Draft for Public Comment

Form 36

DPC: 25/30509480 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000
Fax: +44 (0)20 8996 7400
www.bsigroup.com

Date: 17 January 2025
Origin: European

Latest date for receipt of comments: 12 February 2025

Project No. 2017/03928

Responsible committee: ICT/2 ICT Accessibility

Interested committees:

Title: Draft BS EN IEC 63168 Cooperative multiple systems in connected home environments - AAL functional safety requirements of electronic safety-related systems.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

i) has any issues related to 3rd party IPR, patent or copyright
ii) affects other national standard(s)
iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 12 February 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop http://shop.bsigroup.com or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from https://standardsdevelopment.bsigroup.com/.

Responsible Committee Secretary: Ms Dawn Hunter (BSI)
Direct tel:
E-mail: dawn.hunter@bsigroup.com

Documents
Document Sharing Hub
Full document details: 25/30509480 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at **https://standardsdevelopment.bsigroup.com/**. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex **(e.g. 3.1)**	Paragraph/ Figure/Table/Note	**Type of comment**	**Commend (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations on each comment submitted**
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

SyCAAL/130/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER: **IEC 63168 ED1**	
DATE OF CIRCULATION: **2018-12-07**	CLOSING DATE FOR COMMENTS: **2019-02-01**
SUPERSEDES DOCUMENTS: **SyCAAL/76/NP,SyCAAL/86/RVN**	

IEC SYC AAL : ACTIVE ASSISTED LIVING	
SECRETARIAT: IEC Central Office	SECRETARY: Mr Miroslav Siket
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 23,TC 59,TC 61,SC 65A,TC 79,TC 100,TC 124,SEG 9,ISO/IEC JTC 1/SC 25	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☒ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Cooperative multiple systems in connected home environments - Functional safety of electrical/electronic safety-related systems - AAL aspects

NOTE FROM TC/SC OFFICERS:

Copyright © 2018 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

CONTENTS

FOREWORD - 4 -
INTRODUCTION - 6 -
1 Scope - 8 -
2 Normative references - 8 -
3 Terms and definitions - 8 -
4 Abbreviated terms - 13 -
5 Overall safety Management - 13 -
5.1 Objectives - 13 -
5.2 General - 15 -
5.2.1 Introduction to the safety lifecycle concept - 15 -
5.2.2 H-SIL concept - 15 -
5.2.3 External functional safety measures - 15 -
5.3 Inputs to this clause - 15 -
5.4 Requirements and recommendations - 15 -
5.4.1 Functional safety culture - 15 -
5.4.2 Continuous improvement - 16 -
5.4.3 Training and qualification - 16 -
5.4.4 Safety management during development - 16 -
5.4.5 Assignment of safety responsibilities - 16 -
5.4.6 Assignment of tasks - 16 -
5.4.7 Planning of all safety management activities during development - 16 -
5.5 Work products - 18 -
6 Safety management during the concept phase and the product development - 18 -
6.1 Objectives - 18 -
6.2 Inputs to this clause - 18 -
6.3 Requirements - 19 -
6.3.1 Item and ambient conditions - 19 -
6.3.2 Limits of item and its interfaces with other items - 19 -
6.3.3 Sources of stress - 19 -
6.3.4 Additional determinations - 19 -
6.4 Work products - 19 -
7 Safety management activities after start of production - 20 -
7.1 Objectives - 20 -
7.2 Inputs to this clause - 20 -
7.3 Requirements - 20 -
7.3.1 Management of production and modification procedure - 20 -
7.3.2 Tasks for preparing and conducting production and end of line inspections - 20 -
7.3.3 Tasks for safe item operation and decommissioning - 20 -
7.4 Work products - 20 -
8 Production and installation of safety-related systems - 20 -
8.1 Objectives - 20 -
8.2 General - 20 -
8.3 Prerequisites and recommendations - 21 -
8.4 Requirements - 21 -

