# IEC 63044-4

Edition 1.0 2021-06

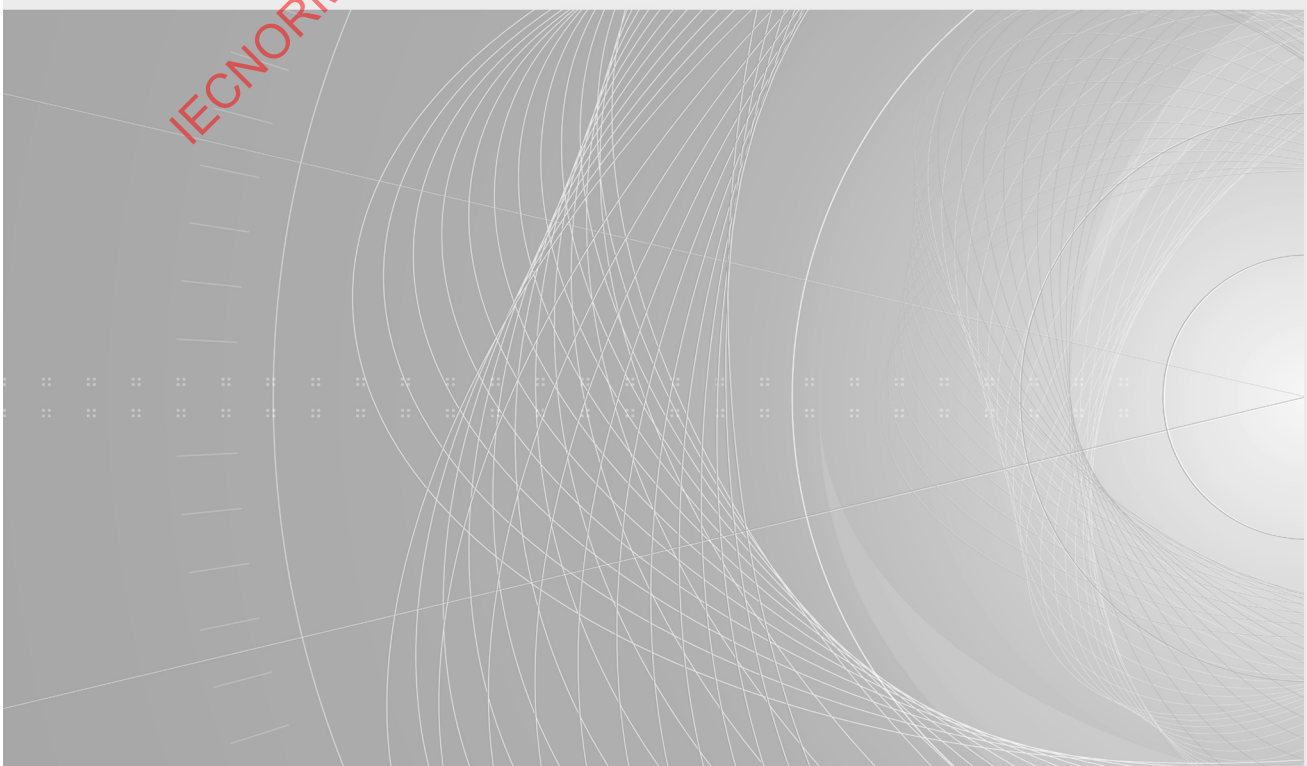
# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## Home and building electronic systems (HBES) and building automation and control systems (BACS) – Part 4: General functional safety requirements for products intended to be integrated in HBES and BACS

## Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) et systèmes de gestion technique du bâtiment (SGTB) – Partie 4: Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les HBES et SGTB



IEC 63044-4:2021-06(en-fr)

**THIS PUBLICATION IS COPYRIGHT PROTECTED**
**Copyright © 2021 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

**IEC publications search - webstore.iec.ch/advsearchform**
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 once a month by email.

**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: sales@iec.ch.

**IEC online collection - oc.iec.ch**
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - www.electropedia.org**
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

**A propos de l'IEC**
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

**A propos des publications IEC**
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

**Recherche de publications IEC - webstore.iec.ch/advsearchform**
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

**IEC Just Published - webstore.iec.ch/justpublished**
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

**Service Clients - webstore.iec.ch/csc**
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

**IEC online collection - oc.iec.ch**
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

**Electropedia - www.electropedia.org**
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

IEC 63044-4

Edition 1.0 2021-06

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## Home and building electronic systems (HBES) and building automation and control systems (BACS) – Part 4: General functional safety requirements for products intended to be integrated in HBES and BACS

## Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) et systèmes de gestion technique du bâtiment (SGTB) – Partie 4: Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les HBES et SGTB

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 29.120.01; 29.120.99

ISBN 978-2-8322-9898-5

**Warning! Make sure that you obtained this publication from an authorized distributor.**
**Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS



IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# HOME AND BUILDING ELECTRONIC SYSTEMS (HBES) AND BUILDING AUTOMATION AND CONTROL SYSTEMS (BACS) –

## Part 4: General functional safety requirements for products intended to be integrated in HBES and BACS

## 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.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

IEC 63044-4 has been prepared by IEC technical committee 23: Electrical accessories. It is an International Standard.

The text of this International Standard is based on the following documents:

| FDIS | Report on voting |
|---|---|
| 23/973/FDIS | 23/975/RVD |

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 63044 series, published under the general title *Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)*, can be found on the IEC website.

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

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

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# INTRODUCTION

Functional safety includes the safe operation of devices and appliances ("products") when installed into and operating on a communications network in a home or building ("premises").

This document specifies installation, control, operating, and failure mode procedures to enhance the functional safety of devices installed in homes and buildings. A device functions safely if it causes no harm while operating and performing an intended task. Such devices might not operate safely due to installation or control problems.

The growing use of home and building networks to interconnect devices introduces additional challenges to maintaining functional safety because of possible device interactions. Therefore, this document addresses the risks of connecting devices to a home or building network, which enables data exchanges and remote control from within the home or building.

Furthermore, if the home or building network is connected to a public network, control from remote locations may be possible. Such control messages might originate from a smart phone app, be sent through a mobile telephone network, routed to a building gateway, and sent via a home or building network to a device communications interface. Thus, there are many opportunities for such messages to be compromised. Remote access poses additional threats to functional safety that are addressed in this document.

This document is part of IEC 63044 series and applies to home and building electronic systems (HBES/BACS).

This document applies to home and building electronic systems (HBES) in general and specifically to systems conforming to the home electronic system (HES) family of ISO/IEC standards.

HBES/BACS products in this document are for non-safety-related systems.

The intention of this document is to specify, as far as possible, all safety requirements for HBES/BACS products in their life cycle.

This document specifies the general functional safety requirements for devices connected to a home or building network following the principles of the basic standard for functional safety, IEC 61508 (all parts). It covers functional safety issues related to device and device installations. The requirements are based on a risk analysis in accordance with IEC 61508.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# HOME AND BUILDING ELECTRONIC SYSTEMS (HBES) AND BUILDING AUTOMATION AND CONTROL SYSTEMS (BACS) –

# Part 4: General functional safety requirements for products intended to be integrated in HBES and BACS

## 1 Scope

This part of IEC 63044 provides the functional safety requirements for HBES/BACS.

In addition, it defines functional safety requirements for the interface of equipment intended to be connected to an HBES/BACS network. It does not apply to interfaces to other networks.

NOTE 1 An example of another network is a dedicated ICT network covered by IEC 62949.

This document does not provide functional safety requirements for safety-related systems.

NOTE 2 Examples of non-safety-related HBES/BACS applications are given in Annex C.

This document does not provide requirements on data protection and security.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60364 (all parts), *Low-voltage electrical installations*

IEC 63044-3:2017, *Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 3: Electrical safety requirements*

IEC 63044-5 (all parts), *Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61709:2017, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

## 3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

**3.1**
**authentication**
means for certifying that the entity sending a message is what or who it purports to be and confirmation that the message is identical to that which was sent

**3.2**
**authorisation**
mechanism to ensure that the entity or person accessing information, functions or services has the authority to do so

**3.3**
**disturbed communication**
communication in which for any reason a message being communicated is incomplete, truncated, contains errors or has the correct format but delivers information which is outside the range of expected parameters for such a message

**3.4**
**functional safety**
freedom from unacceptable risk of harm due to the operation of an HBES/BACS, including that resulting from:

1) normal operation,
2) reasonably foreseeable misuse,
3) failure,
4) temporary disturbances,

and forming part of the overall safety relating to the EUC (equipment under control, see 3.17) and the EUC control system that depends on the correct functioning of the E/E/PE (electrical/electronic/programmable electronic) safety-related systems and other risk reduction measures

Note 1 to entry: The definitions of "functional safety" given in IEC/TR 61000-2-1 and IEC 61000-1-2 are taken into account.

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – Addition of introduction and items 1 to 4 of list, text in brackets, and note.]

**3.5**
**Hamming distance**
number of bits in which two binary codes differ

**3.6**
**harm**
physical injury or damage to the health of people either directly or indirectly as a result of damage to property or the environment

[SOURCE: IEC 61508-4:2010, 3.1.1, modified – Addition of "either directly or indirectly as a result of".]

**3.7**
**hazard**
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2]

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

**3.8**
**hazardous event**
situation which results in harm on normal operation or abnormal condition

Note 1 to entry: Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the consequence of the hazardous event and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

Note 2 to entry: Adapted from IEC 61508-4:2010, 3.1.4.

**3.9**
**product**
device in the form of hardware or firmware, and its associated software and configuration tools

**3.10**
**product documentation**
manufacturer's installation and operations literature, such as manufacturer's catalogue, leaflet and other printed or electronic product information

**3.11**
**safety-related system**
designated system that both

– implements the required safety functions necessary to achieve or maintain a safe state for the EUC, and
– is intended to achieve, on its own or with other E/E/PE safety-related systems and other technology risk reduction measures, the necessary safety integrity for the required safety functions

Note 1 to entry: The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the other risk reduction measures, the necessary risk reduction in order to meet the required tolerable risk. See also Annex A of IEC 61508-5.

Note 2 to entry: Safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on detection of a condition which may lead to a hazardous event. The failure of a safety-related system would be included in the events leading to the determined hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems.

Note 3 to entry: Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.

Note 4 to entry: A safety-related system may

a) be designed to prevent the hazardous event (i.e. if the safety-related systems perform their safety functions then no harmful event arises);
b) be designed to mitigate the effects of the harmful event, thereby reducing the risk by reducing the consequences;
c) be designed to achieve a combination of a) and b).

Note 5 to entry: A person can be part of a safety-related system. For example, a person could receive information from a programmable electronic device and perform a safety action based on this information, or perform a safety action through a programmable electronic device.

Note 6 to entry: A safety-related system includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).

Note 7 to entry: A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

[SOURCE: IEC 61508-4:2010, 3.4.1, modified – The word "technology" has been added to the definition.]

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

**3.12**
**safety integrity**
probability of a safety-related system satisfactorily maintaining the required safety functions under all the stated conditions within a stated period of time

Note 1 to entry: The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the specified safety functions or will fail to adopt a specified state when required.

Note 2 to entry: There are four levels of safety integrity (see 3.5.8 of IEC 61508-4:2010).

Note 3 to entry: In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) that lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the average frequency of failure in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, safety integrity also depends on many factors that cannot be accurately quantified but can only be considered qualitatively.

