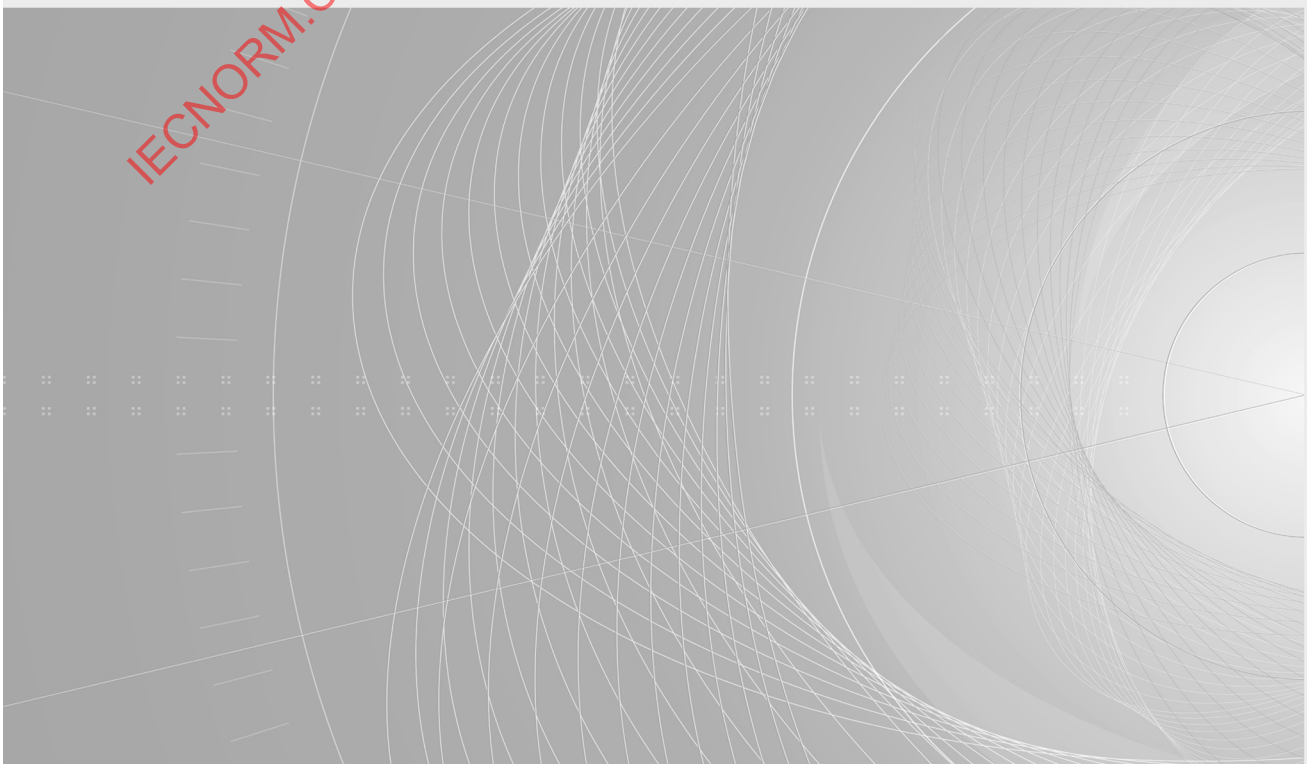
IEC/TR 80001-2-1

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



IEC/TR 80001-2-1:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

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.

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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

CONTENTS

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
CHANGE PERMIT
an outcome of the RISK MANAGEMENT PROCESS consisting of a document that allows a specified change or type of change without further RISK MANAGEMENT activities subject to specified constraints

[SOURCE: IEC 80001-1:2010, definition 2.3]

3.2
CHANGE RELEASE MANAGEMENT
PROCESS that ensures that all changes to the IT-NETWORK are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with CONFIGURATION MANAGEMENT

[SOURCE: IEC 80001-1:2010, definition 2.2]

3.3
CONFIGURATION MANAGEMENT
PROCESS that ensures that configuration information of components and the IT-NETWORK are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the IT-NETWORK

[SOURCE: IEC 80001-1:2010, definition 2.4]

3.4
DATA AND SYSTEMS SECURITY
operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

[SOURCE: IEC 80001-1:2010, definition 2.5, modified – two notes integral to understanding the scope of the definition in the original document have been deleted.]

3.5
EFFECTIVENESS
ability to produce the intended result for the PATIENT and the RESPONSIBLE ORGANIZATION

[SOURCE: IEC 80001-1:2010, definition 2.6]

3.6
ELECTROMAGNETIC INTERFERENCE
EMI
any electromagnetic phenomenon that may degrade the performance of a device, equipment, or system

[SOURCE: IEC 60601-1-2:2007, definition 3.5, modified – the term has been changed, an abbreviation added and the note to the original definition removed.]

3.7
EVENT MANAGEMENT
PROCESS that ensures that all events that can or might negatively impact the operation of the IT-NETWORK are captured, assessed, and managed in a controlled manner

[SOURCE: IEC 80001-1:2010, definition 2.7]

3.8
HARM
physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEMS SECURITY

[SOURCE: IEC 80001-1:2010, definition 2.8]

3.9
HAZARD
potential source of HARM

[SOURCE: IEC 80001-1:2010, definition 2.9]

3.10
HAZARDOUS SITUATION
circumstance in which people, property, or the environment are exposed to one or more HAZARD(S)

[SOURCE: ISO 14971:2007, definition 2.4]

3.11
HEALTH DATA
PRIVATE DATA that indicates physical or mental health

Note 1 to entry: This generically defines PRIVATE DATA and its subset, HEALTH DATA, within this document to permit users of this document to adapt it easily to different privacy compliance laws and regulations. For example, in Europe, the requirements might be taken and references changed to “Personal Data” and “Sensitive Data”; in the USA, HEALTH DATA might be changed to “Protected Health Information (PHI)” while making adjustments to text as necessary.

[SOURCE: IEC 80001-2-2:2012, definition 3.7]

3.12
INTENDED USE
use for which a product, PROCESS or service is intended according to the specifications, instructions and information provided by the MANUFACTURER

[SOURCE: IEC 80001-1:2010, definition 2.10]

3.13
INTEROPERABILITY
property permitting diverse systems or components to work together for a specified purpose

[SOURCE: IEC 80001-1:2010, definition 2.11]

3.14
INFORMATION TECHNOLOGY
IT
technology (computer systems, networks, software) used to PROCESS, store, acquire and distribute information

3.15
IT-NETWORK
INFORMATION TECHNOLOGY NETWORK
system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

[SOURCE: IEC 80001-1:2010, definition 2.12, modified – the two notes to the original definition have not been retained.]

3.16
KEY PROPERTIES
three RISK-managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

[SOURCE: IEC 80001-1:2010, definition 2.13]

3.17
LOCAL AREA NETWORK
LAN
computer network covering a small physical area, such as a home or office, or small group of buildings, such as a school or an airport

3.18
MANUFACTURER
natural or legal person with responsibility for the design, manufacture, packaging, or labelling of a MEDICAL DEVICE, assembling a system, or adapting a medical device before it is placed on the market or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party

[SOURCE: ISO 14971:2007, definition 2.8, modified – Note 1 to the original definition, which provides pertinent information, has not been retained.]

3.19
MEDICAL DEVICE
any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) intended by the MANUFACTURER to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
   - diagnosis, prevention, monitoring, treatment or alleviation of disease,
   - diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
   - investigation, replacement, modification, or support of the anatomy or of a physiological PROCESS,
   - supporting or sustaining life,
   - control of conception,
   - disinfection of MEDICAL DEVICES,
   - providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and
b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means.

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry: Products which may be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:
- aids for disabled/handicapped people;
- devices for the treatment/diagnosis of diseases and injuries in animals;
- accessories for medical devices (see Note 3 to entry);
- disinfection substances;
- devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by MANUFACTURERS to be used together with a 'parent' medical device to enable that medical device to achieve its intended purpose should be subject to the same GHTF procedures as apply to the medical device itself. For example, an accessory will be classified as though it is a medical device in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to medical devices are generally controlled through the MANUFACTURER'S quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'medical device'.

[SOURCE: IEC 80001-1:2010, definition 2.14]

3.20
MEDICAL IT-NETWORK
IT-NETWORK that incorporates at least one MEDICAL DEVICE

[SOURCE: IEC 80001-1:2010, definition 2.16]

3.21
MONITORING
on-going review of all RISK MANAGEMENT activities and RISK CONTROL options that were put in place to achieve acceptable RISK in the use of MEDICAL IT-NETWORK(S).

3.22
OPERATOR
person handling equipment

[SOURCE: IEC 80001-1:2010, definition 2.18]

3.23
PATIENT
individual awaiting or under medical care and treatment

3.24
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: IEC 80001-1:2010, definition 2.19]

3.25
QUALITY OF SERVICE
QoS
the capability or means of providing differentiated levels of networking performance in terms of traffic engineering (packet delay, loss, jitter, bit rate) to different data flows.

3.26
RESIDUAL RISK
RISK remaining after RISK CONTROL measures have been taken

[SOURCE: IEC 80001-1:2010, definition 2.20]

3.27
RESPONSIBILITY AGREEMENT
one or more documents that together fully define the responsibilities of all relevant stakeholders

[SOURCE: IEC 80001-1:2010, definition 2.21, modified – a note to the original definition, containing examples, has not been retained.]

3.28
RESPONSIBLE ORGANIZATION
RO
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

[SOURCE: IEC 80001-1:2010, definition 2.22, modified – a note to the original definition, containg examples, has not been retained.]

3.29
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

[SOURCE: IEC 80001-1:2010, definition 2.23]

3.30
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: IEC 80001-1:2010, definition 2.24]

3.31
RISK ASSESSMENT
overall PROCESS comprising a RISK ANALYSIS and a RISK EVALUATION

[SOURCE: IEC 80001-1:2010, definition 2.25]

3.32
RISK CONTROL
PROCESS in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[SOURCE: IEC 80001-1:2010, definition 2.26]

3.33
RISK EVALUATION
PROCESS of comparing the estimated RISK against given RISK criteria to determine the acceptability of the RISK

[SOURCE: IEC 80001-1:2010, definition 2.27]

3.34
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and MONITORING RISK

[SOURCE: IEC 80001-1:2010, definition 2.28]

3.35
RISK MANAGEMENT FILE
set of records and other documents that are produced by RISK MANAGEMENT

[SOURCE: IEC 80001-1:2010, definition 2.29]

3.36
SAFETY
freedom from unacceptable RISK of physical injury or damage to the health of people or damage to property or the environment

[SOURCE: IEC 80001-1:2010, definition 2.30]

3.37
TOP MANAGEMENT
person or group of people who direct(s) and control(s) the RESPONSIBLE ORGANIZATION accountable for a MEDICAL IT-NETWORK at the highest level

[SOURCE: IEC 80001-1:2010, definition 2.31]

3.38
UNINTENDED CONSEQUENCE
UC
unwanted and negative outcome of an event that results in one or more degraded KEY PROPERTIES

3.39
VERIFICATION
confirmation through provision of objective evidence that specified requirements have been fulfilled

Note 1 to entry: The term “verified” is used to designate the corresponding status.

Note 2 to entry: Confirmation can comprise activities such as:

– performing alternative calculations;
– comparing a new design specification with a similar proven design specification;
– undertaking tests and demonstrations; and

– reviewing documents prior to issue.

Note 3 to entry: In design and development, VERIFICATION concerns the PROCESS of examining the result of a given activity to determine conformity with the stated requirement for that activity.

[SOURCE: IEC 80001-1:2010, definition 2.32]

4 Prerequisites

Before beginning the steps outlined within this technical report, the requirements in subclauses 3.1 to 4.3 of IEC 80001-1:2010 need to be completed. Additionally, the RESPONSIBLE ORGANIZATION (RO) must be prepared to meet the requirements in subclauses 4.5 through 5.2. For example, the RISK MANAGEMENT policy and PROCESSES are in place; the RISK MANAGEMENT plan is complete; any required RESPONSIBILITY AGREEMENTS are in place; probability, severity, and RISK acceptability scales are defined.

For RISK MANAGEMENT of any system to proceed, the system must be defined. In the case of MEDICAL IT-NETWORKS, the network under analysis must be well defined and can already contain some existing controls. This will be important in Steps 3 and 4. For new MEDICAL IT-NETWORKS, this can be a preliminary design.

In addition to defining the system under analysis, fundamental information regarding RO specific use, needs, and concerns are needed in order to complete the RISK estimation. This is referred to as “context” of use and includes information such as:

– acuity of PATIENTS;
– clinical workflow;
– clinical staffing and competencies;
– INTENDED USE/clinical or business use case; and
– clinical and business criticality of the systems/applications using the network.

The steps described in this report will generally be executed by a team of individuals within the RESPONSIBLE ORGANIZATION. It is recommendable to have representation from multiple departments, including IT, biomedical engineering, clinical, and RISK MANAGEMENT. The makeup of the team should align with existing structures within the organization.

5 Study of terms used in RISK MANAGEMENT

5.1 Overview

RISK MANAGEMENT is a very large field of study. This technical report provides an introduction to this subject with examples that can be undertaken with minimal knowledge. It provides step by step instructions for undertaking a RISK ASSESSMENT PROCESS.

IEC 80001-1 provides a RISK MANAGEMENT philosophy. As there are several RISK MANAGEMENT philosophies available, this one might or might not be completely in line with RISK MANAGEMENT approaches and techniques already in place at the RO. The RO should consider taking appropriate steps to reconcile the differences in methodology and terminology.

Figure 1 shows the basic flow of concepts from HAZARD to HAZARDOUS SITUATION to UNINTENDED CONSEQUENCE.

