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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XB

ICS 11.040.01

ISBN 978-2-88910-779-7

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*