Note 4 to entry: Safety integrity comprises hardware safety integrity and systematic safety integrity.

Note 5 to entry: This definition focuses on the reliability of the safety-related systems to perform the safety functions (see IEV 192-01-24 for a definition of reliability).

[SOURCE: IEC 61508-4:2010, 3.5.4, modified – Deletion of "E/E/PE" from the definition, the word "performing" has been replaced with "maintaining", "specified" has been replaced with "required", and "of IEC 61508-4:2010" has been added to Note 2.]

**3.13**
**safety integrity level**
**SIL**
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL $n$ safety-related system" (where $n$ is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to $n$.

[SOURCE: IEC 61508-4:2010, 3.5.8, modified – The date has been added to IEC 61508-1.]

**3.14**
**risk**
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, modified – The date has been added to IEC 61508-1.]

**3.15**
**reasonably foreseeable misuse**
use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behaviour

[SOURCE: IEC 61508-4:2010, 3.1.14]

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

**3.16**
**safety function**
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

EXAMPLE Examples of safety functions include:

– functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor); and

– functions that prevent actions being taken (for example preventing a motor starting).

[SOURCE: IEC 61508-4:2010, 3.5.1]

**3.17**
**EUC**
**equipment under control**
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

Note 1 to entry: The EUC control system is separate and distinct from the EUC.

[SOURCE: IEC 61508-4:2010, 3.2.1]

## 4 General requirements

### 4.1 General

Functional safety of a system relies upon both the performance of the network, and upon the performance of the connected HBES/BACS products:

1) failure of either the network or any other part of the HBES/BACS shall not cause the system, the products, or the controlled equipment to become unsafe;
2) while in operation, individual HBES/BACS products shall not rely solely upon the system for their safe operation;
3) while in operation, the system's interaction of any product(s) with any other product(s) shall not result in unsafe operation of the system.

### 4.2 Method of establishment of the requirements

#### 4.2.1 General

For specification of the functional safety requirements, the life cycle used in IEC 61508 (all parts) shall be followed for:

1) concept phase of products;
2) application environment;
3) identification of hazards and hazardous events;
4) hazard and risk analysis, risk reduction measures;
5) realisation of risk reduction measures;
6) validation;
7) maintenance;
8) installation and commissioning;
9) decommissioning.

The product technical committees and/or developers shall take the requirements of this document into account in the product safety requirements, but it is not necessary to go into the IEC 61508 series process itself.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

#### 4.2.2 HBES/BACS application environment

The HBES/BACS application environment is taken into account.

#### 4.2.3 Sources of hazards

The following sources of hazards have been considered:

1) material and construction;
2) reliability;
3) normal operation;
4) unintentional interaction with other products;
5) interaction with other HBES/BACS products;
6) abnormal conditions;
7) foreseeable misuse, including the download of unauthorised and malicious code;

NOTE This includes unintentional software modifications.

8) life time;
9) environment;
10) installation and maintenance.

#### 4.2.4 Hazardous events

The following is a non-exhaustive list of hazardous events which have been taken into account for the analysis (the bus and mains (230 V/400 V) have been considered):

1) power failure;
2) overvoltage on the bus line;
3) wrong connection;
4) overtemperature;
5) fire;
6) mechanical shock, vibration;
7) corrosion;
8) electromagnetic disturbance;
9) pollution;
10) end of life of a component/product;
11) reasonably foreseeable misuse;
12) software failure;
13) overload;
14) switching of damaged equipment and subsystems;
15) remote control;
16) command from two sources to one product (e.g. actuator).

Other hazardous events may be considered. For example: short circuit on the bus line; corrosion; breakdown of material.

#### 4.2.5 Derivation of requirements

The risk analysis has been carried out for each of the hazardous events (see 4.2.4). Annex B includes an example of risk analysis and the corresponding functional safety measures.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

In all cases where the evaluated risk classes indicate an unacceptable risk, risk reduction measures are required as well as the level of risk reduction effect and its validation. Some risk reduction measures are proposed and what is usually covered by the relevant product standard is also indicated. If manufacturers intend to develop HBES/BACS products/systems which exhibit hazardous events not covered by 4.2.4 the risk analysis shall be carried out according to IEC 61508 (all parts).

# 5 Requirements for functional safety

## 5.1 General

Analysis according to IEC 61508 (all parts) indicates that functional safety depends upon both the design and manufacture of products and upon the appropriate use of the products in installations.

Subclauses 5.2 to 5.6 contain requirements for HBES/BACS products and for the provision of information necessary for the proper installation, operation and maintenance of these products.

Compliance requirements are given for the products as necessary and verification of the provision of the necessary information.

All referenced product tests are type tests.

The basis and reasons for the following requirements are shown in Annex B.

NOTE The hazardous events listed in 4.2.4 are referred to according to their list number in brackets, for example, (1), (2), etc.

## 5.2 Power feeding

**5.2.1** In the event of power failure, the products shall restart safely when power is restored. (1)

NOTE Safe restart can be performed by:

– storing the status information and using this information for rebuilding the functionality after power on,

– switching to a defined state of the product depending on the application,

– calculation of the safe state based on the information available from the system (from a controller, if any and/or from each product),

– maintaining a sufficient power reserve (by providing an appropriate buffer time either in the product and/or in the power supply unit) to enable connected products to enter a safe state.

**5.2.2** Marking and instructions of the products shall be designed to prevent the risk of wrong connections. (2) (3)

The products shall be marked in a legible and durable manner.

It is recommended that labelling be language agnostic.

Compliance shall be checked by inspection of the product documentation and if appropriate according to the test of legible and durable markings in the relevant product standard.

**5.2.3** The construction and design of a product shall have provisions to prevent wrong connections. This may be supported by appropriate grouping of connections. (3)

Compliance shall be checked by inspection of the product.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

### 5.3 Life time

The products shall be designed for a defined useful lifetime according to IEC 61709:2017 or by testing the product according to the relevant product standard endurance test under normal condition.

The datasheet shall give instructions for maintenance if required to reach the specified lifetime. (10)

Compliance shall be checked by inspection of the documentation.

### 5.4 Reasonably foreseeable misuse

**5.4.1** The risk of accidental download of the wrong application software or parameters into the products shall be minimised. (11)

NOTE The following measures could be used:

– design of the configuration tool;
– identification of products and comparison of their profiles by the network management;
– password;
– authentication;
– product documentation;
– training of installers/operators.

Compliance shall be checked by inspection of the product documentation.

**5.4.2** Proper configuration and related parameters shall be ensured. (11)

NOTE The following measures can apply:

– specification of parameter ranges;
– limited configuration possibilities for the end-user;
– access to configuration for skilled persons only;
– consistency check by tools or by the installer;
– check of conformity with configuration.

Compliance shall be verified by check of conformity of the existing configuration with the planned (intended) configuration.

**5.4.3** Measures shall be provided for the detection and/or indication of missing or incompletely configured products during the configuration process. (11)

NOTE The following measures can apply:

– design of the configuration tool;
– formal installation procedures.

Compliance shall be checked by product test or inspection of the product documentation.

### 5.5 Software and communication

NOTE The software and communication requirements of this Subclause 5.5 are not intended to cover data protection and cybersecurity.

**5.5.1** The software development process shall include an appropriate procedure to support the proper operation of this software. (12)

Compliance shall be checked by inspection of the process documentation or of the corresponding certificates.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

**5.5.2** Measures shall be provided to check the proper operation of the product software and the integrity of the configuration. If abnormal operation is detected, the product shall restore the correct values or shall go to a defined state. (12)

Compliance shall be checked by inspection of the product software design documentation.

**5.5.3** If required by the application, measures shall be provided inside the products to limit the traffic load imposed on the communication medium. (13)

The following measures can apply:

– limitation of cyclic transmission;
– limitation of the number of messages per time unit per product;
– limitation of polling cycles.

Compliance shall be checked by inspection of the product documentation and if possible by product testing.

**5.5.4** The reception of messages from several sources shall not disturb the proper function of the product and shall not cause hazards. (16)

NOTE The following measures can apply:

– if there is a hierarchy of the sources, check source address;
– apply the rule: first in, first out;
– apply the rule: last message wins;
– secure the process by finalising before new messages can change the behaviour;
– secure the process by stopping and restarting the process;
– secure the process by disabling and enabling the process.

Compliance shall be checked by inspection of the product documentation and if possible by product testing.

**5.5.5** The products shall respond to a system reset (if any) by going to a defined state.

Compliance shall be checked by inspection of the product documentation and if possible by product testing.

**5.5.6** It shall be possible to restrict access to the manual configuration of system parameters.

NOTE The following measures or exceptions can apply except where manual configuration is explicitly detailed in its instruction manual (also the case for automatic configuration):

– use of a tool (hardware or software);
– use of password and/or authentication;
– ensure that unauthorised access is not possible;
– combination or sequence of actions;
– concealed means for configuration.

Compliance shall be checked by inspection of the product documentation and if possible by product testing.

**5.5.7** The safe operation of a product shall be independent of the operation of other products in the system or application.

NOTE The following measures can apply:

– cyclic transmission;
– range checking of received variables.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

Compliance shall be checked by inspection of the results of the EMC product tests.

**5.5.8** Measures for the identification of disturbed messages shall be provided. If a disturbed message is detected, measures shall be taken to ensure safe operation. (8)

Data integrity shall be maintained with appropriate methods for error detection and correction.

NOTE The following measures can apply:

– the message may be rejected or corrected by the receiving product;

– the message may be repeated by the sender.

Compliance shall be checked by inspection of the results of the product test or by inspection of the product documentation.

**5.5.9** Measures shall be provided to enable message losses to be indicated or to cause messages to be repeated in the event of message loss. (13)

NOTE The following measures can apply:

– communication acknowledgement mechanisms or an application acknowledgement mechanism;

– feedback status indication or visible effects;

– appropriate systematic repeat in the case of unidirectional products.

Compliance shall be checked by inspection of the results of the product test or by inspection of the product documentation.

### 5.6 Remote operations

NOTE The remote operation requirements of this Subclause 5.6 are not intended to cover data protection and cybersecurity.

#### 5.6.1 General recommendations

Remote control inside a room is covered by the previous requirements, set out in 5.5.

The safe operation of products, for example, socket-outlets, under remote control, shall be guaranteed by product and installation requirements. No specific system requirements apply.

#### 5.6.2 Within a single building or in its immediate vicinity

Products or the subsystem connected to the product which may cause harm, intended for remote control within a single building or in its immediate vicinity, shall have provisions for local means of operation, or local means to enable/disable the remote operation.

NOTE The following measures can apply:

– local means of operation on the potentially harmful products;

– local means of operation adjacent to the potentially harmful products;

– communication inputs supporting local operation.

Compliance shall be checked by inspection of the product or of the product documentation.

#### 5.6.3 From outside the building

Products or the subsystem connected to the product which may cause harm and which are intended for remote control from outside the building shall include local means to enabling/disabling the remote operation.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

NOTE The following measures can apply:

– local means of enabling operation on the potentially harmful products;
– local means of enabling operation located adjacent to the potentially harmful products;
– communication inputs supporting local enabling operation;
– local means to disable the gateway or other remote access product.

Compliance shall be checked by inspection of the product or of the product documentation.