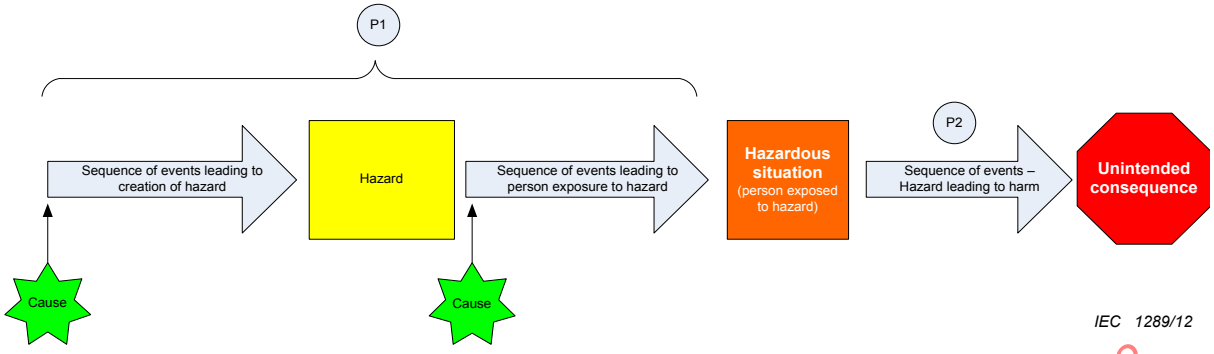


Figure 1 – Basic flow of concepts from HAZARD to HAZARDOUS SITUATION to UNINTENDED CONSEQUENCE

5.2 HAZARDS

IEC 80001-1 addresses three KEY PROPERTIES (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY), each of which can be subject to single or combined HAZARDS and HAZARDOUS SITUATIONS.

Consider HAZARDS as categories of things that could be detrimental to one or more of the three KEY PROPERTIES. Concrete examples include electrical energy, suspended masses, high temperatures, etc., but functional and operational failures must also be considered as HAZARDS. For example, failure of a defibrillator to power up at a time when it is needed is dangerous. In the case of MEDICAL IT-NETWORKS, many of the HAZARDOUS SITUATIONS that can develop are related to the HAZARD "loss of function" (e.g., the MEDICAL IT-NETWORK fails to deliver the data).

HAZARDS are hierarchical and can be organized as such. For example, regarding the HAZARD "energy", this can be broken down into thermal energy, mechanical energy, and electrical energy, which are also HAZARDS. Further subdividing – high temperature, torsion, and high voltage are all HAZARDS. This hierarchical approach can be used to organize RISK ANALYSIS and documentation. For example, high temperatures in a communications cabinet can be a cause of failures to IT equipment. ELECTROMAGNETIC INTERFERENCE can also be a cause of failure in IT-NETWORKS.

Many HAZARDS are inherent to the properties of the device or system, whereas some develop during the life of the system. For example, high temperature is a HAZARD. A cook-top is intended to be hot (inherent to the system), but an overheated surface of a machine might develop after a failure in the machine. As another example, sharp edges are also a type of HAZARD. A knife is intended to be sharp, but a metal burr on a metal enclosure might form during manufacturing. Loss of network function as a HAZARD could develop during the use of networked devices.

5.3 HAZARDOUS SITUATIONS

A HAZARD is a potential source of UNINTENDED CONSEQUENCE. A sharp knife, an icy sidewalk, even a blizzard can be considered a HAZARD. A HAZARDOUS SITUATION is a circumstance in which a person, property, or the environment is exposed to one or more HAZARDS. A HAZARDOUS SITUATION must occur for there to be possibility of UNINTENDED CONSEQUENCE. For example, if no-one ever walks on an icy sidewalk (HAZARDOUS SITUATION), the icy sidewalk itself is still a HAZARD, but there is no possibility of UNINTENDED CONSEQUENCE if the HAZARDOUS SITUATION never occurs.

Multiple different HAZARDOUS SITUATIONS can develop from a single HAZARD, each with different levels of RISK. Given the HAZARD "loss of connectivity", several HAZARDOUS SITUATIONS can develop, such as failure to update medical records, delay in dispatching new physician's

orders, inability to determine if equipment is operating correctly, inability to update a formulary on an IV pump, failure to transmit an active alarm, etc.

With the information given in a HAZARDOUS SITUATION along with the MEDICAL IT-NETWORK definition and context (clinical use case, clinical functionality/workflow, PATIENT acuity, data sensitivity, etc.), UNINTENDED CONSEQUENCES can be determined. In the case of lost connectivity, what data was lost and to whom it belonged are important factors in determining UNINTENDED CONSEQUENCES. Loss of alarm data for a high acuity PATIENT will carry different RISK than loss of electronic medical record data at a walk-in clinic.

5.4 Foreseeable sequences of events and causes

A foreseeable sequence of events transforms the HAZARD into a HAZARDOUS SITUATION. A sequence of events can also lead up to a HAZARD that is not inherent to the MEDICAL IT-NETWORK and then lead to a HAZARDOUS SITUATION. The initial event is referred to as the cause. In the case of a MEDICAL IT-NETWORK, a cause can be network congestion that results in a HAZARD such as lost connectivity. A HAZARDOUS SITUATION occurs when a PATIENT or the organization is exposed to this HAZARD, potentially leading to one or more of the 3 KEY PROPERTIES being negatively affected.

The cause answers the question “why is someone/something in the HAZARDOUS SITUATION?” For simplicity, consider cause the point at which things went wrong (network design flaw, network component failure, etc.), and this is one of the points where RISK CONTROL measures can effectively be applied.

5.5 UNINTENDED CONSEQUENCE

The RISK MANAGEMENT PROCESS used in IEC 80001-1 follows the RISK MANAGEMENT PROCESS of ISO 14971. It is important to note that the realm of RISKS addressed by IEC 80001-1 and this technical report is broader than that of ISO 14971, even though it uses identical terms. HARM as defined in ISO 14971 is related to IEC 80001 KEY PROPERTY SAFETY only (physical injury) where in IEC 80001-1 HARM is defined to address all three KEY PROPERTIES: SAFETY, EFFECTIVENESS and DATA AND SYSTEMS SECURITY. To avoid a single domain interpretation of RISK MANAGEMENT (SAFETY only) this Technical Report explains RISK MANAGEMENT using the more neutral term ‘UNINTENDED CONSEQUENCE’ (or ‘UC’). A physical injury would be an UNINTENDED CONSEQUENCE of a RISK to SAFETY. A HAZARD could be a potential source of a security breach or reduced effectiveness, in addition to physical injury. RISK MANAGEMENT of MEDICAL IT-NETWORKS requires involvement of multiple disciplines that can use domain specific terms regarding RISK, RISK MANAGEMENT or HAZARDS. UNINTENDED CONSEQUENCE is used in this document as a generically descriptive term.

Table 1 gives an overview of the relationship between the terms used.

Table 1 – Relationship of KEY PROPERTIES, SAFETY, EFFECTIVENESS and DATA AND SYSTEMS SECURITY with associated UNINTENDED CONSEQUENCE as used in this technical report

KEY PROPERTY	SAFETY	EFFECTIVENESS	DATA AND SYSTEMS SECURITY
Definition of KEY PROPERTY	Freedom from unacceptable combination of probability and severity of physical injury or damage to the health of people, or damage to the property or the environment	Ability to produce the intended result for the PATIENT and the RESPONSIBLE ORGANIZATION	An operational state of a MEDICAL IT-NETWORK in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability
Description of UNINTENDED CONSEQUENCE	Physical injury or damage to the health of people, or damage to the property or the environment,	Reduction in EFFECTIVENESS	Breach of DATA AND SYSTEMS SECURITY

For a more detailed treatment of how IT security terms relate to SAFETY RISK MANAGEMENT terms, see IEC/TR 80001-2-2. The phrase "breach of DATA AND SYSTEMS SECURITY" is approximately equivalent to an executed exploit in the domain of IT security (i.e., cyber security). A system vulnerability is a system attribute that, when demonstrably exploitable, becomes a HAZARD that can, in turn, lead to a breach event. Although sometimes overlapping in everyday use, vulnerabilities can lead to HARM but cannot be perceived as an immediate danger but a threat tends to be a more palpable, immediate danger with potential to HARM (HAZARDOUS SITUATION) DATA AND SYSTEMS SECURITY (e.g., a vulnerability with a large payoff if exploited).

For information on applying security RISK MANAGEMENT at the organizational level see ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27799:2008. For the incorporation of a MEDICAL DEVICE onto an IT-NETWORK, some might choose to use ISO/IEC 27005:2011 for IT security RISK MANAGEMENT PROCESSES that can be adapted to complement the ISO 14971-based RISK PROCESS in IEC 80001-1 (i.e., SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY).

5.6 RISK CONTROL measures (mitigations)

RISK CONTROL measures are also referred to as mitigations. Mitigations can be applied to lower the probability of occurrence of a HAZARDOUS SITUATION (lowering P1 in Figure 1). Additionally, given the occurrence of the HAZARDOUS SITUATION, RISK CONTROLS can also be used to limit the probability of occurrence of an UNINTENDED CONSEQUENCE resulting from the HAZARDOUS SITUATION (lowering P2 in Figure 1).

For example, a network link down can lead to a HAZARDOUS SITUATION where a centralized clinician is not notified of a PATIENT alarm at the bedside. To lower P1, a redundant link can be added to allow failover. In this case, the link down would not cause the HAZARDOUS SITUATION. To lower P2, a "link down" alarm can be displayed at the centralized location, alerting the clinician of the situation. In this case, the HAZARDOUS SITUATION occurred, but the probability of occurrence of an UNINTENDED CONSEQUENCE is lower.

5.7 Degrees of RISK

It is generally accepted that, although marginal improvements in RISK levels are always possible in principle, as a practical matter zero RISK is unattainable. It is also generally

accepted that there is an upper limit above which RISKS are deemed to be unacceptable barring extraordinary circumstances, and must either be reduced, whatever the cost, or the activity giving rise to the RISK cannot be implemented or must be discontinued.

RISKS below the upper limit are generally considered acceptable, yet can contain RESIDUAL RISKS that could or should be reduced simply because it is easily possible to significantly reduce these RISKS. It is also possible to have a level of RESIDUAL RISK for a given HAZARDOUS SITUATION that is so small that RISK reduction is never really effective or even necessary. Therefore degrees of RISK can be put into categories defined by:

– a higher limit above which RISKS are considered unacceptable;
– a lower limit below which RISKS are regarded as being 'broadly acceptable' and therefore requiring no action to effect further reduction;
– a range between the upper and lower limits in which RISK acceptability or RISK reduction needs further consideration. These considerations should follow pre-defined policies and can include reducing the RISK if reasonably practicable, special team reviews (IT, clinical) or review boards, rationales, or management signoff.

Note that "reasonably practicable" is a narrower term than 'physically possible'. It involves an analysis of the time, effort and expense involved with implementing the RISK CONTROL option which should not be disproportionate to the reduction of RISK it provides. It is possible to have a RISK that has been reduced as far as reasonably practicable, yet still falls in the high level of RISK. Conversely, organizations can choose to continue to reduce RISKS in the low range, if RISK CONTROL measures are easily applied. In the moderate range, the RISK MANAGEMENT policy can either require or strongly recommend reduction if reasonably practicable. It is advised to report the practicability analysis as part of the RESIDUAL RISK report.

5.8 Checking wording

Table 2 shows methods for checking accurate and appropriate wording of causes, HAZARDOUS SITUATIONS, and UNINTENDED CONSEQUENCES.

Table 2 – Methods for checking accurate and appropriate wording of causes, HAZARDOUS SITUATIONS, and UNINTENDED CONSEQUENCES

	Must be defined clearly enough to...	Overly-broad examples (difficult to determine rankings)	More specific examples, (rankings more easily evaluated)...
Cause	Determine P1	"Lost connectivity" is very broad,	"Power loss", "Cleaning crew unplugs switch" is even more easily evaluated.
HAZARDOUS SITUATION along with defined context	Determine possible negative UNINTENDED CONSEQUENCES and associated P2s	Waveform display is choppy and incomplete.	Waveform display is choppy and incomplete. Delay in provision of care because remote clinician is unable to evaluate PATIENT ECG waveform.
UNINTENDED CONSEQUENCES	Determine severity (S)	Delayed treatment	Treatment delayed up to 15 min leads to PATIENT injuries such as minor organ damage

6 The steps

6.1 Overview of the steps

STEP 1: Identify HAZARDS.

STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS.

STEP 3: Determine UNINTENDED CONSEQUENCES and estimate potential severities.

STEP 4: Estimate the probability of the UNINTENDED CONSEQUENCE.

By estimating probability and severity of UNINTENDED CONSEQUENCE, you have estimated RISK.

Iterate STEPS 1 through 4, using both top-down and bottom-up approaches.

There can be multiple HAZARDOUS SITUATIONS per HAZARD, multiple causes per HAZARDOUS SITUATION, multiple HAZARDOUS SITUATIONS per cause.

STEP 5: Evaluate RISK against pre-determined RISK acceptability criteria.

STEP 6: Identify and document proposed RISK CONTROL measures and re-evaluate RISK (i.e. return to STEP 3).

STEP 7: Implement RISK CONTROL measures.

STEP 8: Verify RISK CONTROL measures.

STEP 9: Evaluate any new RISKS arising from RISK CONTROL.

STEP 10: Evaluate and report overall RESIDUAL RISK.

6.2 A basic example using the 10 steps

6.2.1 General

The following is a basic example of executing the 10 steps which illustrates the PROCESS and clarifies the definition of terms. It is not an example of MEDICAL IT-NETWORK RISK MANAGEMENT, but an example that the RESPONSIBLE ORGANIZATION owning a MEDICAL IT-NETWORK can relate to. There are multiple other examples throughout this Technical Report that are specific to IT-NETWORKS.

For RISK ANALYSIS to begin, the system under analysis must be defined. In this case, it is a trained surgeon in closed toed shoes in an OR using a Model X scalpel. Refer to Figure 2.

