ISO/IEC 14762

Edition 1.0 2009-01

INTERNATIONAL STANDARD

Information technology – Functional safety requirements for home and building electronic systems (HBES)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

ISO/IEC 14762

Edition 1.0 2009-01

INTERNATIONAL STANDARD

Information technology – Functional safety requirements for home and building electronic systems (HBES)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE M

ICS 35.200

ISBN 978-2-88910-827-5

CONTENTS

INFORMATION TECHNOLOGY –
FUNCTIONAL SAFETY REQUIREMENTS FOR
HOME AND BUILDING ELECTRONIC SYSTEMS (HBES)

FOREWORD

1) ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

3) The formal decisions or agreements of IEC and ISO 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 and ISO member bodies.

4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

7) All users should ensure that they have the latest edition of this publication.

8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

9) 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.

10) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 14762 has been prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard cancels and replaces ISO/IEC TR 14762, published in 2001, and constitutes a technical revision.

The main changes with respect to the Technical Report are the following:

While the Technical Report lists reasons for harms and some possible counter measures this International Standard extends the list of hazards and specifies specific measures to counter them.

This International Standard applies to all physical media, however, additional aspects of wireless and powerline features covered in ISO/IEC 24767 are not repeated.

This standard has the status of a product family standard and may be used as a normative reference in a dedicated product standard for the safety of home and building electronic systems. It is not intended to be used as a stand-alone publication.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INTRODUCTION

Home and Building Electronic System (HBES) products integrated in a HBES should be safe for the use in intended applications.

This International Standard specifies the general functional safety requirements for HBES following the principles of the basic standard for functional safety, IEC 61508.

This International Standard identifies functional safety issues related to products and their installation. The requirements are based on a risk analysis in accordance with IEC 61508.

The intention of this International Standard is to allocate, as far as possible, all safety requirements for HBES products in their life cycle.

This International Standard only addresses HBES products.

This International Standard is addressed to committees that develop or modify HBES product/system standards, or, where no suitable HBES product standards addressing functional safety exist, to product manufacturers.

HBES and HES products in this International Standard are for non-safety related applications.

For related standards, see the IEC website.

INFORMATION TECHNOLOGY – FUNCTIONAL SAFETY REQUIREMENTS FOR HOME AND BUILDING ELECTRONIC SYSTEMS (HBES)

1 Scope

ISO/IEC 14762 sets the requirements for functional safety for Home and Building Electronic Systems (HBES) products and systems, a multi-application bus system where the functions are decentralised, distributed and linked through a common communication process. The requirements may also apply to the distributed functions of any equipment connected in a home or building control system if no specific functional safety standard exists for this equipment or system.

The functional safety requirements of this International Standard apply together with the relevant product standards for a device if any.

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

2 Normative references

The following referenced documents are indispensable for the application 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.

The provisions of the referenced specifications other than ISO/IEC, IEC, ISO and ITU documents, as identified in this clause, are valid within the context of this International Standard. The reference to such a specification within this International Standard does not give it any further status within ISO or IEC. In particular, it does not give the referenced specification the status of an International Standard.

ISO/IEC 14543-2-1, *Information technology – Home electronic systems (HES) architecture – Part 2-1: Introduction and device modularity*

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

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

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations; including its corrigendum 1 from April 1999*

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels; including its corrigendum 1 from April 1999*

IEC 61709:1996, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

ISO 9000 series, *Quality management systems*

EN 50090-2-2, *Home and Building Electronic Systems (HBES) – Part 2-2: System overview – General technical requirements*

3 Terms, definitions and abbreviations

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

3.1.1
architecture
specific configuration of hardware and software elements in a system

[IEC 61508-4, definition 3.3.5]

3.1.2
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

3.1.3
authorization
mechanism to ensure that the entity or person accessing information, functions or services has the authority to do so

3.1.4
disturbed communication
where 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

3.1.5
functional safety
freedom from unacceptable risk of harm due to the operation of an HBES, including that resulting from

a) normal operation,

b) reasonably foreseeable misuse,

c) failure,

d) temporary disturbances

NOTE 1 See definition 3.1.9 of IEC 61508-4. Part of the overall safety relating to the EUC (equipment under control) and the EUC control system which depends on the correct functioning of the electrical/electronic/ programmable electronic (E/E/PE) safety related systems, other technology safety related systems and external risk reduction facilities.