**5.6.3.1** A mechanism shall be provided for the authorisation or authentication of remote control from outside the building (see also Table 1). (15) This may apply at system (fire wall or gateway) or at product level.

NOTE Authorisation can be:

– password authorisation or authentication,
– access through a dedicated line.

Compliance shall be checked by inspection of the product or of the product documentation.

### 5.6.4 Management

**5.6.4.1** A mechanism shall be provided for the authorisation or authentication of remote management including configuration and download from outside the building (see also Table 1). This may apply at system (fire wall or gateway) or at product level. (15)

Compliance shall be checked by inspection of the product or of the product documentation.

**5.6.4.2** Measures to guarantee consistency between the actual network and its remote image shall be provided. (15)

NOTE The following measures can apply:

– procedure to ensure a single authoritative copy of the system database;
– mechanisms to validate the remote system database against the actual network;
– self-documentation feature in the system (centrally or distributed).

Compliance shall be checked by inspection of the product or of the product documentation.

**Table 1 – Requirements for avoiding inadvertent operations and possible ways to achieve them**

| Requirements | Ways of meeting the requirements |
|---|---|
| Avoid inadvertent operation | Limit external operations<br>• to what has been explicitly authorised by the occupant, for example, with a time delay,<br>• to what has been designed inside the gateway. |
| Inadvertent network management operations should not be possible | A tool should be required – physical or software or the following access code:<br>• simple code, 4 digit;<br>• longer code,<br>(simple and longer code could be used for closed medium but they are insufficient for open medium, since code is transmitted);<br>• encryption and/or authentication. |
| Verify identity of the target product and verify identity of the "downloader" | For example, "certified piece of software" |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# Annex A
(informative)

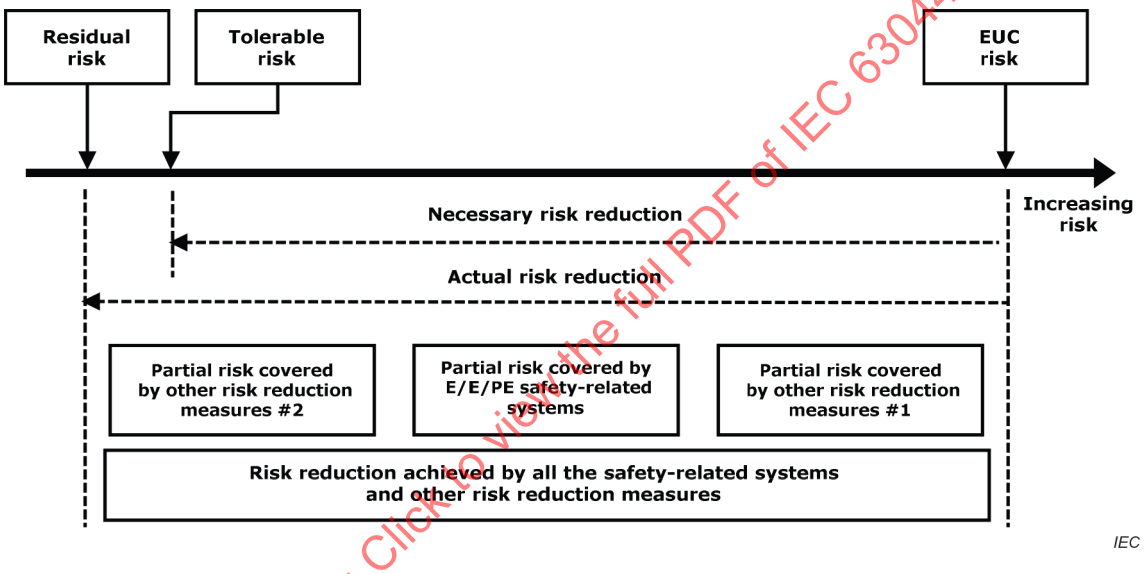
# Example of a method for the determination of safety integrity levels

## A.1 General

This method will enable a description of the tolerable risk for:

- the electrical/electronic/programmable electronic (E/E/PE) safety-related systems,
- other technology safety-related systems,
- external risk reduction facilities to be determined.

Figure A.1 shows the general concept of risk reduction.




[Source: IEC 61508-5:2010, Figure A.1]

**Figure A.1 – Risk reduction – General concept**

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## A.2 As low as reasonably practicable (ALARP) and tolerable risk concepts

Annex B of IEC 61508-5:2010 shall apply. Some of the information stated in Annex B of IEC 61508-5:2010 is repeated in this Annex A, in excerpts.

Table A.1 is an example that shows the dependence of risk probabilities (frequencies), consequences and risk classes, and Table A.2 shows the interpretation of the risk classes using the concept of ALARP.

**Table A.1 – Example of risk classification of accidents**

| Frequency | Consequence | | | |
|---|---|---|---|---|
| | **Catastrophic** | **Critical** | **Marginal** | **Negligible** |
| Frequent | Class I | Class I | Class I | Class II |
| Probable | Class I | Class I | Class II | Class III |
| Occasional | Class I | Class II | Class III | Class III |
| Remote | Class II | Class III | Class III | Class IV |
| Improbable | Class III | Class III | Class IV | Class IV |
| Incredible | Class IV | Class IV | Class IV | Class IV |
| The actual population with risk classes I, II, III and IV will be sector-dependent and will also depend upon what the actual frequencies are for frequent, probable, etc. Therefore, this Table A.1 should be seen as an example of how such a table could be populated, rather than as a specification for future use. | | | | |

**Table A.2 – Interpretation of risk classes**

| Risk class | Interpretation |
|---|---|
| Class I | Intolerable risk |
| Class II | Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained |
| Class III | Tolerable risk if the cost of risk reduction would exceed the improvement gained |
| Class IV | Negligible risk |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# Annex B
(informative)

## Hazards and development of necessary functional safety requirements

This Annex B shows in Table B.1 the development from the hazardous events, mentioned in 4.2.4, and responsible sub-events to the necessary risk reduction measures. Clause 5 contains requirements derived from this analysis.

As a result of following those requirements, the remaining risk is tolerable (risk class III) or negligible (risk class IV).

Product standards include requirements and measures to ensure that a tolerable risk level is reached.

**Table B.1 – Requirements and/or risk reduction measures**

| | Hazardous events<br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| 1 | **Power failure** | 1-1 Bus-power cut off | Bus only | Product shall save all status information relevant for avoiding the risk in the event of return of power and/or shall switch to the safe state of the system/product if necessary. |
| | | 1-2 Bus-power drop out | | |
| | | 1-3 Return of bus supply | | See 1-1. |
| | | 1-4 230 V mains cut off bus supply | | See 1-1.<br>• PSU shall buffer up to 80 ms<br>(PSU – power supply unit) |
| | | 1-5 230 V mains drop out bus supply | e.g. 80 ms | |
| | | 1-6 Auxiliary power cut off product supply | | See 1-1.<br>• Bus product shall save all status information relevant for avoiding the risk in case of return of power and/or shall provide solutions to switch to a local safe state of the system/product if necessary – this is application dependant. |
| | | 1-7 Auxiliary power drop out product supply | | |
| | | 1-8 Return of mains supply only | | See 1-1. |
| | | 1-9 Return of bus and mains supply | | See 1-1. |
| 2 | **Short circuit of bus line** | 2-1 Full short circuit | Products with 230 V and/or auxiliary power supply can no longer be controlled via bus, although powered | See 1-1.<br>• Bus circuit shall be protected against over-current in accordance with IEC 63044-3. |
| | | 2-2 Incomplete short circuit | Parts of the bus line may be still in function;<br>no indication with PSU | See 12 for devices without communication.<br>See 1-1 for products without bus power supply. |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br><br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| | | 2-3 Excessive current on the bus | Bus product stops communicating<br><br>power cut off by protection product | See 12.<br>• alternative: PSU switches off and/or provides an indication<br>• alternative installation measure: segmentation in independent lines and PSUs and keep failure local |
| 3 | **Overvoltage on the bus** | 3-1 No influence | | Covered by requirements of IEC 63044-3.<br>• Electrostatic and inductive charging:<br>– SELV-bus line with protective impedance to ground for temporary overvoltage;<br>– permanent hazardous overvoltage not likely because of SELV.<br>• Break down of insulation:<br>– insulation of HBES/BACS and HBES/BACS products to other circuits with a rated insulation voltage ≥ 250 V respectively. Rated insulation voltage ≥ 80 V AC PELV/SELV according to IEC 63044-3:2017, Table 1;<br>– RCD (on the mains side) protection optional. |
| | | 3-2 Automatic reset | | Optional, no requirement |
| | | 3-3 Manual reset | | Optional, no requirement |
| | | 3-4 Product defect | | Even if an HBES/BACS product were connected to 230 V the product shall not cause harm (not likely because of distinctive connector for SELV).<br><br>NOTE This includes the fail safe mode |
| 4 | **Overvoltage on the mains** | 4-1 No influence on PSU | | Mains 230/400 V:<br><br>Products shall meet requirements of IEC 63044-3.<br><br>Test voltage for solid insulation or encapsulated components for isolation between mains and HBES/BACS, 4 kV AC (tests according to IEC 60664-1:2020) |
| | | 4-2 PSU automatic reset | | Optional, no requirement |
| | | 4-3 PSU manual reset | | Optional, no requirement |
| | | 4-4 PSU defect | | The PSU shall not cause fire or explosion.<br><br>NOTE This includes the fail safe mode |
| 5 | **Insulation damage** | 5-1 Short circuit | | It shall be provided:<br>• Mains: overcurrent protection according to IEC 60364 (all parts)<br>• Bus: current limitation (see IEC 63044-3) |
| | (Temperature, surge, mechanical) | 5-2 Carrying hazardous voltage | | It shall be kept:<br>• for products and cables for mains the installation rule according to IEC 60364 (all parts),<br>• for products and cables of busses the requirements for SELV. |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br><br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| | | 5-3 Accessible live parts | | See IEC 63044-3.<br>Product committees shall specify mechanical stress withstand according to application environment and may add extra external protection if needed. |
| 6 | **Wrong connection** | 6-1 on the bus side | Wrong polarisation | • Construction and design shall support the avoidance of wrong connections |
| | | | | • Marking and description shall support the avoidance of wrong connection |
| | | | | • A product incorrectly connected to the bus shall not work |
| | | | | • The product shall not cause fire or explosion or impair electrical safety |
| | | 6-2 on the mains side | Connection of the bus terminal to mains | See 3-4 and 6-1<br>• Mains and bus connectors shall not be interchangeable. |
| | | | | • Construction and design shall support the avoidance of wrong connections. |
| | | | | • Marking and description shall support the avoidance of wrong connection. |
| | | | | • The product shall not cause fire or explosion or impair electrical safety. |
| | | 6-3 Connection of products with different physical layers / bus systems within the SELV range | | • Construction and design shall support the avoidance of wrong connections.<br>• Marking and description shall support the avoidance of wrong connection.<br>• The product shall not cause fire or explosion or impair electrical safety when supplied to DC 50 V. |
| 7 | **Over temperature** | 7-1 Malfunction | | Product shall work properly in the specified temperature range |
| | | 7-2 Environment | | Control of subsystem which is capable of (environment and/or surface temperature) > 60 °C:<br>• the product is designed for higher environmental temperature<br>• in case of a bus failure the sub-system should be switched to safe state (which may include manual control) |
| 8 | **Fire** | | | Product standards shall specify requirements for fire resistance. |
| 9 | **Mechanical shock, vibration** | | | • HBES products are to comply with their corresponding product standards.<br>• Additional application-dependant requirements may be added by product committees. |
| 10 | **Corrosion** | | | Product standards shall specify relevant requirements. |
| 11 | **EMC** | | | During the EMC tests of IEC 63044-5 (all parts):<br>• identification of disturbed messages shall be ensured,<br>• wrong but formally correct messages shall not be generated. |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br><br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| 12 | **Disturbed communication** | 12-1 Signal disturbed | | • Identification of disturbed messages shall be ensured.<br>• Hamming distance, medium-dependent repetition rate.<br>• The required Hamming distance shall be higher than 2. |
| | | | | • Receiving of proper messages shall be ensured also in the case of collisions (collisions avoidance, collisions detection, repetition, acknowledgement, etc.). |
| | | 12-2 Bus participant missing | For example, storm sensor | Permanent/cyclic transmitters shall be managed.<br>Safe operation shall be independent of other products. |
| 13 | **Pollution** | | | Comply with IEC 63044 |
| 14 | **End of life time of a component / product** | General | | Product committees shall give requirements for minimum lifetime (reliability, cycle tests, etc.), and/or instructions for maintenance rules if advised.<br>For example, date of production |
| | | 14-1 Heat or burn | Unwanted operation | See 7 and 8. |
| | | 14-2 Fail leading to no functionality | No or unwanted operation | See 12-2. |
| | | 14-3 Connection loose or contact corrosion | No or unwanted operation or heat or burn | See 10, 12 and 7. |
| | | 14-4 Loss or change of memory | No operation or wrong communication | See 16. |
| | | 14-5 Loss of communication | Failure of communication | See 12. |
| | | 14-6 Internal loss of power supply | No operation | See 12-2. |
| | | 14-7 Hardware failure on local control function | No external operation | Covered,<br>no additional risk |
| | | 14-8 Hardware failure affecting communication part | | See 12. |
| | | 14-9 Firmware failure | | See 16. |
| | | 14-10 Short circuit on the bus | | See 2. |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br><br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| 15 | **Reasonably foreseeable misuse**<br><br>Data protection and security is not considered under this item | 15-1 Download of wrong software | Switch software in thermostat | Avoid wrong download, for example:<br>• by the tool,<br>• by identification of the product and product capabilities in network management,<br>• by password,<br>• by training of the operator. |
| | | 15-2 Wrong configuration or parameters | | • Application dependant, parameter limits shall be set by the product committees<br>• Limited configuration possibilities for the end user<br>• Configuration access by use of a means accessible only to skilled persons<br>• Consistency check for example by the tool, by the configuration means<br>• Consistency check done by the installer |
| | | 15-3 Incomplete configuration | Product missing | See 12.<br><br>In addition, configuration means shall indicate incomplete configuration during configuration time. |
| | | 15-4 Misuse of variable types/commands, etc. | | • Configuration access by use of a means accessible only to skilled persons<br>• Interworking rules checked by configuration means<br>• Conformity to the interworking rules for HBES/BACS products/systems/applications |
| 16 | **Software failure** | 16-1 Software bugs | | Development process covered by ISO 9000 or similar |
| | | 16-2 Memory failure | | Regularly check of memory integrity and take appropriate measures. |
| 17 | **Overload** | 17-1 Bus traffic overload | Delay in signalling | • Permanent/cyclic transmitters shall be managed.<br>• The optimum/maximum traffic load per medium shall be regarded.<br>• Optimisation of bus traffic by application design |
| | | | Lost messages | • Protocol manages message losses (e.g. retransmission)<br>• Status indication |
| 18 | **Reliability** | | | This is no hazard, only a measure of frequency. |
| 19 | **Breakdown of material** (mechanically) | 19-1 Failure due to ageing | Accessible live parts | Electrical safety relevant:<br>• Product standards or generic IEC 63044-3;<br>• Check that the instructions include rules for proper mounting. |
| | | 19-2 Inappropriate for application | Accessible live parts | |
| | | 19-3 Wrong mounting | Accessible live parts | |
| | | 19-4 Wrong type of material | Accessible live parts | |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br><br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| 20 | **Inappropriate design / construction** | 20-1 Lifetime considerably reduced | | See 14 |
| | | 20-2 Fire emission / explosion due to overload | | To be covered adequately by product standards |
| | | 20-3 Overheating due to overload | | |
| | | 20-4 Break of connection wires | | |
| | | 20-5 Mechanical blocking of switching mechanism due to deformation of housing | | |
| | | 20-6 Mechanical blocking due to corrosion | | |
| | | 20-7 Injury/harm caused by housing edges | | |
| | | 20-8 Exposure of hazardous live parts | | |
| | | 20-9 Malfunction due to overload | | |
| | | 20-10 Malfunction due to insufficient EMC | | |
| 21 | **Switching of damaged equipment and subsystems** | 21-1 Housing broken | • Fire emission, explosion<br>• No arc extinction<br>• Short circuit<br>• Exposure of live parts | Functional safety has to be taken into account by the equipment standard itself. |
| | | 21-2 Blocked mechanics | • No function<br>• Overload leading to further damage | |
| | | 21-3 Broken terminal or wire with electrical contact causing arc | | |
| | | 21-4 Damaged electronic circuits | • No function<br>• Malfunction<br>• Short circuit leading to over-heating | |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| 22a | **Remote control inside one room** | | | No additional hazards |
| 22b | **Remote control from in house** | 22b-1 Rotating machine starts | Motion not controlled by the operator | • No function<br>• Appliance standards<br>• External measure, e.g. manual emergency button<br>• Local means |
| | | 22b-2 Heating product heats up, and heater has flammable surroundings | | • External measure, e.g. bimetal<br>• Remote control enabled if authorised before or by any means<br>• Authentication of person<br>• Local means/measure |
| | | 22b-3 Equipment function is stopped | Running process becomes uncontrolled | Disable remote stop during running process or external measure |
| | | 22b-4 Remote control of mains socket outlets | For example, a lamp | Label for remote controlled socked outlets |
| | | 22b-5 Remote reconfiguration | | Only possible inside buildings |
| 22c | **Remote control from outside** | 22c-1 Rotating machine starts | Motion not controlled by the operator | • External measure, e.g. manual emergency button<br>• Local means<br>• Authentication of person |
| | | 22c-2 Heating product heats-up, in case of flammable surroundings of the heater | | • External measure, e.g. bimetal<br>• Remote control enabled if authorised before or by any means<br>• Authentication of person |
| | | 22c-3 Equipment function is stopped | Running process becomes uncontrolled | • Disable remote stop during running process or external measure<br>• Authentication of person |
| | | 22c-4 Remote control of mains socket outlets | Lamp | • Label for remote controlled socket outlets<br>• Authorised person |
| | | 22c-5 Remote reconfiguration | | Authentication of person |
| 23 | **Command from two sources to one product (actuator)** | 23-1 Uncoordinated multiple access | | Configuration solutions e.g.:<br>• sources with hierarchy only: check of source address<br>• first in – first out |
| | | 23-2 Injection of a command into a sequence | Unexpected results | • Secure the products.<br>• Product/function locking/disabling/priority<br>• Variable sharing<br>• Secure the process by encapsulation not allowing injection |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Hazardous events<br><br>4.2.4 | Sub-events | Details | Requirements / risk reduction measures according to Clause 5 |
|---|---|---|---|---|
| 24 | **System failures** | 24-1 System does not react | No function | Reset and go to a defined state |
| | | 24-2 Damaged message | EMC | See 12. |
| | | 24-3 Wrong message | Very unlikely, could initiate wrong action | See 12. |
| | | 24-4 Unintended modification of bus products | Wrong configuration or parameters<br><br>Self-configuration | See 15-4.<br><br>Manufacturer ID access authorisation or authentication for configuration software |
| | | 24.5 System busy | No function | See 17. |

This document contains no requirements related to risks numbered 4, 5, 8, 10, 13, 18, 19, 20, 21, which are to be considered in other standards.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# Annex C
(informative)

# Some examples of non-safety-related HBES/BACS applications

## C.1 General

The following examples are taken from various fields, and describe potential issues and ways to solve them. They may be used by product committees as an inspiration source for their own domain. They have neither been checked nor approved by the relevant product committees, which may well have different recommendations for their specific products.

## C.2 Examples of non-safety-related HBES/BACS applications

### C.2.1 Example 1: Oven

Comment: Can an oven or cooking range be switched on from a distant point, via the HBES/BACS?

Response: Yes, if "distant" is within the same kitchen.

Comment: What if "distant" is on the other side of the apartment and somebody has put something flammable in the oven in the meantime? What if distant means over the phone? Shouldn't this be forbidden?

Response: Time-switching of ovens has been available for years; there is no difference between a clock on the oven and a distant order.

Comment: The decision about activating the clock is a conscious action which is carried out manually while standing next to the oven.

Response: Then a "remote switch-on enable" button on the oven would be a solution: it would have to be set before the oven can be switched-on from a distance. You do not need this button to be set in advance to switch the device off from a distance. The oven would still need to comply with all the intrinsic safety standards that apply to traditional ovens.

Comment: This does not solve the problem for the cooking range as there is no door to control access.

Response: Remote control of a cooking range should be limited to a few metres, and within the same room.

It may be necessary to allow only one binding for the device for control (as opposed to monitoring). If only one binding for control is allowed, it is easier to ensure that it has been done properly and with full knowledge during the installation and commissioning phase. More bindings may be allowed for monitoring (for example to show usage or measure energy consumption).

### C.2.2 Example 2: Devices presenting a high potential risk of hazard

Some devices may be recognised by their manufacturer as presenting a particularly high risk of hazard. These devices usually require the presence of a local operator.

Comment: Can we only allow the switching on of such devices from a point that is visible from the device?

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

Response: Yes, if this is the product committee requirement.

Comment: Does this prevent the integration of HBES/BACS access into such products?

Response: Not necessarily: An infrared HBES/BACS access requires the presence of the operator within visible distance of the device, and can therefore be used within the requirement to be in sight of the device.

Comment: A gateway between another medium and this infrared may allow the operation by a distant operator.

Response: Commands transmitted over a gateway from another medium to infrared should then be recognised as "non-locally-originated" (or should not be transmitted at all) to avoid problems.

### C.2.3 Example 3: Mains plugs, socket outlets and circuits

Mains plugs operated via an HBES/BACS, mains socket outlets operated via an HBES/BACS and mains circuits operated via an HBES/BACS in the distribution board are:

- useful, because they allow connection of traditional devices to "HBES mains plugs" or "HBES mains socket outlets" or "HBES mains circuits", since one of the brown and white goods manufacturers will be able to offer a full range of HBES/BACS products in the first phase,
- potentially dangerous, because they allow connection of any type of devices. These devices can therefore be activated with functions that are a priori unknown to the plug (or socket outlet or mains circuit) manufacturer or installer.

Installation rules already allow socket outlets that are controlled by remote switches usually located in the same room. "Add-ons" for socket outlets that are time-switches or controlled remotely (via power lines or radio frequency) are also available in "Do It Yourself" shops. This kind of device generates the same kind of safety hazards as HBES/BACS-operated plugs or socket outlets.