6.2.2 Initial RISK – Steps 1 – 5 (Figure 2)

STEP 1: Identify the HAZARD: *Sharp edge on scalpel.*

STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS:
Cause = *Slippery handle*,
Sequence of events: *Clinician drops scalpel, scalpel falls unimpeded onto clinician's foot.*
HAZARDOUS SITUATION = *Clinician exposed to an uncontrolled sharp edge.*

STEP 3: Document the UC and estimate the potential severity of the UC:
The UC is laceration, the severity is low

STEP 4: Estimate the probability of UC:
Occasional

NOTE This is the comprehensive probability (P1 and P2) of the entire chain, including the laceration)

STEP 5: Evaluate RISK against pre-determined RISK acceptability criteria:
Moderate (use Table D.3). Evaluation includes answering the question "Is the RISK low enough to go live?"

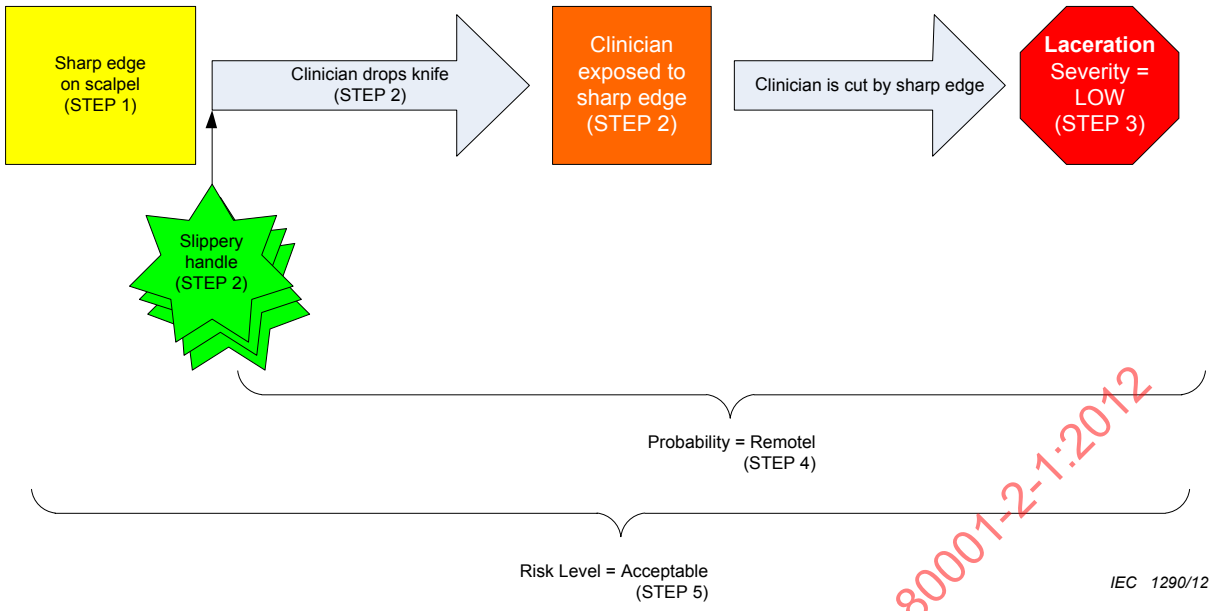


Figure 2 – Steps 1 – 5: HAZARD identification through RISK EVALUATION

6.2.3 RISK CONTROL and final RISK – Steps 6 – 10 (Figure 3)

STEP 6: Identify and document proposed RISK CONTROL measures and evaluate individual RESIDUAL RISK:

RISK CONTROL *Measure: Use Model Y of scalpel that has a slip resistant grip. (This lowers P1, and therefore lowers overall probability).*

Now return to STEP 3.

New probability = Remote.

Severity has not changed because the UC has not changed.

The new RESIDUAL RISK is now *acceptable.*

STEP 7: Implement RISK CONTROL measures: *Trial run*

STEP 8: Verify RISK CONTROL measures:

A) Verify implementation - *by inspection of stock*

B) Verify effectiveness – *pilot, research, MANUFACTURER studies, etc.*

STEP 9: Evaluate any new RISKS arising from RISK CONTROL:

For example: Model Y scalpel results in loss of articulation for surgeon. This would launch the whole 10-step RISK MANAGEMENT PROCESS over again

STEP 10: Evaluate and report overall RESIDUAL RISK:

This RISK as described above would be added to all other RESIDUAL RISKS. The policy for evaluating overall RESIDUAL RISK could then be applied.

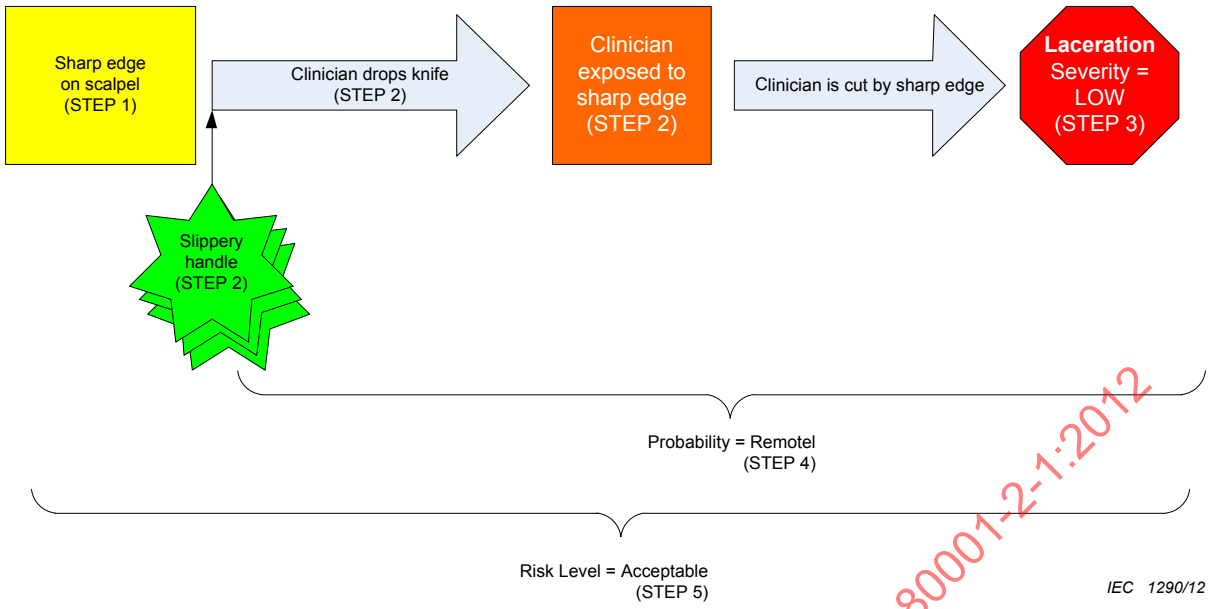


Figure 3 – Steps 6 – 10: RISK CONTROL measures through overall RESIDUAL RISK

Figure 4 illustrates how this example might be documented following the summary RISK ASSESSMENT register format used in this technical report.

#	HAZARD	HAZARDOUS SITUATION	Cause(s), Contributing factor(s)	UNINTENDED CONSEQUENCE	Initial RISK			Mitigation/ RISK CONTROL measures by design, protective measures or clinical PROCESS, or information for SAFETY	Reference to responsible organization specifications, policies or test reports or to other item in this document (whatever is applicable for traceability)	RESIDUAL RISK		
					Severity	Probability	RISK			Severity	Probability	RISK
1	HAZ01. Sharp edge	HS01. Clinician exposed to uncontrolled sharp edge	C01. Slippery Model X scalpel handle. Clinician drops scalpel, scalpel falls unimpeded.	Foot laceration	Low	Occasional	Moderate	RC01. Use Model Y scalpel that has a slip resistant grip.	Reference: Materials management and the OR Procedure Control Committee's meeting minutes	Low	Remote	Low

IEC 1291/12

Figure 4 – Sample summary RISK ASSESSMENT register format

7 IEC 80001-1:2010, Subclause 4.4: Step by step

7.1 General

RISK MANAGEMENT using the 10 steps described in this clause is an iterative PROCESS which may not be completed in one iteration. For various reasons, it might be necessary or advisable to loop back and repeat any activity because of evaluation results. Readers should feel encouraged that iteration is "allowed" and normal during all stages of a RISK MANAGEMENT PROCESS.

These 10 steps are considered to be universally applicable to all changes, large or small. The team executing these steps can apply them in a manner proportional to the size and effects of a change. A change to an existing MEDICAL IT-NETWORK can, for instance, require only a minor update of the already available RISK MANAGEMENT information.

7.2 Application of Subclause 4.4.1: Document all RISK MANAGEMENT elements

For each MEDICAL IT-NETWORK, establish and maintain a table or database that lists each HAZARDOUS SITUATION that can develop during operation of the network, along with its associated causes/probabilities and associated UNINTENDED CONSEQUENCES/severities. For the purposes of this technical report, this table will be referred to as the RISK ASSESSMENT register. The completed register will summarize the individual and overall RISKS associated with this particular MEDICAL IT-NETWORK. This register will be developed using the steps below and will be a living document that can change with subsequent changes to the network, or as a result of MONITORING after go-live.

For large networks, the register could potentially become quite large. Also, consider that one cause can lead to multiple HAZARDOUS SITUATIONS, or multiple causes can lead to one HAZARDOUS SITUATION. For these reasons, care should be taken in formatting the RISK ASSESSMENT register. A database can be considered to manage the relationship between HAZARDOUS SITUATIONS and causes.

7.3 Note about RISK EVALUATION

Subclause 4.4.2 of IEC 80001-1:2010 calls for the following activity: "For each identified HAZARD, the RESPONSIBLE ORGANIZATION shall estimate the associated RISKS". Although this step occupies only a single sentence in the IEC 80001-1:2010 standard, it is a multi-step PROCESS requiring both a RISK MANAGEMENT plan for the MEDICAL IT-NETWORK and a RISK ANALYSIS procedure to be in place before it can be executed. Steps 2 through 4 below apply to this activity.

This RISK MANAGEMENT plan must define the scale and acceptability criteria for RISK (see 4.3.5 of IEC 80001-1:2010) and should also include probability and severity scales. Refer to Appendix D in this technical report for the particular scales used in the examples in the next clause.

7.4 The 10-step PROCESS

7.4.1 STEP 1: Identify HAZARDS and HAZARDOUS SITUATIONS

The first step in RISK MANAGEMENT is to identify the HAZARDS. When using top-down analysis, start with the HAZARD and then identify the ways in which a HAZARDOUS SITUATION can be triggered (causes). When using a bottom-up approach, identify all the ways something can fail (causes), then determine if these failure modes can result in a HAZARD or HAZARDOUS SITUATION. In either case, there is benefit in identifying the HAZARDS first, which is why that is the first step in RISK MANAGEMENT per IEC 80001-1.

It is recommended to use both methods (top-down and bottom-up) to arrive at a complete list of HAZARDs and HAZARDOUS SITUATIONS associated with the MEDICAL IT-NETWORK. Fault tree analysis (FTA), is

a typical top-down method and failure modes and effects analysis (FMEA) is a typical bottom-up method.

Loss of function and more specific versions of it are HAZARDS that must be considered. Use the list in Annex A and the questions provided in Annex B of this document to help identify HAZARDS associated with the MEDICAL IT-NETWORK under analysis.

7.4.2 STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS

7.4.2.1 General

For each identified HAZARD, consider causes and sequences of events which could lead to the HAZARD or to a HAZARDOUS SITUATION. The list of common potential causes in Annex A can help facilitate your analysis. The examples in this technical report can assist in identifying a complete list of causes and HAZARDS.

As the list of potential causes is developed and connections are made between causes and HAZARDOUS SITUATIONS, additional HAZARDOUS SITUATIONS or causes can be identified. For example, once a cause has been identified that leads to a HAZARDOUS SITUATION, consider that cause again to determine if there are any other HAZARDOUS SITUATIONS it could lead to, thus making a connection between causes (that led to at least one known HAZARDOUS SITUATION) and other HAZARDOUS SITUATIONS. Continue until the list of HAZARDOUS SITUATIONS and associated causes is satisfactorily complete. Although it is important to identify all relevant HAZARDOUS SITUATIONS and associated causes, this inherits a high complexity and can be overwhelming especially during the first implementation of RISK MANAGEMENT activities. To reduce complexity, consider starting with a limited number of known HAZARDOUS SITUATIONS. The number can then be gradually increased, thus avoiding excessive demand in identification of all possible HAZARDOUS SITUATIONS and associated causes.

Causes of HAZARDS and HAZARDOUS SITUATIONS can also be non-technical in nature. User errors and organizational mismatches need to be considered. A recommended way to cover such areas of possible causes is to involve knowledgeable users in the RISK MANAGEMENT PROCESS.

Consider HAZARDOUS SITUATIONS related to each of the KEY PROPERTIES - physical injury, loss of effectiveness, or breach of security.

7.4.2.2 Multiple causes per HAZARDOUS SITUATION

Several different causes can in the end lead to a single HAZARDOUS SITUATION. It is essential that all causes are considered separately. Although the effect (UNINTENDED CONSEQUENCE/severity) of a HAZARDOUS SITUATION can be the same with different causes, the probability and overall RISK of that HAZARDOUS SITUATION might not.

For example, all of the following causes can lead to a loss of function HAZARD, or more specifically a loss of connectivity:

– cable in duct damaged from work in cable duct;
– cable in duct damaged at installation;
– cable unintentionally or intentionally disconnected in patch cabinet;
– unintentional or intentional disconnection in PATIENT room;
– overloaded link;
– poor network design;

– switch failure;
– network configuration error;
– IP ADDRESS conflict;
– EMI (ELECTROMAGNETIC INTERFERENCE);
– RF (radio frequency) dropout;
– virus;
– deterioration of equipment, cables, etc.

7.4.2.3 Multiple HAZARDOUS SITUATIONS per cause

Also note that a single cause can lead to multiple HAZARDOUS SITUATIONS, and different levels of RISK can result depending on the details and context of each different HAZARDOUS SITUATION. It is important that all HAZARDOUS SITUATIONS are considered and recorded in order to account for all RISK levels. For example, loss of network connection for a high acuity ward, such as a neonatal intensive care unit, is a higher RISK to the PATIENTS than when the network connection is lost for a low acuity ward.

For example, all of the following HAZARDOUS SITUATIONS can result from a cable fault:

– failure to deliver PATIENT related data such as lab results or drug dosages;
– failure to display medications due to be administered;
– loss of monitoring;
– inability to admit a PATIENT in the emergency room.

7.4.3 STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential severities

For each HAZARDOUS SITUATION, determine the UNINTENDED CONSEQUENCE that might result for the PATIENT, clinician, organization, etc. Estimate the potential severity of that UNINTENDED CONSEQUENCE. The UNINTENDED CONSEQUENCE might be injury of a PATIENT or clinician, loss of the organization's ability to effectively deliver quality care to PATIENTS, or exposed HEALTH DATA and subsequent consequence to the PATIENT's or organization's reputation. These track directly to the KEY PROPERTIES of IEC 80001-1 of SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY (see Table 1).

7.4.4 STEP 4: Estimate the probability of UNINTENDED CONSEQUENCE

7.4.4.1 General

For each HAZARDOUS SITUATION / cause combination, determine the probability that the defined UNINTENDED CONSEQUENCE occurs (combination of P1, and P2 in Figure 1). This probability can be considered in two components – the probability that the cause actually leads to the HAZARDOUS SITUATION (P1 in Figure 1), and the probability that once the HAZARDOUS SITUATION occurs the UNINTENDED CONSEQUENCE of the defined severity results (P2 in Figure 1). An organization can choose to formally define a method for combining P1 and P2.

As described in 5.2, some HAZARDS are inherent to the system and some arise from a cause. For simplicity, consider the probability of the sequence of events that ultimately leads to the HAZARDOUS SITUATION. This probability is called P1, and includes the creation of the HAZARD if it was not present already. In terms of loss of function, particularly for a network, the relevant sequences of events are usually those that lead to the specific loss of function HAZARD, such as loss of data, incorrect data, or incorrect timing of data delivery.

Also, it is acknowledged that estimation of probability is difficult and not precise. Monitoring and EVENT MANAGEMENT can be used to refine the estimation in future revisions. Refer to Annex E for more information on monitoring.

7.4.4.2 Probability estimations

To evaluate probability of occurrence for a particular HAZARDOUS SITUATION, it can be helpful to evaluate the probability of each associated cause independently, and conceptually combine these to an estimated probability for the HAZARDOUS SITUATION. Note that the overall probability of occurrence of the HARM includes the probability of occurrence of the HAZARDOUS SITUATION conditional probability of the defined UNINTENDED CONSEQUENCE occurring once the HAZARDOUS SITUATION is present. Use all the information available (defined HAZARDOUS SITUATIONS, all related causes, context, defined UCs, etc.) to estimate probability.

Refer to Figure 5 and note the following:

– P1 can be evaluated for a particular cause regardless of what HAZARDOUS SITUATION the cause leads to. In fact, the cause can lead to more than one HAZARDOUS SITUATION. Consider keeping an independent list of causes and associated P1s.

– Severity can be evaluated for any UNINTENDED CONSEQUENCE regardless of what HAZARDOUS SITUATION it arises from. In fact, a particular UNINTENDED CONSEQUENCE can result from several different HAZARDOUS SITUATIONS. Consider keeping an independent list of common UNINTENDED CONSEQUENCE and associated severities.

– P2 is specific to a particular *combination* of HAZARDOUS SITUATION and UNINTENDED CONSEQUENCE. In the approach described in this technical report, one primary UC is considered for each HAZARDOUS SITUATION (HARM-j in the figure below). In reality, a given HAZARDOUS SITUATION can result in different UCs with different severities and values of P2. Of all potential UCs identified, the UC selected as primary is the UC that, given the same P1, results in the highest RISK level (see Step 5). In some examples, if P2 is lowered through RISK CONTROL measures to negligible or impossible, a different UC with a lower severity might become the primary in subsequent iterations of analysis. An alternate approach is to consider each UC independently and evaluate RISK for each. This approach is more thorough and detailed, but requires a more sophisticated RISK ANALYSIS report to manage.

– The overall probability for the HAZARDOUS SITUATION is a function of P1a and P1b, as well as the particular P2 for the UC that was used.

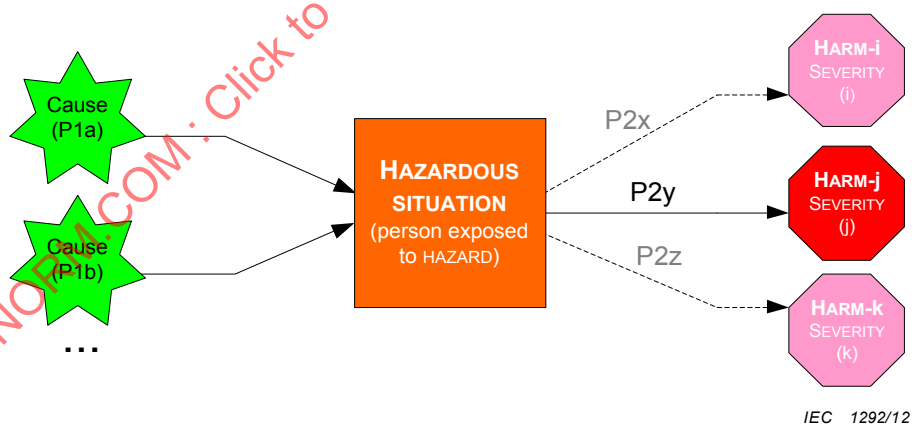


Figure 5 – Relation of cause to HARM

7.4.5 STEP 5: Evaluate RISK

At this point, a primary UC with a particular severity has been identified for each HAZARDOUS SITUATION and the overall probability of occurrence has been estimated for each of these primary UCs.

RISK is a function of severity and probability. For example, a short-term pain is acceptable at a higher probability of occurrence than would be morbidity or mortality where the severity is so high that the probability must be very low to achieve acceptability. RISK levels should be predefined by the RESPONSIBLE ORGANIZATION for all possible probability and severity combinations and compared against predetermined acceptability criteria. It is common

practice to summarize this in a RISK acceptability matrix, see Annex D for an example. For each HAZARDOUS SITUATION, apply the RISK acceptability criteria defined in the RISK MANAGEMENT plan to evaluate whether the RISK is acceptable.

In this Technical Report, the example RISK acceptability matrix has been subdivided into 3 areas – high, moderate, and low. High is considered unacceptable. Low is considered acceptable. Moderate RISK must follow policies defined in the RISK MANAGEMENT plan, which can include reduction if reasonably practicable, further organizational reviews, etc. Refer to Annex D for the acceptability matrix and a flow chart describing application of STEPs 5 and 6. In this technical report, it is assumed that RO policy requires moderate RISK to be investigated for further RISK reduction if practicable.

7.4.6 STEP 6: Identify and document proposed RISK CONTROL measures and re-evaluate RISK (return to Step 3)

7.4.6.1 General

If the evaluation in STEP 5 shows that the RISK is high, RISK CONTROL options need to be identified (this step). Often there will be more than one way to reduce RISK so the best RISK CONTROL measures need to be selected.

If the evaluation in STEP 5 shows that the RISK is moderate, then, per the assumption used in this TR as stated above, further RISK CONTROL options need to be identified (this step) and implemented if they are reasonably practicable. If further RISK reduction for those RISKS is not practicable, or if the RO policies nevertheless determine that the RISK for this case is acceptable, STEPS 7 through 9 can be omitted.

If the evaluation in STEP 5 has shown that the RISK is low, further RISK CONTROL options are not needed and STEPS 6 through 9 can be omitted.

7.4.6.2 Identify RISK CONTROL measures

As explained in 4.6 RISK CONTROL measures can reduce the probability of occurrence of the HAZARDOUS SITUATION, or can reduce the probability of occurrence of UNINTENDED CONSEQUENCEs once a HAZARDOUS SITUATION has occurred. For example, RISK resulting from a single point of failure can be reduced by eliminating that single point of failure (e.g. redundant link) or by reducing effects of failure (e.g. notification of link down).

As specified in 4.4.4.1 of IEC 80001-1:2010, when assessing which RISK CONTROL measures to implement, the following options should be considered in the priority order listed:

a) Inherent control by design (e.g. proper network capacity planning). The preferred means of controlling RISK is to eliminate or reduce its potential through design of the network system or components.

b) Protective measures (e.g. monitoring network capacity usage and alarming on limit violations). If the RISK cannot be eliminated or reduced to acceptable levels by design, then implementing a protective measure is another option. This option is less desired since it would typically require a response, which can be variable in predictability. This category can also include specific clinical or IT PROCESSES.

c) Information for assurance of the KEY PROPERTIES (e.g. warnings, user documentation, training). Providing information on the RISK is considered less effective as a RISK CONTROL option because it can rely on recognition of the RISK, along with a response.

Examples of RISK CONTROL measures are included in IEC 80001-1 and also in the practical examples clause (Clause 8) of this document.

The RISK CONTROL measures selected need to be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE. If the RESPONSIBLE ORGANISATION decides, as a result of RISK MANAGEMENT activities, that a specified type of routine change can be performed with acceptable RISK,

subject to specified constraints, then the RESPONSIBLE ORGANIZATION can define a CHANGE PERMIT which allows such routine changes and specifies the constraints. See Annex F for more consideration on CHANGE PERMITS.

7.4.6.3 Select RISK CONTROL measure

After identifying the RISK CONTROL options, select the RISK CONTROL(s) that need to be implemented to reduce the RESIDUAL RISKS to acceptable levels.

In some cases the practicability of the RISK CONTROL needs to be evaluated. A RISK CONTROL is considered not practicable if the time, effort and expense involved is disproportionate to the benefit. A procedure for evaluating proportionality and practicability could include but is not limited to:

– a qualitative analysis of the benefits and burdens of the RISK CONTROL option;
– evaluation of the increased manageability of the MEDICAL IT-NETWORK;
– evaluation of the increase in robustness of the MEDICAL IT-NETWORK.

7.4.6.4 Re-evaluate RISK

Once the RISK CONTROL measures have been selected, the probability and primary UC must be reassessed (return to STEP 3 and 4), and the RESIDUAL RISK associated with the individual HAZARDOUS SITUATION after RISK CONTROL needs to be re-evaluated (STEP 5). RESIDUAL RISK is the RISK that remains following implementation of RISK CONTROL measures. This is equivalent to the final RISK level for the HAZARDOUS SITUATION.

At this point the RISK CONTROL option is an idea only and therefore re-evaluation is based on assumptions of the expected effect on the associated RISK. A pitfall is that the assumptions are too positive towards the expected effects of the RISK CONTROL option. Record the assumptions of the re-evaluated RISK as these assumptions could be used as a requirement for the implementation of the RISK CONTROL option and/or for MONITORING the effectiveness of the RISK CONTROL option in the live environment. Document these assumptions in the RISK MANAGEMENT FILE. The correctness of this initial re-evaluation shall be demonstrated in STEP 9.

7.4.6.5 RISK/benefit analysis

It is recognized that one possible result of RISK CONTROL option analysis is that there is no practical way of reducing RISK to acceptable levels. Generally, if a HAZARDOUS SITUATION is evaluated to be unacceptable and RISK CONTROL measures are insufficient to reduce RISKS to acceptable levels, the proposed project or change should be abandoned and the decision documented in the RISK MANAGEMENT FILE. In some cases, however, the greater RISKS can be justified if they are outweighed by the expected benefits of the change. In this case, the RESPONSIBLE ORGANIZATION should conduct and document a RISK/benefit analysis to determine if the benefits of the project outweigh the potential RISKS.

After all RISK CONTROL options have been identified and selected, proceed to STEP 7.

7.4.7 STEP 7: Implement RISK CONTROL measures

In order to reduce RISK, the identified RISK CONTROL measures need to be implemented. Implementation cannot be in the live-system unless the RISK MANAGEMENT PROCESS has successfully been completed. Theoretical analysis or practical analysis within test environments should be used to evaluate the effectiveness of RISK CONTROL measures

When a specific RISK CONTROL measure is selected and implemented in the live network, CHANGE RELEASE MANAGEMENT PROCESSES need to be followed and recorded in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE. Refer to 4.5 of IEC 80001-1:2010.

7.4.8 STEP 8: Verify RISK CONTROL measures

7.4.8.1 General

VERIFICATION of RISK CONTROL measures includes verifying the implementation as well as the effectiveness of the measures. The order of execution of VERIFICATION of implementation versus VERIFICATION of effectiveness will depend on the type of RISK CONTROL measure and whether or not effectiveness can be VERIFIED in a test environment.

7.4.8.2 VERIFICATION of effectiveness

The effectiveness of the RISK CONTROL measure needs to be VERIFIED and documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE. VERIFY that the control measure has the expected effect. For example, a RISK CONTROL measure for network link failure can be to implement a redundant link. VERIFICATION of effectiveness would involve simulating a primary link failure and verifying the redundant link was effective as a RISK CONTROL measure. VERIFICATION can take place on a test implementation in a test environment prior to actual implementation in the operational system. VERIFICATION that must be performed on a live system would create the need for a change window (see below for further explanation). Verification needs to be finalized before the end of that window (go-live).

