

PD IEC/TR 80002-1:2009



BSI Standards Publication

Medical device software

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

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This Published Document is the UK implementation of IEC/TR 80002-1:2009.

The UK participation in its preparation was entrusted by Technical Committee CH/62, Electrical Equipment in Medical Practice, to Subcommittee CH/62/1, Common aspects of Electrical Equipment used in Medical Practice.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2010

ISBN 978 0 580 58674 3

ICS 11.040.01; 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2010.

Amendments issued since publication

Amd. No.	Date	Text affected
----------	------	---------------



TECHNICAL REPORT



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

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

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

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.

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.

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).

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.

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.

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

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.

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.

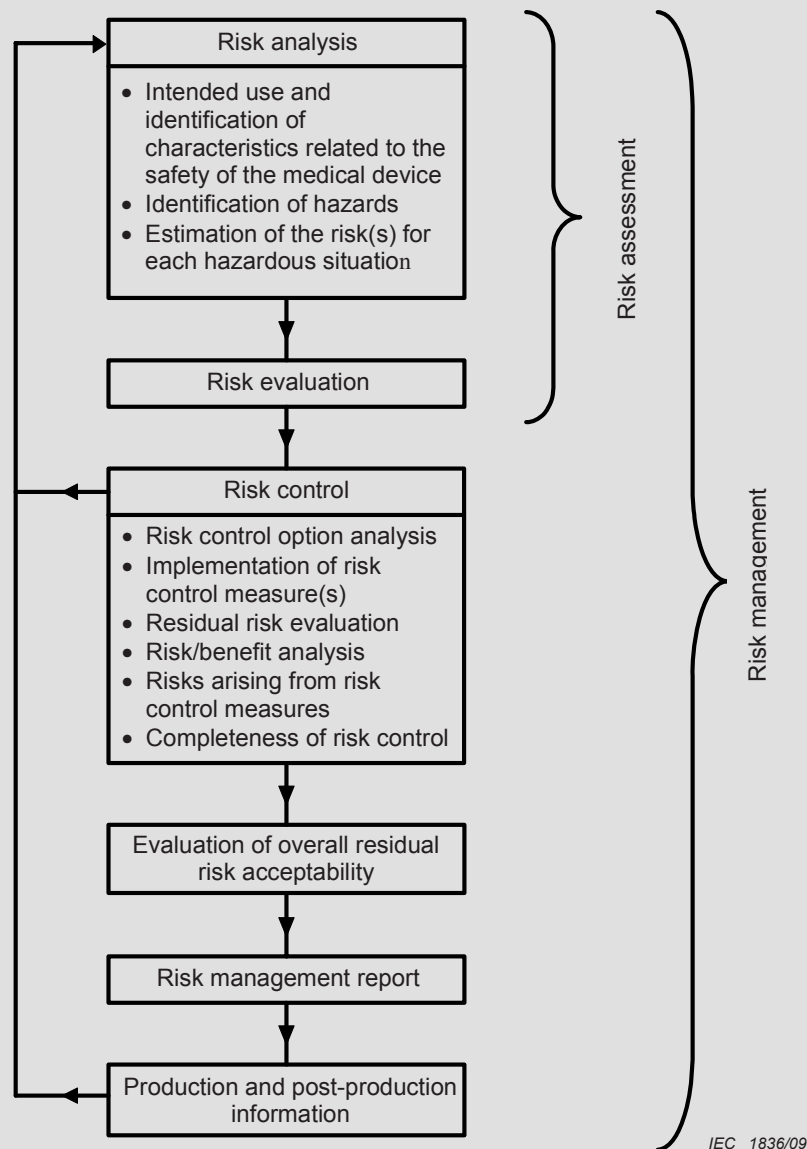


Figure 1 – A schematic representation of the RISK MANAGEMENT PROCESS

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:

- 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 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

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.

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.

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.

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

remaining after testing. It is important to include experienced staff in the software development team and to give them appropriate authority to mentor, oversee and challenge less experienced staff.