NOTE 2 Definition of IEC TR3 61000-2-1 and IEC TS 61000-1-2 are taken into account.

3.1.6
hamming distance
numbers of bits in which two binary codes differ

3.1.7
harm
physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment

[IEC 61508-4, definition 3.1.1]

3.1.8
hazard
potential source of harm

[ISO/IEC Guide 51, definition 3.5]

NOTE 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).

[IEC 61508-4, definition 3.1.2]

3.1.9
hazardous event
situation which results in harm on normal operation or abnormal condition

NOTE Definition of IEC 61508-4, 3.1.3 and 3.1.4; circumstance in which a person is exposed to hazard(s) which results in harm.

3.1.10
home and building electronic systems
HBES
multi-application bus system where the functions are decentrally distributed and linked through a common communication process

NOTE 1 HBES is used in homes and buildings including their surroundings. Functions of the system are for example switching, open loop controlling, closed loop controlling, monitoring and supervising.

NOTE 2 When an HBES is used in a home, it is often referred to as HES (home electronic system).

3.1.11
HBES product
devices such as hardware, firmware, their associated software and of configuration tools, intended to be used in an HBES

NOTE HBES products when used in a home are often referred to as HES products.

3.1.12
product
devices such as hardware, firmware, their associated software and configuration tools

3.1.13
product documentation
manufacturer's installation and operations' literature which accompanies the product;

the product information contained in the manufacturer's catalogue and other product marketing material-information;

the description, definitions, product literature and usage as presented in electronic format on the manufacturer's (or supplier's) website on the World Wide Web/Internet

3.1.14
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, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions

NOTE 1 The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the external risk reduction facilities (see IEC 61508-4,, definition 3.4.3), the necessary risk reduction in order to meet the required tolerable risk (see IEC 61508-4,, definition 3.1.6). See also Annex A of IEC 61508-5.

NOTE 2 The safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on receipt of commands. 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, and have two modes of operation (IEC 61508-4, definition 3.5.12).

NOTE 3 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 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 hazardous event arises),
b) be designed to mitigate the effects of the hazardous event, thereby reducing the risk by reducing the consequences,
c) be designed to achieve a combination of a) and b).

NOTE 5 A person can be part of a safety-related system (IEC 61508-4, definition 3.3.1). 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 The term 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 A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic technologies.

[IEC 61508-4, definition 3.4.1]

3.1.15
risk

combination of the probability of occurrence of harm and the severity of that harm

[ISO/IEC Guide 51, definition 3.2]
[IEC 61508-4, definition 3.1.5]

NOTE For risk classes, see Annex A.

3.1.16
reasonably foreseeable misuse

use of a product, process or service under conditions or for purposes not intended by the supplier, but which may happen, induced by the product, process or service in combination with, or as result of, common human behaviour

[IEC 61508-4, definition 3.1.11]

3.1.17
safety function

function to be implemented by an E/E/PE safety related system, other technology safety-related systems or external risk reduction facilities, which is intended to achieve and maintain a safe state for the EUC, in respect of a specific hazardous event (see IEC 61508-4, definition 3.1.4)

[IEC 61508-4, definition 3.5.1]

3.2 Abbreviations

ALARP	As Low As Reasonably Practicable
EUC	Equipment Under Control
HBES	Home and Building Electronic Systems
HES	Home Electronic Systems

4 Conformance

Development and deployment of a product that conforms to this standard shall be analysed for possible risks in accordance with Clause 5.

Products that conform to this standard shall meet the requirements specified in Clause 6.

5 General requirements

5.1 General

Functional safety of a system relies upon both the performance of the network and upon the performance of the connected HBES products.

a) Failure of either the network or any other part of HBES system shall not cause the system, the products or the controlled equipment to become unsafe.

b) Whilst in operation, individual HBES products shall not rely solely upon the system for their safe operation.

c) While in operation, the systems interaction of any product(s) with any other product(s) shall not result in unsafe operation of the system.