In some cases, effectiveness cannot be VERIFIED objectively, and sometimes rationalization is sufficient, i.e. training, clinical procedures, etc. In these cases, MONITORING the effectiveness of the RISK CONTROL measure provides truer insight into the effectiveness of the RISK CONTROL measure.

The VERIFICATION of effectiveness of RISK CONTROL measures in this step is performed using information and appropriate methods that are available at the moment this step is executed. After go-live and during the entire period of use of the MEDICAL IT-NETWORK, MONITORING is in place to assure sustained effectiveness of RISK CONTROL measures. New technological developments, changes in the actual use of the MEDICAL IT-NETWORK, user organization, or evaluation of events can show unanticipated weaknesses in RISK CONTROL measures that require improvements. Annex E shows example methods of evaluation of the effectiveness of RISK CONTROL measures as part of MONITORING.

Effectiveness of RISK CONTROL measures can only be determined with a clear understanding of the required effect of that RISK CONTROL measure. Sustained effectiveness in the live phase can only be monitored when the required effect is clearly defined and recorded with the implemented RISK CONTROL measure.

VERIFICATION of implementation

The implementation of all RISK CONTROL measures needs to be VERIFIED and documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE. This VERIFICATION effort confirms that the RISK CONTROL measure is actually implemented in the MEDICAL IT-NETWORK, and it should take place before go-live. Go-live refers to putting the MEDICAL IT-NETWORK into use, usually PATIENT use. This can mean one of the following:

– for new networks, completing VERIFICATION before go-live, or,
– in cases where the network is already in use, defining a “change window” where the network is considered to be in a state of change. Back-out or roll-back plans are in effect and possibly temporary clinical procedures (e.g. bedside monitoring vs. central monitoring). VERIFICATION of implementation should occur before the end of the change window. Refer to Annex G for an example of items to consider as part of a change window.

VERIFICATION of implementation should be facilitated by the CHANGE RELEASE MANAGEMENT PROCESS.

7.4.9 STEP 9: Evaluate any new RISKS arising from RISK CONTROL

It is possible that the implementation of new RISK CONTROL measures can introduce new RISKs. An example might be the addition of too much security, resulting in a clinician being unable to get information for a PATIENT when needed. In this case, it might be necessary to modify or change the RISK CONTROL measure to be a clinical practice rather than an IT solution.

The evaluation for new RISKS needs to be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE. Any new RISK needs to be evaluated following STEPs 2 to 9. This is an iterative PROCESS which can consist of more than one iteration cycle.

7.4.10 STEP 10: Evaluate and report overall RESIDUAL RISK

In addition to any RESIDUAL RISKS associated with individual HAZARDOUS SITUATIONS, the RESPONSIBLE ORGANIZATION needs to also determine the overall RESIDUAL RISK associated with the MEDICAL IT-NETWORK. Determining overall RESIDUAL RISK involves evaluating all the individual RESIDUAL RISKS and determining if the RISK of the whole is more than the sum of the parts. For example, while two individual HAZARDOUS SITUATIONS might each have acceptable RESIDUAL RISK, if both HAZARDOUS SITUATIONS are likely to occur at the same time, the overall RESIDUAL RISK might not be acceptable.

The RESPONSIBLE ORGANIZATION needs to define and document a RESIDUAL RISK summary containing a list of all individual RESIDUAL RISKS and the overall RESIDUAL RISK remaining after the RISK CONTROL measures have been implemented. This is the RISK ASSESSMENT register.

As described in 7.4.6, one type of RISK CONTROL measure is to provide information for the users of the system. This information often contains training, labeling, or warnings of particular uses that can lead to HAZARDOUS SITUATIONS. When evaluating overall RESIDUAL RISK, consider whether there is any other additional information about RISK in the system that should be communicated to users of the MEDICAL IT-NETWORK and whether channels for this communication need to be established.

There is no preferred method of evaluating the acceptability of overall RESIDUAL RISK – the RESPONSIBLE ORGANIZATION needs to determine the method and criteria to be followed in the policy for RISK MANAGEMENT. Approaches might be qualitative or quantitative. An example of a more qualitative approach to evaluating overall RESIDUAL RISK might be to define an acceptable maximum number of HAZARDOUS SITUATIONS that remain at a medium RISK level following RISK CONTROL measures. A more quantitative approach might be to predict the cumulative rate of UNINTENDED CONSEQUENCE or number of injuries due to all HAZARDOUS SITUATIONS following RISK CONTROL, and compare that overall RESIDUAL RISK to a pre-established acceptance level.

If reduction of overall RESIDUAL RISK to an acceptable level is not practicable, a RISK/benefit analysis of the overall RESIDUAL RISK against the benefit accrued from the planned change to the MEDICAL IT-NETWORK needs to be conducted and documented.

Both the individual RESIDUAL RISKS and overall RESIDUAL RISK need to be documented in the MEDICAL IT-NETWORK RISK MANAGEMENT FILE.

7.5 The steps and their relationship to IEC 80001-1 and ISO 14971

Table 3 shows the relationship between this technical report, IEC 80001-1:2010 and ISO 14971:2007. Clauses and subclauses that are not in this technical report are not shown.

Table 3 – Relationship between this technical report, IEC 80001-1:2010 and ISO 14971:2007

14971 clause/subclause		80001 subclause		STEPS
4	RISK ANALYSIS			
4.1	RISK ANALYSIS PROCESS	n/a		
4.2	INTENDED USE and identification of characteristics related to SAFETY		(Medical IT network documented and defined per 4.3)	
4.3	Identification of HAZARDS	4.4.2	RISK ANALYSIS	STEP 1. Identify HAZARDS
4.4	Estimation of the RISK (s) for each HAZARDOUS SITUATION "Reasonably foreseeable sequences or combinations of events that can result in a HAZARDOUS SITUATION shall be considered and the resulting HAZARDOUS SITUATION (s) shall be recorded" "For each identified HAZARDOUS SITUATION, the associated RISK (s) shall be estimated"		"For each identified HAZARD, the RO shall estimate the associated RISKS…"	STEP 2. Identify causes and resulting HAZARDOUS SITUATIONS STEP 3. Determine UNINTENDED CONSEQUENCES and estimate potential severities* STEP 4. Estimate the probability* of the UNINTENDED CONSEQUENCE *By estimating probability and severity of UNINTENDED CONSEQUENCE, you have estimated RISK. Iterate STEPS 1 through 4, use top-down and bottom-up. Potentially multiple HAZARDOUS SITUATIONS per HAZARD, multiple causes per HAZARDOUS SITUATION, multiple HAZARDOUS SITUATIONS per cause
5	RISK EVALUATION	4.4.3	RISK EVALUATION	STEP 5. Evaluate RISK against pre-determined RISK acceptability criteria
6	RISK CONTROL	4.4.4	RISK CONTROL	
6.1	RISK reduction	n/a		
6.2	RISK CONTROL option analysis	4.4.4.1	RISK CONTROL option analysis	STEP 6. Identify and document proposed RISK CONTROL measures and re-evaluate RISK (i.e. return to STEP 3)
6.3	Implementation of RISK CONTROL measures	4.4.4.3	Implementation of RISK CONTROL measures	STEP 7. Implement RISK CONTROL measures
		4.4.4.4	VERIFICATION of RISK CONTROL measures	STEP 8. Verify RISK CONTROL measures
6.4	RESIDUAL RISK evaluation		(addressed in 4.4.4.1)	
6.5	RISK/benefit analysis		(addressed in both 4.4.4.1 and 4.4.5)	(addressed in STEP 6 and STEP 10)
6.6	RISKS arising form RISK CONTROL measures	4.4.4.5	New RISKS arising from RISK CONTROL	STEP 9. Evaluate any new RISKS arising from RISK CONTROL
7	Evaluation of overall RESIDUAL RISK acceptability	4.4.5	RESIDUAL RISK evaluation and reporting	STEP 10. Evaluate and report overall RESIDUAL RISK

8 Practical examples

8.1 General

The examples below will follow development of a small set of applicable HAZARDOUS SITUATIONS and causes for each of three scenarios. These are not exhaustive examples. Rather, they represent specific threads through the RISK ANALYSIS and control PROCESS for one or two particular HAZARDOUS SITUATIONS and one or two related causes in each case. For RISK to be evaluated, the details and scope of the system under analysis must be fully defined.

Also, the actual use of the network and the MEDICAL DEVICES attached to it must be known. The examples below begin with an explanation of the context as well as a description of the network under analysis. They then follow each of the steps through the PROCESS, as detailed above. Unique identifiers are assigned to each unique HAZARD, HAZARDOUS SITUATION, cause, and RISK CONTROL measure.

The examples are fictional and should not be considered applicable to all organizations.

The examples in this clause use the following format:

– define full description of context (clinical use case);
– define network under analysis;
– unique identifiers are applied:
  - HAZARDS are denoted as HAZ01, HAZ02…;
  - HAZARDOUS SITUATIONS are denoted as HS01, HS02…;
  - causes are denoted as C01, C02…;
  - RISK CONTROL measures are denoted as RC01, RC02…

8.2 Example 1: Wireless PATIENT monitoring during PATIENT transport

8.2.1 Full description of context

A wireless network is used to transfer real-time data of a PATIENT in transport mode. The acuity of PATIENTS can vary widely. The PATIENT might be transferred between the emergency room, radiology, or other diagnostic areas to the general ward, or to an ICU (intensive care unit). The PATIENT is attached to an 802.11b/g wireless enabled PATIENT monitor. During transport, the real time PATIENT data is sent from the PATIENT monitor to nurse stations for PATIENT surveillance and to the hospital electronic medical record system for archiving.

8.2.2 Description of network under analysis

The 802.11 wireless area network (WLAN) covers the entire hospital, and uses the 802.11a/b/g (2.4 & 5 GHz) band. There are eight network identifiers in use on the WLAN, including a guest access SSID (service set identifier) and in certain areas of coverage there can be a large number of wireless users. One of the SSIDs is dedicate to PATIENT monitoring. The radiology department is located near the main kitchen, which uses high power commercial microwave ovens. The hospital also uses cordless DECT (Digital Enhanced Cordless Telecommunication) telephones in the 2,4 GHz band. Also refer to 80001-2-3:2012 for further discussion of RISK CONTROLS for wireless networks.

8.2.3 The 10 Steps

STEP 1: Identify HAZARDS

HAZ01: Complete loss of connectivity.

HAZ02: Intermittent connectivity.

STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS

C01: RF interference from a microwave oven causes immediate loss of connectivity between client device and WAP (Wireless Access Point).

C02: RF interference from DECT phones causes intermittent loss of connectivity between client device and WAP.

C03: Too many client devices cause WAP overload, causing intermittent data loss.

The following HAZARDOUS SITUATIONS are identified:

HS01: Clinician is unaware of PATIENT in need of treatment. Delay in treatment due to loss of data (alarms are not received by the clinician). ***(from Cause C01, C02 or C03).***

STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential **severities.**

Refer to Table D.2 for severity scales. Note this severity estimation is based on knowing the acuity level of the PATIENT.

UC for **HS01**: In this case, because the acuity of the PATIENTS can vary widely and they are not under local/direct observation by a clinician during transport, loss of real-time data for high acuity PATIENTS could lead to severe injury. (Note that mitigations can be customized based on the acuity of the PATIENTS). Severity: *catastrophic*.

STEP 4: Estimate the **probability** of the UNINTENDED CONSEQUENCE

In this example, we are estimating the probability that any of the causes listed above lead to the UC stated above with specified severity.

Refer to Table D.1 for probability scales.

HS01: *Remote*

STEP 5: Evaluate **RISK** against pre-determined RISK acceptability criteria

Using Table D.3, the initial RISK level was determined to be high based on the probability and severity determined in STEPS 3 and 4.

HS01: (catastrophic/remote). RISKlevel = *high*

STEP 6: Identify and document proposed RISK CONTROL measures and evaluate individual RESIDUAL RISK

In this case, RISK CONTROL measures were identified that reduce both P1 and P2.

To reduce P1, each cause was examined separately and RISK CONTROL measures were determined.

Cause 1: RF interference (microwave oven):

RC01: Replace the old microwave oven effectively reducing the RF emissions because newer units are better shielded.

Cause 3: WAP capacity overload:

RC02: Design the capacity of the network to overprovision the number of WAPs in an area such that fewer clients are serviced by a single WAP.

To reduce P2, the following RISK CONTROL measure is identified:

RC03: A clinician attends the PATIENT during transport. The clinical protocol can be designed such that clinician attendance during transport is only required for PATIENTS above a pre-determined acuity level. This RISK CONTROL measure serves to reduce the probability of severe injury, effectively reducing the potential maximum severity of the injury.

Note that no mitigation was selected specifically for Cause 2 low probability of occurrence and low practicability of mitigation (remove all DECT phones).

HS01: (new severity/probability = *medium/improbable*). RISKlevel = *low*

STEP 7: Implement RISK CONTROL measures

RISK CONTROL measures must be implemented so that they can be VERIFIED before go-live.

RC01: Replace microwave – Replace microwave with newer, lower emissions microwave. Amend purchasing requirements for microwave ovens to include appropriate RF shielding requirements to assure installation of EM compatible microwaves in the future.

RC02: Overprovision WAPs – Identify physical/geographical locations (e.g. nurses station, etc.) that have a higher number of users and dense wireless traffic per square foot and increase the density of WAPs in that area.

RC03: Clinical procedure – A clinical transport policy is created/updated. At the conclusion of RISK MANAGEMENT activities, RISK CONTROL measures will be instituted in the live system. This would need to include clinician training and staff availability.

STEP 8: VERIFY RISK CONTROL measures

RC01 VERIFICATION:

Implementation: Verify that EM compatibility requirements are included in the purchasing documentation. Selected microwave fulfils additional requirement through review of independent test reports (preferred) or local measurements. Check that old microwaves are removed.

