SLOVENSKI STANDARD

SIST EN 50090-2-3:2005

september 2005

Stanovanjski in stavbni elektronski sistemi (HBES) – 2-3. del: Sistemski pregled – Zahteve splošne funkcionalne varnosti za proizvode, ki so namenjeni za vgradnjo v HBES

Home and Building Electronic Systems (HBES) – Part 2-3: System overview – General functional safety requirements for products intended to be integrated in HBES

ICS 97.120

Referenčna številka
SIST EN 50090-2-3:2005(en)

EUROPEAN STANDARD **EN 50090-2-3**

NORME EUROPÉENNE

EUROPÄISCHE NORM February 2005

ICS 97.120

English version

Home and Building Electronic Systems (HBES) Part 2-3: System overview - General functional safety requirements for products intended to be integrated in HBES

Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) Partie 2-3: Vue d'ensemble du système - Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les systèmes HBES

Elektrische Systemtechnik für Heim und Gebäude (ESHG) Teil 2-3: Systemübersicht - Anforderungen an die funktionale Sicherheit für Produkte, die für den Einbau in ESHG vorgesehen sind

This European Standard was approved by CENELEC on 2004-09-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 50090-2-3:2005 E

Foreword

This European Standard has been prepared by the Technical Committee CENELEC TC 205, Home and Building Electronic Systems (HBES), joined by the co-operating partner Konnex Association.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50090-2-3 on 2004-09-01.

The following dates were fixed:

–	latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2005-09-01
–	latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2007-09-01

This European Standard shall be used as family standard; it is also addressed to Product Committees or, where no suitable product standards exist, to product manufacturer.

EN 50090-2-3 is part of the EN 50090 series of European Standards, which will comprise the following parts:

Part 1: Standardisation structure
Part 2: System overview
Part 3: Aspects of application
Part 4: Media independent layers
Part 5: Media and media dependent layers
Part 6: Interfaces
Part 7: System management
Part 8: Conformity
Part 9: Installation requirements
TRs: CENELEC TC 205 Technical Reports

Contents

Introduction **4**

1 Scope **4**

2 Normative references **4**

3 Definitions **5**

4 General requirements **7**

4.1 General 7

4.2 Method of establishment for the requirements 8

4.2.1 HBES application environment 8

4.2.2 Sources of hazards 8

4.2.3 Hazardous events 8

4.2.4 Derivation of requirements 9

5 Requirements for functional safety **9**

5.1 General 9

5.2 Power feeding 10

5.3 Environment 10

5.4 Life time 10

5.5 Reasonably foreseeable misuse 11

5.6 Software and communication 11

5.7 Remote operations 13

5.7.1 General recommendations 13

5.7.2 Within a single building or in its immediate vicinity 13

5.7.3 From outside the building 13

5.7.4 Management 14

Annex A (informative) **Example of a method for the determination of safety integrity levels** **15**

Annex B (informative) **Hazards and development of necessary Functional Safety Requirements** **17**

Annex C (informative) **Some examples of non safety related HBES applications** **23**

Bibliography **25**

Figure A.1 – Risk reduction: General concept 15

Table 1 – Requirements for avoiding inadvertent operations and possible ways to achieve them 14

Table A.1 – Example of risk classification of accidents 16

Table A.2 – Interpretation of risk classes 16

Introduction

HBES products integrated in a HBES should be safe for the use in intended applications.

This European Standard specifies the general functional safety requirements for HBES following the principles of the basic standard for functional safety EN 61508 and Technical Report R205-012 in particular.

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

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

This European Standard only addresses HBES products.
This European Standard is addressed to committees that develop or modify HBES product/system standards or, where not suitable HBES product standards addressing functional safety exist, to product manufacturer.

HBES and HBES products in this European Standard are for non-safety related applications. Additional requirements for safety related HBES will be described, according to EN 61508, in Part 2-4 of the EN 50090-series (under consideration).

1 Scope

This European Standard sets the requirements for functional safety for 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 exist for this equipment or system.

The functional safety requirements of this European Standard apply together with the relevant product standard for the device if any.

This European Standard is used as a product family standard. It is not intended to be used as a stand-alone standard.

This European 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.

EN 50090-2-1	*Home and Building Electronic Systems (HBES) – Part 2-1: System overview - Architecture*
EN 50090-2-2	*Home and Building Electronic Systems (HBES) – Part 2-2: System overview - General technical requirements*
EN 61508-4:2001	*Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations* (IEC 61508-4:1998 + corrigendum 1999)

EN 61508-5:2001	*Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels* (IEC 61508-5:1998 + corrigendum 1999)
EN 61709:1998	*Electronic components - Reliability - Reference conditions for failure rates and stress models for conversion* (IEC 61709:1996)
CEN/CLC Guide 9	*Guidelines for the inclusion of Safety Aspects in standards* (ISO/IEC Guide 51)
EN ISO 9000 series	*Quality management systems*

3 Definitions

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

3.1
architecture
specific configuration of hardware and software elements in a system

[EN 61508-4:2001, definition 3.3.5]

3.2
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

3.3
authorisation
mechanism to ensure that the entity or person accessing information, functions or services has the authority to do so

3.4
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

3.5
functional safety
freedom from unacceptable risk of harm due to the operation of an HBES, including that resulting from

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

NOTE 1 Definition of EN 61508-4:2001, 3.1.9: 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 (IEC/TC 77) are taken into account.

3.6
Hamming distance
numbers of bits in which two binary codes differ

3.7
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

[EN 61508-4:2001, definition 3.1.1]

3.8
hazard
a potential source of harm

[CEN/CLC Guide 9, respectively ISO/IEC Guide 51:1990]

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).

[EN 61508-4:2001, definition 3.1.2]

3.9
hazardous event
situation which results in harm on normal operation or abnormal condition

NOTE Definition of EN 61508-4:2001, 3.1.3 and 3.1.4: circumstance in which a person is exposed to hazard(s) which results in harm

3.10
HBES, Home and Building Electronic Systems
a multi-application bus system where the functions are decentrally distributed and linked through a common communication process

NOTE HBES is used in homes and buildings plus their surroundings. Functions of the system are e.g: switching, open loop controlling, closed loop controlling, monitoring and supervising.

3.11
HBES product
HBES products consist of devices in the form of hardware, firmware, their associated software and of configuration tools, intended to be used in an HBES

3.12
product
HBES products consist of devices in the form of hardware, firmware, their associated software and of configuration tools

3.13
product documentation
- the 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

3.14
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 EN 61508-4:2001, definition 3.4.3), the necessary risk reduction in order to meet the required tolerable risk (see EN 61508-4:2001, definition 3.1.6). See also Annex A of EN 61508-5:2001.

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 (EN 61508-4:2001, 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 (EN 61508-4:2001, 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.

[EN 61508-4:2001, definition 3.4.1]

3.15
risk
combination of the probability of occurrence of a harm and the severity of that harm

[CEN/CLC Guide 9, respectively ISO/IEC Guide 51:1990, modified]
[EN 61508-4:2001, definition 3.1.5]

NOTE For risk classes see Annex A.

3.16
reasonably foreseeable misuse
the 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

[EN 61508-4:2001, definition 3.1.11]

3.17
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 EN 61508-4:2001, definition 3.4.1)

[EN 61508-4:2001, definition 3.5.1]

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 products.

1) 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.

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

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

4.2 Method of establishment for the requirements

For specification of the functional safety requirements the life-cycle used in EN 61508 was followed:

1) concept phase of products;
2) application environment;
3) identification of hazards and hazard 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 European Standard into account in the product safety requirements, but it is not necessary to go into the EN 61508 process itself.

4.2.1 HBES application environment

The HBES application environment is taken into account.

4.2.2 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 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.

4.2.3 Hazardous events

The following hazardous events have been taken into account for the analysis (the bus and mains (230 V/400 V) 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.

4.2.4 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 in 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 4.2.3 the risk analysis shall be carried out according to EN 61508.

5 Requirements for functional safety

NOTE Reference to the hazardous events of 4.2.3 are given within brackets ( ).

5.1 General

Analysis according to EN 61508 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 5.7 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.