5.2 Method of establishment for the requirements

5.2.1 General

The functional safety requirements were specified according to the life-cycle used in ISO/IEC 61508-1:

a) concept phase of products;

b) application environment;

c) identification of hazards and hazard events;

d) hazard and risk analysis, risk reduction measures;

e) realization of risk reduction measures;

f) validation;

g) maintenance;

h) installation and commissioning;

i) decommissioning.

The product technical committees and/or developers shall take the requirements of this International Standard into account in the product safety requirements, but it is not necessary to go into the ISO/IC 61508-1 process itself.

5.2.2 HBES application environment

The HBES application environment is taken into account.

5.2.3 Sources of hazards

The following sources of hazards have been considered:

a) material and construction;

b) reliability;

c) normal operation;

d) unintentional interaction with other products;

e) interaction with other HBES products;

f) abnormal conditions;

g) foreseeable misuse, including the download of unauthorised and malicious code;

NOTE This includes unintentional software modifications.

h) life time;

i) environment.

5.2.4 Hazardous events

The following hazardous events have been taken into account for the analysis (the bus and mains have been considered):

(1) power failure;

(2) short circuit of bus line;

(3) overvoltage on the bus line;

(4) overvoltage on the mains;

(5) insulation damage (temperature, surge, mechanical);

(6) wrong connection;

(7) over temperature;

(8) fire;

(9) mechanical shock, vibration;

(10) corrosion;

(11) electromagnetic disturbance;

(12) disturbed communication;

(13) pollution;

(14) end of life time of a component/products;

(15) reasonably foreseeable misuse;

(16) software failure;

(17) overload;

(18) loss of reliability;

(19) breakdown of material (mechanically);

(20) inappropriate design/construction;

(21) switching of damaged equipment and subsystems;

(22) remote control;

(23) command from two sources to one product (e.g. actuator);

(24) system failures.

5.2.5 Derivation of requirements

The risk analysis has been carried out for each of the hazard events; see Annex B. The likelihood of the event has been estimated and the risk class has been taken into account according to the method of Annex A.

In all cases where the evaluated risk classes indicate an unacceptable risk, risk reduction measures are requested 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 products/systems which exhibit hazardous events not covered by 5.2.4 the risk analysis shall be carried out according to IEC 61508.

6 Requirements for functional safety

NOTE Reference to the hazardous events of 5.2.4 are given within brackets ( ).

6.1 General

Analysis according to ISO/IEC 61508-1 indicates that functional safety depends upon both the design and manufacture of products and upon the appropriate use of the products in installations.

Subclauses 6.2 to 6.7 contain requirements for HBES 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 of the following requirements are shown in the Annex B.

6.2 Power feeding

6.2.1 Safe restart after power is restored (1)

In case of power failure the products shall restart safely when power is restored.

Safe restart can be performed by

- storing the status information and usage the information for rebuilding the functionality after power on,
- switching to a defined state of the product depending on the application of the products,
- 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 assume a safe state.

6.2.2 Product marking and instructions prevent risk of wrong connections (3) (6)

Marking and instructions of the products shall be designed to prevent the risk of wrong connections.

Products shall be marked in a legible and durable manner.

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.

6.2.3 Product construction and design prevent wrong connections

The construction and design of a product shall prevent wrong connections.

This may be supported by appropriate grouping of connections. (6)

Compliance shall be checked by inspection of the product.

6.3 Environment

6.3.1 Product designed for application environment and specified temperature range (7)

Products shall be designed for the working temperature appropriate to their maximum rated voltages needed for the application environment and shall work properly in the specified temperature range.

Compliance shall be checked by testing the product according to the relevant product standard and if this does not exist to EN 50090-2-2 and the relevant basic safety standards.

6.3.2 Resistance to abnormal heat and prevention of fire propagation (8)

The products and components shall be designed for resistance to abnormal heat and shall not propagate fire.

Compliance shall be checked by testing the product according to the relevant product standard and if this does not exist to the relevant basic safety standards.

6.3.3 Withstand of mechanical stress appropriate to the application(s) (9)

The products shall be designed to withstand the mechanical stress appropriate to the application(s).

Compliance shall be checked by testing the product according to the relevant product standard and if this does not exist to EN 50090-2-2 and the relevant basic safety standards.

6.4 Lifetime

The products shall be designed for a defined useful lifetime according to 5.2 of IEC 61709:1996, and Annex A or defined number of switching cycles under normal condition.

The datasheet shall give instructions for maintenance if required to reach the specified lifetime. (14)

Compliance shall be checked by inspection of the documentation.

6.5 Reasonably foreseeable misuse

6.5.1 Minimization of accidental download of wrong application software or parameters (15)

The risk of accidental download of the wrong application software or parameters into the products shall be minimised.

The following measures may apply:

- 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 product test and/or inspection of the product documentation.

6.5.2 Proper configuration and related parameters (15)

Proper configuration and related parameters shall be ensured.

The following measures may apply:

- specification of parameter ranges;
- limited configuration possibilities for the end-user;
- access to configuration only for skilled persons (see ISO/IEC 14543-2-1);
- consistency check by tools or by the installer;
- check of conformity with configuration.

Compliance shall be checked by check of conformity of existing with planed (intended) configuration.

6.5.3 Detection and/or indication of missing or incompletely configured products during configuration process (15)

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

The following measures may apply:

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

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

6.6 Software and communication

6.6.1 Development process compliance with ISO 9000 or similar standards (16)

The software development process shall comply with ISO 9000 or similar standards.

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

6.6.2 Check for proper operation of product software and integrity of the configuration (16)

Measures shall be provided to check for 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.

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

6.6.3 Limitation of the traffic load imposed on the communication medium (12) (17)

Measures, if required by the application, shall be provided inside the products to limit the traffic load imposed on the communication medium.

The following measures may 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.

6.6.4 Proper function of product and exclusion of hazards on reception of messages from multiple sources (23)

The reception of messages from several sources shall not disturb the proper function of the product and shall not cause hazards.

The following measures may apply:

- check source address in case there is a hierarchy of the sources;
- apply the rule: first in, first out;
- apply the rule: last message wins;
- secure the process by finalising before new messages may 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.

6.6.5 Defined state after a system reset (if any) (24)

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.

6.6.6 Restricted access to manual configuration of system parameters (24)

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

The following measures or exceptions may apply:

- 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;
- except where manual configuration is explicitly detailed in its instruction manual (also the case for automatic configuration).

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

6.6.7 Disturbed communication

6.6.7.1 Safe operation of a product independent of operation of other products in the system or application (12)

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

The following measures may apply:

- cyclic transmission;
- range checking of received variables.

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

6.6.7.2 Identification of disturbed messages and measures to ensure safe operation (11) (12)

Measures for the identification of disturbed messages shall be provided. In case of detection of disturbed messages, measures shall be taken to ensure safe operation. The hamming distance shall be not lower than 2.

The following measures may 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.

6.6.7.3 Prevention of falsely triggered messages

Sending of wrong but formally correct messages shall be prevented.

Compliance is checked by the relevant EMC test of EN 50090-2-2. (11) (12)

6.6.7.4 Indication and repetition of lost messages (12) (17)

Measures to enable message losses to be indicated or to cause messages to be repeated in the event of loss shall be provided.

The following measures may apply:

- communication acknowledge mechanisms or an application acknowledge mechanism;
- feedback status indication or visible effects;
- appropriate systematic repeat in case of unidirectional products.

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

6.7 Remote operations

6.7.1 General recommendations

Remote control inside a room is covered by the previous requirements.

Socket outlets under remote control should be marked in such a way that they are visibly differentiated for the user, or they should be of specific construction to exclude the use of normal plugs designed for use in sockets not remotely controlled. (22)

6.7.2 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.

The following measures may apply:

- local means of operation on the potentially harmful products;
- local means of operation adjacent the potentially harmful products;
- communication inputs supporting local operation.

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

6.7.3 From outside the building

6.7.3.1 Provision for local means to explicitly enable the remote operation from outside the building

Products or a subsystem which may cause harm and are intended for remote control from outside the building shall have provision for local means to explicitly enable the remote operation.

The following measures may apply:

- local means of enabling operation on the potentially harmful products;
- local means of operation enabling adjacent 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.

