Technical Information Report

AAMI/ISO TIR80001-2-5:2014

Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems

AAMI
Advancing Safety in Healthcare Technology

Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems

Approved 24 October 2014 by
Association for the Advancement of Medical Instrumentation

Registered 24 December 2014 by
American National Standards Institute

Abstract: This Technical Report gives guidance and practical techniques for responsible organizations, medical device manufacturers and providers of other information technology in the application of IEC 80001-1:2010 for the risk management of distributed alarm systems. This Technical Report applies to the transmission of alarm conditions between sources, integrator and receivers where at least one source is a medical device and at least one communication path utilizes a medical IT-network. It provides recommendations for the integration, communication of responses and redirection (to another operator) of alarm conditions from one or more sources to ensure safety, effectiveness and data and systems security.

Keywords: alarms, risk management, IT-network

Published by

Association for the Advancement of Medical Instrumentation
4301 N Fairfax Drive, Suite 301
Arlington, VA 22203-1633

Printed in the United States of America

ISBN 1-57020-578-7

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years. For a TIR, AAMI consults with a technical committee about five years after the publication date (and periodically thereafter) for guidance on whether the document is still useful—that is, to check that the information is relevant or of historical value. If the information is not useful, the TIR is removed from circulation.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are *voluntary*, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

ANSI Registration

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

Contents

Page

Glossary of equivalent standards

International Standards adopted in the United States may include normative references to other International Standards. AAMI maintains a current list of each International Standard that has been adopted by AAMI (and ANSI). Available on the AAMI website at the address below, this list gives the corresponding U.S. designation and level of equivalency to the International Standard.

www.aami.org/standards/glossary.pdf

Committee representation

Association for the Advancement of Medical Instrumentation

AAMI/SM/WG 02, Information Technology Working Group

The adoption of the IEC/TR 80001-2-5 as a new AAMI/IEC Technical Information Report was initiated by the AAMI Information Technology Working Group.

Committee approval of the standard does not necessarily imply that all committee members voted for its approval.

At the time this document was published, **the AAMI Information Technology Working Group** had the following members:

Chair: Bill Hintz, Medtronic Inc

Members:
John Collins, American Hospital Association
Todd Cooper
Becky Crossley, Susquehanna Health
Conor Curtin, Fresenius Medical Care
Yadin David, Biomedical Engineering Consultants LLC
Richard De La Cruz, Hospira Worldwide Inc
Christina DeMur, Draeger Medical Systems Inc
Sherman Eagles, SoftwareCPR
Scott Eaton, Mindray DS USA Inc
Kurt Elliason, Smiths Medical
Jim Gabalski, Getinge USA
George Gray, Ivenix Inc
Thomas Grobaski, Belimed Inc
Catherine Li, FDA/CDRH
Yimin Li, St Jude Medical Inc
Jared Mauldin, Integrated Medical Systems
Mary Beth McDonald, Mary Beth McDonald Consulting
Dave Osborn, Philips Electronics North America
Geoff Pascoe
Steven Rakitin, Software Quality Consulting
Rick Schrenker, Massachusetts General Hospital
Neal Seidl, GE Healthcare
Xianyu Shea, Stryker Medical Division
Ray Silkaitis, Amgen Inc
Bob Steurer, Spacelabs Medical Inc
Donna-Bea Tillman, Biologics Consulting Group
Daidi Zhong, Chongqing University

Alternates:
Denise Adams, B Braun of America Inc
James Dundon, Spacelabs Medical Inc
Brian Fitzgerald, FDA/CDRH
Rich Gardner, GE Healthcare
Andrew Northup, Medical Imaging & Technology Alliance a Division of NEMA
Phil Raymond, Philips Electronics North America
Thomas Schultz, Medtronic Inc WHQ Campus
Chandresh Thakur, CareFusion
Fei Wang, Fresenius Medical Care

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Background of AAMI adoption of IEC TR 80001-2-5

As indicated in the foreword to the main body of this document, the International Electrotechnical Commission (IEC) is a worldwide federation of national standards bodies. The United States is one of the IEC members that took an active role in the development of this technical report.

International Technical Report IEC/TR 80001-2-5:2014 was developed jointly by Sub-Committee IEC/SC 62A, Common aspects of electrical equipment used in medical practice and ISO/TC 215, Health informatics, to define the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security.

U.S. participation in this IEC SC is organized through the U.S. Technical Advisory Group for IEC/SC 62A, administered by AAMI on behalf of the American National Standards Institute (ANSI).

AAMI encourages its committees to harmonize their work with international documents as much as possible. The AAMI Information Technology Working Group, together with the U.S. Technical Advisory Group for IEC/SC 62A, reviewed IEC/TR 80001-2-5 to formulate the U.S. position while the document was being developed. This close collaboration helped gain widespread U.S. consensus on the document. As the U.S. Technical Advisory Group for IEC/SC 62A, the AAMI Information Technology Working Group voted to adopt the IEC Technical Report as written.

The concepts incorporated into this technical report should not be considered inflexible or static. This technical information report, like any other, must be reviewed and updated periodically to assimilate progressive technological developments. To remain relevant, it must be modified as technological advances are made and as new date comes to light.

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer (AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633). This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature.

Suggestions for improving this TIR are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N Fairfax Drive, Suite 301, Arlington VA 22203-1633.

NOTE—Beginning with the IEC foreword on page viii, AAMI/ISO TIR80001-2-5, *Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems* is identical to IEC/TR 80001-2-5.

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 80001-2-5, 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/943/DTR	62A/955/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.

A list of all parts of the IEC 80001 series, published under the general title *Application of risk management for it-networks incorporating medical devices ,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website 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 'color inside' logo on the cover page of this publication indicates that it contains colors which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a color printer.

Introduction

An increasing number of MEDICAL DEVICES are designed to exchange information electronically with other equipment, including other MEDICAL DEVICES. Such information is frequently exchanged through an information technology network (IT-NETWORK) that also transfers data of a more general nature. IEC 80001-1:2010 addresses RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES.

ALARM SIGNALS are frequently used to indicate unsatisfactory physiological PATIENT states, unsatisfactory functional states of the MEDICAL DEVICE or other parts of system to distribute ALARM CONDITIONS, or to warn the OPERATOR of HAZARDS to the PATIENT or OPERATOR. The ALARM CONDITIONS that cause these ALARM SIGNALS are often transmitted across the MEDICAL IT-NETWORK, creating a system to distribute ALARM CONDITIONS.

A system to distribute ALARM CONDITIONS provides great benefits; however, as with any technology, certain RISKS are introduced that can affect the three KEY PROPERTIES of SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY.

This technical report is consistent with other guidance documents of this series [1][2][3][4][5][1].

1 Numbers in square brackets refer to the Bibliography.

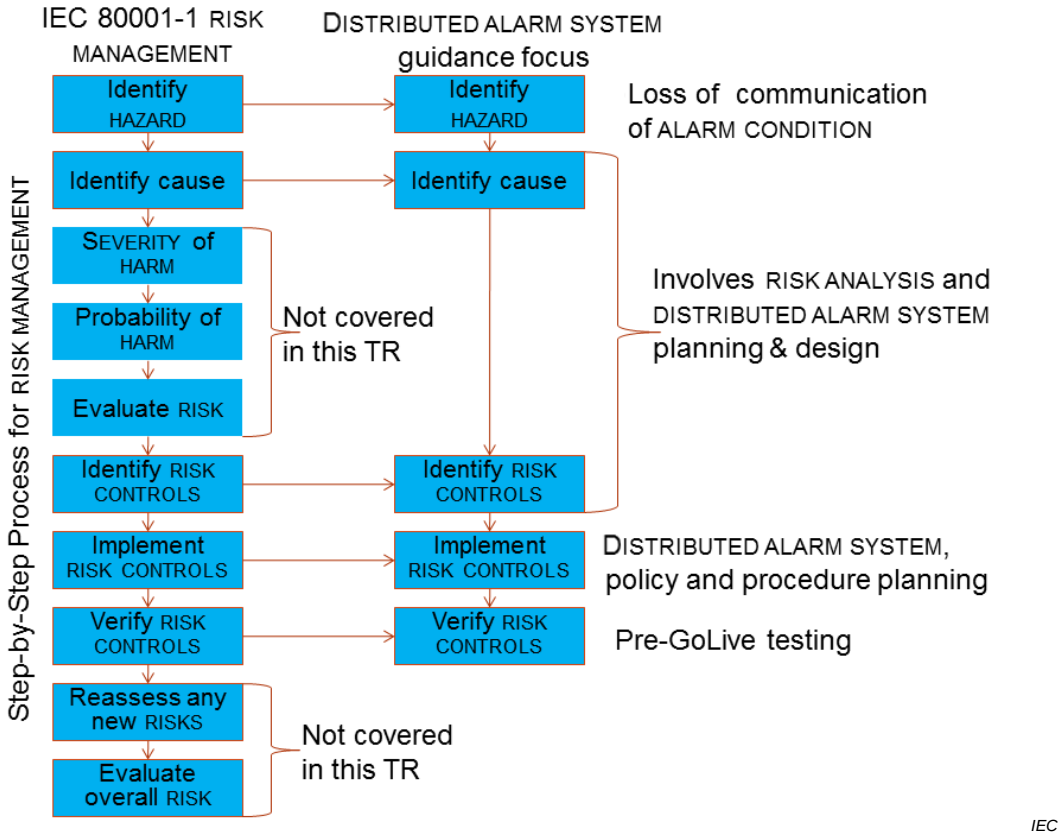


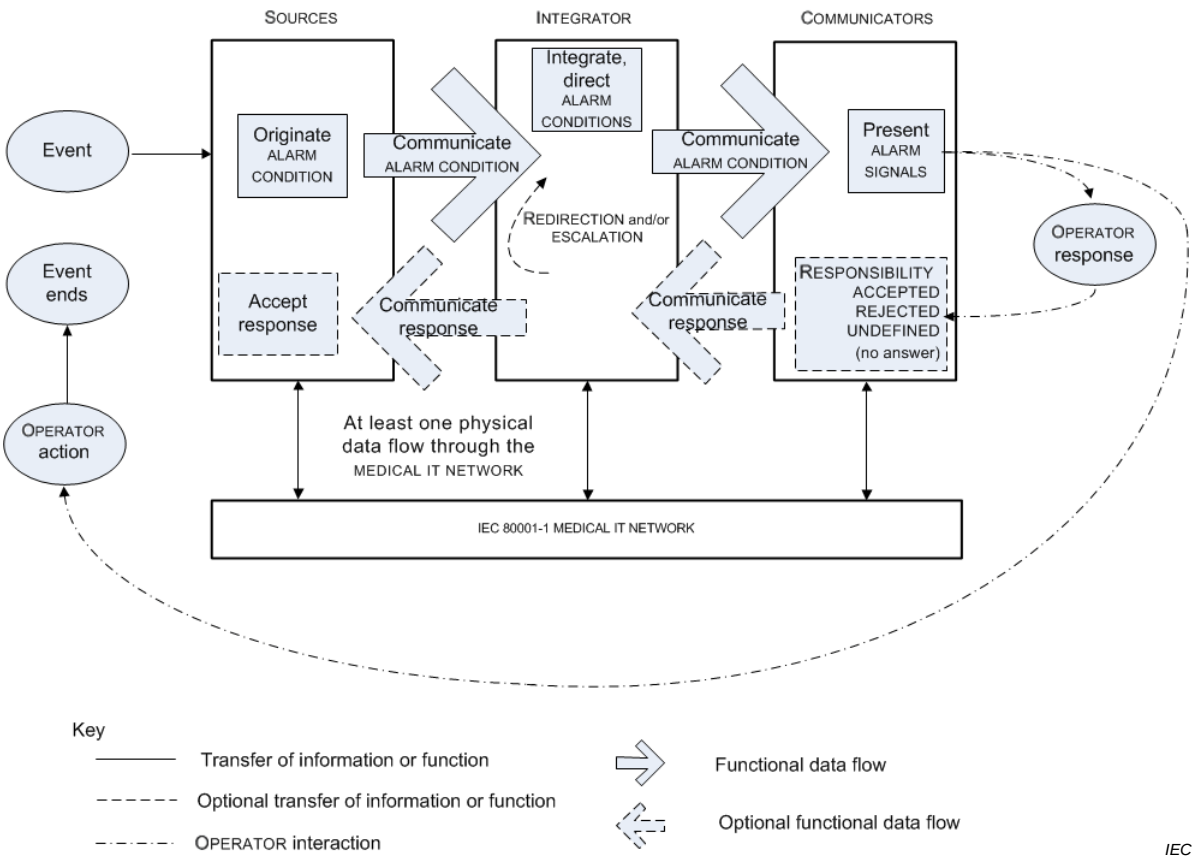
Figure 1 – Focus of this technical report

Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems

1 Scope

This part of IEC 80001, which is a technical report, gives guidance and practical techniques for RESPONSIBLE ORGANIZATIONS, MEDICAL DEVICE manufacturers and providers of other information technology in the application of IEC 80001-1:2010 for the RISK MANAGEMENT of DISTRIBUTED ALARM SYSTEMS. This technical report applies to the transmission of ALARM CONDITIONS between SOURCES, INTEGRATOR and COMMUNICATORS where at least one SOURCE is a MEDICAL DEVICE and at least one communication path utilizes a MEDICAL IT-NETWORK.

This technical report provides recommendations for the integration, communication of responses and REDIRECTION (to another OPERATOR) of ALARM CONDITIONS from one or more SOURCES to ensure SAFETY and EFFECTIVENESS. DATA AND SYSTEMS SECURITY is an important consideration for the RISK MANAGEMENT of DISTRIBUTED ALARM SYSTEMS. Figure 2 illustrates the functions of a MEDICAL IT-NETWORK incorporating SOURCES, an INTEGRATOR and COMMUNICATORS to distribute ALARM CONDITIONS.



NOTE This is a functional diagram and does not imply that these functions are in separate components. It is possible for functionality to be provided in one or more components.

Figure 2 – Functions of a MEDICAL IT-NETWORK incorporating SOURCES, an INTEGRATOR and COMMUNICATORS to distribute ALARM CONDITIONS

The following is a typical chain of events. An event is detected by a SOURCE that initiates an ALARM CONDITION. The SOURCE sends the ALARM CONDITION to the INTEGRATOR. Based on the RESPONSIBLE ORGANIZATION-established assignment protocol, the INTEGRATOR directs the ALARM CONDITION to the assigned COMMUNICATOR. The COMMUNICATOR generates the appropriate ALARM SIGNALS. The INTEGRATOR now waits for an OPERATOR response from the COMMUNICATOR or for the SOURCE to indicate that the ALARM CONDITION no longer exists.

If the COMMUNICATOR is capable of accepting a response and the OPERATOR responds, the OPERATOR indicates that it either accepts or rejects responsibility for the ALARM CONDITION. If the OPERATOR rejects the responsibility, the INTEGRATOR redirects the ALARM CONDITION to a different COMMUNICATOR (i.e. a different OPERATOR) and might also escalate the priority of the ALARM CONDITION. Eventually an OPERATOR accepts responsibility for the ALARM CONDITION. When an OPERATOR has taken appropriate action, the ALARM CONDITION subsequently ends. Alternately, the ALARM CONDITION could end without OPERATOR action in which case when the SOURCE notifies the INTEGRATOR that the ALARM CONDITION is no longer present, the INTEGRATOR instructs the COMMUNICATOR to stop generating ALARM SIGNALS. Should an ALARM CONDITION remain uncorrected for an extended period of time, the ALARM SYSTEM should cause the ESCALATION of the ALARM CONDITION, notify additional OPERATORS, etc.

EXAMPLE A pulse oximeter detects a low SpO_2 level in the PATIENT, initiates an ALARM CONDITION and sends that ALARM CONDITION to the INTEGRATOR via a MEDICAL IT-NETWORK. The INTEGRATOR then directs that ALARM CONDITION to the COMMUNICATOR that is mapped to the clinical OPERATOR assigned to the PATIENT via a MEDICAL IT-NETWORK.

OPERATOR A responds by rejecting responsibility for the ALARM CONDITION. The COMMUNICATOR sends this response information back to the INTEGRATOR, which then redirects the ALARM CONDITION to the

COMMUNICATOR of clinical OPERATOR B. OPERATOR B then accepts responsibility for the ALARM CONDITION. The COMMUNICATOR sends this response information back to the INTEGRATOR, which then sends it back to the SOURCE causing an ALARM SIGNAL inactivation state (e.g. AUDIO PAUSED) to be generated. OPERATOR B adjusts the oxygen concentration in the gas going to the PATIENT and the ALARM CONDITION ceases (e.g. the event ends).

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.

NOTE 1 The way in which these referenced documents are cited in normative requirements determines the extent (in whole or in part) to which they apply.

NOTE 2 Informative references are listed in the bibliography on page 33.

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.

NOTE An index of defined terms is found beginning on page 34.

3.1
ALARM CONDITION
state of the ALARM SYSTEM when it has determined that a potential or actual HAZARDOUS SITUATION exists for which OPERATOR awareness or response is required

Note 1 to entry: An ALARM CONDITION can be invalid, i.e. a FALSE POSITIVE ALARM CONDITION.

Note 2 to entry: An ALARM CONDITION can be missed, i.e. a FALSE NEGATIVE ALARM CONDITION.

[SOURCE: IEC 60601-1-8:2006 and IEC 60601-1-8:2006/AMD1:2012, 3.1]

3.2
ALARM SETTINGS
ALARM SYSTEM configuration, including but not limited to:

– ALARM LIMITS;

– the characteristics of any ALARM SIGNAL inactivation states; and

– the values of variables or parameters that determine the function of the ALARM SYSTEM

Note 1 to entry: Some algorithmically-determined ALARM SETTINGS can require time to be determined or re-determined.

[SOURCE: IEC 60601-1-8:2006, 3.8]

3.3
ALARM SIGNAL
type of signal generated by the ALARM SYSTEM or COMMUNICATOR to indicate the presence (or occurrence) of an ALARM CONDITION

[SOURCE: IEC 60601-1-8:2006, 3.9, modified – added 'or COMMUNICATOR'.]

3.4
ALARM SIGNAL GENERATION DELAY
time from the onset of an ALARM CONDITION to the generation of its ALARM SIGNAL(S)

[SOURCE: IEC 60601-1-8:2006, 3.10]

3.5
ALARM SYSTEM
parts of a MEDICAL DEVICE that detect ALARM CONDITIONS and, as appropriate, generate ALARM SIGNALS

[SOURCE: IEC 60601-1-8:2006, 3.11, modified – The term MEDICAL DEVICE replaces 'ME EQUIPMENT or a ME SYSTEM'.]

3.6
COMMUNICATOR
COM
function that generates ALARM SIGNALS to notify an OPERATOR

Note 1 to entry: A COM can receive an OPERATOR response.

Note 2 to entry: An OPERATOR response is not limited to direct OPERATOR action.

3.7
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

Note 1 to entry: Security, when mentioned in this standard, should be taken to include DATA AND SYSTEMS SECURITY.

Note 2 to entry: DATA AND SYSTEMS SECURITY is assured through a framework of policy, guidance, infrastructure, and services designed to protect information assets and the systems that acquire, transmit, store, and use information in pursuit of the organization's mission.

Note 3 to entry: For the purposes of this technical report, 'reasonably' should be interpreted to mean necessarily.

[SOURCE: IEC 80001-1:2010, 2.5, modified – a third note to entry has been added.]

3.8
DISTRIBUTED ALARM SYSTEM
DAS
ALARM SYSTEM that involves more than one MEDICAL DEVICE intended for delivery of ALARM CONDITIONS with technical confirmation

Note 1 to entry: The parts of a DISTRIBUTED ALARM SYSTEM can be widely separated in distance.

Note 2 to entry: A DISTRIBUTED ALARM SYSTEM is intended to notify OPERATORS of the existence of an ALARM CONDITION.

Note 3 to entry: The requirements for a DAS are described in IEC 60601-1-8:2005 and IEC 60601-1-8:2005/AMD1:2012, 6.11.2.2.1.

Note 4 to entry: For the purposes of this technical report, technical confirmation means that each element of a DISTRIBUTED ALARM SYSTEM confirms or guarantees the successful delivery of the ALARM CONDITION to the next element or appropriate TECHNICAL ALARM CONDITIONS are created as described in IEC 60601-1-8:2006 and IEC 60601-1-8:2006/AMD1:2012, 6.11.2.2.1.

[SOURCE: IEC 60601-1-8:2006, 3.17, modified – Replaced 'item of equipment of a ME SYSTEM' with 'MEDICAL DEVICE', added 'intended for delivery of ALARM CONDITIONS with technical confirmation' and added notes to entry 2, 3 and 4.]

3.9
DISTRIBUTED ALARM SYSTEM WITH OPERATOR CONFIRMATION
CDAS
DISTRIBUTED ALARM SYSTEM that includes the capability to receive an OPERATOR response

3.10
DISTRIBUTED INFORMATION SYSTEM
DISTRIBUTED INFORMATION SYSTEM ABOUT ALARM CONDITIONS
DIS
system that involves at least one MEDICAL DEVICE that is intended to provide information about ALARM CONDITIONS but does not guarantee delivery of that information

Note 1 to entry: A DIS is not intended to notify OPERATORS of the existence of an ALARM CONDITION as a RISK CONTROL measure. A DIS is intended to provide information about an ALARM CONDITION to an OPERATOR that has otherwise been made aware of the existence of the ALARM CONDITION by an ALARM SYSTEM.

Note 2 to entry: This is in terms of IEC 60601-1-8:2005 and IEC 60601-1-8:2005/AMD1:2012, 6.11.2.2.2, a 'DISTRIBUTED ALARM SYSTEM not intended for confirmed delivery of ALARM CONDITIONS'.

3.11
EFFECTIVENESS

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

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

3.12

ESCALATION

PROCESS by which an ALARM SYSTEM increases the priority of an ALARM CONDITION or increases the sense of urgency of an ALARM SIGNAL

[SOURCE: IEC 60601-1-8:2006, 3.18]

3.13

FALSE NEGATIVE ALARM CONDITION

absence of an ALARM CONDITION when a valid triggering event has occurred in the PATIENT, the equipment or the ALARM SYSTEM

Note 1 to entry: An ALARM CONDITION can be rejected or missed because of spurious information produced by the PATIENT, the PATIENT-equipment interface, other equipment or the ALARM SYSTEM itself.

[SOURCE: IEC 60601-1-8:2006, 3.20, modified – replaced last 'equipment' with 'ALARM SYSTEM' in the note to entry.]

3.14

FALSE POSITIVE ALARM CONDITION

presence of an ALARM CONDITION when no valid triggering event has occurred in the PATIENT, the equipment or the ALARM SYSTEM

Note 1 to entry: A FALSE POSITIVE ALARM CONDITION can be caused by spurious information produced by the PATIENT, the PATIENT-equipment interface, other equipment or the ALARM SYSTEM itself.