The general answer is that the installer and the user are responsible. A possible idea would be to impose a configuration and commissioning tool that clearly separates the different mains circuits (lighting, heating, etc.). Another alternative would be a new plug and socket outlet standard for remotely controlled appliances. This socket outlet would not accept traditional plugs; the new plug would fit both old and new sockets. The new plug would then be fitted only to appliances which are safe to control remotely and these could be plugged into the old or new sockets depending on whether the user wants local or remote control.

### C.2.4 Example 4: Water temperature adjustment

Comment: What mechanisms might be appropriate to allow the installer to set the upper limit on installation but prevent the user from subsequently changing that upper limit? For example, might a special tool be needed to set a temperature above 60 °C? In the absence of an adjustment by the installer, what should the default value for the upper temperature limit be?

Response: It is generally understood that the maximum temperature of a domestic hot water storage cylinder should be limited (to about 60 °C) to avoid the risk of accidental scalding. Clearly the user of the system may wish to set a lower set-point if they consider this appropriate and that set-point should therefore be user-accessible. The heater unit might include software or hardware provision to prevent the user setting a temperature above 60 °C. This might be inappropriate in cases when (a) the heater also has industrial uses requiring a higher set-point, or (b) the particular installation has other mechanisms to prevent scalding, such as thermostatic mixers on all taps and shower-heads.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# Bibliography

IEC 60364 (all parts), *Low-voltage electrical installations*

IEC 60664-1:2020, *Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests*

IEC 60950-1, *Information technology equipment – Safety – Part 1: General requirements*

IEC 61000-1-2, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC/TR 61000-2-1, *Electromagnetic compatibility (EMC) – Part 2: Environment – Section 1: Description of the environment – Electromagnetic environment for low-frequency conducted disturbances and signalling in public power supply systems*

IEC 61000-6-1, *Electromagnetic compatibility (EMC) – Part 6-1: Generic standards – Immunity standard for residential, commercial and light-industrial environments*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments*

IEC 61000-6-3, *Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for equipment in residential environments*

IEC 61000-6-4, *Electromagnetic compatibility (EMC) – Part 6-4: Generic standards – Emission standard for industrial environments*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC TR 63044-2, *Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 2: Environmental conditions*[1]

IEC Guide 104, *The preparation of safety publications and the use of basic safety publications and group safety publications*

IEC Guide 110, *Home control systems – Guidelines relating to safety*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

ISO 9000, *Quality management systems – Fundamentals and vocabulary*

EN 41003, *Particular safety requirements for equipment to be connected to telecommunication networks and/or a cable distribution system*

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

---

[1] Under preparation. Stage at the time of publication: IEC CDTR 63044-2:2021.

# SOMMAIRE



IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# SYSTÈMES ÉLECTRONIQUES POUR LES FOYERS DOMESTIQUES ET LES BÂTIMENTS (HBES) ET SYSTÈMES DE GESTION TECHNIQUE DU BÂTIMENT (SGTB) –

## Partie 4: Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les HBES et SGTB

## AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

IEC 63044-4 a été établie par le comité d'études 23 de l'IEC: Appareils électriques. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

| FDIS | Rapport de vote |
|---|---|
| 23/973/FDIS | 23/975/RVD |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 63044, publiées sous le titre général *Systèmes Électroniques pour les Foyers Domestiques et les Bâtiments (HBES) et Systèmes de Gestion Technique du Bâtiment (SGTB)*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# INTRODUCTION

La sécurité fonctionnelle comprend le fonctionnement en toute sécurité des dispositifs et des appareils ("produits") lorsqu'ils sont installés sur des réseaux de communications dans les foyers domestiques ou les bâtiments ("locaux").

Le présent document spécifie les procédures d'installation, de commande, de fonctionnement et de mode de défaillance pour améliorer la sécurité fonctionnelle des dispositifs installés dans les foyers domestiques et les bâtiments. Un dispositif fonctionne en toute sécurité s'il ne provoque aucun dommage au moment du fonctionnement et de la réalisation d'une tâche prévue. Les dispositifs de ce type peuvent ne pas fonctionner en toute sécurité en raison de l'installation ou des problèmes de commande.

L'usage croissant des réseaux domestiques et du bâtiment pour interconnecter les dispositifs entraîne des défis supplémentaires pour le maintien de la sécurité fonctionnelle en raison des interactions possibles avec les dispositifs. Le présent document traite donc des risques liés à la connexion de dispositifs à un réseau domestique ou de bâtiment, assurant ainsi des échanges de données et la commande à distance depuis l'intérieur du foyer domestique ou du bâtiment.

En outre, si le réseau domestique ou du bâtiment est connecté à un réseau public, la commande depuis des emplacements distants peut être possible. Les messages de commande de ce type peuvent provenir d'une application pour mobile multifonction, être envoyés par l'intermédiaire d'un réseau de téléphonie mobile, acheminés vers une passerelle du bâtiment et envoyés par l'intermédiaire d'un réseau domestique ou du bâtiment vers une interface de communication de dispositif. Il existe ainsi de nombreux risques de compromettre les messages de ce type. L'accès à distance constitue des menaces supplémentaires pour la sécurité fonctionnelle qui sont traitées dans le présent document.

Le présent document fait partie de la série IEC 63044 et s'applique aux systèmes électroniques pour les foyers domestiques et les bâtiments (HBES/SGTB).

Le présent document s'applique aux systèmes électroniques pour les foyers domestiques et les bâtiments (HBES/SGTB) en général, et plus particulièrement aux systèmes conformes à la famille des normes ISO/IEC relatives au système électronique pour les foyers domestiques (HES).

Les produits HBES/SGTB du présent document sont destinés aux systèmes non relatifs à la sécurité.

Le présent document a pour objet de spécifier, dans toute la mesure du possible, toutes les exigences de sécurité des produits HBES/SGTB dans leur cycle de vie.

Le présent document spécifie les exigences générales de sécurité fonctionnelle des dispositifs connectés à un réseau domestique ou du bâtiment qui suivent les principes de la norme fondamentale IEC 61508 relative à la sécurité fonctionnelle (toutes les parties). Il couvre les problèmes de sécurité fonctionnelle relatifs aux dispositifs et à leurs installations. Les exigences reposent sur une analyse du risque conformément à l'IEC 61508.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# SYSTÈMES ÉLECTRONIQUES POUR LES FOYERS DOMESTIQUES ET LES BÂTIMENTS (HBES) ET SYSTÈMES DE GESTION TECHNIQUE DU BÂTIMENT (SGTB) –

## Partie 4: Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les HBES et SGTB

## 1 Domaine d'application

La présente partie de l'IEC 63044 spécifie les exigences de sécurité fonctionnelle pour HBES/SGTB.

De plus, elle spécifie des exigences de sécurité fonctionnelle relatives à l'interface des équipements destinés à être connectés à un réseau HBES/SGTB. Elle ne s'applique pas aux interfaces avec d'autres réseaux.

NOTE 1 Un réseau ICT (*information and communication technology* - technologie de l'information et de la communication) dédié traité par l'IEC 62949 constitue un exemple d'autre réseau.

Le présent document ne spécifie pas d'exigences de sécurité fonctionnelle des systèmes relatifs à la sécurité.

NOTE 2 Des exemples d'applications HBES/SGTB non relatives à la sécurité sont donnés à l'Annexe C.

Le présent document ne spécifie pas d'exigences relatives à la protection et la sécurité des données.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## 2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60364 (toutes les parties), *Installations électriques à basse-tension*

IEC 63044-3:2017, *Systèmes Électroniques pour les Foyers Domestiques et les Bâtiments (HBES) et Systèmes de Gestion Technique du Bâtiment (SGTB) – Partie 3: Exigences de sécurité électrique*

IEC 63044-5 (toutes les parties), *Systèmes Électroniques pour les Foyers Domestiques et les Bâtiments (HBES) et Systèmes de Gestion Technique du Bâtiment (SGTB)*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité*

IEC 61709:2017, *Composants électriques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles de contraintes pour la conversion*

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

**3.1**
**authentification**
moyen de certifier que l'entité qui envoie un message est celle qu'elle prétend être, et confirmation que le message est identique à celui qui a été envoyé

**3.2**
**autorisation**
mécanisme qui permet d'assurer que l'entité ou la personne qui accède aux informations, aux fonctions ou aux services soit autorisée à le faire

**3.3**
**communication perturbée**
communication dans laquelle, pour une certaine raison, un message communiqué est incomplet, tronqué, contient des erreurs ou, malgré l'exactitude de son format, délivre des informations hors de la plage de paramètres prévus pour ce type de message

**3.4**
**sécurité fonctionnelle**
absence de risque inacceptable de dommage dû au fonctionnement d'un HBES/SGTB, y compris les risques qui découlent:

1) du fonctionnement normal,
2) d'un mauvais usage raisonnablement prévisible,
3) d'une défaillance,
4) de perturbations temporaires

Sous-ensemble de la sécurité globale se rapportant à un "Équipement commandé" (EUC, voir 3.17), et à son système de commande qui dépend du fonctionnement correct des systèmes électriques/électroniques/électroniques programmables (E/E/PE) relatifs à la sécurité et des dispositifs externes de réduction de risque

Note 1 à l'article: Les définitions de "sécurité fonctionnelle" de l'IEC/TR 61000-2-1 et de l'IEC 61000-1-2 sont prises en compte.

[SOURCE: IEC 61508-4:2010, définition 3.1.12 modifiée – par l'ajout de l'introduction et des points 1 à 4 de liste, du texte entre crochets et de la note.]

**3.5**
**distance de Hamming**
nombre minimal de bits dans lequel deux codes binaires diffèrent

**3.6**
**dommage**
blessure physique ou atteinte à la santé des personnes, soit directement, soit indirectement, en raison d'une atteinte aux biens ou à l'environnement

[SOURCE: IEC 61508-4:2010, définition 3.1.1 modifiée – par l'ajout de "soit directement soit indirectement".]

**3.7**
**danger**
source potentielle de dommage

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

Note 1 à l'article: Ce terme comprend le danger sur des personnes qui survient dans un laps de temps très court (par exemple, feu et explosion), mais aussi le danger à long terme sur la santé d'une personne (par exemple, dégagement d'une substance toxique).

[SOURCE: IEC 61508-4:2010, définition 3.1.2]

**3.8**
**événement dangereux**
situation qui conduit à un dommage sur le fonctionnement normal ou une condition anormale

Note 1 à l'article: Le fait qu'un événement dangereux conduise ou non à un dommage dépend de l'éventualité que des personnes, des biens ou l'environnement soient exposés aux conséquences de l'événement dangereux et, dans le cas de dommage aux personnes, que les personnes exposées puissent éviter les conséquences de l'événement après son occurrence.

Note 2 à l'article: Adaptée de l'IEC 61508-4:2010, définition 3.1.4.

**3.9**
**produit**
dispositif sous la forme d'un matériel, d'un micrologiciel, de ses logiciels associés et des outils de configuration

**3.10**
**documentation du produit**
document de référence du fabricant relatif à l'installation et au fonctionnement (catalogue, prospectus et autres informations imprimées ou électroniques relatives au produit, par exemple)

**3.11**
**système relatif à la sécurité**
système désigné qui, à la fois,

– met en œuvre les fonctions de sécurité requises pour atteindre ou maintenir un état de sécurité de l'EUC et
– est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/PE relatifs à la sécurité, et à d'autres dispositifs de réduction de risques relatifs à la technologie, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises

Note 1 à l'article: Ce terme fait référence aux systèmes désignés comme systèmes relatifs à la sécurité qui, avec les dispositifs externes de réduction de risque, sont destinés à réaliser la réduction de risque nécessaire, afin de satisfaire au niveau de risque tolérable requis. Voir également l'Annexe A de l'IEC 61508-5.

