IEC/TR 80001-2-1

Edition 1.0 2012-07

TECHNICAL REPORT

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XB

ICS 11.040.01; 35.240.80

ISBN 978-2-83220-201-2

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
2 Normative references 8
3 Terms and definitions 8
4 Prerequisites 14
5 Study of terms used in RISK MANAGEMENT 14
5.1 Overview 14
5.2 HAZARDS 15
5.3 HAZARDOUS SITUATIONS 15
5.4 Foreseeable sequences of events and causes 16
5.5 UNINTENDED CONSEQUENCE 16
5.6 RISK CONTROL measures (mitigations) 17
5.7 Degrees of RISK 17
5.8 Checking wording 18
6 The steps 18
6.1 Overview of the steps 18
6.2 A basic example using the 10 steps 19
6.2.1 General 19
6.2.2 Initial RISK – Steps 1 – 5 (Figure 2) 19
6.2.3 RISK CONTROL and final RISK – Steps 6 – 10 (Figure 3) 20
7 IEC 80001-1:2010, Clause 4.4: Step by step 23
7.1 General 23
7.2 Application of Subclause 4.4.1: Document all RISK MANAGEMENT elements 23
7.3 Note about RISK EVALUATION 23
7.4 The 10-step PROCESS 23
7.4.1 STEP 1: Identify HAZARDs and HAZARDOUS SITUATIONS 23
7.4.2 STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS 24
7.4.3 STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential severities 25
7.4.4 STEP 4: Estimate the probability of UNINTENDED CONSEQUENCE 25
7.4.5 STEP 5: Evaluate RISK 26
7.4.6 STEP 6: Identify and document proposed RISK CONTROL measures and re-evaluate RISK (return to Step 3) 27
7.4.7 STEP 7: Implement RISK CONTROL measures 28
7.4.8 STEP 8: Verify RISK CONTROL measures 29
7.4.9 STEP 9: Evaluate any new RISKS arising from RISK CONTROL 30
7.5 The steps and their relationship to IEC 80001-1 and ISO 14971 30
8 Practical examples 31
8.1 General 31
8.2 Example 1: Wireless PATIENT monitoring during PATIENT transport 32
8.2.1 Full description of context 32
8.2.2 Description of network under analysis 32
8.2.3 The 10 Steps 32
8.3 Example 2: Remote ICU / Distance medicine 35

8.3.1 Full description of context 35
8.3.2 Description of network under analysis 35
8.3.3 The 10 Steps 35
8.4 Example 3: Post Anaesthesia Care Unit (PACU) 38
8.4.1 Full description of context 38
8.4.2 Description of network under analysis 38
8.4.3 The 10 Steps 39
8.5 Example 4: Ultrasound –Operating system (OS) vulnerability 44
8.5.1 Full description of context 44
8.5.2 Description of network under analysis 44
8.5.3 The 10 Steps 44
Annex A (informative) Common HAZARDS, HAZARDOUS SITUATIONS, and causes to consider in MEDICAL IT-NETWORKS 48
Annex B (informative) List of questions to consider when identifying HAZARDs of the MEDICAL IT-NETWORK 52
Annex C (informative) Layers of MEDICAL IT-NETWORKS where errors can be found 53
Annex D (informative) Probability, severity, and RISK acceptability scales used in the examples in this technical report 56
Annex E (informative) MONITORING RISK mitigation effectiveness 59
Annex F (informative) RISK ANALYZING small changes in a MEDICAL IT-NETWORK 62
Annex G (informative) Example of Change Window Form 63
Annex H (informative) Template for examples 64
Bibliography 66

Figure 1 – Basic flow of concepts from HAZARD to HAZARDOUS SITUATION to UNINTENDED CONSEQUENCE 15
Figure 2 – Steps 1 – 5: HAZARD identification through RISK EVALUATION 20
Figure 3 – Steps 6 – 10: RISK CONTROL measures through overall RESIDUAL RISK 21
Figure 4 – Sample summary RISK ASSESSMENT register format 22
Figure 5 – Relation of cause to HARM 26
Figure 6 – Schematic of the post anaesthesia care unit (PACU) 39
Figure 7 – Example of the use of colour coding cables 42
Figure 8 – Sample summary RISK ASSESSMENT register for the PACU example 43
Figure D.1 – Application of STEPs 5 and 6 with 3 levels of RISK acceptability 58
Figure F.1 – Overview of RISK ANALYZING small changes in a MEDICAL IT-NETWORK 62

Table 1 – Relationship of KEY PROPERTIES, SAFETY, EFFECTIVENESS and DATA AND SYSTEMS SECURITY with associated UNINTENDED CONSEQUENCE as used in this technical report 17
Table 2 – Methods for checking accurate and appropriate wording of causes, HAZARDOUS SITUATIONS, and UNINTENDED CONSEQUENCES 18
Table 3 – Relationship between this technical report, IEC 80001-1:2010 and ISO 14971:2007 31
Table A.1 – HAZARDS related to potential required network characteristics 50
Table A.2 – Relationship between HAZARDS, foreseeable sequences, and causes 50
Table A.3 – Relationship between HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS 51

Table C.1 – Layers of an MEDICAL IT-NETWORK 53
Table C.2 – Example of the layers of an MEDICAL IT-NETWORK 55
Table D.1 – Probability scales used in the examples in this technical report 56
Table D.2 – Severity scales 56
Table D.3 – RISK level matrix 57

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 80001-2-1, which is a technical report, has been prepared by a Joint Working Group of subcommittee 62A: Common aspects of electrical equipment used in medical practice, of IEC technical committee 62*:* Electrical equipment in medical practice and ISO technical committee 215: Health informatics.

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

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

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

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

Terms used throughout this technical report that have been defined in Clause 3 appear in SMALL CAPITALS.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

IMPORTANT – The '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 document using a colour printer.

INTRODUCTION

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

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

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

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

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

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

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

1 Scope

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

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

2 Normative references

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

IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities*