IEC TR 80001-2-5

Edition 1.0 2014-12

TECHNICAL REPORT

colour inside

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

IEC TR 80001-2-5:2014-12(en)

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online 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 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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 80001-2-5

Edition 1.0 2014-12

TECHNICAL REPORT

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE W

ICS 11.040.01; 35.240.80

ISBN 978-2-8322-1969-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

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

Part 2-5: Application guidance – Guidance on distributed alarm systems

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 '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

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].

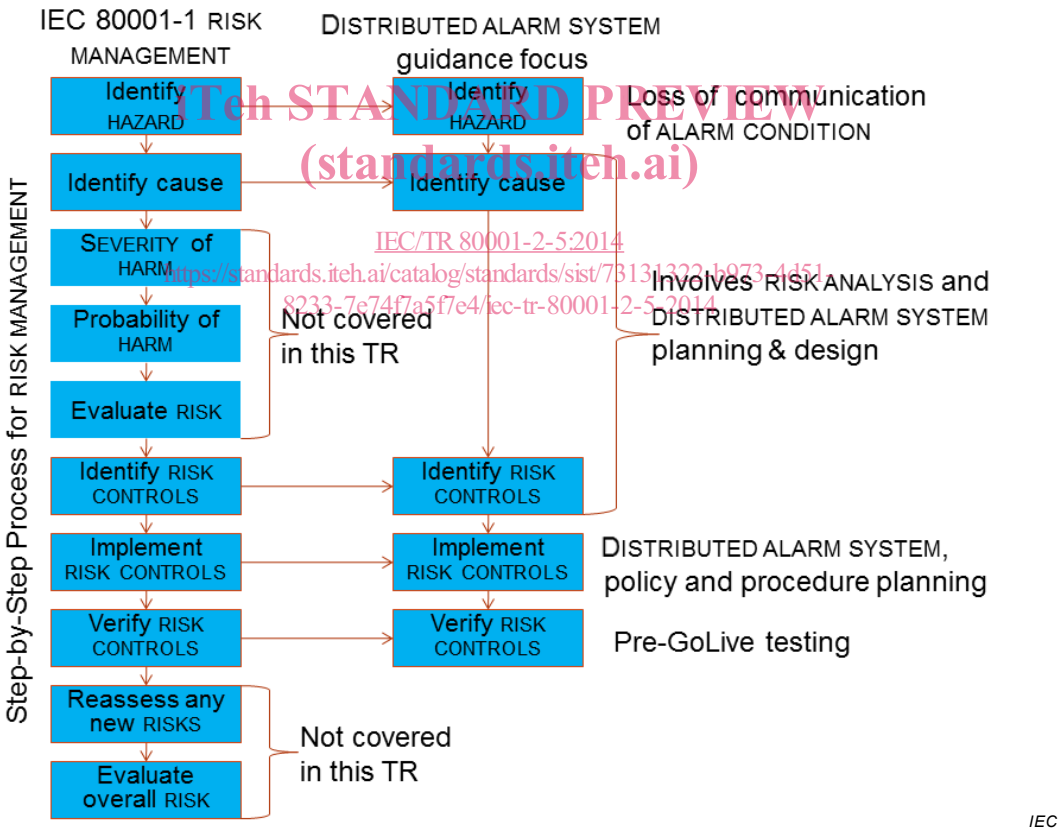


Figure 1 – Focus of this technical report

1 Numbers in square brackets refer to the Bibliography.

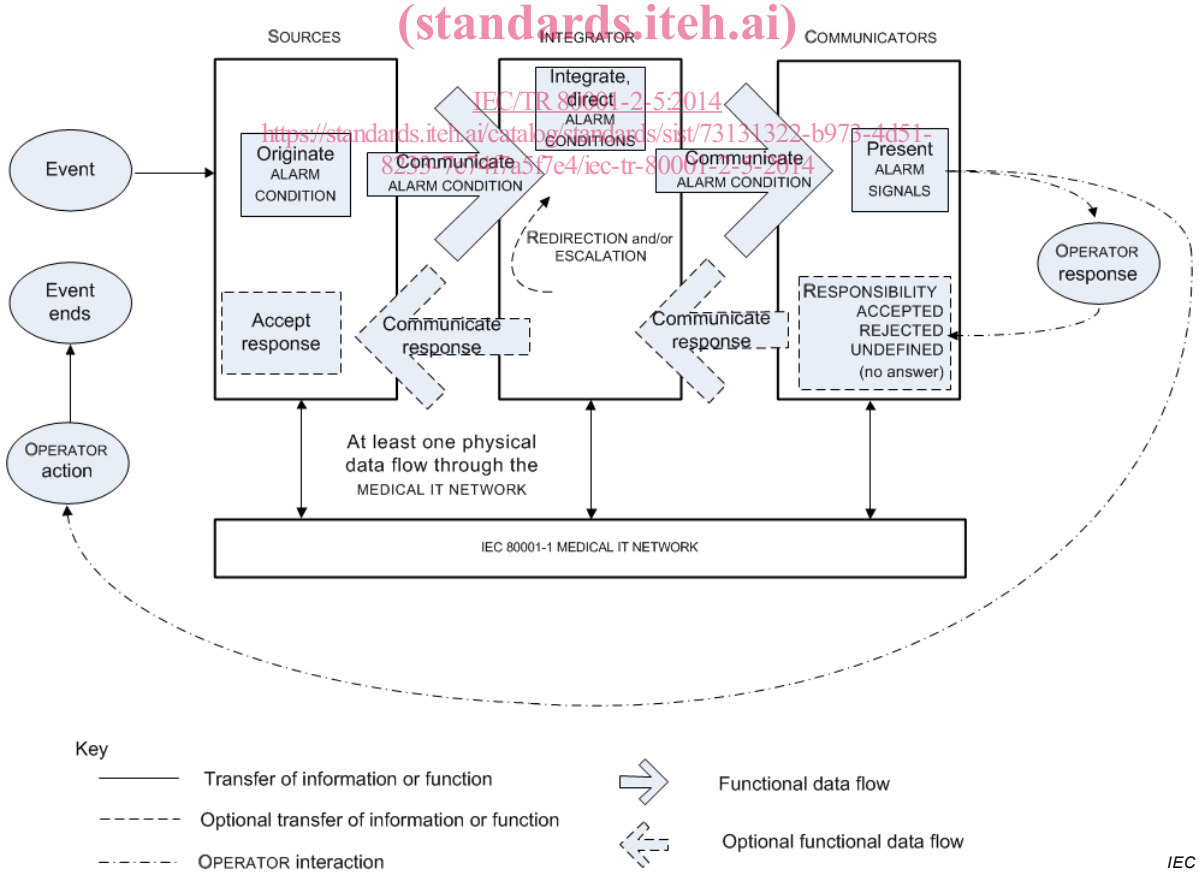
APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

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 37.

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 38.

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]