

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Home and building electronic systems (HBES) and building automation and control systems (BACS) – (standards: itb-01)

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

IEC 63044-4:2021

<https://standards.iteh.ai/catalog/standards/sist/bcb1b260-e229-409e-be22->

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



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 Varembe
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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**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**

[IEC 63044-4:2021](#)

<https://standards.iteh.ai/catalog/standards/sist/bcb1b260-e229-409e-be22-63044-4/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**

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.**

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	6
3 Terms and definitions	6
4 General requirements	10
4.1 General.....	10
4.2 Method of establishment of the requirements	10
4.2.1 General	10
4.2.2 HBES/BACS application environment	11
4.2.3 Sources of hazards.....	11
4.2.4 Hazardous events.....	11
4.2.5 Derivation of requirements.....	11
5 Requirements for functional safety.....	12
5.1 General.....	12
5.2 Power feeding.....	12
5.3 Life time.....	13
5.4 Reasonably foreseeable misuse.....	13
5.5 Software and communication	13
5.6 Remote operations.....	15
5.6.1 General recommendations.....	15
5.6.2 Within a single building or in its immediate vicinity.....	15
5.6.3 From outside the building.....	15
5.6.4 Management.....	16
Annex A (informative) Example of a method for the determination of safety integrity levels.....	17
A.1 General.....	17
A.2 As low as reasonably practicable (ALARP) and tolerable risk concepts	17
Annex B (informative) Hazards and development of necessary functional safety requirements.....	19
Annex C (informative) Some examples of non-safety-related HBES/BACS applications	27
C.1 General.....	27
C.2 Examples of non-safety-related HBES/BACS applications.....	27
C.2.1 Example 1: Oven	27
C.2.2 Example 2: Devices presenting a high potential risk of hazard	27
C.2.3 Example 3: Mains plugs, socket outlets and circuits.....	28
C.2.4 Example 4: Water temperature adjustment	28
Bibliography.....	29
Figure A.1 – Risk reduction – General concept	17
Table 1 – Requirements for avoiding inadvertent operations and possible ways to achieve them	16
Table A.1 – Example of risk classification of accidents.....	18
Table A.2 – Interpretation of risk classes	18
Table B.1 – Requirements and/or risk reduction measures.....	19

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.

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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[IEC 63044-4:2021](https://standards.iteh.ai/catalog/standards/sist/bcb1b260-e229-409e-be22-f93ede1b2a77/iec-63044-4-2021)

<https://standards.iteh.ai/catalog/standards/sist/bcb1b260-e229-409e-be22-f93ede1b2a77/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.

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 (standards.iteh.ai)

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>

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

<https://standards.iteh.ai/catalog/standards/sist/bcb1b260-e229-409e-be22-f93ede1b2a77/iec-63044-4-2021>

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]

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.]

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 IEC 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]

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.

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.

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.

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.