6.7.3.2 Authorization or authentication of remote control from outside the building (22)

Mechanism shall be provided for the authorization or authentication of remote control from outside the building (see also Table 1). (22) This may apply at system (fire wall or gateway) or at product level.

Authorization may be

- password authorization or authentication,
- access through a dedicated line.

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

6.7.4 Management

6.7.4.1 Authorization or authentication of remote management including configuration and download from outside the building (22)

Mechanism shall be provided for the authorization 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. (22)

Authorization may be

- password authorization or authentication,
- access through a dedicated line.

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

6.7.4.2 Consistency between the actual network and its remote image (22)

Measures to guarantee consistency between the actual network and its remote image shall be provided. (22)

The following measures may 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 to achieve them
Avoid inadvertent operation	Limit external operations • to what has been explicitly authorised by the occupant, e.g. 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”	e.g. ”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 to describe 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, see IEC 61508-5, Figure A.1.

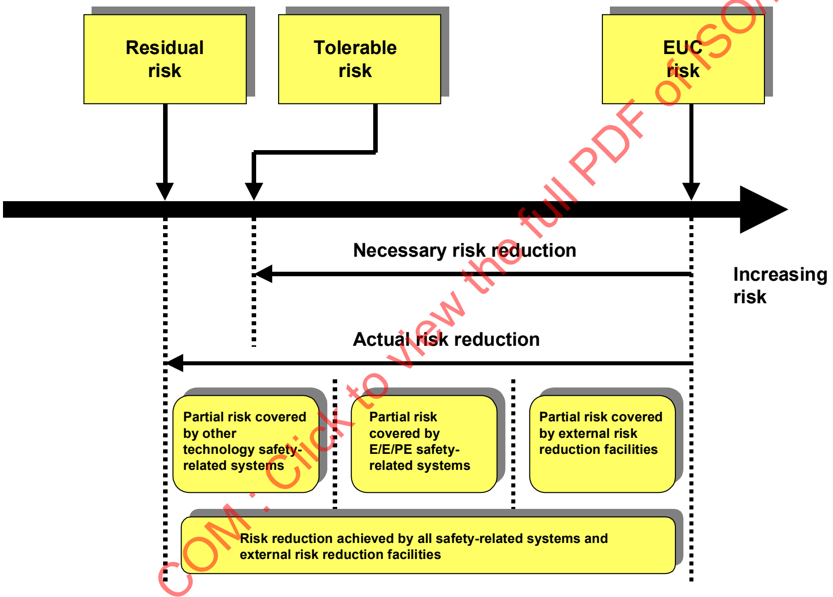
Residual risk
Tolerable risk
EUC risk
Necessary risk reduction
Increasing risk
Actual risk reduction
Partial risk covered by other technology safety-related systems
Partial risk covered by E/E/PE safety-related systems
Partial risk covered by external risk reduction facilities
Risk reduction achieved by all safety-related systems and external risk reduction facilities

Figure A.1 – Risk reduction – General concept

A.2 Terms and definitions

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

A.2.1
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

[IEC 61508-4, definition 3.5.2, modified]

A.2.2
safety integrity level

discrete level for (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

[IEC 61508-4, definition 3.5.6]

A.3 As low as reasonably practicable (ALARP) and tolerable risk concepts

Annex B of IEC 61508-5 applies. Some of the information stated in Annex B of IEC 61508-5 is repeated here for the convenience of the reader.

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

NOTE 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 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 the development from the hazardous events, mentioned in 5.2.4, and responsible sub-events to the necessary risk reduction measures. Clause 6 contains requirements derived from this analysis

The requirements shall be such that the remaining risk is tolerable (risk class III) or negligible (risk class IV).

Product standards shall include requirements and measures to reach tolerable risks as provided in Table B.1.