[SOURCE: IEC 60601-1-8:2006, 3.21]

3.15

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 SYSTEM SECURITY

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

3.16
HAZARD
potential source of HARM

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

3.17
HAZARDOUS SITUATION
circumstance in which people, property, or the environment are exposed to one or more HAZARD(S)

[SOURCE: ISO 14971: 2007, 2.4]

3.18
HIGH PRIORITY
indicating that immediate OPERATOR response is required

Note 1 to entry: The priority is assigned through RISK ANALYSIS.

[SOURCE: IEC 60601-1-8:2006, 3.22]

3.19
INTEGRATOR
INT
function that handles communication between SOURCES and COMMUNICATORS or to other INTEGRATORS

Note 1 to entry: An INTEGRATOR can direct or redirect an ALARM CONDITION to another OPERATOR.

Note 2 to entry: An INTEGRATOR can send the acceptance of responsibility from a COMMUNICATOR to a SOURCE.

3.20
INTENDED USE
INTENDED PURPOSE
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, 2.10]

3.21
IT-NETWORK
INFORMATION TECHNOLOGY NETWORK
a system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

Note 1 to entry: Adapted from IEC 61907:2009, definition 3.1.1.

Note 2 to entry: The scope of the MEDICAL IT-NETWORK in this standard is defined by the RESPONSIBLE ORGANIZATION based on where the MEDICAL DEVICES in the MEDICAL IT-NETWORK are located and the defined use of the network. It can contain IT infrastructure, home health and non-clinical contexts. See also 80001-1:2010, 4.3.3.

[SOURCE: IEC 80001-1:2010, 2.12]

3.22
KEY PROPERTIES
three risk managed characteristics (SAFETY, EFFECTIVENESS, and DATA AND SYSTEMS SECURITY) of MEDICAL IT-NETWORKS

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

3.23
LOW PRIORITY
indicating that OPERATOR awareness is required

Note 1 to entry: The priority is assigned through RISK ANALYSIS.

[SOURCE: IEC 60601-1-8:2006, 3.27]

3.24
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, 2.14]

3.25

MEDICAL ELECTRICAL EQUIPMENT

ME EQUIPMENT

electrical equipment having an APPLIED PART or transferring energy to or from the PATIENT or detecting such energy transfer to or from the PATIENT and which is:

a) provided with not more than one connection to a particular SUPPLY MAINS; and

b) intended by its MANUFACTURER to be used:

1) in the diagnosis, treatment, or monitoring of a PATIENT; or

2) for compensation or alleviation of disease, injury or disability

Note 1 to entry: ME EQUIPMENT includes those ACCESSORIES as defined by the MANUFACTURER that are necessary to enable the NORMAL USE of the ME EQUIPMENT.

Note 2 to entry: Not all electrical equipment used in medical practice falls within this definition (e.g. some in vitro diagnostic equipment).

Note 3 to entry: The implantable parts of active implantable medical devices can fall within this definition, but they are excluded from the scope of this standard (IEC 60601-1) by appropriate wording in Clause 1.

Note 4 to entry: This standard (IEC 60601-1) uses the term "electrical equipment" to mean ME EQUIPMENT or other electrical equipment.

Note 5 to entry: See also IEC 60601-1:2005, 4.10.1, 8.2.1 and 16.3.

Note 6 to entry: ME EQUIPMENT is a MEDICAL DEVICE.

[SOURCE: IEC 60601-1:2005, 3.63, modified – Added Note 6 to entry.]

3.26

MEDICAL ELECTRICAL SYSTEM

ME SYSTEM

combination, as specified by its MANUFACTURER, of items of equipment, at least one of which is ME EQUIPMENT to be inter-connected by functional connection or by use of a multiple socket-outlet

Note 1 to entry: Equipment, when mentioned in this standard, should be taken to include ME EQUIPMENT.

Note 2 to entry: An ME SYSTEM is a MEDICAL DEVICE.

[SOURCE: IEC 60601-1:2005, 3.64, modified – Added Note 2 to entry.]

3.27

MEDICAL IT-NETWORK

an IT-NETWORK that incorporates at least one MEDICAL DEVICE

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

3.28
MEDIUM PRIORITY
indicating that prompt OPERATOR response is required

Note 1 to entry: The priority is assigned through RISK ANALYSIS.

[SOURCE: IEC 60601-1-8:2006, 3.28]

3.29
NURSE CALL SYSTEM
system intended to call or search for requested persons or send information, including ALARM CONDITIONS between individuals, including PATIENTS, and healthcare staff

Note 1 to entry: A NURSE CALL SYSTEM typically provides a REDIRECTION to help ensure timely action.

Note 2 to entry: In some jurisdictions based on the INTENDED USE, a NURSE CALL SYSTEM may be considered a MEDICAL DEVICE.

3.30
OPERATOR
person handling equipment

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

3.31
PATIENT
living being (person or animal) undergoing a medical, surgical or dental procedure or receiving other healthcare services

Note 1 to entry: A PATIENT can be an OPERATOR.

Note 2 to entry: PATIENT is also referred to as the subject of care.

[SOURCE: IEC 60601-1:2005 and IEC 60601-1:2005/AMD1:2012, 3.76, modified – Added 'or receiving other healthcare services' and Note 2 to entry.]

3.32
PHYSIOLOGICAL ALARM CONDITION
ALARM CONDITION arising from a monitored PATIENT-related variable

EXAMPLE 1 High exhaled anaesthetic agent concentration.

EXAMPLE 2 Low exhaled tidal volume.

EXAMPLE 3 Low oxygen saturation measured by pulse oximetry.

EXAMPLE 4 High arterial pressure.

EXAMPLE 5 High heart rate.

[SOURCE: IEC 60601-1-8:2006, 2.31]

3.33
PROCESS
set of interrelated or interacting activities which transforms inputs into outputs

Note 1 to entry: The term "activities" covers use of resources.

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

3.34
REDIRECTION
means by which an INTEGRATOR provides a response hierarchy for directing an ALARM CONDITION to a COMMUNICATOR or redirects an ALARM CONDITION to another COMMUNICATOR

3.35
RESPONSIBILITY ACCEPTED
state created by an OPERATOR response accepting ownership for addressing an ALARM CONDITION

Note 1 to entry: A RESPONSIBILITY ACCEPTED can be used to initiate an ALARM SIGNAL inactivation state.

3.36
RESPONSIBILITY REJECTED
state created by an OPERATOR response rejecting ownership for addressing an ALARM CONDITION

Note 1 to entry: A RESPONSIBILITY REJECTED can be used to initiate an ESCALATION or REDIRECTION.

3.37
RESPONSIBILITY UNDEFINED
state, automatically initiated when neither a RESPONSIBILITY ACCEPTED nor RESPONSIBILITY REJECTED is received within a specified period, which indicates that an OPERATOR is not responding

3.38
RESPONSIBLE ORGANIZATION
entity accountable for the use and maintenance of a MEDICAL IT-NETWORK

Note 1 to entry: The accountable entity can be, for example, a hospital, a private clinician or a telehealth organization.

Note 2 to entry: Adapted from IEC 60601-1:2005, definition 3.101.

[SOURCE: IEC 80001-1:2010, 2.22]

3.39
RISK
combination of the probability of occurrence of HARM and the severity of that HARM

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

3.40
RISK ANALYSIS
systematic use of available information to identify HAZARDS and to estimate the RISK

[SOURCE: ISO 14971:2007, 2.17]

3.41
RISK CONTROL
process in which decisions are made and measures implemented by which RISKS are reduced to, or maintained within, specified levels

[SOURCE: ISO 14971:2007, 2.19]

3.42
RISK MANAGEMENT
systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring RISK

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

3.43
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, 2.30]

3.44
SEVERITY
measure of the possible consequences of a HAZARD

[SOURCE: ISO 14971:2007, 2.25]

3.45
SOURCE
SRC
function that has the capability to initiate an ALARM CONDITION

Note 1 to entry: The SOURCE can accept an assignment of responsibility.

3.46
TECHNICAL ALARM CONDITION
ALARM CONDITION arising from a monitored equipment-related or ALARM SYSTEM-related variable

EXAMPLE 1 An electrical, mechanical or other failure.

EXAMPLE 2 Failure of a sensor or component (unsafe voltage, high impedance, signal impedance, artefact, noisy signal, disconnection, calibration error, tubing obstruction, etc.).

EXAMPLE 3 An algorithm that cannot classify or resolve the available data.

EXAMPLE 4 A failure of a DISTRIBUTED ALARM SYSTEM, a system TECHNICAL ALARM CONDITION.

[SOURCE: IEC 60601-1-8:2006, 3.36, modified – Added Example 4.]

3.47
USE ERROR
act or omission of an act that results in a different MEDICAL DEVICE response than intended by the manufacturer or expected by the user

Note 1 to entry: USE ERROR includes slips, lapses, and mistakes

Note 2 to entry: An unexpected physiological response of the PATIENT is not in itself considered a USE ERROR.

[SOURCE: IEC 62366:2007, 3.21, modified – Deleted note 2.]

4 Functions of the distribution of ALARM CONDITIONS

4.1 General

When a manufacturer chooses as a means of RISK CONTROL to have a MEDICAL DEVICE notify the OPERATOR that a HAZARDOUS SITUATION can exist, then the MEDICAL DEVICE is expected to include an ALARM SYSTEM for that purpose. The creation of ALARM CONDITIONS and the notification of OPERATORS are a RISK CONTROL measure. If the OPERATOR is not effectively notified, the RISK CONTROL measure is ineffective.

When ALARM CONDITIONS are distributed, the effectiveness of the ALARM SYSTEM can be improved by employing the functions of SOURCES, INTEGRATOR and COMMUNICATORS in a MEDICAL IT-NETWORK as described in this technical report.

4.2 SOURCES and their ALARM CONDITIONS

SOURCES are the part of the system for the distribution of ALARM CONDITIONS that have the capability to initiate an ALARM CONDITION. They communicate ALARM CONDITIONS to an INTEGRATOR. A SOURCE can receive an indication RESPONSIBILITY ACCEPTED originating at a COMMUNICATOR (from an OPERATOR) that was transferred by an INTEGRATOR.

SOURCES can include, *inter alia*, MEDICAL DEVICES (e.g., MEDICAL ELECTRICAL EQUIPMENT and *in vitro* diagnostics), fire alarm systems, call systems, and building security systems. Annex B contains expanded information regarding types of SOURCES.

ALARM CONDITIONS can be classified into three types as follows:

a) TECHNICAL ALARM CONDITION;

   EXAMPLE 1 A TECHNICAL ALARM CONDITION arising from a SOURCE indicating a technical problem with a PATIENT measurement.

   EXAMPLE 2 A TECHNICAL ALARM CONDITION arising from a SOURCE, INTEGRATOR, COMMUNICATOR or MEDICAL IT-NETWORK indicating a technical problem with the equipment or communication capability.

b) PHYSIOLOGICAL ALARM CONDITION; and

c) other ALARM CONDITIONS, arising from other events.

   EXAMPLE 3 ALARM CONDITION arising from a building security breach.

   EXAMPLE 4 ALARM CONDITION arising from a personnel or service call.

   EXAMPLE 5 ALARM CONDITION arising from notification of a critical lab result, medication arrival, or bed availability.

An ALARM CONDITION can only originate from a SOURCE. Most MEDICAL DEVICES that have an ALARM SYSTEM have both SOURCE and COMMUNICATOR functions as well as an INTEGRATOR function.

4.3 INTEGRATOR

An INTEGRATOR is the part of the system for the distribution of ALARM CONDITIONS that combines ALARM CONDITIONS from SOURCES, at least one of which is part of a MEDICAL DEVICE, and handles the communication between those SOURCES and COMMUNICATORS. An INTEGRATOR can map SOURCES and their ALARM CONDITIONS to specific COMMUNICATORS and can provide REDIRECTION to additional or different COMMUNICATORS based on the response or lack of response from COMMUNICATORS.

4.4 COMMUNICATOR

A COMMUNICATOR is a part of a system that generates ALARM SIGNALS to alert an OPERATOR of a situation that requires attention. A COMMUNICATOR can also process or direct an OPERATOR response to the INTEGRATOR. An OPERATOR response need not be limited to direct OPERATOR action and can be achieved by other means, e.g. an OPERATOR locator system.

ALARM SIGNALS can be generated at various COMMUNICATORS:

a) MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS:

   ALARM SIGNALS compliant with IEC 60601-1-8;

   EXAMPLE 1 Directly at the PATIENT bedside and/or at a central monitoring station.

b) general IT equipment and software;

   EXAMPLES 2 Voice terminals, smart phones, PCs, tablets.

c) MEDICAL DEVICES, other than MEDICAL ELECTRICAL EQUIPMENT or MEDICAL ELECTRICAL SYSTEMS.

   NOTE This category includes software-only MEDICAL DEVICES.

In all cases, the COMMUNICATOR needs to be in compliance with IEC 60601-1-8 when it is generating ALARM SIGNALS for MEDICAL ELECTRICAL EQUIPMENT.

4.5 MEDICAL IT-NETWORK

In the system for the distribution of ALARM CONDITIONS, a MEDICAL IT-NETWORK is a general purpose linking communications network consisting of hard-wired or wireless transmissions between two or more specified functions of the system for the distribution of ALARM CONDITIONS.

5 Types of systems for distributing ALARM CONDITIONS

5.1 General

The RESPONSIBLE ORGANIZATION should consider which performance properties are needed to support the desired clinical workflow. Based on their needs, the RESPONSIBLE ORGANIZATION should select the appropriate system from the following:

– DISTRIBUTED INFORMATION SYSTEM ABOUT ALARM CONDITIONS (DIS);

– DISTRIBUTED ALARM SYSTEM (DAS);

– DISTRIBUTED ALARM SYSTEM WITH OPERATOR CONFIRMATION (CDAS).

A general comparison of the properties of these types of systems is found in Table 1.

Table 1 – General comparison of system properties for ALARM CONDITION integration

Type of system	System properties			
	Delivery of ALARM CONDITIONS with technical confirmation	**Prioritization of ALARM CONDITIONS**	**Direction/ REDIRECTION of ALARM CONDITION**	**Collection of OPERATOR response**
DIS DISTRIBUTED INFORMATION SYSTEM ABOUT ALARM CONDITIONS EXAMPLES Pager, E-Mail, SMS.	羊	X	X	?
DAS DISTRIBUTED ALARM SYSTEM NOTE Minimium requirements according to IEC 60601-1-8. EXAMPLE PATIENT monitor connected to a central station.	X	X	?	羊
CDAS DISTRIBUTED ALARM SYSTEM WITH OPERATOR CONFIRMATION	X	X	X	X
Key 羊 property not included ? property not needed but can be included X property included				

5.2 DISTRIBUTED INFORMATION SYSTEM ABOUT ALARM CONDITIONS

A DIS has been shown to be effective in improving the productivity of the clinical staff in hospital settings when used as intended. [17][2] Providing information about ALARM CONDITIONS allows OPERATORS to assess the immediacy of the needed response.

EXAMPLE 1 The OPERATOR can decide whether or not to finish the task at hand before responding to an ALARM CONDITION from another PATIENT (typically in a different room).

A typical DIS can direct ALARM CONDITIONS, either of a particular type or from a particular SOURCE, to a specific COMMUNICATOR. This can be one approach to reducing 'alarm fatigue'. A DIS can include the capability to receive an OPERATOR response, but neither the information about ALARM CONDITIONS nor the OPERATOR response has technical confirmation.

Experience has shown that a DIS is not suitable for reliably notifying the OPERATOR of the existence of an ALARM CONDITION [15]. This is because a DIS does not include technical confirmation of the delivery of the ALARM CONDITION from the SOURCE to the COMMUNICATOR and hence the OPERATOR might not be aware when ALARM CONDITIONS cannot be received.

EXAMPLE 2 One-way pager that is out of range.

5.3 DISTRIBUTED ALARM SYSTEM

A DAS is suitable for reliably notifying the OPERATOR of the existence of an ALARM CONDITION. This is because a DAS includes technical confirmation of the delivery of the ALARM CONDITION from the SOURCE to the COMMUNICATOR. A DAS has been shown to be effective in enlarging the area where OPERATORS can be notified of the existence of ALARM CONDITIONS. This allows OPERATORS to be more mobile in a typical clinical environment since they are able to respond to ALARM CONDITIONS from a wider area.

2 Numbers in square brackets refer to the Bibliography.

EXAMPLE A PATIENT monitoring system with bedside monitors connected to one or more central stations expands the area where an OPERATOR can receive ALARM SIGNALS.

Experience has shown that a DAS is suitable for reliably notifying the OPERATOR of the existence of an ALARM CONDITION [15]. This is because a DAS includes technical confirmation of the delivery of the ALARM CONDITION from the SOURCE to the COMMUNICATOR. As a result, the OPERATOR can be made aware when ALARM CONDITIONS cannot be received. IEC 60601-1-8 permits a DAS to provide ESCALATION.

NOTE A DAS without direction or REDIRECTION can contribute to 'alarm fatigue' since every ALARM CONDITION is presented at the same time at multiple COMMUNICATORS.

5.4 DISTRIBUTED ALARM SYSTEM WITH OPERATOR CONFIRMATION

A CDAS is suitable for reliably notifying the OPERATOR of the existence of an ALARM CONDITION. This is because a CDAS includes technical confirmation of the delivery of the ALARM CONDITION from the SOURCE to the COMMUNICATOR. As a result, the OPERATOR can be made aware when ALARM CONDITIONS cannot be received. Furthermore, a CDAS provides the OPERATOR a means to confirm the receipt of an ALARM SIGNAL and to communicate a response to the INTEGRATOR and optionally to the SOURCE. This enhanced capability permits the INTEGRATOR to provide REDIRECTION or ESCALATION if the OPERATOR does not respond (RESPONSIBILITY UNDEFINED) or if the OPERATOR responds with a RESPONSIBILITY REJECTED indication. Thus, a CDAS combines the advantages of both a DIS and DAS without the drawbacks.

6 RISK MANAGEMENT

6.1 General explanation

A system for distributing ALARM CONDITIONS can be intended to:

– notify the appropriate OPERATOR of the existence of an ALARM CONDITION (DAS or CDAS); or

– provide information to the appropriate OPERATOR about an ALARM CONDITION (DIS).

IEC 80001-1:2010 requires comprehensive RISK MANAGEMENT to be applied to MEDICAL IT-NETWORKS, as they are often complex systems of systems. ALARM SYSTEMS that are distributed across multiple systems and networks fall into this category. IEC 80001-2-1 defines 10 steps in the RISK MANAGEMENT process, specifically as detailed in subclause 4.4 in IEC 80001-1:2010.

Clause 6 is intended to guide the reader in applying the following steps from IEC 80001-2-1 to a system for distributing ALARM CONDITIONS:

– Step 1: Identify HAZARDS and HAZARDOUS SITUATIONS (see 6.3);

– Step 2: Identify causes and resulting HAZARDOUS SITUATIONS (see 6.4);

– Steps 6, 7 and 8: RISK CONTROL measures (see 6.5).

Figure 1 shows the relationship between the subclauses of this technical report to the steps of IEC 80001-2-1. This technical report assumes that prior to applying the 10 steps of IEC 80001-2-1, the RESPONSIBLE ORGANIZATION has established its purpose for using the system for distributing ALARM CONDITIONS (see 6.2).

When carrying out the RISK MANAGEMENT PROCESS, the RESPONSIBLE ORGANIZATION should take into account all available information, including the overall context for which the MEDICAL IT-NETWORK is intended to be used, all information from the MEDICAL DEVICE manufacturers, the design and capabilities of the MEDICAL DEVICES as well as the network, clinical and IT PROCESSES, etc. The PROCESS ultimately leads the RESPONSIBLE ORGANIZATION to a decision on RISK acceptability. Go-live should proceed only after overall RESIDUAL RISK is determined to be acceptable.

The RESPONSIBLE ORGANIZATION'S ALARM SYSTEM-related workflow should be used to inform the PROCESS of developing, deploying and maintaining a system for the distribution of ALARM CONDITIONS. This context in addition to PATIENT acuity and IT policy is used to frame the RISK MANAGEMENT PROCESS and is a starting point for the step-by-step PROCESS described in IEC TR 80001-2-1:2012.

6.2 Determining the RESPONSIBLE ORGANIZATION'S objective purpose

The RESPONSIBLE ORGANIZATION should define its objective purpose for using a system for distributing ALARM CONDITIONS including:

a) the purpose of the distributed system;

b) the type and sources of ALARM CONDITIONS allowed to be transmitted (based on criticality and reaction time);

c) the level of response capabilities needed to fulfil the system purpose;

d) a list of designated OPERATOR types to be notified, including the communication pathways and COMMUNICATORS to be utilized;

e) the time needed for the OPERATOR to act.

6.3 HAZARDS and HAZARDOUS SITUATIONS related to DIS, DAS and CDAS

In the context of a system for distributing ALARM CONDITIONS, a HAZARDOUS SITUATION exists when a PATIENT, OPERATOR or another person is exposed to one or more HAZARDS and an initiated ALARM CONDITION, intended to notify an OPERATOR about the HAZARDOUS SITUATION, cannot be adequately addressed by the OPERATOR due to different causes (see 6.4).

At least the following HAZARDS should be considered by the RESPONSIBLE ORGANIZATION:

a) HAZARDS
   1) non-provision of care, PATIENT gets no help;
   2) delivery of inappropriate care or treatment, PATIENT gets wrong help;
   3) delay in provision of care, help arrives too late.

Each of the steps described below leads to a HAZARDOUS SITUATION:

b) when an event occurs and no ALARM CONDITION gets initiated;

c) when an ALARM CONDITION gets initiated but is not transmitted;

d) when an ALARM CONDITION gets transmitted but is not presented via ALARM SIGNALS;

e) when an ALARM SIGNAL is presented to an inappropriate OPERATOR;

f) when an ALARM SIGNAL is presented to an OPERATOR but the OPERATOR does not recognize that an ALARM SIGNAL is present; and

g) when an appropriate OPERATOR recognizes that an ALARM SIGNAL is present but takes no action.

At least the following HAZARDOUS SITUATIONS should be considered by the RESPONSIBLE ORGANIZATION:

h) OPERATOR not notified of a PATIENT ALARM CONDITION:
   – ALARM CONDITION is lost;
   – ALARM CONDITION is misdirected;
   – ALARM CONDITION is modified;
   – THE SOURCE'S ability to initiate an ALARM CONDITION is delayed;
   – OPERATOR is unaware of being out of range (DIS COMMUNICATOR);
   – ALARM SIGNAL has been placed into an inactivation state;
   – ALARM SIGNAL is inaudible;
   – ALARM SIGNAL is ignored;

i) 'alarm fatigue' caused by:
   – ALARM CONDITION is clinically irrelevant;
   – auditory volume of the ALARM SIGNAL is inappropriate;
   – undefined responsibilities for responding to ALARM CONDITIONS;
   – ALARM CONDITION is duplicated.