It is particularly important to assign experienced staff to the following software TASKS:

- identification of the ways in which software can fail;
- analysis of RISKS associated with software failure;
- identification of RISK CONTROL measures;
- analysis of post-release PROBLEM REPORTS;
- design and implementation of changes, especially post-release.

In all these TASKS, experience will lead to an appreciation of the sort of things that can go wrong with software and with software development PROCESSES, and an awareness of the difficulties of making a change while maintaining the integrity of a software design.

3.4 RISK MANAGEMENT plan

3.4.1 General

Text of ISO 14971:2007

3.4 RISK MANAGEMENT plan

RISK MANAGEMENT activities shall be planned. Therefore, for the particular MEDICAL DEVICE being considered, the MANUFACTURER shall establish and document a RISK MANAGEMENT plan in accordance with the RISK MANAGEMENT PROCESS. The RISK MANAGEMENT plan shall be part of the RISK MANAGEMENT FILE.

This plan shall include at least the following:

- a) the scope of the planned RISK MANAGEMENT activities, identifying and describing the MEDICAL DEVICE and the LIFE-CYCLE phases for which each element of the plan is applicable;
- b) assignment of responsibilities and authorities;
- c) requirements for review of RISK MANAGEMENT activities;
- d) criteria for RISK acceptability, based on the MANUFACTURER'S policy for determining acceptable RISK, including criteria for accepting RISKS when the probability of occurrence of HARM cannot be estimated;
- e) VERIFICATION activities;
- f) activities related to collection and review of relevant production and POST-PRODUCTION information.

NOTE 1 Refer to Annex F for guidance on developing a RISK MANAGEMENT plan.

NOTE 2 Not all parts of the plan need to be created at the same time. The plan or parts of it can be developed over time.

NOTE 3 The criteria for RISK acceptability are essential for the ultimate effectiveness of the RISK MANAGEMENT PROCESS. For each RISK MANAGEMENT plan the MANUFACTURER should choose appropriate RISK acceptability criteria.

Options could include, among others:

- indicating in a matrix, such as Figures D.4 and D.5, which combinations of probability of HARM and SEVERITY of HARM are acceptable or unacceptable;
- further subdividing the matrix (e.g. negligible, acceptable with RISK minimization) and requiring that RISKS first be made as low as reasonably practicable before determining that they are acceptable (see D.3).

Whichever option is chosen, it should be determined according to the MANUFACTURER'S policy for determining criteria for RISK acceptability and thus be 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 (see 3.2). Refer to D.4 for guidance on establishing such criteria.

If the plan changes during the LIFE-CYCLE of the MEDICAL DEVICE, a RECORD of the changes shall be maintained in the RISK MANAGEMENT FILE.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

The RISK MANAGEMENT plan should address the fact that software is part of the MEDICAL DEVICE by including:

- a description of the MEDICAL DEVICE including what functionality of the MEDICAL DEVICE will be implemented in software;
- a statement that software will be developed according to IEC 62304;
- a reference to software development aspects unique to software RISK MANAGEMENT (see Note);
- the RISK acceptance criteria for software-caused or software-controlled RISKS if they differ from acceptance criteria for other components of the MEDICAL DEVICE.

NOTE A reference to the software development plan may be the simplest way to address the inclusion of software development aspects unique to software RISK MANAGEMENT. See also 3.4.2 and 3.4.3 which discuss the relationship between the RISK MANAGEMENT plan and the software development plan and also specific RISK-related topics of the software development plan according to IEC 62304.

One reason that RISK acceptance criteria for software-caused or software-controlled RISKS might differ from acceptance criteria for other components is that the probability of HARM cannot be estimated. In this case the RISK acceptance criteria should be based on the SEVERITY of HARM. (See 4.4.3 for a discussion of probability for software caused HARM). If it can be concluded that the HAZARD is of little practical consequence, the RISK can be judged to be acceptable and no RISK CONTROL measures are necessary. However, for significant HAZARDS, that is, HAZARDS which could inflict HARM of high SEVERITY, no level of exposure can be identified that corresponds to a RISK so low that the RISK is acceptable. In this case RISK CONTROL measures need to be implemented.