Effectiveness: Use a spectrum analyzer to measure the RF emissions in the vicinity of the microwave. Additionally, use the RF interference measurement capabilities of the WLAN (if available) to determine the levels of interference as seen by the WAP(s). Perform these measurements prior to replacing the older microwave oven and again after replacement. Document the difference in RF interference and perform a connectivity test with a test unit in the vicinity of the microwave ovens to verify the elimination of connectivity dropout.

RC02 VERIFICATION:

Implementation: Confirm WAP density and availability is as per updated design before go-live. Use a set of actual endpoint devices to emulate the peak loading situation and confirm capacity availability meets design target (50 % in this case).

Effectiveness: Verify that at peak usage the increase in the number of WAPs in the physical area eliminates any WAP overload. Do this by using the actual types and quantity of devices that will be used in this area and measure a peak usage scenario loading of the WAP(s). This can be measured with a 3rd party airtime usage tool, or the actual infrastructure's built-in capacity analysis tools. Verify that each device maintains connectivity per its required network characteristics and that no WAP sees its available capacity reduced below 50 % (refer to Wireless Technical Report for further discussion on capacity planning).

RC03 VERIFICATION:

Implementation: Verify protocol is in place, staff is trained accordingly and available at go-live.

Effectiveness: Verify training effectiveness via test or certification.

STEP 9: Evaluate any new RISKs arising from RISK CONTROL

Evaluation has concluded no new RISKs have been introduced by the added RISK CONTROLS.

STEP 10: Evaluate and report overall RESIDUAL RISK

Because these examples represent only one or two threads through the PROCESS for a given MEDICAL IT-NETWORK, the concept of overall RESIDUAL RISK is difficult to demonstrate. For the purposes of this Technical Report, assume that the overall RESIDUAL RISK is determined to be acceptable per RO policy.

8.3 Example 2: Remote ICU / Distance medicine

8.3.1 Full description of context

In this scenario, a METROPOLITAN AREA NETWORK (MAN) is used to transfer real-time PATIENT data from a remote site to be used by a local clinician for purposes of monitoring, diagnosing and determining treatment. PATIENTS being monitored are those in a post heart surgery step-down unit. Acuity is typically lower than critical care units. The “local clinician” in this case is a telemetry clinician (technician, nurse, doctor, etc.) who is geographically separated from the remote PATIENT. In this case, the clinician’s site is connected to the PATIENT’s site via a MAN.

8.3.2 Description of network under analysis

The network under analysis includes an enterprise level 10/100 access switch to which the PATIENT monitors are attached in the step-down unit, a leased MANUFACTURER with a guaranteed bandwidth of 12 gigabytes for all traffic from this site (includes other applications besides the remote monitoring), and an enterprise level 10/100 access switch at the clinician side. Based on bandwidth and delay requirements from the MANUFACTURER, the MANUFACTURER has been provisioned to accommodate the traffic from the monitors as well as that predicted to be used by other applications sharing the link. The MANUFACTURER provider has guaranteed a minimum service level which includes bandwidth sufficient for all of these applications (current use).

8.3.3 The 10 Steps

STEP 1: Identify HAZARDS

The network in this example is intended to transport real-time PATIENT data from the PATIENT site to the clinician site. Failure to do so would be a HAZARD.

HAZ01: Intermittent connectivity

HAZ02: Complete loss of connectivity

STEP 2: Identify causes and resulting HAZARDOUS SITUATIONS

In this case, as is often the case, for this HAZARD in the given context, multiple causes can be identified, and they might lead to one or more HAZARDOUS SITUATIONS.

C01: Unplanned non-real-time traffic attempting to use link causes overloaded MAN link.

C02: A MAN outage out of RO control (provider failure) causes a complete network outage.

The following HAZARDOUS SITUATIONS are identified:

HS01: Waveform display is choppy and incomplete. Delay in provision of care because remote clinician is unable to evaluate PATIENT ECG waveform. ***(from Cause C01)***

HS02: Alarm data not received. Delay in provision of care because clinician is unaware of PATIENT in need of treatment. (From Cause C01)

HS03: Remote clinician must determine treatment without access to real-time PATIENT data. ***(From Cause C02)***

STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential **severities**

Refer to Table D.2 for severity scales. Note this severity estimation is based on knowing the acuity level of the typical PATIENT in this use case.

UC for **HS01**: Short treatment delay can lead to PATIENT injuries such as minor organ damage. Severity is Low.

UC for **HS02**: Short treatment delay can lead to PATIENT injuries such as minor organ damage. Severity is Low.

UC for **HS03**: Incorrect treatment can lead to permanent PATIENT injuries. Severity is Medium.

STEP 4: Estimate the **probability** of the UNINTENDED CONSEQUENCE

To evaluate probability of occurrence for a particular HAZARDOUS SITUATION, it can be helpful to evaluate the probability of each associated cause independently, and conceptually "roll up" these to an estimated probability for the HAZARDOUS SITUATION. Note that the overall probability includes the probability of the defined UNINTENDED CONSEQUENCE occurring once the HAZARDOUS SITUATION is present. Use all the information available (defined HAZARDOUS SITUATIONS, all related causes, context, defined UCs, etc) to estimate probability. Refer to Table D.1 for probability scales.

HS01: *Probable*

HS02: *Occasional*

HS03: *Remote*

STEP 5: Evaluate **RISK** against pre-determined RISK acceptability criteria

Using Table D.3, calculate the initial RISK level based on the probability and severity determined in STEPS 3 and 4.

HS01: (Low/Probable). RISK level = *Moderate*

HS02: *(Low/Occasional).* RISK level = *Moderate*

HS03: *(Medium/Remote).* RISK level = *Moderate*

STEP 6: Identify and document proposed RISK CONTROL measures and evaluate individual RESIDUAL RISK

RC01: Implementation of a QoS policy so that high priority traffic is not interrupted by lower priority traffic

RC02: Redundant connection to the remote site.

In this example, only RISK CONTROL measures that affect probability of the HAZARDOUS SITUATION occurring are used. Therefore, the defined UNINTENDED

CONSEQUENCES and associated severities are not changed. New probabilities are listed below.

HS01: *Remote*

HS02: *Remote*

HS03: *Improbable*

New RISK levels are listed below.

HS01: (new severity/probability = *low/remote*). RISK level = *low*

HS02: (new severity/probability = *low/remote*). RISK level = *low*

HS03: (new severity/probability = *medium/improbable*). RISK level = *low*

STEP 7: Implement RISK CONTROL measures

RISK CONTROL measures must be implemented so that they can be VERIFIED before go-live.

RC01: In the case of a QoS policy, this could be implemented on a small sample network in a lab, or the RO can include design and testing of such a policy in the RESPONSIBILITY AGREEMENT with the IT Vendor providing the network equipment.

RC02: Implementation of a redundant link would need to be coordinated with the provider.

STEP 8: Verify RISK CONTROL measures

RC01 VERIFICATION:

Effectiveness: The new QoS configuration would be tested in a lab prior to implementation in the live system to verify that it performs as expected.

Implementation: In this example, CHANGE RELEASE MANAGEMENT would ensure that the implementation is completed and in the actual MEDICAL IT-NETWORK.

RC02 VERIFICATION:

Effectiveness: The new redundant link would be simulated and tested in a lab prior to implementation in the live system to verify that it performs as expected particularly with respect to failover. If possible, perform the test on the actual network in a controlled change window.

Implementation: In this example, CHANGE RELEASE MANAGEMENT would ensure that the implementation is completed and in the actual MEDICAL IT-NETWORK.

STEP 9: Evaluate any new RISKs arising from RISK CONTROL

Evaluation has concluded no new RISKs have been introduced by the added RISK CONTROLS.

STEP 10: Evaluate and report overall RESIDUAL RISK

Because these examples represent only one or two threads through the PROCESS for a given MEDICAL IT-NETWORK, the concept of overall RESIDUAL RISK is difficult to show. For the purposes of this technical report, assume that the overall RESIDUAL RISK is determined to be acceptable per RO policy

8.4 Example 3: Post Anaesthesia Care Unit (PACU)

8.4.1 Full description of context

The Post Anaesthesia Care Unit (PACU) is a department within the critical care service line. The PATIENTS range from infant to geriatric. Immediate postoperative care and monitoring is provided for PATIENTS who have had general or monitored anaesthesia care, and who have just undergone an invasive procedure up to and including surgery. The PATIENT acuity extends from less acute to complex critically ill PATIENTS requiring multiple invasive monitoring modalities and treatment including mechanical ventilation. Service is provided for 1 000 to 1 200 PATIENTS per month and the department is operated on a 24-hour basis.

The PACU department is designed in an open bay layout. The nurse station has a "line of sight" on all of the PACU beds. The clinician is within close proximity to the PATIENT at all times.

8.4.2 Description of network under analysis

The existing PATIENT monitoring equipment has reached full depreciation, is no longer supported by the manufacture (end of life) and is not used in any of the other critical care areas. Therefore an equipment replacement project has been approved by the capital committee.

The existing fourteen (14) PACU PATIENT monitors will be replaced with fourteen (14) new PATIENT monitors connected to a Central Information Center (CIC). The new monitors and the CIC are connected via a hard-wired network using CAT5 data cabling (see Figure 6). The real-time waveform PATIENT data will be sent to the CIC for central alarms, printing and historical data recording. The new PATIENT monitors will interface to the hospital's cardiology information system for the transmission of 12 lead ECG's from the 14 bedside monitors. The connection between the new PATIENT monitors and the Cardiology Information System will be accomplished by using dedicated multi-mode fiber optic lines between the PACU dedicated network switch and the dedicated router for the cardiology information system.

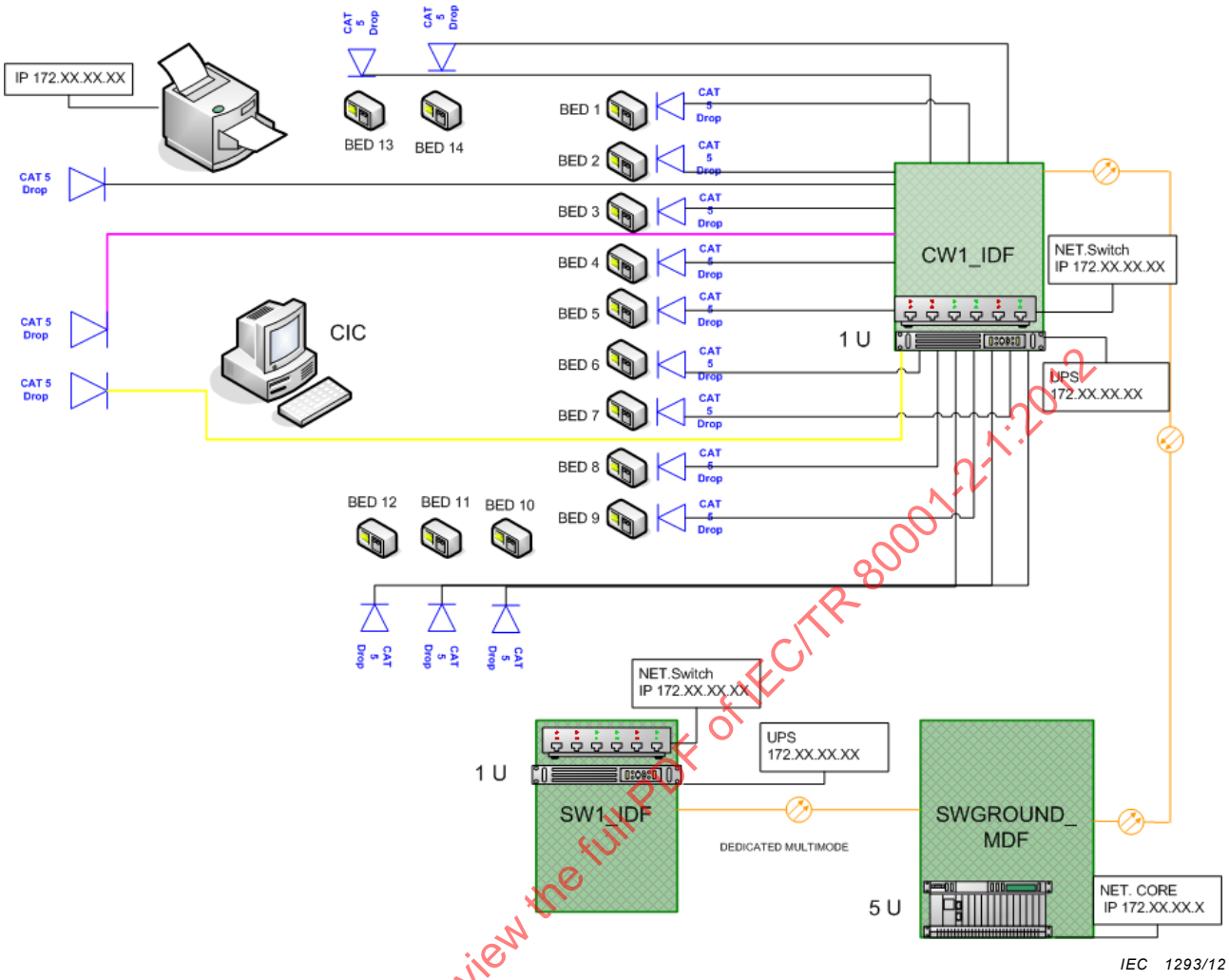


Figure 6 – Schematic of the Post Anaesthesia Care Unit (PACU)

8.4.3 The 10 Steps

STEP 1: Identify HAZARDS

HAZ01: Complete loss of connectivity (See Figure 8)

STEP 2: Identify Causes and resulting HAZARDOUS SITUATIONS

C01: Network switch not configured properly

C02: Hardware Failure on network switch

C03: Power loss to network switch

The following HAZARDOUS SITUATIONS are identified:

HS01: Delay in or non-provision of care due to loss of real-time PATIENT data and alarms. ***(from Cause C01, C02, and C03)***

HS02: Delay in or non-provision of care due to loss of historical PATIENT data, including 12-lead ECG reports and strip recorder and laser printing. ***(from Cause C01, C02, and C03)***

STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential **severities**

In the PACU, clinicians are line-of-sight with the PATIENTS, and the bedside monitor alarms are audible. Historical data is not as critical compared to other care areas such as the ICU. Standalone portable physiological monitors could be used to print

strips in the event of a total network failure. Portable ECG machines could be used to send a PATIENT's ECG to the Cardiology Information System via an analog phone line.