Table B.1 – Safety requirements and risk reduction

	Hazardous events 5.2.4	**Sub-events**	**Details**	**Requirements / risk reduction measures**
1	**Power failure**	1-1 Bus-power cut off	Bus only	Product shall save all status information relevant for avoiding the risk in case 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, see EN 50090-2-2.
		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
		2-3 Excessive current on the bus	Bus product stops communicating power cut off by protection product	See 12 • alternative: PSU (EN 50090-2-2) switches off and/or provides an indication • alternative installation measure: segmentation in independent lines and PSUs + keep failure local

	Hazardous events 5.2.4	**Sub-events**	**Details**	**Requirements / risk reduction measures**
3	**Overvoltage on the bus**	3-1 No influence		Covered by requirements of EN 50090-2-2. • 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 and HES products to other circuits with $U_R \geq 250$ V, respextively $U_R \geq 80$ V AC PELV/SELV, in accordance with EN 50090-2-2 - 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 a HBES product would be connected to 230 V the product shall not cause harm (not likely, because of distinctive connector for SELV)
4	**Overvoltage on the mains**	4-1 No influence on PSU		Mains: Products shall meet the requirements of IEC 60038 EN 50090-2-2 Test voltage for solid insulation or encapsulated components for isolation between mains and HBES, 4 kV AC (tests according to IEC 60664-1)
		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
5	**Insulation damage**	5-1 Short circuit		It shall be provided: • Mains: overcurrent protection acc to HD 384 • Bus: current limitation (see EN 50090-2-2)
	(temperature, surge, mechanical)	5-2 Carrying hazardous voltage		It shall be kept: • for products and cables for mains the installation rule accoording to IEC 60364 (HD 384) • for products and cables of busses the requirements for SELV
		5-3 Accessible live parts		See EN 50090-2-2 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 to avoid wrong connections • Marking and description shall support to avoid 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 to avoid wrong connections • Marking and description shall support to avoid wrong connection • The product shall not cause fire or explosion or impair el. safety
		6-3 Connection of products with different physical layers / bus systems wihting the SELV range		• Construction and design shall support to avoid wrong connections • Marking and description shall support to avoid wrong connections • The product shall not cause fire of explosion or impair electrical safety

	Hazardous events 5.2.4	**Sub-events**	**Details**	**Requirements / risk reduction measures**
7	**Over temperature**	7-1 Malfunction		Product shall properly work in the specified temperature range EN 50090-2-2
		7-2 Environment		Control of subsystem with 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 to comply with EN 50090-2-2 • 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 EN 50090-2-2 • identification of disturbed messages shall be ensured, • wrong but formally correct messages shall not be generated.
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 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 EN 50090-2-2
14	**End of life time of a component / product**	General		Product committees shall give requirements for minimum lifetime (reliability, cycles tests,…), 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 ➔ 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 5.2.4	Sub-events	Details	Requirements / risk reduction measures
15	**Reasonably foreseeable misuse** Sabotage is not a topic for the HBES product	15-1 Download of wrong software	Switch software in thermostat	Avoid wrong download, e.g.: • by the tool, • by identification of the product and products 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, e.g. by the tool, by the configuration means…. • Consistency check done by the installer
		15-3 Incomplete configuration	Product missing	See 12 + Configuration means shall indicate it during configuration time
		15-4 Misuse of variable types/commands,….		• 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 products/systems/applications
16	**Software failure**	16-1 Software bugs		Development process covered by the ISO 9000 series 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 EN 50090-2-2; • 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	

	Hazardous events 5.2.4	Sub-events	Details	Requirements / risk reduction measures
20	**Inappropriate design / construction**	20-1 Life time 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 Injure/harm 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 • No arc extinction • Short circuit • Exposure of live parts	Functional safety has to be taken into account by the equipment standard itself
		21-2 Blocked mechanics	• No function • Overload ➔further damage	
		21-3 Broken terminal or wire with electrical contact ➔ arc		
		21-4 Damaged electronic circuits	• No function • Mall-function • Short circuit ➔over-heating	
22a	**Remote control inside one room**			No additional hazards
22b	**Remote control within the house**	22b-1 Rotating machine starts	Motion not controlled by the operator	• No function • Appliance standards • External measure, e.g. manual emergency button • Local means
		22b-2 Heating product heats-up, in case of flammable surroundings of the heater		• External measure, e.g. bimetal • Remote control enabled if authorised before or by any means • Authentication of person • 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, Lamp	Label for remote controlled socked outlets
		22b-5 Remote reconfiguration		Only possible inside buildings