Note 2 à l'article: Les systèmes relatifs à la sécurité sont conçus pour empêcher l'EUC d'entrer dans un état dangereux en prenant les mesures appropriées de détection d'une condition susceptible d'occasionner un événement dangereux. La défaillance d'un système relatif à la sécurité serait incluse dans les événements à l'origine du ou des dangers déterminés. Bien qu'il puisse exister d'autres systèmes possédant des fonctions de sécurité, ce sont les systèmes relatifs à la sécurité qui ont été choisis pour obtenir à leur façon le niveau de risque tolérable requis. Les systèmes relatifs à la sécurité peuvent globalement être répartis en systèmes relatifs à la sécurité de commande et en systèmes relatifs à la sécurité de protection.

Note 3 à l'article: Les systèmes relatifs à la sécurité peuvent faire partie intégrante du système de commande de l'EUC ou peuvent être interfacés avec l'EUC par l'intermédiaire de capteurs et/ou d'actionneurs. Cela signifie qu'il est possible d'atteindre le niveau d'intégrité de sécurité requis en mettant en œuvre les fonctions de sécurité dans le système de commande de l'EUC (et éventuellement également par l'adjonction de systèmes séparés et indépendants) ou que ces fonctions de sécurité peuvent être exécutées par des systèmes séparés et indépendants dédiés à la sécurité.

Note 4 à l'article: Un système relatif à la sécurité peut:

a) être conçu pour prévenir un événement dangereux (c'est-à-dire qu'aucun événement dangereux ne survient tant que les systèmes relatifs à la sécurité exécutent leurs fonctions de sécurité);
b) être conçu pour réduire les effets de l'événement préjudiciable, réduisant ainsi le risque en limitant les conséquences de ce risque;
c) être conçu pour réaliser une combinaison de a) et de b).

Note 5 à l'article: Une personne peut faire partie d'un système relatif à la sécurité. Par exemple, une personne peut recevoir des informations d'un dispositif électronique programmable et exécuter une activité de sécurité à partir de cette information, ou exécuter une activité de sécurité par l'intermédiaire d'un dispositif électronique programmable.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

Note 6 à l'article: Un système relatif à la sécurité recouvre l'ensemble des matériels, logiciels, ainsi que tous les équipements annexes (par exemple, alimentation) nécessaires pour exécuter la fonction de sécurité spécifiée (les capteurs, les autres dispositifs d'entrée, les éléments terminaux (actionneurs) ainsi que les autres dispositifs de sortie sont par conséquent compris dans le système relatif à la sécurité).

Note 7 à l'article: Un système relatif à la sécurité peut être basé sur une large gamme de technologies, comprenant les technologies électrique, électronique, électronique programmable, hydraulique et pneumatique.

[SOURCE: IEC 61508-4:2010, définition 3.4.1, modifiée – "aux dispositifs externes de réduction de risque" a été remplacé par "à d'autres dispositifs de réduction de risques relatifs à la technologie".]

**3.12**
**intégrité de sécurité**
probabilité pour qu'un système relatif à la sécurité maintienne de manière satisfaisante les fonctions de sécurité exigées dans toutes les conditions énoncées et dans une période de temps spécifiée

Note 1 à l'article: Plus le niveau d'intégrité de sécurité d'un système relatif à la sécurité est élevé, plus la probabilité d'une défaillance du système dans l'exécution des fonctions de sécurité spécifiées ou dans l'adoption d'un état spécifié lorsque requis est faible.

Note 2 à l'article: Il existe quatre niveaux d'intégrité de sécurité (voir 3.5.8 de l'IEC 61508-4:2010).

Note 3 à l'article: Il convient que l'évaluation de l'intégrité de sécurité prenne en compte toutes les causes de défaillance (à la fois les défaillances aléatoires du matériel et les défaillances systématiques) conduisant à un état de non-sécurité, par exemple les défaillances de matériel, les défaillances induites du logiciel et les défaillances dues aux perturbations électriques. Certaines de ces défaillances, en particulier les défaillances aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance en mode de défaillance dangereux ou la probabilité de non-fonctionnement en cas de sollicitation d'un système de protection relatif à la sécurité. Cependant, l'intégrité de sécurité dépend également de plusieurs facteurs qui ne peuvent être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif.

Note 4 à l'article: L'intégrité de sécurité comprend l'intégrité de sécurité du matériel ainsi que l'intégrité de sécurité systématique.

Note 5 à l'article: Cette définition est centrée sur la fiabilité des systèmes relatifs à la sécurité dans l'exécution des fonctions de sécurité (voir l'IEV 192-01-24 pour une définition de la fiabilité).

[SOURCE: IEC 61508-4:2010, 3.5.4, modifiée – "E/E/PE" est supprimé de la définition, le terme "exécute" a été remplacé par "maintienne", "spécifiées" a été remplacé par "exigées", et "de l'IEC 61508-4:2010" a été ajouté à Note 2.]

**3.13**
**niveau d'intégrité de sécurité**
**SIL**
niveau discret (parmi quatre possibles) correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité et le niveau 1 possède le plus bas

Note 1 à l'article: Les objectifs chiffrés de défaillance (voir 3.5.17) pour les quatre niveaux d'intégrité de sécurité sont indiqués dans les Tableaux 2 et 3 de l'IEC 61508-1:2010.

Note 2 à l'article: Les niveaux d'intégrité de sécurité sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à attribuer aux systèmes E/E/PE relatifs à la sécurité.

Note 3 à l'article: Un niveau d'intégrité de sécurité (SIL) ne constitue pas une propriété d'un système, sous-système, élément ou composant. L'interprétation correcte de l'expression "Système relatif à la sécurité à SIL $n$" (où $n$ is 1, 2, 3 ou 4) signifie que le système est potentiellement capable de prendre en charge les fonctions de sécurité avec un niveau d'intégrité de sécurité jusqu'à $n$.

Note 4 à l'article: L'abréviation "SIL" est dérivée du terme anglais développé correspondant "safety integrity level"

[SOURCE: IEC 61508-4:2010, définition 3.5.8, modifiée – la date a été ajoutée à l'IEC 61508-1.]

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

**3.14**
**risque**
combinaison de la probabilité d'un dommage et de sa gravité

Note 1 à l'article: Pour plus d'information sur ce concept, voir Annexe A de l'IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, définition 3.1.6, modifiée – la date a été ajoutée à l'IEC 61508-1.]

**3.15**
**mauvais usage raisonnablement prévisible**
utilisation d'un produit, procédé ou service dans des conditions ou à des fins non prévues par le fournisseur, mais qui peut provenir d'un comportement humain envisageable

[SOURCE: IEC 61508-4:2010, définition 3.1.14]

**3.16**
**fonction de sécurité**
fonction à réaliser par un système E/E/PE relatif à la sécurité ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'EUC par rapport à un événement dangereux spécifique

EXEMPLE Des exemples de fonctions de sécurité comprennent:

– les fonctions devant être réalisées en tant qu'actions positives pour éviter des situations dangereuses (par exemple, arrêt d'un moteur) et

– les fonctions de prévention de réalisation d'actions (par exemple, empêcher le démarrage d'un moteur).

[SOURCE: IEC 61508-4:2010, définition 3.5.1]

**3.17**
**EUC**
**équipement commandé**
équipement, machine, appareil ou installation utilisés pour les activités de fabrication, de traitement, de transport, médicales ou d'autres activités

Note 1 à l'article: Le système de commande de l'EUC est séparé et distinct de l'EUC.

Note 2 à l'article: L'abréviation "EUC" est dérivée du terme anglais développé correspondant "equipment under control"

[SOURCE: IEC 61508-4:2010, définition 3.2.1]

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## 4 Exigences générales

### 4.1 Généralités

La sécurité fonctionnelle d'un système s'appuie autant sur les performances du réseau que sur celles des produits HBES/SGTB connectés:

1) la défaillance de l'un des réseaux ou de toute autre partie des HBES/SGTB ne doit pas compromettre la sécurité du système, des produits ou de l'équipement commandé;
2) pendant le fonctionnement, les produits HBES/SGTB individuels ne doivent pas seulement s'appuyer sur le système pour fonctionner en toute sécurité;
3) pendant le fonctionnement, l'interaction du système d'un ou de plusieurs produits avec un ou plusieurs autres produits ne doit pas compromettre la sécurité de fonctionnement du système.

### 4.2 Méthode d'établissement des exigences

#### 4.2.1 Généralités

Pour la spécification des exigences de sécurité fonctionnelle, le cycle de vie utilisé dans l'IEC 61508 (toutes les parties) doit être suivi pour:

1) la phase de conception des produits;
2) l'environnement d'application;
3) l'identification des dangers et des événements dangereux;
4) l'analyse des dangers et des risques, les dispositifs externes de réduction de risque;
5) la réalisation des dispositifs externes de réduction de risque;
6) la validation;
7) la maintenance;
8) l'installation et la mise en service;
9) la mise hors service.

Les comités d'études des produits et/ou les développeurs doivent prendre en compte les exigences du présent document dans les exigences de sécurité du produit, mais il n'est pas nécessaire d'entrer dans le processus de la série IEC 61508 lui-même.

#### 4.2.2 Environnement d'application HBES/SGTB

L'environnement d'application HBES/SGTB est pris en compte.

#### 4.2.3 Sources de dangers

Les sources de dangers suivantes ont été prises en considération:

1) matériau et construction;
2) fiabilité;
3) fonctionnement normal;
4) interaction involontaire avec d'autres produits;
5) interaction avec d'autres produits HBES/SGTB;
6) conditions anormales;
7) mauvais usage prévisible, y compris le téléchargement de code non autorisé et malveillant;

NOTE Cela comprend les modifications logicielles involontaires.

8) durée de vie;
9) environnement.
10) Installation et maintenance

#### 4.2.4 Événements dangereux

Ce qui suit est une liste non exhaustive des événements dangereux qui ont été pris en compte pour l'analyse: (le bus et l'alimentation secteur (230 V/400 V) ont été pris en considération):

1) défaillance d'alimentation;
2) surtension sur la ligne bus;
3) mauvaise connexion;
4) surchauffe;
5) incendie;

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

6) chocs mécaniques, vibrations;
7) corrosion;
8) perturbation électromagnétique;
9) pollution;
10) fin de vie d'un composant/produit;
11) mauvais usage raisonnablement prévisible;
12) défaillance du logiciel;
13) surcharge;
14) commutation des équipements et sous-systèmes endommagés;
15) commande à distance;
16) commande entre deux sources et un produit (actionneur, par exemple);

D'autres événements dangereux peuvent être pris en considération. Par exemple: court-circuit sur la ligne bus, corrosion, rupture du matériau…

### 4.2.5 Déduction des exigences

L'analyse du risque a été réalisée pour chacun des événements dangereux (voir 4.2.4). L'Annexe B comprend un exemple d'analyse du risque et les mesures de sécurité fonctionnelle correspondantes.