RISK acceptance criteria for RESIDUAL RISK where probability cannot be estimated should take into account the RISK CONTROL measures that have been implemented and the effectiveness of those RISK CONTROL measures in reducing the probability of occurrence of HARM. RISK CONTROL measures should be a combination of all reasonable practicable measures, fulfil applicable standards and regulations, and be state of the art (see Annex D.4 of ISO 14971:2007).

When planning the activities related to collection and review of relevant production and POST-PRODUCTION information the following specific aspects for software should be considered:

- If SOFTWARE OF UNKNOWN PROVENANCE (SOUP) is used, then actively monitoring and evaluating publicly available ANOMALY lists and information about the SOUP field performance should be planned. Where possible, this should be supported by a contractual agreement with the SOUP supplier at the time of SOUP acquisition. If the users of the MEDICAL DEVICE may (intentionally or not) modify the SOUP of the MEDICAL DEVICE on their own (e.g. SOUP patches or updates), then special care should be taken in monitoring the provision of new SOUP VERSIONS for the market. See also Clause 9 regarding SOUP and POST-PRODUCTION monitoring.
- The MANUFACTURER should make it possible for the originator of a complaint to identify and report the software VERSION.

3.4.2 Relationship between RISK MANAGEMENT plan and software development plan

The requirements of ISO 14971 for a RISK MANAGEMENT plan and the requirements of IEC 62304 for a software development plan should not be taken as requiring specific documents with specific titles. Planning elements may be embodied in any documents to suit the MANUFACTURER'S quality management system, provided that:

- the combination of the planning documents satisfy the requirements of both standards in a verifiable manner;
- all plans are consistent with each other;
- all plans are available for use in a timely manner;
- all plans are kept up to date to reflect changing circumstances.

3.4.3 Specific RISK-related topics of the software development plan according to IEC 62304

The software development plan should ensure that the software development PROCESS, standards, methods, and tools associated with the development of software (described in the software development plan according to Clause 5 of IEC 62304:2006) are effective RISK CONTROL measures (see 6.2.2.6 for a discussion of PROCESS as a RISK CONTROL measure). This may be done by provision of evidence by other organisations, suppliers, and other projects within the organization. If not known, plan for and verify effectiveness within the project.

When establishing the MEDICAL DEVICE RISK MANAGEMENT PROCESS, aspects unique to software RISK MANAGEMENT should be considered, such as safe coding standards, VERIFICATION methods (e.g. formal proofs, peer reviews, walk-throughs, simulations, etc), and use of syntactic and logic checkers. If such aspects are considered RISK CONTROL measures, then they would also be subject to VERIFICATION (see Table B.2 for examples of verifying RISK CONTROL measures).

Software RISK MANAGEMENT activities should be addressed for each stage of MEDICAL DEVICE development in plans, PROCEDURES, and training, as appropriate.

3.5 RISK MANAGEMENT FILE

Text of ISO 14971:2007

3.5 RISK MANAGEMENT FILE

For the particular MEDICAL DEVICE being considered, the MANUFACTURER shall establish and maintain a RISK MANAGEMENT FILE. In addition to the requirements of other clauses of this International Standard, the RISK MANAGEMENT FILE shall provide traceability for each identified HAZARD to:

- the RISK ANALYSIS;
- the RISK EVALUATION;
- the implementation and VERIFICATION of the RISK CONTROL measures;
- the assessment of the acceptability of any RESIDUAL RISK(S).

NOTE 1 The RECORDS and other documents that make up the RISK MANAGEMENT FILE can form part of other documents and files required, for example, by a MANUFACTURER'S quality management system. The RISK MANAGEMENT FILE need not physically contain all the RECORDS and other documents; however, it should contain at least references or pointers to all required documentation. The MANUFACTURER should be able to assemble the information referenced in the RISK MANAGEMENT FILE in a timely fashion.

NOTE 2 The RISK MANAGEMENT FILE can be in any form or type of medium.

The software PROCESS should set up a system that makes this TRACEABILITY possible, starting from the software-related HAZARDS and the software RISK CONTROL measures and tracing their implementation to the corresponding SAFETY-related software requirements and the SOFTWARE ITEMS that satisfy those requirements.