6.4 Causes and resulting HAZARDOUS SITUATIONS

The range of causes, as to how a PATIENT, OPERATOR or other persons are exposed to a HAZARDOUS SITUATION, is very wide. A systematic analysis of these causes is very beneficial. In principle, two major areas can be distinguished:

a) Wrong configuration of, e.g.,
   - SOURCE,
   - INTEGRATOR,
   - COMMUNICATOR,
   - MEDICAL IT-NETWORK, or
   - list of available OPERATORS;

b) failure of transmission, due to e.g.
   - failure modes of individual components,
   - failure modes of connections,
   - lack of power supply,
   - lack of connectivity,
   - electromagnetic interference,
   - inappropriate shutdown of IT equipment,
   - quality of service (QoS) issues, or
   - USE ERROR by OPERATOR.

At least the following example of causes should be considered when evaluating the implementation of a system for the distribution of ALARM CONDITIONS:

- poor quality of the PATIENT connection;

  EXAMPLE 1 Mispositioned sensor or dry ECG electrodes.

- improper installation configuration of the SOURCE to the MEDICAL IT-NETWORK;

  EXAMPLE 2 Incorrect IP address.

- improper clinical configuration of the SOURCE to the PATIENT;

  EXAMPLE 3 Incorrect PATIENT type or ALARM SETTINGS.

- poor quality of the SOURCE algorithm;

  EXAMPLE 4 Excessive FALSE POSITIVE or FALSE NEGATIVE ALARM CONDITIONS.

- improper installation configuration of the INTEGRATOR;

  EXAMPLE 5 Incorrect assignment of SOURCE to OPERATOR or OPERATOR to COMMUNICATOR.

- inadequate or inaccurate mapping of the OPERATOR/ALARM CONDITION/PATIENT;

  EXAMPLE 6 Not updating the assignment mapping in the INTEGRATOR at the shift change of OPERATORS.

- concurrent ALARM CONDITIONS from multiple PATIENTS;

  EXAMPLE 7 Two different PATIENTS with ALARM CONDITIONS occurring at the same time.

- limited capability or configuration of the INTEGRATOR REDIRECTION/ESCALATION algorithm;

  EXAMPLE 8 The nurse manager receives too many LOW PRIORITY ALARM CONDITIONS.

  EXAMPLE 9 A HIGH PRIORITY ALARM CONDITION is lost in a flood of LOW PRIORITY ALARM CONDITIONS.

- inadequate placement or configuration of COMMUNICATORS; and

  EXAMPLE 10 Insufficient number of COMMUNICATORS resulting in areas where the OPERATOR cannot see or hear the ALARM SIGNALS.

- missing or inadequate OPERATOR response to an ALARM SIGNAL.

  EXAMPLE 11 Each OPERATOR thinks that another OPERATOR is handling the ALARM CONDITION.

EXAMPLE 12 The OPERATOR responds RESPONSIBILITY ACCEPTED but does not solve the problem.

Additional communication-related examples of causes should be considered when evaluating the implementation for the distribution of ALARM CONDITIONS:

– ALARM CONDITION communication is lost/delayed/duplicated;

  EXAMPLE 13 The COMMUNICATOR does not receive the ALARM CONDITION from the INTEGRATOR.

– ALARM CONDITION communication is misdirected;

  EXAMPLE 14 The SOURCE sends the ALARM CONDITION to the wrong INTEGRATOR.

  EXAMPLE 15 The INTEGRATOR sends the ALARM CONDITION to the wrong COMMUNICATOR.

– response communication is lost/delayed/duplicated;

  EXAMPLE 16 The INTEGRATOR does not receive the response or fails to provide REDIRECTION.

– inappropriate ALARM CONDITION prioritization; and

  EXAMPLE 17 The SOURCE has a conflicting ALARM CONDITION prioritization scheme to IEC 60601-1-8.

  EXAMPLE 18 The INTEGRATOR poorly integrates the ALARM CONDITION prioritization schemes of the different connected devices.

– response communication is misdirected.

  EXAMPLE 19 The INTEGRATOR sends the OPERATOR response to the wrong SOURCE.

6.5 RISK CONTROL measures related to the integration of ALARM CONDITIONS

6.5.1 Technical RISK CONTROL measures implemented in equipment

In a system for the distribution of ALARM CONDITIONS, at least the following performance features and behaviours should be considered for every SOURCE, INTEGRATOR and COMMUNICATOR as needed to bring RISK to an acceptable level:

a) SOURCES, INTEGRATORS and COMMUNICATORS have self-surveillance functionality to support ensuring that the system is functioning.

   EXAMPLE Presence of integrated watchdog timers or integrated self-testing means disclosed in the instructions for use.

b) The self-surveillance functionality or the connections between SOURCE, INTEGRATOR and COMMUNICATOR are monitored (e.g. send heartbeats, system life-tick or session awareness) and each SOURCE, INTEGRATOR and COMMUNICATOR initiates a system TECHNICAL ALARM CONDITION when the connection fails.

   NOTE 1 This is a requirement for MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS in IEC 60601-1-8.

c) When a system TECHNICAL ALARM CONDITION exists, the relevant affected functionally connected COMMUNICATORS generate ALARM SIGNALS to ensure that the intended OPERATORS receive notification. This is because the intended OPERATORS could be at any one of these relevant affected functionally connected COMMUNICATORS.

   A COMMUNICATOR that cannot generate ALARM SIGNALS for this system TECHNICAL ALARM CONDITION is marked with a warning to the effect that it should not be relied upon for notification purposes.

   NOTE 2 This is a requirement for MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS in IEC 60601-1-8. In some jurisdictions, an OPERATOR can be required to be always within audible range of a MEDICAL DEVICE.

   NOTE 3 When communications is lost between an INTEGRATOR and a COMMUNICATOR, the TECHNICAL ALARM CONDITION can be REDIRECTED to a back-up COMMUNICATOR automatically by the INTEGRATOR or dynamically by an OPERATOR for a DIS.

d) Each SOURCE, INTEGRATOR and COMMUNICATOR generates ALARM SIGNALS locally in an appropriate way when an ALARM CONDITION has been initiated locally. In this case, the local ALARM SIGNAL presentation has a minimal INTEGRATOR that handles the ALARM CONDITION and hands it over to the local COMMUNICATOR.

e) When an ALARM CONDITION is transmitted from a SOURCE via the INTEGRATOR to the COMMUNICATOR, each INTEGRATOR and COMMUNICATOR that receives and assumes ownership of the ALARM CONDITION technically confirms or guarantees to the previous function that it assumes the responsibility for the handling of that ALARM CONDITION.

f) When an OPERATOR response is transmitted from a COMMUNICATOR to the INTEGRATOR or from the INTEGRATOR to the SOURCE, each INTEGRATOR and SOURCE that receives and assumes ownership of the response technically confirms or guarantees to the previous function that it assumes the responsibility for the handling of that response.

g) When a COMMUNICATOR assumes responsibility for an ALARM CONDITION, the COMMUNICATOR presents the ALARM CONDITION to the OPERATOR by generating ALARM SIGNALS.

NOTE 4 This is a requirement for MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS in IEC 60601-1-8.

h) The INTEGRATOR records and logs with a time/date stamp all occurrences associated with responsibility events initiated by OPERATORS (i.e., RESPONSIBILITY ACCEPTED, RESPONSIBILITY REJECTED), as well as all ESCALATED, REDIRECTED and RESPONSIBILITY UNDEFINED events initiated by the INTEGRATOR.

i) A means by which the OPERATOR response to the presented ALARM SIGNAL is fed back to the INTEGRATOR and, when needed, to the SOURCE.

j) When RESPONSIBILITY UNDEFINED or RESPONSIBILITY REJECTED has been received or determined by the INTEGRATOR, the INTEGRATOR initiates REDIRECTION of the ALARM CONDITION to another COMMUNICATOR (OPERATOR).

k) The INTEGRATOR continues directing or redirecting the ALARM CONDITION, until a RESPONSIBILITY ACCEPTED is received or the SOURCE indicates the end of the ALARM CONDITION.

NOTE 5 It is important to ensure that an ALARM CONDITION is not lost and at least one COMMUNICATOR is generating ALARM SIGNALS.

l) REDIRECTION of an ALARM CONDITION to one or more additional COMMUNICATORS (OPERATORS) by the INTEGRATOR can trigger ESCALATION of that ALARM CONDITION.

m) An OPERATOR needs to be able to undo any response (i.e., RESPONSIBILITY ACCEPTED, RESPONSIBILITY REJECTED) that has been initiated.

NOTE 6 This is consistent with the IEC 60601-1-8 requirement that an ALARM SYSTEM needs to provide the means for the OPERATOR to terminate any ALARM SIGNAL inactivation state.

n) A RESPONSIBILITY ACCEPTED at the COMMUNICATOR can be returned to the SOURCE.

o) A RESPONSIBILITY ACCEPTED at the COMMUNICATOR can initiate an appropriate ALARM SIGNAL inactivation state.

p) The OPERATOR can initiate an appropriate ALARM SIGNAL inactivation state manually at the SOURCE.

q) An INTEGRATOR logs information about received, directed, redirected and escalated ALARM CONDITIONS as well as system failures.

NOTE 7 The log could be internal to the INTEGRATOR or located on the MEDICAL IT-NETWORK.

NOTE 8 The log could be a ‘black-box’ recorder or part of a clinical archive.

NOTE 9 This is a requirement for ALARM SYSTEMS in MEDICAL ELECTRICAL EQUIPMENT and MEDICAL ELECTRICAL SYSTEMS required by IEC 60601-1-8:2006/AMD1:2012, 6.12 a).

r) Clear distinction between the auditory, visual and vibratory ALARM SIGNALS of different priorities (HIGH PRIORITY, MEDIUM PRIORITY, or LOW PRIORITY).

NOTE 10 This is consistent with the IEC 60601-1-8 requirement that ALARM SIGNALS are prioritized. IEC 60601-1-8 places requirements on the auditory and visual ALARM SIGNALS.

s) Higher priority ALARM SIGNALS take precedence over lower priority ALARM SIGNALS.

NOTE 11 This is consistent with the IEC 60601-1-8 requirement that higher priority ALARM SIGNALS take precedence over lower priority ALARM SIGNALS.

6.5.2 Typical RISK CONTROL measures for implementation by the RESPONSIBLE ORGANIZATION

At least the following RISK CONTROL measures should be considered by the RESPONSIBLE ORGANIZATION.

a) System configuration done in a way that [15][16]
   - OPERATOR response is optimized;
     - the intended OPERATOR receives the intended ALARM CONDITION both by priority and type of ALARM CONDITION,
     - the intended OPERATOR receives appropriate information about ALARM CONDITIONS,
     - the unintended OPERATORS do not receive unintended ALARM CONDITIONS, and
   - equipment configuration and management are consistent;
     - have a process for safe ALARM SYSTEM management and response,
     - inspect, check, and maintain ALARM SYSTEM-equipped MEDICAL DEVICES,
     - have guidelines for tailoring ALARM SETTINGS and ALARM LIMITS for individual PATIENTS, AND
   - consideration is given to whether or not to allow remote ALARM SIGNAL inactivation.

b) RESPONSIBLE ORGANIZATION determines OPERATOR acceptable reaction time for each PATIENT or PATIENT group and type of ALARM CONDITION (pre-requisite):
   - overall reaction time of the DISTRIBUTED ALARM SYSTEM meets the RESPONSIBLE ORGANIZATION reaction time requirements;
   - monitoring time of the components and interfaces is no more than the reaction time required by the RESPONSIBLE ORGANIZATION; and
   - location system to generate TECHNICAL ALARM CONDITIONS when OPERATOR is out of range to react within an appropriate time.

c) PATIENT priority assignments to OPERATORS:
   - appropriate ALARM SETTINGS for PATIENT to OPERATOR (triage example);
   - assign priorities among PATIENTS;
   - consider the number of ALARM CONDITIONS and their priority;
   - consider the origination of ALARM CONDITIONS from multiple SOURCES on same PATIENT;
   - consider the origination of ALARM CONDITIONS from multiple PATIENTS;
   - consider the origination of ALARM CONDITIONS from multiple SOURCES on multiple PATIENTS; AND
   - consolidate multiple ALARM CONDITIONS from same PATIENT:
     i) Highest priority ALARM CONDITION; AND
     ii) Only one TECHNICAL ALARM CONDITION – simultaneously.

d) OPERATOR SAFETY, availability and personal protection (technical RISK MANAGEMENT):
   - real-time location system:
   - status message for OPERATOR availability;
   - OPERATOR mobility / immobility recognition; and
   - OPERATOR remote emergency button.

e) Technical resources assigned to OPERATORS:
   - allocation of COMMUNICATORS;
   - CDAS allocated for CDAS requirements;
   - CDAS or DAS allocated for DAS requirements; and
   - DAS or DIS allocated for DIS requirements.

f) Isolation wards:
   - to protect the PATIENT; and
   - to protect the OPERATOR.

g) Opened and closed doors – silent environment for PATIENT:

- a TECHNICAL ALARM CONDITION results in the automatic opening of PATIENT doors provided that there is no contraindication to opening them;
- a TECHNICAL ALARM CONDITION results in the OPERATOR'S opening of doors – organizational; and
- reactivate SOURCE ALARM SIGNALS (i.e., inactivate AUDIO OFF) – local ALARM SIGNALS reactivated.

h) Integration of medical and non-medical ALARM CONDITIONS:

- possible conflict between the priorities of ALARM CONDITIONS within same type and between types; and
- resource and configuration considerations.

i) Proper network design:

- physical electrical and logical isolation of essential and non-essential networks;
- quality of service;
- redundant no single point failure of MEDICAL IT-NETWORK;
- adequate bandwidth;
- proper protocols and versions for MEDICAL DEVICE to DAS communications;
- communications software configuration management – upgrades/downgrades/etc.;
- equipment compatibility issues; and
- adequate latency.

j) Identification and assignments of PATIENTS with OPERATORS:

- RFID (radio frequency identification) tags or bar codes to ensure right OPERATOR is attending to PATIENT;
- PIN codes for DAS and OPERATOR administrative functions (e.g., login, special reporting); and
- PIN code for access to or modification of PATIENT confidential information.

6.5.3 Organizational policies and procedures as RISK CONTROL measures for implementation by the RESPONSIBLE ORGANIZATION

At least the following policies or procedures should be considered by the RESPONSIBLE ORGANIZATION.

a) Definition of ALARM SYSTEM management procedures to minimize 'alarm fatigue':

1) SOURCE configuration to PATIENT context:
   - ALARM CONDITION ALARM LIMITS,
   - ALARM CONDITION priorities,
   - and other ALARM SETTINGS, and
   - identification and assignment of PATIENT to SOURCE;
2) INTEGRATOR:
   - PATIENT assignments to SOURCES,
   - REDIRECTION policies, and
   - ESCALATION policies;
3) COMMUNICATOR:
   - assess proper quantity and placement to ensure ALARM CONDITIONS are received,
   - identification and assignment of caregiver to COMMUNICATOR, and
   - quality of COMMUNICATOR (guaranteed delivery);
4) operational maintenance to ensure reliable signal acquisition at the SOURCE.

b) Alternative plans need to be implemented to ensure PATIENT SAFETY due to failure as well as degradation or loss of communication within the DAS:

5) provide method of labelling defective DAS components;

6) USER notification procedures and responsibilities; and

7) redundancy and spare components.

c) Respond to failures in the DAS:

8) written procedures that document backup workflow to respond to ALARM CONDITIONS;

9) simulation of failures and recoveries;

10) periodic training; and

11) documentation of training completion.

d) Preventative maintenance procedures to minimize potential failure in the DAS.

e) Define policies that ensure transfer of responsibility during shift changes and re-assignment of the SOURCES of ALARM CONDITIONS to OPERATORS and COMMUNICATORS.

f) Pre go-live testing.

g) Labelling:

12) DIS RECEIVER is properly labelled, and

13) components of the DAS are identified to prevent unauthorized access.

h) Training.

i) Retrospective assessment of policies/procedures.

j) Document installation of components/versions/integration of the DAS.

k) Assess impact of the DAS on existing ALARM SYSTEMS (e.g. nurse call, fire alarm).

Annex A
(informative)

Correspondence between the RISK CONTROL measures of this technical report and IEC 60601-1-8

Table A.1 shows the correspondence of the equipment RISK CONTROL measures of this technical report to those of IEC 60601-1-8.

Table A.1 – Correspondence of the technical RISK CONTROL measures of this technical report for a CDAS and IEC 60601-1-8 for a DAS

Technical RISK CONTROL measures implemented in equipment (subclause 6.5.1 of this technical report for a CDAS)	Related subclause of IEC 60601-1-8:2006 and IEC 60601-1-8:2006/AMD1:2012 for a DAS
a) Self-surveillance functionality	–
b) Connection monitoring with generation of a system TECHNICAL ALARM CONDITION upon failure	6.11.2.2.1 b) 1)
c) Affected functionally connected COMMUNICATORS generate ALARM SIGNALS to ensure that the intended OPERATORS receive notification	6.11.2.2.1 b) 2)
c) A COMMUNICATOR that cannot provide this TECHNICAL ALARM CONDITION should be marked with a warning	6.11.2.2.1 b) 1), 2)
d) Local ALARM SIGNAL generation when the remote COMMUNICATORS are not available	6.11.2.2.3
e) Technical confirmation or guarantee of responsibility upon receipt of ALARM CONDITION	–
f) OPERATOR response to INTEGRATOR and when needed to the SOURCE with technical confirmation or guarantee	–
g) COMMUNICATOR generates ALARM CONDITION for the OPERATOR using an ALARM SIGNAL	6.3.3.1
h) INTEGRATOR logs responsibility events as well as all ESCALATED, REDIRECTED and RESPONSIBILITY UNDEFINED events initiated by the INTEGRATOR	–
i) Means by which the OPERATOR response to the presented ALARM SIGNAL is fed back to the INTEGRATOR and, when needed, to the SOURCE	–
j) INTEGRATOR initiates REDIRECTION when RESPONSIBILITY UNDEFINED or RESPONSIBILITY REJECTED has been received	–
k) INTEGRATOR continues directing or redirecting the ALARM CONDITION, until a RESPONSIBILITY ACCEPTED is received or the SOURCE indicates the end of the ALARM CONDITION	–
l) REDIRECTION of an ALARM CONDITION to one or more additional COMMUNICATORS (OPERATORS) by the INTEGRATOR can trigger ESCALATION of that ALARM CONDITION	–
m) OPERATOR able to undo any response	6.8.4
n) RESPONSIBILITY ACCEPTED at the COMMUNICATOR can be returned to the SOURCE	6.11.2.3

o) RESPONSIBILITY ACCEPTED at the COMMUNICATOR can initiate an appropriate ALARM SIGNAL inactivation state	6.11.2.3
p) OPERATOR can initiate an appropriate ALARM SIGNAL inactivation state manually at the SOURCE	6.11.2.3
q) INTEGRATOR logs information about received, directed and redirected and escalated ALARM CONDITIONS as well as system failures	6.12
r) Clear distinction between ALARM SIGNALS of different priorities (HIGH PRIORITY, MEDIUM PRIORITY, LOW PRIORITY)	6.3.3.1
s) Higher priority ALARM SIGNALS take precedence over lower priority ALARM SIGNALS	6.3.2.2

Annex B
(informative)

Types of SOURCES

B.1 MEDICAL DEVICES

The types of MEDICAL DEVICES from which ALARM CONDITIONS are initiated (MEDICAL DEVICES that contain SOURCES) differ widely based on typical characteristics and INTENDED USES as defined by their MANUFACTURERS. The definition of the term MEDICAL DEVICE differs slightly between various jurisdictions and global regulatory frameworks. Using the definition of MEDICAL DEVICE as provided in this technical report, the following types of MEDICAL DEVICES are considered by this technical report when addressing the origins of ALARM CONDITIONS. Most MEDICAL DEVICES that include an ALARM SYSTEM also contain a SOURCE, a COMMUNICATOR and a simple INTEGRATOR.

a) MEDICAL ELECTRICAL EQUIPMENT

According to IEC 60601-1:2005, MEDICAL ELECTRICAL EQUIPMENT is one type of an electrically powered MEDICAL DEVICE provided with not more than one connection to a particular SUPPLY MAINS having direct PATIENT contact (by at least one APPLIED PART) or transferring energy to or from the PATIENT or detecting such an energy transfer.

b) MEDICAL ELECTRICAL SYSTEMS

It also is common practice for a MEDICAL DEVICE manufacturer, RESPONSIBLE ORGANIZATION or OPERATOR to connect MEDICAL ELECTRICAL EQUIPMENT with other MEDICAL DEVICES or non-medical equipment to achieve the desired functionality. Any combination of at least one MEDICAL ELECTRICAL EQUIPMENT, with items of other equipment such as office devices, home use equipment or other MEDICAL DEVICES, where the interconnection is by a FUNCTIONAL CONNECTION or by the use of a multiple socket outlet, is considered to be a MEDICAL ELECTRICAL SYSTEM. A MEDICAL ELECTRICAL SYSTEM is expected to comply with the requirements of IEC 60601-1:2005.

c) *In vitro* diagnostic (IVD) MEDICAL DEVICE

An '*in vitro* diagnostic medical device' means any MEDICAL DEVICE which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, equipment or system, whether used alone or in combination, intended by the MEDICAL DEVICE manufacturer to be used *in vitro* for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information:

– concerning a physiological or pathological state, or
– concerning a congenital abnormality, or
– to determine the safety and compatibility with potential recipients, or
– to monitor therapeutic measures.

If an IVD is electrically powered and used outside the environment of the PATIENT (greater than 1.5 m around a PATIENT) it is generally covered by the scope of IEC 61010-1 [1].

d) Active implantable MEDICAL DEVICE

An 'active implantable medical device' means any MEDICAL DEVICE relying for its functioning on a source of electrical energy or any source of power other than that directly generated by the human body or gravity, which is intended to be totally or partially introduced, surgically or medically, into the human body or by medical intervention into a natural orifice, and which is intended to remain after the procedure.

EXAMPLE 1 A pacemaker or internal defibrillator.

NOTE 1 An improper handling of ALARM CONDITIONS from these types of MEDICAL DEVICES could very quickly become life-threatening.

e) Software as a MEDICAL DEVICE

Stand-alone software whose INTENDED USE fulfils at least one criterion listed in definition 3.24 is a MEDICAL DEVICE, even if the hardware environment necessary to execute this software is not a MEDICAL DEVICE and so regulated. Any ALARM CONDITION deriving from such a SOURCE has to be treated with the same care as those from any other MEDICAL DEVICE.