Dans tous les cas, si les classes de risques évaluées indiquent un risque inacceptable, des dispositifs externes de réduction de risque sont exigés, ainsi que les effets sur la réduction du niveau de risque et sa validation. Certains dispositifs externes de réduction de risque sont proposés et les éléments en général couverts par la norme de produit correspondante sont également indiqués. Si les fabricants ont pour objectif de développer des produits/systèmes HBES/SGTB qui présentent des événements dangereux non couverts par 4.2.4, l'analyse du risque doit être réalisée conformément à l'IEC 61508 (toutes les parties).

## 5 Exigences en matière de sécurité fonctionnelle

### 5.1 Généralités

L'analyse conformément à l'IEC 61508 (toutes les parties) indique que la sécurité fonctionnelle dépend autant de la conception et de la fabrication des produits que de l'utilisation appropriée des produits dans les installations.

Les paragraphes 5.2 à 5.6 contiennent des exigences relatives aux produits HBES/SGTB et à la mise à disposition des informations nécessaires à l'installation, au fonctionnement et à la maintenance corrects de ces produits.

Les exigences de conformité sont données pour les produits selon le cas, et la vérification de la disposition des informations nécessaires.

Tous les essais de produits référencés sont des essais de type.

Le fondement et les raisons des exigences suivantes sont présentés à l'Annexe B.

NOTE Les événements dangereux répertoriés au 4.2.4 sont cités en référence avec leur numéro entre parenthèses, par exemple (1), (2) …

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## 5.2 Alimentation en énergie

**5.2.1** En cas de défaillance d'alimentation, les produits doivent redémarrer en toute sécurité lorsque l'alimentation est rétablie. (1)

NOTE Un redémarrage sûr peut être assuré

- en stockant les informations d'état et en utilisant ces informations pour reconstruire la fonctionnalité après la mise sous tension,
- en passant à un état défini du produit qui dépend de l'application,
- en calculant l'état sûr en fonction des informations disponibles qui proviennent du système (d'un contrôleur, le cas échéant, et/ou de chaque produit),
- en maintenant une réserve de puissance suffisante (en prévoyant un temps de réserve approprié dans le produit et/ou le bloc d'alimentation) afin de permettre aux produits connectés de passer à un état sûr.

**5.2.2** Le marquage et les instructions des produits doivent être conçus pour empêcher tout risque de mauvaise connexion. (2) (3)

Les produits doivent être marqués de manière lisible et durable.

Il est recommandé que l'étiquetage soit indépendant de la langue.

La vérification doit être effectuée par examen de la documentation du produit et, le cas échéant, selon l'essai des marquages lisibles et durables présenté dans la norme de produit appropriée.

**5.2.3** Des dispositions doivent être prévues en matière de construction et de conception pour empêcher les mauvaises connexions. Cela peut être assuré par un regroupement approprié des connexions. (3)

La vérification doit être effectuée par examen du produit.

## 5.3 Durée de vie

Les produits doivent être conçus pour une durée de vie utile définie conformément à l'IEC 61709:2017 ou en soumettant à l'essai le produit selon l'essai d'endurance normalisé correspondant du produit dans les conditions normales.

La fiche technique doit donner des instructions de maintenance, si une maintenance est exigée pour atteindre la durée de vie spécifiée. (10)

La vérification doit être effectuée par examen de la documentation.

## 5.4 Mauvais usage raisonnablement prévisible

**5.4.1** Le risque de téléchargement accidentel du mauvais logiciel d'application ou des mauvais paramètres dans les produits doit être réduit le plus possible. (11)

NOTE Les mesures suivantes peuvent être utilisées:

- conception de l'outil de configuration;
- identification des produits et comparaison de leurs profils par la gestion du réseau;
- par mot de passe;
- authentification;
- documentation du produit;
- formation des installateurs/opérateurs.

La vérification doit être effectuée par examen de la documentation du produit.

**5.4.2** La configuration correcte et les paramètres associés doivent être assurés. (11)

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

NOTE Les mesures suivantes peuvent s'appliquer:

– spécification des plages de paramètres;
– possibilités de configuration limitées pour l'utilisateur final;
– accès à la configuration uniquement pour les personnes qualifiées;
– contrôle de cohérence par des outils ou par l'installateur;
– vérification de la conformité à la configuration.

La vérification doit être effectuée par vérification de la conformité des éléments existants avec la configuration (prévue) planifiée.

**5.4.3** Des mesures doivent être prévues pour détecter et/ou indiquer des produits manquants ou configurés de manière incomplète pendant le processus de configuration. (11)

NOTE Les mesures suivantes peuvent s'appliquer:

– conception de l'outil de configuration;
– procédures formelles d'installation.

La vérification doit être effectuée en soumettant le produit à l'essai ou par examen de la documentation du produit.

## 5.5 Logiciel et communication

NOTE Les exigences logicielles et de communication du présent paragraphe ne sont pas destinées à couvrir la protection des données et la cybersécurité.

**5.5.1** Le processus de développement de logiciel doit comprendre une procédure appropriée de prise en charge du bon fonctionnement de ce logiciel. (12)

La vérification doit être effectuée par examen de la documentation du processus ou des certificats correspondants.

**5.5.2** Des mesures doivent être prévues pour vérifier le bon fonctionnement du logiciel de produit et l'intégrité de la configuration. Si un fonctionnement anormal est détecté, le produit doit rétablir les valeurs correctes ou doit passer à un état défini. (12)

La vérification doit être effectuée par examen de la documentation sur la conception du logiciel.

**5.5.3** Si l'application l'exige, des mesures doivent être prévues à l'intérieur des produits pour limiter le volume de trafic imposé sur le moyen de communication. (13)

Les mesures suivantes peuvent s'appliquer:

– limitation de la transmission cyclique;
– limitation du nombre de messages par unité de temps et par produit;
– limitation des cycles d'interrogation.

La vérification doit être effectuée par examen de la documentation du produit et, dans la mesure du possible, en soumettant le produit à l'essai.

**5.5.4** La réception de messages qui proviennent de plusieurs sources ne doit pas gêner le bon fonctionnement du produit et ne doit pas provoquer de dangers. (16)

NOTE Les mesures suivantes peuvent s'appliquer:

– vérifier l'adresse source en présence d'une hiérarchie de sources;
– appliquer la règle: premier entré, premier sorti;
– appliquer la règle: le dernier message l'emporte;
– sécuriser le processus par finalisation avant que de nouveaux messages puissent modifier le comportement;
– sécuriser le processus en l'arrêtant, puis en le redémarrant;

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

– sécuriser le processus en le désactivant et en l'activant.

La vérification doit être effectuée par examen de la documentation du produit et, dans la mesure du possible, en soumettant le produit à l'essai.

**5.5.5** Les produits doivent réagir à une réinitialisation du système (le cas échéant) en passant à un état défini.

La vérification doit être effectuée par examen de la documentation du produit et, dans la mesure du possible, en soumettant le produit à l'essai.

**5.5.6** Il doit être possible de limiter l'accès à la configuration manuelle des paramètres du système.

NOTE Les mesures ou exceptions suivantes peuvent s'appliquer sauf si la configuration manuelle est explicitement détaillée dans son manuel d'instructions (également le cas pour la configuration automatique).

– utiliser un outil (matériel ou logiciel);
– utiliser un mot de passe et/ou une authentification;
– assurer qu'un accès non autorisé ne soit pas possible;
– combinaison ou suite d'actions;
– moyens dissimulés de configuration;

La vérification doit être effectuée par examen de la documentation du produit et, dans la mesure du possible, en soumettant le produit à l'essai.

**5.5.7** Le fonctionnement sûr d'un produit doit être indépendant du fonctionnement des autres produits dans le système ou l'application.

NOTE Les mesures suivantes peuvent s'appliquer:

– transmission cyclique;
– vérification de plage des variables reçues.

La vérification doit être effectuée par examen des résultats des essais de CEM du produit.

**5.5.8** Des mesures d'identification des messages perturbés doivent être prévues. Si des messages perturbés sont détectés, des mesures doivent être prises pour assurer un fonctionnement sûr. (8)

L'intégrité des données doit être maintenue avec des méthodes appropriées de détection et de correction des erreurs.

NOTE Les mesures suivantes peuvent s'appliquer:

– le message peut être rejeté ou corrigé par le produit destinataire;
– le message peut être répété par l'émetteur.

La vérification doit être effectuée par examen des résultats d'essai du produit ou de la documentation du produit.

**5.5.9** Des mesures doivent être prévues pour permettre de signaler les pertes de message ou de répéter des messages en cas de perte de message. (13)

NOTE Les mesures suivantes peuvent s'appliquer:

– mécanismes d'acquittement de communication ou un mécanisme d'acquittement d'application;
– indication ou effets visibles de l'état après action;
– répétition systématique appropriée dans le cas des produits unidirectionnels.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

La vérification doit être effectuée par examen des résultats d'essai du produit ou de la documentation du produit.

### 5.6 Opérations à distance

NOTE Les exigences d'opération à distance du présent paragraphe 5.6 ne sont pas destinées à couvrir la protection des données et la cybersécurité.

#### 5.6.1 Recommandations générales

La commande à distance à l'intérieur d'une pièce est couverte par les précédentes exigences, énoncées au 5.5.

Le fonctionnement sûr des produits (socles de prise de courant, par exemple) sous commande à distance doit être garanti par les exigences du produit et de l'installation. Aucune exigence système spécifique ne s'applique.

#### 5.6.2 À l'intérieur d'un seul bâtiment ou dans son voisinage immédiat

Les produits ou le sous-système connecté au produit qui peuvent être à l'origine d'un dommage et qui sont destinés à la commande à distance à l'intérieur d'un seul bâtiment ou dans son voisinage immédiat, doivent comprendre des dispositions relatives aux moyens locaux de fonctionnement ou d'activation/de désactivation du fonctionnement à distance.

NOTE Les mesures suivantes peuvent s'appliquer:

– moyens locaux de fonctionnement sur les produits potentiellement dangereux;
– moyens locaux de fonctionnement à côté des produits potentiellement dangereux;
– entrées de communication prenant en charge le fonctionnement local

La vérification doit être effectuée par examen du produit ou de la documentation du produit.

#### 5.6.3 Depuis l'extérieur du bâtiment

Les produits ou le sous-système connecté au produit qui peuvent être à l'origine d'un dommage et qui sont destinés à la commande à distance depuis l'extérieur du bâtiment doivent comprendre des dispositions relatives aux moyens locaux d'activation/de désactivation du fonctionnement à distance.

NOTE Les mesures suivantes peuvent s'appliquer:

– moyens locaux d'activation du fonctionnement sur les produits potentiellement dangereux;
– moyens locaux d'activation du fonctionnement à côté des produits potentiellement dangereux;
– entrées de communication prenant en charge l'activation locale du fonctionnement;
– moyens locaux de désactivation de la passerelle ou d'un produit d'accès à distance.

La vérification doit être effectuée par examen du produit ou de la documentation du produit.

**5.6.3.1** Un mécanisme doit être prévu pour l'autorisation ou l'authentification de la commande à distance depuis l'extérieur du bâtiment (voir également le Tableau 1). (15) Cela peut s'appliquer au niveau du système (pare-feu ou passerelle) ou du produit.

NOTE L'autorisation peut être:

– une autorisation ou authentification par mot de passe,
– un accès par l'intermédiaire d'une ligne dédiée.