All of the above should be traceable to their VERIFICATION (see Subclause 7.3.3 of IEC 62304:2006).

Because software may change frequently during development, and because it may be released in different VERSIONS, that part of the RISK MANAGEMENT FILE relating to software may also be subject to change and multiple VERSIONS.

Table 1 lists IEC 62304:2006 requirements for documentation to be included in the RISK MANAGEMENT FILE in addition to ISO 14971:2007 requirements.

Table 1 – Requirements for documentation to be included in the RISK MANAGEMENT FILE in addition to ISO 14971:2007 requirements

IEC 62304:2006 Subclause	RISK MANAGEMENT FILE documentation
4.3c)	Software SAFETY class assigned to each SOFTWARE SYSTEM
4.3f)	Rationale for using a lower software SAFETY class (than the SOFTWARE SYSTEM) for a SOFTWARE ITEM in the SOFTWARE SYSTEM which does not implement SAFETY-related functions
7.1.4	Potential causes of the SOFTWARE ITEM contributing to a HAZARDOUS SITUATION
7.1.5	Sequences of events that could result in a HAZARDOUS SITUATION that are identified in Subclause 7.1.2 of IEC 62304:2006
7.2.1	RISK CONTROL measures defined for each potential cause of the SOFTWARE ITEM contributing to a HAZARDOUS SITUATION
7.3.2	If a RISK CONTROL measure is implemented as SOFTWARE ITEM, the MANUFACTURER is to evaluate the RISK CONTROL measure to identify and document any new sequences of events that could result in a HAZARDOUS SITUATION
9.5	The MANUFACTURER is to maintain RECORDS of PROBLEM REPORTS and their resolution including their VERIFICATION. The MANUFACTURER is to update the RISK MANAGEMENT FILE as appropriate

4 RISK ANALYSIS

4.1 RISK ANALYSIS PROCESS

Text of ISO 14971:2007

4 RISK ANALYSIS

4.1 RISK ANALYSIS PROCESS

RISK ANALYSIS shall be performed for the particular MEDICAL DEVICE as described in 4.2 to 4.4. The implementation of the planned RISK ANALYSIS activities and the results of the RISK ANALYSIS shall be recorded in the RISK MANAGEMENT FILE.

NOTE 1 If a RISK ANALYSIS, or other relevant information, is available for a similar MEDICAL DEVICE, that analysis or information can be used as a starting point for the new analysis. The degree of relevance depends on the differences between the devices and whether these introduce new HAZARDS or significant differences in outputs, characteristics, performance, or results. The extent of use of an existing analysis is also based on a systematic evaluation of the effects the changes have on the development of HAZARDOUS SITUATIONS.

NOTE 2 Some RISK ANALYSIS techniques are described in Annex G.

NOTE 3 Additional guidance on RISK ANALYSIS techniques for *IN VITRO* DIAGNOSTIC MEDICAL DEVICES is given in Annex H.

NOTE 4 Additional guidance on RISK ANALYSIS techniques for toxicological HAZARDS is given in Annex I.

In addition to the RECORDS required in 4.2 to 4.4, the documentation of the conduct and results of the RISK ANALYSIS shall include at least the following:

- a) a description and identification of the MEDICAL DEVICE that was analyzed;
- b) identification of the person(s) and organization who carried out the RISK ANALYSIS;
- c) scope and date of the RISK ANALYSIS.

NOTE 5 The scope of the RISK ANALYSIS can be very broad (as for the development of a new device with which a MANUFACTURER has little or no experience) or the scope can be limited (as for analyzing the impact of a change to an existing device for which much information already exists in the MANUFACTURER'S files).

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

As described in ISO 14971:2007, RISK ANALYSIS is a term used to encompass three distinct activities;

- identification of INTENDED USE,
- identification of known or foreseeable HAZARDS (and their causes), and
- estimating the RISK of each HAZARD and HAZARDOUS SITUATION.