NOTE 2 A prominent example of software as a MEDICAL DEVICE is a smart phone app with an INTENDED USE matching the criteria given in definition 3.24.

f) Intelligent biomedical clothing (IBC) as a MEDICAL DEVICE

There are a number of possible IBC applications ranging from a personal health watch to PATIENTS' disease and life management, including rehabilitation.

EXAMPLE 2 Diabetes management, cardiovascular diseases prevention and emergency intervention, drug delivery and stress management.

Based on dry-electrode technology that can be built into common items of clothing such as bras, briefs or waist belts, wireless monitoring technology continuously monitors the wearer's body signals such as the heart activity to detect abnormal health conditions. This new technology enables the development of a new category of products in the personal healthcare area, which meets definition 3.24.

g) Other MEDICAL DEVICES

There is a huge variety of products, which easily could cross the borderline by their manufacturer's marketing claims, to become MEDICAL DEVICES in the near future. Products that are currently used for convenience purposes, such as an entertainment function, phone system or smart phone application fall into this category. The ultimate criterion for crosschecking this borderline is when at least one of the characteristics listed in definition 3.24 has been obviously fulfilled. *De facto*, the publically available statements made by the manufacturer in commercializing a product provide the objective evidence to determine when such a product becomes a MEDICAL DEVICE. Insofar as those products are used in conjunction with a MEDICAL IT-NETWORK and initiate ALARM CONDITIONS, they will need to consider the information in this technical report.

h) ACCESSORIES to a MEDICAL DEVICE

In many jurisdictions and legal frameworks, ACCESSORIES necessary to provide the full functionality of the INTENDED USE of a MEDICAL DEVICE are required to be safe and effective as well, even if such an ACCESSORY is not classified as a MEDICAL DEVICE in its own right. Therefore, ACCESSORIES to MEDICAL DEVICES have to be evaluated for their impact on SAFETY and effectiveness for the PATIENT, OPERATOR and third parties. ALARM CONDITIONS deriving from an ACCESSORY (such as a charging device, data storage or IT-platform) can be as important as an ALARM CONDITION from any other MEDICAL DEVICE SOURCE itself.

B.2 NURSE CALL SYSTEM

A NURSE CALL SYSTEM is used in hospitals, nursing homes, nursing wards, elderly homes and similar institutions. A NURSE CALL SYSTEM can be a SOURCE. A NURSE CALL SYSTEM also can be the INTEGRATOR and provide the MEDICAL IT NETWORK for a DIS, DAS or CDAS.

A NURSE CALL SYSTEM provides the means to initiate ALARM CONDITIONS, manually or automatically, and the means to present this information to OPERATORS at different locations throughout a healthcare facility.

The INTENDED USE of a NURSE CALL SYSTEM is to communicate PATIENT or clinical staff calls for assistance, code calls, emergency ALARM CONDITIONS and MEDICAL DEVICE ALARM CONDITIONS. A NURSE CALL SYSTEM can also communicate PATIENT- and staff-related information to optimize the workflow of the care management PROCESS.

EXAMPLE 1 Signalling a critical ALARM CONDITION from a MEDICAL DEVICE.

EXAMPLE 2 Voice communication, staff presence indication, system fault status, etc.

In various countries, there are different standards and national requirements for a NURSE CALL SYSTEM and their functions [7][8][9][10][11][12][13]. Detailed descriptions of the different NURSE CALL SYSTEMS and their functions are not part of this technical report.

The way in which a MANUFACTURER intends a NURSE CALL SYSTEM to be used in combination with a DIS, DAS or CDAS, should be defined in the documentation accompanying the NURSE CALL SYSTEM.

EXAMPLE 3 Standalone NURSE CALL SYSTEM.

EXAMPLE 4 NURSE CALL SYSTEM with DISTRIBUTED INFORMATION ABOUT ALARM CONDITIONS.

EXAMPLE 5 NURSE CALL SYSTEM utilizing a MEDICAL IT-NETWORK AND COMMUNICATORS with confirmation.

Annex C
(informative)

Applicability of types of system for the distribution of ALARM CONDITIONS

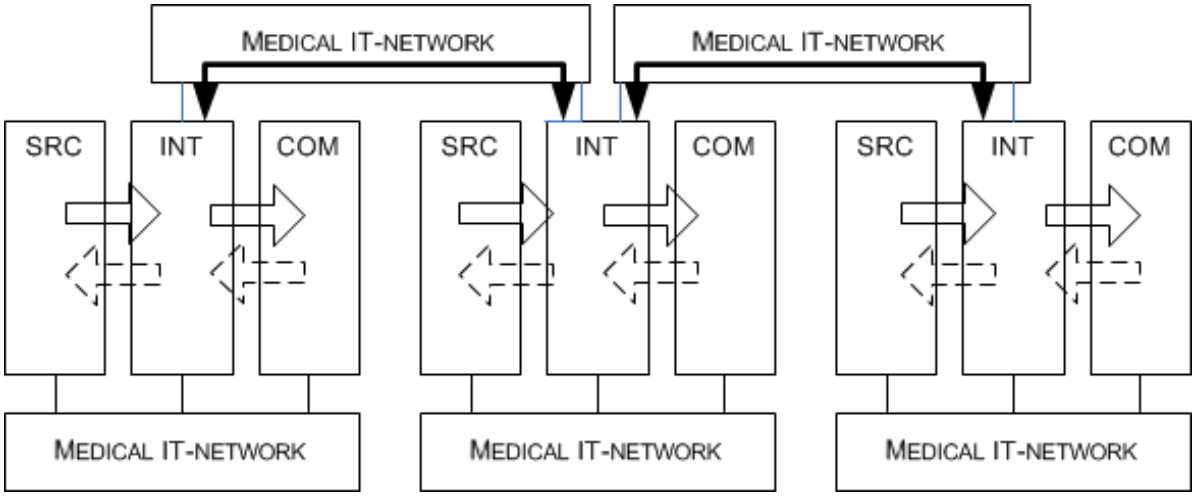
A system for the distribution of ALARM CONDITIONS consists of four components:

– SOURCE;
– INTEGRATOR;
– COMMUNICATOR; and
– MEDICAL IT-NETWORK.

These components can be treated as one system that does not need to be evaluated according to IEC 80001-1 when:

– these components are grouped together into a CDAS developed by a single MEDICAL DEVICE manufacturer using a network provided as part of the system (see IEC 80001-1, Annex C.2); or
– regional requirements are in place (such as VDE 0834 [12][13] for NURSE CALL SYSTEMS, or VDE 14675 [14] for fire alarm systems).

When systems are combined, the ALARM CONDITIONS and responses should be communicated between INTEGRATORS as illustrated in Figure C.1.



Key

SRC = SOURCE
INT = INTEGRATOR
COM = COMMUNICATOR

Figure C.1 – Cascading structure of system for the distribution of ALARM CONDITIONS

With these rules a complex systems can be divided into “atomic” parts, which allows one to easily identify the subjects of RISK MANAGEMENT according to IEC 80001-1.

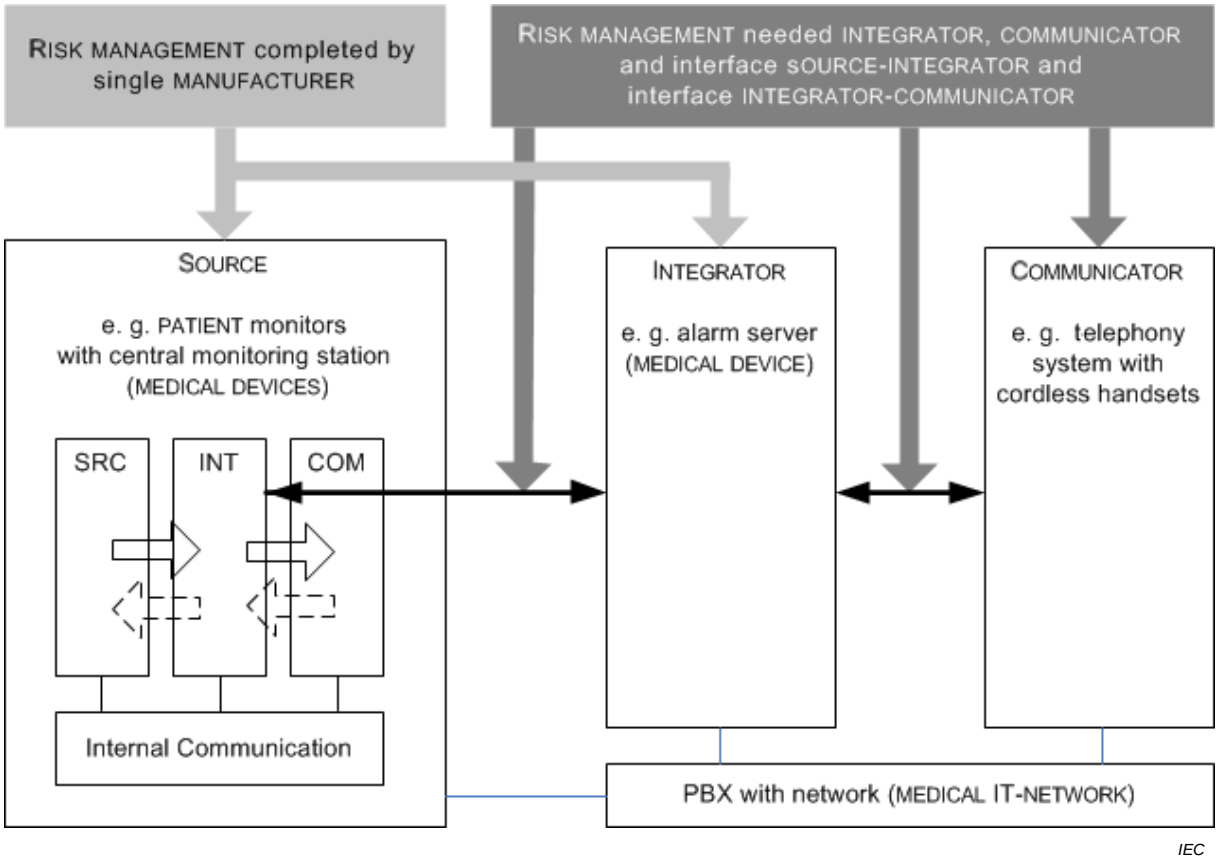
In Figure C.2 an isolated monitoring system is connected to a telephony system and ALARM CONDITIONS are distributed.

In this example, RISK MANAGEMENT according to IEC 80001-1 is not required for:

– PATIENT monitor with central monitoring station (MEDICAL DEVICE); and
– alarm server (MEDICAL DEVICE).

In this example, the RISK MANAGEMENT should be performed for:

– DECT (Digital Enhanced Cordless Telecommunications) handsets;
– interface between the PATIENT monitor, the central monitoring station and the alarm server; and
– interface between alarm server and telephony system with cordless handsets.



Key

SRC = SOURCE
INT = INTEGRATOR
COM = COMMUNICATOR

Figure C.2 – Example for INTEGRATOR of a PATIENT monitor with central monitoring station to distribute ALARM CONDITIONS in a physically isolated IT-NETWORK in a CDAS

In Figure C.3, a PATIENT monitor is connected to a NURSE CALL SYSTEM and ALARM CONDITIONS are distributed.

The NURSE CALL SYSTEM itself is not a MEDICAL IT-NETWORK, when no MEDICAL DEVICE is connected. A NURSE CALL SYSTEM that is used in a DISTRIBUTED ALARM SYSTEM becomes a MEDICAL IT-NETWORK when:

– a MEDICAL DEVICE is connected to the NURSE CALL SYSTEM, or
– the NURSE CALL SYSTEM itself is a MEDICAL DEVICE.