Refer to Table D.2 for severity scales. Note this severity estimation is based on knowing the acuity level of the typical PATIENT in this use case.

UC for **HS01**: In this case, because a clinician is within line-of-sight of the PATIENTs, loss of real-time data to the CIC is expected to lead to a UC which is no more severe than temporary or minor injury. Severity is *medium*

UC for **HS02**: In this case, because the lost data is non-real-time or historical, the severity of the UC is expected to be no more severe than temporary discomfort. Severity is *low*

STEP 4: Estimate the **probability** of the UNINTENDED CONSEQUENCE

Refer to Table D.1 for probability scales.

HS01: *Remote*

HS02: *Remote*

STEP 5: Evaluate **RISK** against pre-determined RISK acceptability criteria

Using Table D.3, calculate the initial RISK level based on the probability and severity determined in STEPS 3 and 4.

HS01: (Medium/Remote). RISK level = *Moderate*

HS02: (Low/Remote). RISK level = *Low*

STEP 6: Identify and document proposed RISK CONTROL measures and evaluate individual RESIDUAL RISK

In this case, each cause was examined separately and RISK CONTROL measures were determined.

Cause 1: Lost connectivity due to network switch not configured properly:

RC01: Utilize the practice of Network Switch Management. Assign biomedical (life critical) network switches a unique naming convention that distinguishes the network switch apart from regular IT data switches.

RC02: Physically identify the network switch by using colour coded patch cables indicating a clear and obvious difference from other regular IT data switches

Cause 2: Hardware failure on network switch:

RC03: Keep a spare pre-configured network switch in the Biomedical Engineering Department that could be used to physically replace a defective network switch. This approach will greatly minimize system downtime.

Cause 3: Power loss to network switch:

RC04: Connect the network switch to a managed uninterruptible battery power supply (UPS). If there is a power fail to the network closet an email is sent to the Biomedical Engineering Department and IT support indicating the power loss and that the network switch is running on battery power.

RC01, RC02, and RC04 reduce the probability of the HAZARDOUS SITUATION occurring in the first place (P1). RC03 is in effect after the HAZARDOUS SITUATION occurs, so therefore reduces the probability that the HAZARDOUS SITUATION leads to an UC (P2). Together, they reduce the probability to *improbable*.

HS01: (new severity/probability = *medium/improbable*). RISK level = *low*

HS01: (new severity/probability = low/improbable). RISK level = low

STEP 7: Implement RISK CONTROL measures

RISK CONTROL measures must be implemented so that they can be VERIFIED before go-live.

RC01: **Network switch management** – the network switch used for PATIENT monitoring has been given a naming convention called "Unity_Biomed" to distinguish this device as a PATIENT monitoring component.

RC02: **Color coded patch cables** - Unique colour coded patch cables "Pink & Yellow" are used to patch in the data cables from the PATIENT monitor to the network switch. Pink and yellow patch cables are used for PATIENT monitoring equipment only. Pink indicates mission critical (MC), real-time data. Yellow indicates Information Exchange (IX), non-real-time data flow such as print requests and full disclosure.

RC03: **Spare switch** - A spare pre-configured switch is located in the Biomed shop that could be used if the PATIENT monitoring system has a switch failure

RC04: **UPS** - The network switch is connected to a managed UPS

In this example, the old network can continue to be used in the live environment while the new network and monitors are installed. This affords the opportunity to implement all RISK CONTROL measures prior to go-live. (Note that in cases where implementation must occur on a live network, a change window can be used.)

STEP 8: VERIFY RISK CONTROL measures

RC01 VERIFICATION:

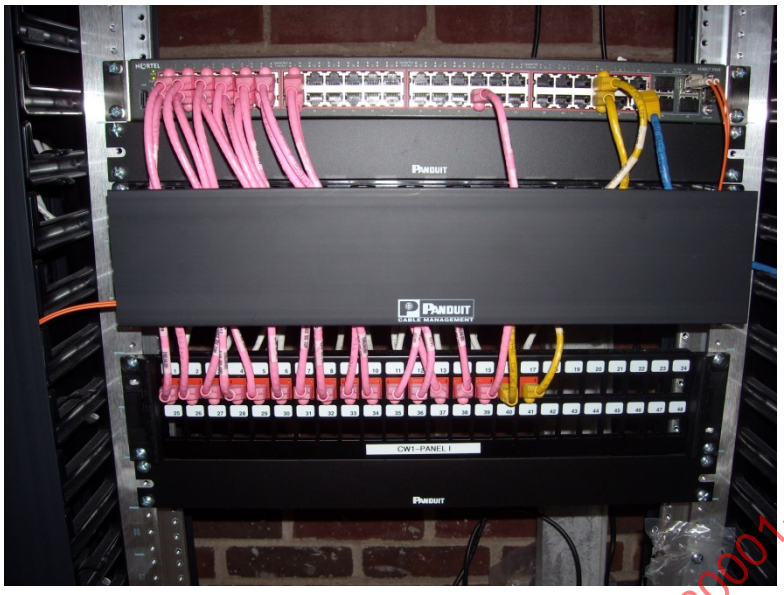
Implementation: Network switches are shown to have properly configured names according to defined naming convention.

Effectiveness: In this case, the assertion is that a network that is actively managed is less likely to fail than one that is not. VERIFICATION of effectiveness of this RISK CONTROL measure can consist of a rationale as to why this assertion is made.

RC02 VERIFICATION:

Implementation: By inspection, network switches are show to have properly color-coded cables.

Effectiveness: In this case, the assertion is that physical network identifiers and colour coded cables reduce the RISK of misconfiguration. VERIFICATION of effectiveness of this RISK CONTROL measure can consist of a rationale as to why this assertion is made (see Figure 7).



IEC 1294/12

Figure 7 – Example of the use of colour coding cables

RC03 VERIFICATION:

Implementation: Confirm biomedical department inventory contains spare switch.

Effectiveness: Simulate a failed switch condition and measure time to replace with backup switch.

RC04 VERIFICATION:

Implementation: Simulate a power loss and confirm that UPS is engaged and that biomedical or IT personnel are notified.

Effectiveness: Simulate a power loss and confirm that UPS is engaged, and that no loss of connectivity is realized (see Figure 8).

STEP 9: Evaluate any new RISKS arising from RISK CONTROL

Evaluation has concluded no new RISKs have been introduced by the added RISK CONTROLS.

STEP 10: Evaluate and report overall RESIDUAL RISK

Because these examples represent only one or two threads through the PROCESS for a given MEDICAL IT-NETWORK, the concept of overall RESIDUAL RISK is difficult to show. For the purposes of this technical report, assume that the overall RESIDUAL RISK is determined to be acceptable per RO policy.

#	HAZARD	Cause(s), Contributing Factors	HAZARDOUS SITUATION	UNINTENDED CONSEQUENCE	Initial RISK			Mitigation/ RISK CONTROL measures by design, protective measures or clinical PROCESS, Or information for SAFETY	Reference to RESPONSIBLE ORGANIZATION'S specifications, policies or test reports or to other item in this document (whatever is applicable for traceability)	RESIDUAL RISK		
					Severity	Probability	RISK			Severity	Probability	RISK
1	**HAZ01.** Complete Loss of Network Connectivity	**C01**. network switch not configured properly	**HS01.** Delay in or non-provision of care due to loss of real-time PATIENT data and alarms. (from Cause C01, C02 and C03)	Delay in delivery of care. In the PACU, clinicians are line-of-sight with the PATIENTs, and the bedside monitor alarms are audible. Historical data is not as critical compared to other care area such as ICU. Standalone portable physiological monitors could be used to monitor and print strips in the event of a total network failure. Portable ECG machines could be used to send a PATIENT's ECG to the Cardiology Information System via an analog phone line.	MEDIUM	REMOTE	MODERATE	**RC01**. Network Switch Management - switch uses a unique naming convention "Unity_Biomed" to distinguish this device as a PATIENT monitoring component **RC02**. Physical - Unique color coded patch cables "Pink & Yellow" used to patch in the data cables from the PATIENT monitor to the network switch. Pink and Yellow patch cables are used for PATIENT monitoring only.	Refer to Clinical Policy for PACU emergency situation	MEDIUM	IMPROBABLE	LOW
		C02. hardware failure on network switch	**HS02**. Delay in or non-provision of care due to loss of historical PATIENT data, including 12-lead ECG reports and strip recorder and laser printing (from cause C01, C02 and C03)		LOW	REMOTE	LOW	**RC03.** Spare pre-configured switch in Biomed shop that could be installed	Insert name and date VERIFIED in RISK MANAGEMENT file	LOW	IMPROBABLE	LOW
		C03. power loss to network switch						**RC04.** Switch is connected to a managed UPS	Confirmed by test email from device. Part of RISK MANAGEMENT file			

Figure 8 – Sample summary RISK ASSESSMENT register for the PACU example

8.5 Example 4: Ultrasound –Operating System (OS) vulnerability

8.5.1 Full description of context

An OS vendor releases a patch to their operating system which closes an exploitable vulnerability (a worm that has been identified) on an ultrasound system. Impact to the delivery of care could result (reduced speed; unusable functions) if the ultrasound system is exposed. The ultrasound MANUFACTURER requires time to verify and validate the patch before it can be applied to the MEDICAL DEVICE. The worm has been found on network-connected devices in the RO. The network is used to retrieve PATIENT information and scheduled procedures from a hospital information system (e.g, DICOM modality worklist server). The network provides the means to archive by moving ultrasound image studies from an ultrasound system to a Picture Archiving and Communication System (PACS). As a final step in the procedure the network is used to report back to the hospital information system successful study completion. A workstation component can be added and then used to pull the ultrasound Images from a PACS server in order perform additional processing such as measurements and reporting off the ultrasound system, to create an efficient workflow for PATIENTs and diagnostic radiologists. Once the worm settles on the ultrasound system, it can use vulnerabilities in the OS of other devices that are connected to the RO's IT-NETWORK. The RO realizes that the RISKs associated with the (unpatched) vulnerable ultrasound must be managed.

8.5.2 Description of network under analysis

The Ethernet network covers the entire hospital and supports 100 MB / Gigabit network speeds. A DHCP (Dynamic Host Configuration Protocol) server is available to automatically manage IP ADDRESS configuration. The ultrasound system is a mobile MEDICAL DEVICE and moves between catheterization suite, emergency room, and clinical rooms throughout the hospital. There are VLANs defined to create enclaves (protected networks) where MEDICAL DEVICES are used, and to separate MEDICAL DEVICE from standard desktop computers. All devices connected to the PACS are in one VLAN (Virtual LOCAL AREA NETWORK).

8.5.3 The 10 Steps

STEP 1: Identify HAZARDS

HAZ01:Unauthorized access to data (PATIENT information or organization information)

HAZ02 Degraded function of MEDICAL DEVICE (Loss of functional use of the system)

HAZ03:Loss of availability (access to data required for procedures is limited or denied)

STEP 2 Identify causes and resulting HAZARDOUS SITUATIONS

C01: Expose HEALTH DATA – Malicious software is downloaded to the system which could mine for personal identifiable information (PII: e.g., social security number, medical record number, birth date …) and export off the system if found.

C02: System performance impact – Malicious or non-malicious software downloaded and installed on system. System resources being consumed for password crackers, network congestion, scanning or, peer-to-peer network activity.

C03: Expose private data – The ultrasound device can become a source of threats to other devices connected to the IT-NETWORK for that vulnerability.

The following HAZARDOUS SITUATIONS are identified:

HS01: (Security of data) Unknown to the clinician or radiologist a virus or worm installs a key logger, or can automatically mine for personally identifiable information and export login and PII to an unauthorized location. ***(from Cause C01)***

HS02: (SAFETY) During a clinical scan (obstetrics, cardiology, gastrointestinal) consumption of hardware resources by the malicious software degrades performance resulting in the imaging procedure failing or treatment compromised (e.g., amniocentesis needle navigation impossible). ***(from Cause C02)***

HS03: (Effectiveness) Loss of availability - access to a Modality Worklist Server is denied due to heavy network congestion; , or System is not able to access a PACS server to store acquired image data for use in off cart or other medical procedures. Scheduling system failure and clinician/technician must resort to manual methods ***(from Cause C02)***

HS04: (Security and effectiveness) Unknown to clinicians or staff, multiple devices are exposed to the vulnerability causing HS01 and HS03 on other devices in the network enclave. ***(from Cause C03)***

STEP 3: Determine UNINTENDED CONSEQUENCES and estimate the potential **severities**

Refer to Table D.2 for severity scales. Note this severity estimation is based on knowing the acuity level of the typical PATIENT in this use case.

UC for **HS01**: Breach of privacy, PATIENT'S HEALTH DATA exposed, unauthorized medical disclosure and breach reporting for RESPONSIBLE ORGANIZATION. Irrevocable disclosure of PATIENT'S HEALTH DATA can lead to unauthorized use of PATIENT data. Severity is *low*.

UC for **HS02**: Aborted procedure or delayed treatment. Needle localization failure is detectable and procedures would be abandoned. Severity is *medium*.

UC for **HS03**: Clinician must resort to manual methods leading to limited or inconveniencing effect on operation. Severity is *low.*

UC for **HS04**: Multiple other MEDICAL DEVICES are affected by the vulnerability. Severity is *high*

STEP 4: Estimate the **probability** of the UNINTENDED CONSEQUENCE

To assess probability, existing RISK CONTROL measure already inherent in the MEDICAL DEVICE must be taken into account. With these control measures in place, probability of UNINTENDED CONSEQUENCE is evaluated as shown below. RISK CONTROL measures vary by device and will affect probability ranking based on the controls in place.