It is essential to recognize that RISK ANALYSIS is performed as an integral part of the entire software development PROCESS—not as one or two discrete events—for it to be effective because HAZARD and failure mode information accrue over the software development LIFE-CYCLE PROCESS and need to be considered at each stage of design.

Since it is very difficult to estimate the probability of software ANOMALIES that could contribute to HAZARDOUS SITUATIONS, the focus of software aspects of RISK ANALYSIS is on identification of potential software functionality and ANOMALIES that could result in HAZARDOUS SITUATIONS—not on estimating probability. See 4.4.3 for more details on estimating probability.

The SEVERITY of the worst case HARM for which software is a contributing factor is a primary input in determining the level of rigour of software development PROCESSES (see Subclause 4.3 of IEC 62304:2006). The information provided in 4.2, 4.3, and 4.4 is intended to help identify software-specific aspects of an effective RISK MANAGEMENT PROCESS. In addition, software aspects of the RISK ANALYSIS should be identifiable in the resulting documentation and should include both software used to implement RISK CONTROL measures for hardware failures and software causes for HAZARDS and their associated RISK CONTROL measures.

4.2 INTENDED USE and identification of characteristics related to the SAFETY of the MEDICAL DEVICE

4.2.1 General

Text of ISO 14971:2007

4.2 INTENDED USE and identification of characteristics related to the SAFETY of the MEDICAL DEVICE

For the particular MEDICAL DEVICE being considered, the MANUFACTURER shall document the INTENDED USE and reasonably foreseeable misuse. The MANUFACTURER shall identify and document those qualitative and quantitative characteristics that could affect the SAFETY of the MEDICAL DEVICE and, where appropriate, their defined limits. This documentation shall be maintained in the RISK MANAGEMENT FILE.

NOTE 1 In this context, misuse is intended to mean incorrect or improper use of the MEDICAL DEVICE.

NOTE 2 Annex C contains questions such as those relating to use that can serve as a useful guide in identifying MEDICAL DEVICE characteristics that could have an impact on SAFETY.

Compliance is checked by inspection of the RISK MANAGEMENT FILE.

While each MEDICAL DEVICE has an INTENDED USE, the potential for misuse—intentional or otherwise—should also be considered. While this is not a software-specific concern, the use of software may lead to an increased RISK of misuse because:

- the MEDICAL DEVICE's behaviour is more complex and therefore more difficult to master or understand;
- the user may become over-reliant on software, not understanding its limitations;
- the MEDICAL DEVICE may be configurable, and the user may be unaware of the current configuration.
- MEDICAL DEVICES may communicate with MEDICAL and non-MEDICAL DEVICES in a manner that cannot be anticipated in detail by the MEDICAL DEVICE MANUFACTURER.

The person responsible for producing SYSTEM requirements and the software engineer have a joint responsibility to RECORD in the RISK MANAGEMENT FILE the INTENDED USE of the SYSTEM including its software, together with all SYSTEM and software requirements that relate to SAFETY and safe use. The software engineer is specifically responsible for identifying aspects of INTENDED USE that are too subtle to be apparent at the SYSTEM level.

4.2.2 User interface

Software makes it possible to design flexible user interfaces, which may affect users' behaviour, leading to new forms of reasonably foreseeable misuse. Common misuses arise from misunderstanding of an over-complex user interface and over-reliance on software to avoid errors and unsafe states. It is important to anticipate such misuse and to change the design to avoid them as far as possible.

This includes implementation of multi-lingual labelling, especially when such labelling is a RISK CONTROL measure. Special care should be taken of:

- a) different need for memory size for different languages;
- b) use of different character sets;
- c) use of characters instead of symbols;
- d) use of different units which may require additional scaling of numerical results;
- e) date formatting and numerical punctuation;
- f) different layout requirements for different languages and/or character sets;
- g) support of validation.

See IEC 62366 [5] for a usability PROCESS complementary to ISO 14971.

4.2.3 MEDICAL DEVICE interconnection

The use of software in MEDICAL DEVICES makes possible a range of interconnections and intercommunication between MEDICAL and non-MEDICAL DEVICES. Such connections and communications are likely to give rise to new uses (and misuses) of the SYSTEM COMPONENTS.