La vérification doit être effectuée par examen du produit ou de la documentation du produit.

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

### 5.6.4 Gestion

**5.6.4.1** Le mécanisme doit être prévu pour l'autorisation ou l'authentification de la gestion à distance, y compris la configuration et le téléchargement depuis l'extérieur du bâtiment (voir également le Tableau 1). Cela peut s'appliquer au niveau du système (pare-feu ou passerelle) ou du produit. (15)

La vérification doit être effectuée par examen du produit ou de la documentation du produit.

**5.6.4.2** Des mesures qui visent à garantir la cohérence entre le réseau réel et son image à distance doivent être prévues. (15)

NOTE Les mesures suivantes peuvent s'appliquer:

– procédure qui vise à assurer une seule copie faisant foi de la base de données du système;

– mécanismes de validation de la base de données du système à distance par rapport au réseau réel;

– fonction d'autodocumentation dans le système (centralisée ou répartie).

La vérification doit être effectuée par examen du produit ou de la documentation du produit.

**Tableau 1 – Exigences qui permettent d'éviter des opérations involontaires et moyens possibles de les satisfaire**

| Exigences | Moyens de satisfaire aux exigences |
|---|---|
| Éviter le fonctionnement involontaire | Limiter les opérations externes<br>• à ce qui a été explicitement autorisé par l'occupant (avec un délai, par exemple),<br>• à ce qui a été conçu à l'intérieur de la passerelle. |
| Il convient que des opérations involontaires de gestion de réseau ne soient pas possibles | Il convient d'exiger un outil – physique, logiciel ou le code d'accès suivant:<br>• code simple, 4 chiffres;<br>• code plus long,<br>(un code simple et plus long peut être utilisé en milieu fermé, mais est insuffisant en milieu ouvert, étant donné que le code est transmis);<br>• chiffrement et/ou authentification. |
| Vérifier l'identité du produit cible + vérifier l'identité du "téléchargeur" | par exemple: "élément de logiciel certifié" |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# Annexe A
(Informative)

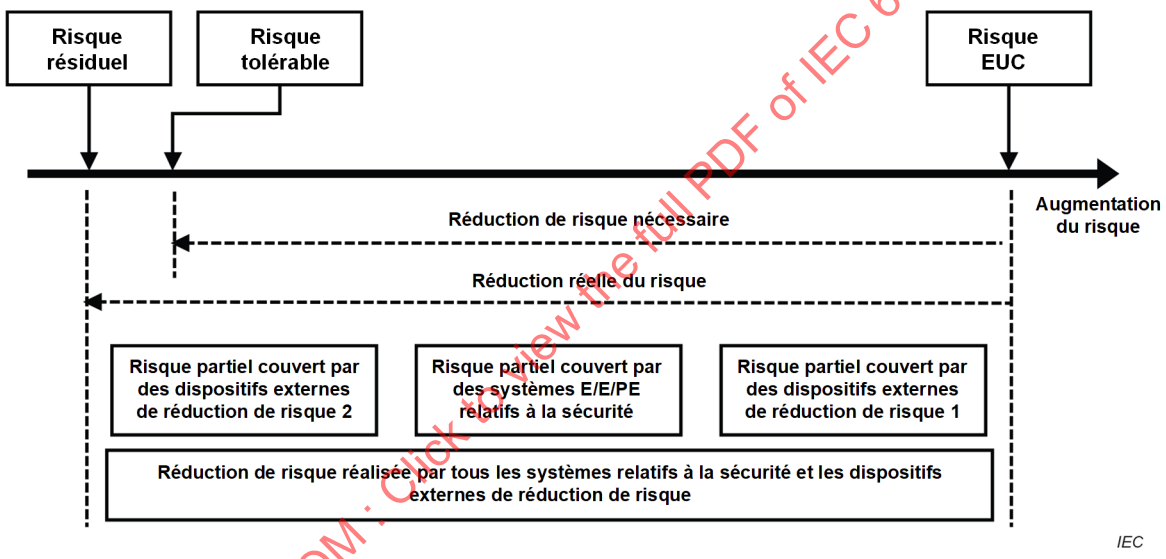
# Exemple de méthode de détermination des niveaux d'intégrité de sécurité

## A.1 Généralités

Cette méthode permet de décrire le risque tolérable pour:

- les systèmes électriques/électroniques/électroniques programmables (E/E/PE) relatifs à la sécurité,
- d'autres technologies de systèmes relatifs à la sécurité,
- les installations externes de réduction du risque à déterminer.

La Figure A.1 représente le concept général de réduction du risque.




[Source: IEC 61508-5:2010, Figure A.1]

**Figure A.1 – Réduction du risque – Concept général**

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

## A.2 Aussi faible que raisonnablement possible (ALARP) et concepts de risque tolérable

L'Annexe B de l'IEC 61508-5:2010 doit s'appliquer. Certaines informations données à l'Annexe B de l'IEC 61508-5:2010 sont répétées dans la présente annexe.

Le Tableau A.1 est un exemple qui présente la dépendance des probabilités de risque (fréquences), les conséquences et les classes de risque. Le Tableau A.2 présente l'interprétation des classes de risque à l'aide du concept d'ALARP (*as low as reasonably practicable*).

**Tableau A.1 – Exemple de classement des accidents en fonction des risques**

| Fréquence | Conséquence | | | |
|---|---|---|---|---|
| | **Catastrophique** | **Critique** | **Marginal** | **Négligeable** |
| Fréquent | Classe I | Classe I | Classe I | Classe II |
| Probable | Classe I | Classe I | Classe II | Classe III |
| Occasionnel | Classe I | Classe II | Classe III | Classe III |
| Peu fréquent | Classe II | Classe III | Classe III | Classe IV |
| Improbable | Classe III | Classe III | Classe IV | Classe IV |
| Non crédible | Classe IV | Classe IV | Classe IV | Classe IV |
| L'attribution réelle des classes de risque I, II, III et IV dépend du secteur d'application et également des fréquences réelles (fréquent, probable, etc.). En conséquence, il convient que le présent tableau soit perçu comme un exemple de la manière suivant laquelle un tel tableau peut être enrichi, plutôt que comme une spécification pour une utilisation future. | | | | |

**Tableau A.2 – Interprétation des classes de risque**

| Classe de risque | Interprétation |
|---|---|
| Classe I | Risque intolérable |
| Classe II | Risque indésirable, et tolérable uniquement s'il est impossible de le réduire ou si le coût de la réduction est disproportionné par rapport à l'amélioration apportée |
| Classe III | Risque tolérable si le coût de la réduction de risque est supérieur à l'amélioration apportée |
| Classe IV | Risque négligeable |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

# Annexe B
(informative)

## Dangers et développement des exigences de sécurité fonctionnelle nécessaires

La présente Annexe B présente dans le Tableau B.1 le développement des événements dangereux, mentionnés en 4.2.4, et des sous-événements responsables aux dispositifs externes de réduction de risque nécessaires. L'Article 5 contient les exigences déduites de cette analyse.

Par suite de la satisfaction à ces exigences, le risque restant est tolérable (classe de risque III) ou négligeable (classe de risque IV).

Les normes de produits comprennent des exigences et des mesures qui permettent d'atteindre des niveaux de risques tolérables.

**Tableau B.1 – Exigences et/ou dispositifs externes de réduction de risque**

| | Événements dangereux<br>4.2.4 | Sous-événements | Informations détaillées | Exigences/dispositifs externes de réduction de risque selon l'Article 5 |
|---|---|---|---|---|
| 1 | **Défaillance d'alimentation** | 1-1 Coupure d'alimentation du bus | Bus uniquement | Le produit doit conserver toutes les informations d'état qui permettent d'éviter le risque en cas de retour de puissance et/ou doit passer à l'état sûr du système/produit si cela est nécessaire. |
| | | 1-2 Perte de puissance du bus | | |
| | | 1-3 Retour de l'alimentation du bus | | Voir 1-1. |
| | | 1-4 L'alimentation secteur 230 V coupe l'alimentation du bus | | Voir 1-1.<br>• Le PSU doit mettre en mémoire tampon jusqu'à 80 ms<br>(PSU - *power supply unit*, bloc d'alimentation) |
| | | 1-5 L'alimentation secteur 230 V relâche l'alimentation du bus | par exemple, 80 ms | |
| | | 1-6 L'alimentation auxiliaire coupe l'alimentation du produit | | Voir 1-1.<br>• Le produit bus doit conserver toutes les informations d'état qui permettent d'éviter le risque en cas de retour de puissance et/ou doit apporter des solutions pour passer à un état sûr local du système/produit si cela est nécessaire (dépend de l'application). |
| | | 1-7 L'alimentation auxiliaire relâche l'alimentation du produit | | |
| | | 1-8 Retour de l'alimentation secteur uniquement | | Voir 1-1. |
| | | 1-9 Retour de l'alimentation du bus et de l'alimentation secteur | | Voir 1-1. |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021

| | Événements dangereux<br><br>4.2.4 | Sous-événements | Informations détaillées | Exigences/dispositifs externes de réduction de risque selon l'Article 5 |
|---|---|---|---|---|
| 2 | **Court-circuit de la ligne bus** | 2-1 Court-circuit complet | Les produits avec une alimentation de 230 V et/ou une source d'alimentation auxiliaire ne peuvent plus être commandés par l'intermédiaire du bus, même sous tension | Voir 1-1.<br>• Le circuit bus doit être protégé contre les surintensités conformément à l'IEC 63044-3. |
| | | 2-2 Court-circuit incomplet | Des parties de la ligne bus peuvent toujours être en fonction;<br><br>aucune indication avec le PSU | Voir 12 pour les dispositifs sans communication.<br><br>Voir 1-1 pour les produits sans alimentation électrique du bus. |
| | | 2-3 Courant excessif sur le bus | Le produit bus arrête de communiquer<br><br>coupure d'alimentation par le produit de protection | Voir 12.<br>• alternative: PSU procède à la mise hors tension et/ou donne une indication<br>• autre mesure d'installation: segmentation dans les lignes indépendantes et les PSU + maintien de défaillance locale |
| 3 | **Surtension sur le bus** | 3-1 Aucun impact | | Couvert par les exigences de l'IEC 63044-3.<br>• Charge électrostatique et inductive:<br>– Ligne bus TBTS avec impédance de protection à la terre pour les surtensions temporaires;<br>– surtension dangereuse permanente improbable en raison de TBTS.<br>• Coupure de l'isolement:<br>– isolement de HBES/SGTB et des produits HBES/SGTB par rapport à d'autres circuits avec une tension assignée d'isolement ≥ 250 V respectivement. Tension assignée d'isolement ≥ 80 V en courant alternatif TBTS/TBTP conformément à l'IEC 63044-3:2017, Tableau 1;<br>– Protection par dispositif à courant différentiel résiduel (côté alimentation secteur) facultative. |
| | | 3-2 Réinitialisation automatique | | Facultative, aucune exigence |
| | | 3-3 Réinitialisation manuelle | | Facultative, aucune exigence |
| | | 3-4 Défaut du produit | | Même si un produit HBES/SGTB est connecté à 230 V, il ne doit pas être à l'origine d'un dommage (improbable en raison du connecteur distinctif pour TBTS).<br><br>NOTE Cela comprend le mode de sécurité intégrée |

IECNORM.COM : Click to view the full PDF of IEC 63044-4:2021