– Ultrasound device has OS Hardened: No web browsers available on device, services limited to only those needed for INTENDED USE; access controls in place.

– Ports needed to be open for use: Ultrasound device has a software firewall that blocks all ports except port 104 used for DICOM INTEROPERABILITY.

– No worms were detected in the VLAN indicating protection in the VLAN enclave stands under the current challenge,

Refer to Table D.1 for probability scales.

HS01: *remote*

HS02*: improbable*

HS03*: remote*

HS04*: occasional*

STEP 5: Evaluate **RISK** against pre-determined RISK acceptability criteria

Using Table D.3, calculate the initial RISK level based on the probability and severity determined in STEPS 3 and 4.

HS01: (low/remote). RISK level = *low*

HS02: (medium/improbable). RISK level = low

HS03: (low/remote). RISK level = low

HS04: (high/occasional). RISK level = moderate

STEP 6: Identify and document proposed RISK CONTROL measures and evaluate individual RESIDUAL RISK

There are easily practicable RISK CONTROL measures that can be applied at the network level.

RC01: Use DHCP reservations for specific range for ultrasound machines such that monitoring of network traffic can trigger alerts.

RC02: Network firewalls to protect VLANs from unwanted traffic.

RC03: Apply the patch to the ultrasound system.

RC04: Disconnect the ultrasound system from the network

All of these RISK CONTROL measures reduce P1. In this example, the probabilities were already in the Low region, but RC01 and RC02 are considered best practices RC03 (applying an OS patch or antivirus application to the ultrasound device) was not selected because it can affect the device in unknown ways or create an invalidated configuration, which could lead to HS02, and therefore was not appropriate.

RC04 (disconnecting the ultrasound system from the network) was not selected. It lowers SAFETY because it increases the probability for mistakes by introducing several months of manual data handling resulting in increased probability for incomplete or mislaid PATIENT records from which possible mistreatment follows.

New RISK Levels:

HS01: *low*

HS02: *low*

HS03: *low (unchanged)*

HS04: *moderate (unchanged)*

STEP 7: Implement RISK CONTROL measures

RISK CONTROL measures must be implemented so that they can be VERIFIED before go-live.

RC01: DHCP reservations can be implemented on a system while not in clinical use. This system can be used for RISK CONTROL VERIFICATION.

RC02: The firewalls can be tested on a small sample network in a lab, or a change window could be used to implement it on the live network.

STEP 8: Verify RISK CONTROL measures

RC01 VERIFICATION:

Implementation: Confirm that the ultrasound system is receiving a proper IP ADDRESS and use a simulated clinical situation to confirm connectivity.

Effectiveness: In this case, the assertion is that malicious traffic is blocked from reaching the MEDICAL DEVICE. VERIFICATION of effectiveness of this RISK CONTROL measure can consist of a rationale as to why this assertion is made.

RC02 VERIFICATION:

Implementation: Simulate unwanted traffic and confirm that it is not allowed past the firewall.

Effectiveness: In this case, the assertion is that malicious traffic is blocked from reaching the MEDICAL DEVICE. VERIFICATION of effectiveness of this RISK CONTROL measure can consist of a rationale as to why this assertion is made.

STEP 9: Evaluate any new RISKS arising from RISK CONTROL

Evaluation has concluded no new RISKS have been introduced by the added RISK CONTROLS.

STEP 10: Evaluate and report overall RESIDUAL RISK

Because these examples represent only one or two threads through the PROCESS for a given MEDICAL IT-NETWORK, the concept of overall RESIDUAL RISK is difficult to show.

Per 80001-1:2010, “To the extent that RISK CONTROL entails tradeoffs in KEY PROPERTIES, the KEY PROPERTIES shall be considered in priority order of SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY.” In this example, RISK for SAFETY and security has been improved by implementation of two RISK CONTROLS. The acceptable yet unwanted RISK for HS04 cannot be improved because identified RISK CONTROLS increase RISK for PATIENT SAFETY which is unacceptable by RO policy. Overall RISK complies to RO policy and is thus acceptable.

Annex A
(informative)

Common HAZARDS, HAZARDOUS SITUATIONS, and causes to consider in MEDICAL IT-NETWORKS

A.1 Typical HAZARDS in MEDICAL IT-NETWORKS

The following HAZARDS should be considered when performing a RISK ANALYSIS of a MEDICAL IT-NETWORK. Note that they are structured hierarchically which helps to organize both the RISK ASSESSMENT activities as well as the documentation.

It is important to note that any of the HAZARDS listed below can affect one or more of the three KEY PROPERTIES.

1) Loss of Function (compromised availability)
   a) Major loss of function
      i) Loss of data (loss of connectivity)
         1) Intermittent connectivity
         2) Complete loss of connectivity
      ii) Loss of function of MEDICAL DEVICE
         1) Incorrect data (compromised integrity)
         2) Incorrect data (PATIENT mismatch)
   b) Degraded function
      i) Incorrect or inappropriate timing of data
      ii) Incorrect or inappropriate data interchange or INTEROPERABILITY
      iii) Unintended interactions between endpoints
      iv) Degraded function of MEDICAL DEVICE
2) Loss of Confidentiality
   a) Unauthorized access to data

Organizations can consider aligning their HAZARDS with adverse events detailed in other specifications such as ISO 19218.

A.2 Types of HAZARDOUS SITUATIONS

Note that once a HAZARDOUS SITUATION is defined, one should be able to predict possible UNINTENDED CONSEQUENCES and their associated severities. This detail can be written into the HAZARDOUS SITUATION (i,e. amount of delay in minutes) and/or described in the context associated with the network under analysis.

– Delay in provision of care
– Non provision of care
– Delivery of inappropriate care or treatment
– Breach of privacy or confidentiality (PATIENT HEALTH DATA exposed)
– Incorrect or incomplete medical/legal record
– failure to deliver lab data or drug dosages
– failure to display medications due to be administered

– inability to admit a PATIENT in the emergency room

A.3 Common causes in MEDICAL IT-NETWORKS

– Overloaded link
– Improper QoS configuration
– Wireless dropout
– IP ADDRESS conflict
– Too aggressive security prevents connection
– Faulty cabling
– Network hardware failure
– Network software failure
– Misconfiguration (intentional)
– Misconfiguration (unintentional)
– Power loss
– Cable unintentionally disconnected in patch cabinet
– Cable unintentionally disconnected in PATIENT room
– Virus
– Security policy too strict
– User errors
– Inadequate procedures
– Incorrect execution of procedures
– Inadequate training
– Network configuration error
– EMI
– Faulty cabling
– Infected computer joins network
– Virus enters network from outside/neighboring network
– Remote servicing
– Failed or incomplete upgrade
– Hostile attack to the MEDICAL IT-NETWORK
– Unintended leakage of information
– Reduced communication functionality of a device due to software or hardware upgrade

A.4 Relationship between required network characteristics and HAZARDS

The following table lists items that can be specified for a device that requires connection to the MEDICAL IT-NETWORK. These are referred to as “required characteristics” in subclause 3.5 of IEC 80001-1:2010. Each of these can be associated with a HAZARD as shown in Table A.1.

Table A.1 – HAZARDS related to potential required network characteristics

Potential required network characteristics	Related HAZARDS
The network must provide connectivity (deliver packets at particular rate)	Loss of data (loss of connectivity)
The network must deliver traffic only to addressee	Incorrect or inappropriate data interchange or unexpected receipt of data
Fidelity – The network must not corrupt data	Incorrect data
Delay <= x	Incorrect or inappropriate timing of data
Jitter <= y	
Security: The network must not allow malicious traffic to reach the device	Loss of function (more specific HAZARD depends on device)
Security: The network must protect sensitive data	Unauthorized access to data
NOTE HAZARDS listed are based on IEC 60601-1:2005, subclauses 14.6.1 and H.7.2	

A.5 Relationship between HAZARDS, foreseeable sequences, and causes

Table A.2 is intended to aid the reader in understanding the relationship between HAZARDS, and causes.

Table A.2 – Relationship between HAZARDS, foreseeable sequences, and causes *(1 of 2)*

HAZARD	More specific HAZARD (MANUFACTURER use this as cause)	Cause
Loss of data	intermittent connectivity (dropped packets)	Overloaded link Improper QoS configuration Wireless dropout IP ADDRESS conflict Too aggressive security prevents connection RF dropout Faulty cabling
	Complete loss of connectivity	Network hardware failure Network software failure Misconfiguration (intentional or unintentional) Power loss Cable unintentionally disconnected in patch cabinet Cable unintentionally disconnected in PATIENT room Virus Security policy too strict User errors Organizational mismatches
Incorrect or inappropriate data interchange or unexpected receipt of data		IP ADDRESS conflict Network hardware failure Network software failure Network configuration failure
Incorrect data		EMI Faulty cabling

Table A.2 *(2 of 2)*

HAZARD	More specific HAZARD (MANUFACTURER use this as cause)	Cause
Incorrect or inappropriate timing of data	delay > x	Overloaded link Improper QoS configuration
	jitter > y	Overloaded link Improper QoS configuration
Loss of function (of the device)		Infected computer joins network Virus enters network from outside/neighboring network
Unauthorized access to data		Personal data shown on screen in public area Malicious sniffing of wireless data Malicious sniffing of wired data in network closet
User Errors		Inadequate training Difficult workflows Inadequate communication channels established between departments

A.6 HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS

Table A.3 is intended to aid the reader in understanding the relationship between HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS.

Table A.3 – Relationship between HAZARDS, causes, foreseeable sequences, and HAZARDOUS SITUATIONS

HAZARD	Foreseeable sequence	HAZARDOUS SITUATION
1.0 Loss of Function HAZARDS		
Loss of data	Misconfiguration of network component (cause) Lost connectivity Alarm data not received	Clinician is not notified of a PATIENT alarm
Loss of data	Poor network design (cause) Overloaded link Intermittent connectivity Real-time waveform dropout	Clinician unable to properly diagnose PATIENT
Subclause 7.3:		
Intermittent connectivity	Unplanned non-real-time traffic attempting to use link (Cause) Overloaded MAN link Intermittent packet loss	Waveform display is choppy and incomplete. Delay in provision of care because remote clinician is unable to evaluate PATIENT ECG waveform
Intermittent connectivity	Unplanned non-real-time traffic attempting to use link (Cause) Overloaded MAN link Intermittent packet loss	Alarm data not received. Delay in provision of care because clinician is unaware of PATIENT in need of treatment.
Complete loss of connectivity	MAN outage out of RO control (provider failure)	Remote clinician must determine treatment without access to real-time PATIENT data Delivery of inappropriate care or treatment.

Annex B
(informative)

List of questions to consider when identifying HAZARDS of the MEDICAL IT-NETWORK

Supplementing Annex C of ISO 14971:2007 when considering potential causes and HAZARDS, the following questions should be taken into account:

a) Reasonably foreseeable misuses

Is connection to the network inconsistent with the INTENDED USE of each constituent MEDICAL DEVICE?

b) Incorrect data flow to or from each constituent MEDICAL DEVICE

What are the data transferred by the network used for, and to which tasks are they related?

c) Excessive use/load of the MEDICAL IT-NETWORK by the network nodes

What is the planned number of network nodes and their assumed degree of use? Are the resources sufficient to meet the needs of both the IT-NETWORK itself and the devices connected to it?

d) Use errors

What skills are required by the OPERATOR for the effective operation of the system?

e) Inadequate CONFIGURATION MANAGEMENT

Do periodic service tasks alter the network's characteristics (e.g. after remote access, updates or upgrades)? Does the RESPONSIBLE ORGANIZATION ensure that modifications to each constituent MEDICAL DEVICE are reviewed and approved?

f) Information in wrong place

Does data arrive at a convenient and predictable location? Is it accompanied by irrelevant data that could confuse the OPERATOR or obscure the wanted data? When it arrives, is its source adequately indicated?

Annex C
(informative)

Layers of MEDICAL IT-NETWORKS where errors can be found

C.1 Overview

The MEDICAL IT-NETWORK can be considered to exist in two general layers (see Table C.1):

1) Attached device – those systems using the network
2) Network infrastructure – the network components and their associated topology and configuration (LAN, WAN, provider network, cellular, etc.)

Each of these layers can be further divided into subsystem and system layers (see Table C.1):

1) Subsystem – an individual component or set of components(hardware/software)
2) System – the subsystems working together

Table C.1 – Layers of an MEDICAL IT-NETWORK

			Examples
Supersystem	**Attached devices**	System	Device-to-device interactions, Device configurations
		Subsystem	Servers, hosts Endpoints (i.e. PATIENT monitor)
	Network infrastructure	System	All network components working together
		Subsystem	Switches, routers Access points, Intrusion prevention system (IPS) Intrusion detection system (IDS) Firewalls Appliances, Cellular components

C.2 Errors and faults

The layers can be further broken down into functionality (does the subsystem or system do what it is expected to do) and performance (can it continue to behave correctly under loads and extreme/edge conditions).

From an RO perspective, in considering where errors or faults can exist in the entire MEDICAL IT-NETWORK, there are two categories of faults:

a) Faults that are not within RO control. These are errors that already existed in the subsystem when it was delivered to the RO, whether that is a switch, router, server, or a MEDICAL DEVICE. This category also includes faults in connectivity services provided to the RO (i.e. leased line or internet connectivity.)
b) Faults that are within RO control. The subsystems delivered by the IT vendor or MANUFACTURER function and perform according to specification, but the topology,

configuration, or workflows instantiated within the RO are not supported. An overburdened uplink is a good example.

Table C.2 shows these layers and where faults of the above two varieties can be found.