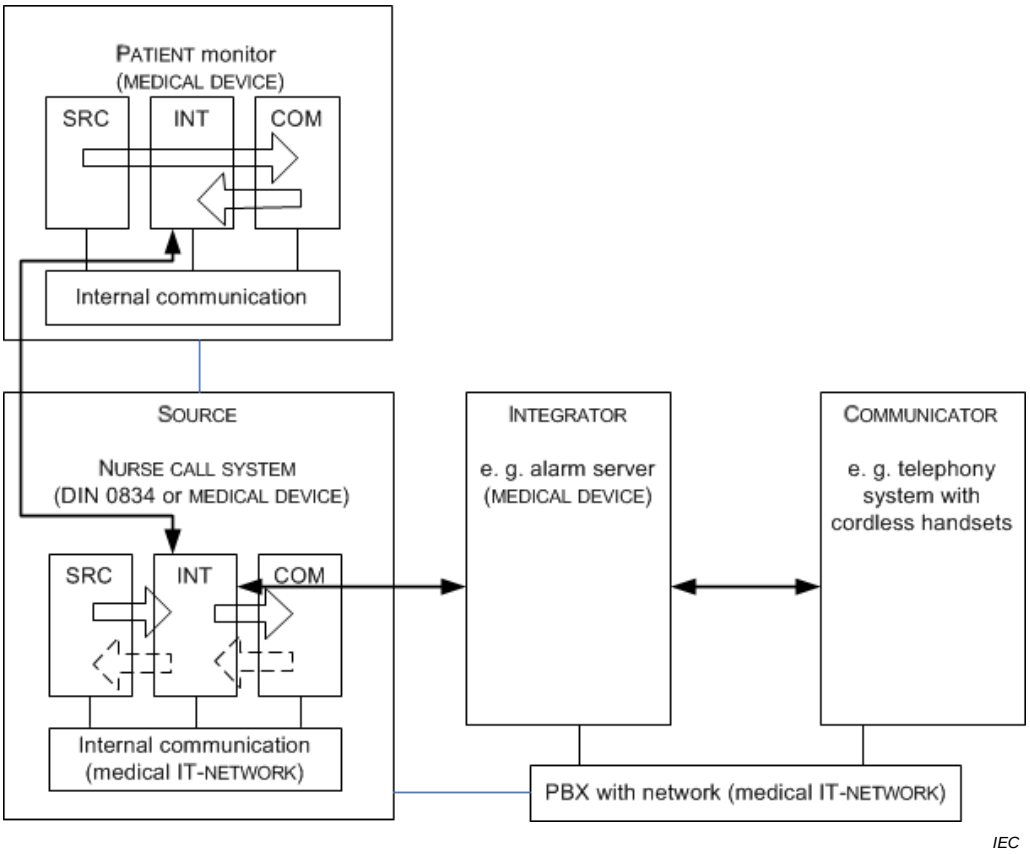
In this example, RISK MANAGEMENT according to IEC 80001-1 is not required for:

– NURSE CALL SYSTEM;
– PATIENT monitor (MEDICAL DEVICE); and
– alarm server (MEDICAL DEVICE).

In this example, the RISK MANAGEMENT should be performed for:

– DECT/IP handsets;
– interface between PATIENT monitor and INTEGRATOR of a NURSE CALL SYSTEM;
– interface between PATIENT monitor and alarm server;
– interface between NURSE CALL SYSTEM and alarm server; and
– interface between alarm server and PBX (private branch exchange)/DECT handsets.

NOTE Other interface types are used including ESPA-X (Enhanced Signaling Protocol for Alarm Processes – XML-based) and various TCP/IP (Transmission Control Protocol/IP) systems.



Key

SRC = SOURCE
INT = INTEGRATOR
COM = COMMUNICATOR

Figure C.3 – Example for INTEGRATOR of a PATIENT monitor to distribute ALARM CONDITIONS in a NURSE CALL SYSTEM, and via a PBX with handsets

Annex D
(informative)

Scalability of types of system for the distribution of ALARM CONDITIONS

Using the model of a system for the distribution of ALARM CONDITIONS, very flat and easy systems can be described, but also highly integrated and combined structures. Figure D.1 shows a complex scenario with many different types of interferences between the individual systems.

The scenario shown here consists of the following parts:

– PATIENT monitors:

  In the intensive care rooms, the hospital uses PATIENT monitors that are integrated in a local DISTRIBUTED ALARM SYSTEM. The COMMUNICATOR is a display in the central station located at the nurses' station. Each monitor has its own INTEGRATOR with local COMMUNICATOR.

– NURSE CALL SYSTEM:

  In the intensive care rooms, and across other hospital stations and wards, NURSE CALL SYSTEMS are installed. These systems have their own COMMUNICATOR and flashing signal lights along the corridors to communicate ALARM CONDITIONS TO OPERATORS.

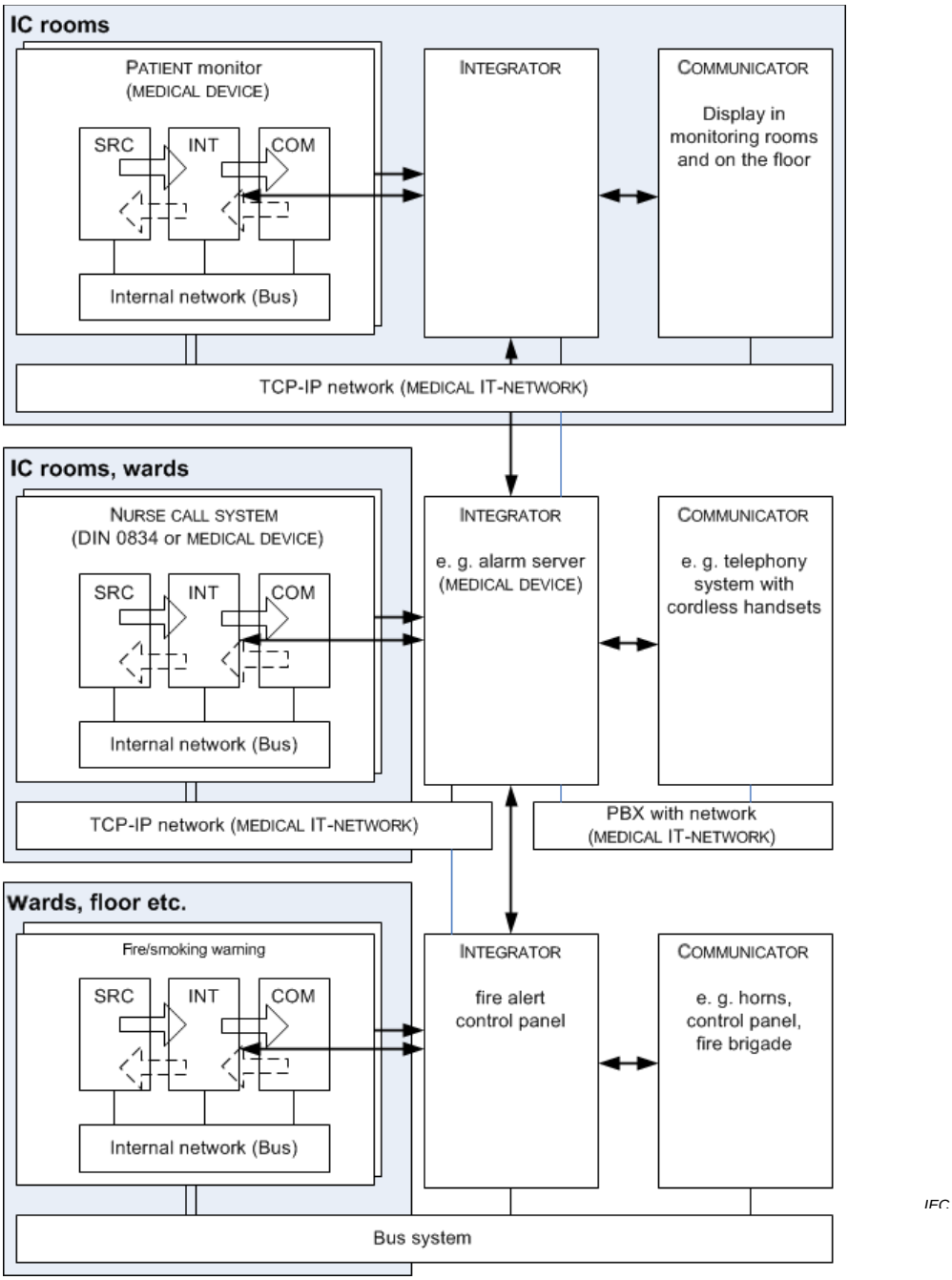
– fire alarm system:

  The fire alarm system has to declare conformity to regional requirements [8][14] with its own COMMUNICATORS (e. g. signal horns along the corridors, control panel of the fire brigade).

When these components are connected to a common INTEGRATOR, the system becomes a DISTRIBUTED ALARM SYSTEM in the sense of IEC 80001-1. In so doing, a new INTENDED USE is created, and new HAZARDOUS SITUATIONS are added to the system, for example:

– use of non-reliable COMMUNICATORS;
– limited resources (e. g. PBX channels);
– concurrent ALARM CONDITIONS (e. g. fire, cardiac, ventilator);
– insufficient or inadequate staffing;
– additional training required.

To make a DAS a CDAS, the considerations of Clause 5 should be fulfilled, and the appropriate RISK MANAGEMENT performed.



Key

SRC = SOURCE

INT = INTEGRATOR

COM = COMMUNICATOR

Figure D.1 – Example hospital-wide DISTRIBUTED ALARM SYSTEM

Bibliography

[1] IEC 61010-1, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 1: General requirements*

[2] IEC TR 80001-2-1:2012, *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*

[3] IEC TR 80001-2-2, *Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*

[4] IEC TR 80001-2-3, *Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks*

[5] IEC TR 80001-2-4, *Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations*

[6] ISO 14971:2007, *Medical devices – Application of risk management to medical devices*

[7] HTM 08-03:2013, *Management of bedhead services in the health sector, UK Department of Health*

[8] NFPA 72:2013, *National Fire Alarm and Signaling Code*

[9] NFPA 99:2012, *Health Care Facilities Code*

[10] UL 1069:2012 (Ed. 7), *Hospital Signaling and Nurse Call Equipme*nt

[11] UL 2560:2011 (Ed. 1), *Standard for Safety for Emergency Call Systems for Assisted Living and Independent Living Facilities*

[12] VDE 0834-1:2000, *Call systems in hospitals, nursing homes and similar institutions Part 1: Requirements for equipment, erection and operation*

[13] VDE 0834-2:2000, *Call systems in hospitals, nursing homes and similar institutions – Part 2: Environment conditions and electromagnetic compatibility*

[14] VDE 14675:2003, *Fire detection and fire alarm systems – Design and operation*

[15] AAMI, *Clinical Alarms Summit – Final report*, 2011

[16] Joint Commission, *Medical device alarm safety in hospitals. Sentinel Event Alert*, Issue 50, April 8, 2013

[17] MILLER, J.B. Wireless technology allows close monitoring of cardiac status. *Nurses.com newsletter*, September 12, 2000

[18] IEC 60601-1-8:2006, *Medical electrical equipment – Part 1-8: General requirements for basic safety and essential performance – Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems*
IEC 60601-1-8:2006/AMD1:2012

Index of defined terms used in this technical report