IEC 63044-4

Edition 1.0 2021-06

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

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)

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 It also gives information on projects, replaced and withdrawn publications.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.

IEC 63044-4

Edition 1.0 2021-06

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

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

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.

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

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

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 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]

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.

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.

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.

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 • to what has been explicitly authorised by the occupant, for example, with a time delay, • 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: • simple code, 4 digit; • longer code, (simple and longer code could be used for closed medium but they are insufficient for open medium, since code is transmitted); • encryption and/or authentication.
Verify identity of the target product and verify identity of the "downloader"	For example, "certified piece of software"

Annex A
(informative)

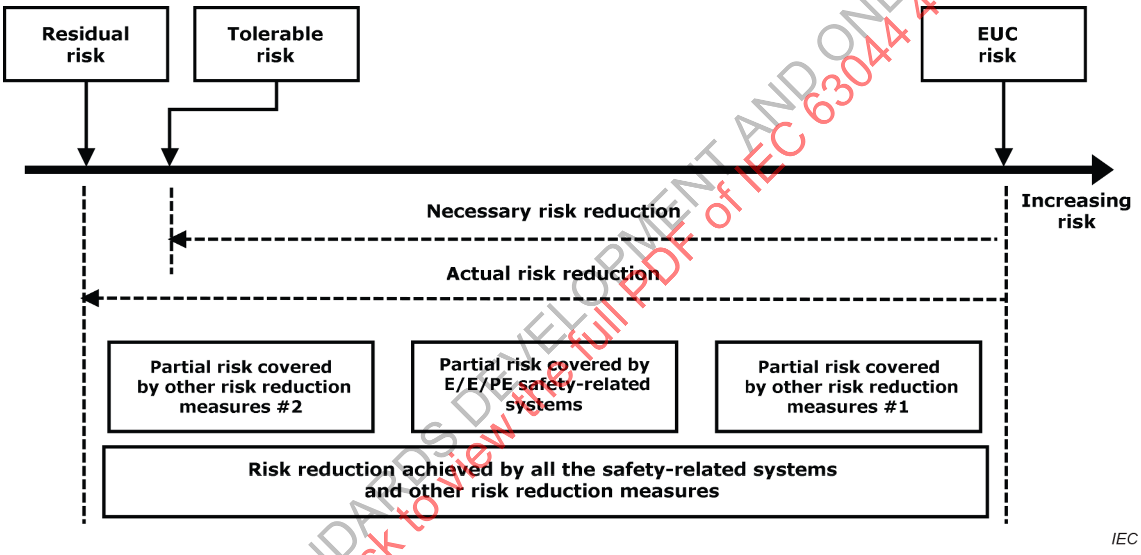
Example of a method for the determination of safety integrity levels

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.


Residual risk
Tolerable risk
EUC risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other risk reduction measures #2
Partial risk covered by E/E/PE safety-related systems
Partial risk covered by other risk reduction measures #1
Risk reduction achieved by all the safety-related systems and other risk reduction measures
IEC

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

Figure A.1 – Risk reduction – General concept

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

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 **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. • PSU shall buffer up to 80 ms (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. • 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. • 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; no indication with PSU	See 12 for devices without communication. See 1-1 for products without bus power supply.

	Hazardous events **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 power cut off by protection product	See 12. • alternative: PSU switches off and/or provides an indication • 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. • Electrostatic and inductive charging: – SELV-bus line with protective impedance to ground for temporary overvoltage; – permanent hazardous overvoltage not likely because of SELV. • Break down of insulation: – 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; – 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). NOTE This includes the fail safe mode
4	**Overvoltage on the mains**	4-1 No influence on PSU		Mains 230/400 V: Products shall meet requirements of IEC 63044-3. 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. NOTE This includes the fail safe mode
5	**Insulation damage**	5-1 Short circuit		It shall be provided: • Mains: overcurrent protection according to IEC 60364 (all parts) • Bus: current limitation (see IEC 63044-3)
	(Temperature, surge, mechanical)	5-2 Carrying hazardous voltage		It shall be kept: • for products and cables for mains the installation rule according to IEC 60364 (all parts), • for products and cables of busses the requirements for SELV.

	Hazardous events **4.2.4**	**Sub-events**	**Details**	**Requirements / risk reduction measures according to Clause 5**
		5-3 Accessible live parts		See IEC 63044-3. 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 • 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. • Marking and description shall support the avoidance of wrong connection. • 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: • the product is designed for higher environmental temperature • 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. • 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): • identification of disturbed messages shall be ensured, • wrong but formally correct messages shall not be generated.

	Hazardous events **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. • Hamming distance, medium-dependent repetition rate. • 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. 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. 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, 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.

	Hazardous events **4.2.4**	**Sub-events**	**Details**	**Requirements / risk reduction measures according to Clause 5**
15	**Reasonably foreseeable misuse** 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: • by the tool, • by identification of the product and product capabilities in network management, • by password, • by training of the operator.
		15-2 Wrong configuration or parameters		• Application dependant, parameter limits shall be set by the product committees • Limited configuration possibilities for the end user • Configuration access by use of a means accessible only to skilled persons • Consistency check for example by the tool, by the configuration means • Consistency check done by the installer
		15-3 Incomplete configuration	Product missing	See 12. 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 • Interworking rules checked by configuration means • 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. • The optimum/maximum traffic load per medium shall be regarded. • Optimisation of bus traffic by application design
			Lost messages	• Protocol manages message losses (e.g. retransmission) • 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: • Product standards or generic IEC 63044-3; • 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	