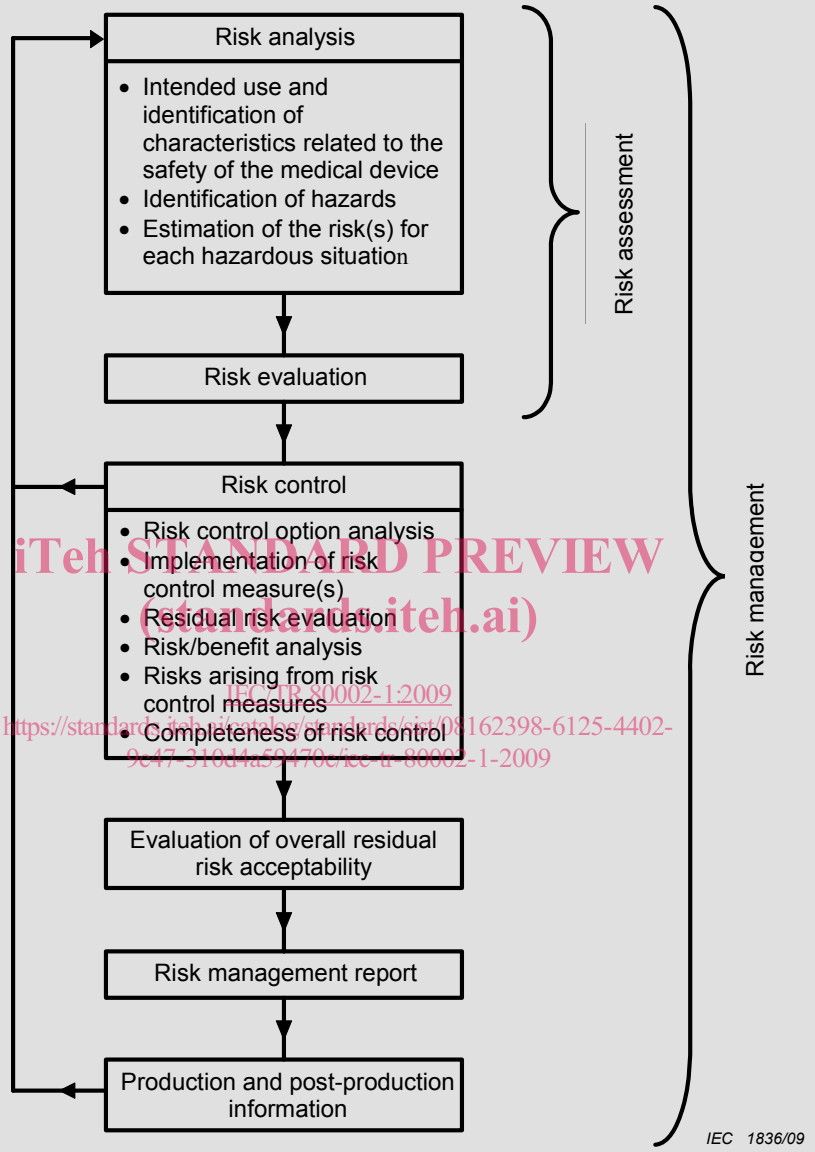
NOTE 1 A documented quality management system PROCESS can be used to deal with SAFETY in a systematic manner, in particular to enable the early identification of HAZARDS and HAZARDOUS SITUATIONS in complex MEDICAL DEVICES and systems.

---

1) Figures in square brackets refer to the Bibliography.

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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.

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 finalised.

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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

- 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/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08102598-6125-4462-9c47-310d4a59470c/iec-tr-80002-1-2009

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 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 behaviours 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/00816298-6125-4402-9417-310414504f70/iec-tr-80002-1-2009

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/TR 80002-1:2009
https://standards.iteh.ai/catalog/standards/sist/08162398-6125-4402-9c47-310d4a59470c/iec-tr-80002-1-2009

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.

3.3.2 INTENDED USE/domain knowledge

At all stages of the design of a MEDICAL DEVICE, it is important to deploy knowledge of the INTENDED USE. This is particularly important both for designers of software and for staff carrying out RISK MANAGEMENT of software. The complex behaviour of software can easily contribute to misuse or to confusion of the user, leading to previously unforeseen HAZARDS and HAZARDOUS SITUATIONS. A thorough appreciation of clinical practice will allow RISK managers to identify HAZARDS and HAZARDOUS SITUATIONS, and allow software engineers to avoid HAZARDS and HAZARDOUS SITUATIONS or to design RISK CONTROL measures.

MANUFACTURERS should ensure that clinical experts (such as clinical support and technical service experts, and experts on other relevant subjects) are available to participate in, or at least advise on, both the design activities and the RISK MANAGEMENT activities.

In addition, MANUFACTURERS should consider training software engineers and RISK managers in the clinical use of the MEDICAL DEVICE.

3.3.3 Programming experience and attitude

Experienced software developers and testers learn to be realistic about the difficulty of discovering all software defects during testing, and hence the density of software defects