ISO/IEC 14762

Edition 1.0 2009-01

INTERNATIONAL STANDARD

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

ISO/IEC 14762:2009(E)

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 It also gives information on projects, withdrawn and replaced publications.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