Documents
Document Sharing Hub
Full document details: 25/30509480 DC

8.4.1 Production plan - 21 -
8.4.2 Test plan - 21 -
8.4.3 Production and testing - 21 -
8.4.4 Process capability - 21 -
8.4.5 Documentation - 21 -
8.4.6 Non-compliance - 21 -
8.4.7 Traceability - 21 -
8.4.8 Storage and transport conditions - 22 -
8.4.9 Modification - 22 -
8.5 Work products - 22 -
Annex A (informative) Examples of system analysis for safety based on use case – using AAL use case template - 23 -
A.1 Objectives - 23 -
A.2 Activities about system analysis for safety based on use case - 23 -
A.2.1 Objectives - 23 -
A.2.2 Preparing before writing the use case with AAL use case template - 23 -
A.2.3 Writing with AAL use case template - 24 -
A.2.4 Doing safety activities including discussions, using AAL use case - 25 -
A.3 Use case example: Intelligent lighting fixtures - 25 -
A.3.1 General - 25 -
A.3.2 Preparing before writing the use case with AAL use case template - 25 -
A.3.3 Making use case with filling AAL use case template of this example - 27 -
A.3.4 AAL Use case of this example - 28 -
A.4 Use case example: Indoor movement guidance display system and automatic robot cleaner - 34 -
A.4.1 General - 34 -
A.4.2 Preparing before writing the use case with AAL use case template - 35 -
A.4.3 Making use case with filling AAL use case template of this example - 37 -
A.4.4 AAL use case of this example - 38 -
Annex B (informative) List of publications related to functional safety of cooperative systems in connected home environment - 43 -
B.1 Objectives - 43 -
B.2 List of International Standards - 43 -
Bibliography - 45 -

Figure 1 – Cooperative multiple systems - 7 -
Figure 2 – Iterative process for design of safety-related components of control systems - 14 -
Figure 3 – Safety lifecycle - 15 -
Figure A.1 – System diagram of example - 26 -
Figure A.2 – System diagram of example - 35 -
Figure A.3 – Use case diagram of example - 37 -

Table 1 – Verification measures — Safety audit, safety review and safety assessment - 18 -
Table B.1 – List of publications related to functional safety of cooperative system in connected home environment - 43 -

Documents
Document Sharing Hub
Full document details: 25/30509480 DC

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COOPERATIVE MULTIPLE SYSTEMS IN CONNECTED HOME ENVIRONMENTS -- FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC SAFETY-RELATED SYSTEMS -- AAL ASPECTS

Part 1: General requirements for design and development

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.

International Standard IEC 63168-1 has been prepared by IEC SyC AAL: System committee on Active Assisted Living

A list of all components in the IEC 63168 series, published under the general title Cooperative multiple systems in connected home environments - Functional safety of electrical/electronic safety-related systems - AAL aspects, can be found on the IEC website.

The text of this document is based on the following documents:

FDIS	Report on voting
SyCAAL/XX/FDIS	SyCAAL/XX/RVD

Full information on the voting for the approval of this document can be found in the report on voting indicated in the above table.

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

Documents
Document Sharing Hub
Full document details: 25/30509480 DC

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.

The National Committees are requested to note that for this document the stability date is …. THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

INTRODUCTION

This document provides a framework of lifecycle processes with activities and tasks necessary for the safe design and maintenance of cooperative multiple systems in connected home environments.

In connected home environment, multiple systems are connected via a network. Various information including operation instructions are mutually exchanged between the respective systems. Each system determines its operation content based on the acquired information and executes it. Figure 1 shows the relationship between each system and cooperative multiple systems in connection home environment. In the safety design of each system, it is necessary to grasp the whole of multiple systems in connected home environment and to reduce the occurrence risk of un-safe states caused by the interconnection to socially acceptable level.

Users in connected home environments, including residents, visitors, and helpers, operate the system directly and/or indirectly, and are affected by the actions the system performs. In the safety design for realizing the safe operation of the systems, it is necessary to consider the fact that the user includes human beings having such a characteristic as needing assistance from others in life such as infants and the elderly.

This document provides a comprehensive approach to the realization of a system composed of elements for executing safety functions (safety-related system), which is required for each cooperative system. Where the non-cooperating system in connected home environment does not have other international standards relating to safety design, it does not preclude applying this approach.

This document provides the provisions:

– on the safety lifecycle of cooperating systems in connected home environment;
– for the activities and tasks required at each stage in the safety lifecycle;
– on the safety integrity level for connected home environment that take into account user characteristics, mainly the need for assistance from others; and
– on risk reduction processes of cooperative system using the safety integrity levels for connected home environment.

The reader of this document is supposed to be:

– developers of cooperative systems in connected home environment;
– developers of system components in connected home environment; and
– installer of cooperative systems in connected home environment.

This document consists of the following parts, under the general title Cooperative multiple systems in connected home environments – functional safety of electrical/electronic safety-related systems – AAL aspects -:

– Part 1: General requirements for design and development
– Part 2: Concept phase of product design
– Part 3: Product development
– Part 4: Production, operation, modification of product

It is recognized that some products specific standards may have specific applicable requirements concerning functional safety of the relevant products that integrate or complement the requirements of IEC 63168 series of standards.

NOTE 1 Regarding the safety of individual products in cooperative multiple systems, the relevant international standards (e.g. IEC 60335 series for home appliances) should be referred.

NOTE 2 See Annex B about international standards for safety to be referred to.

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

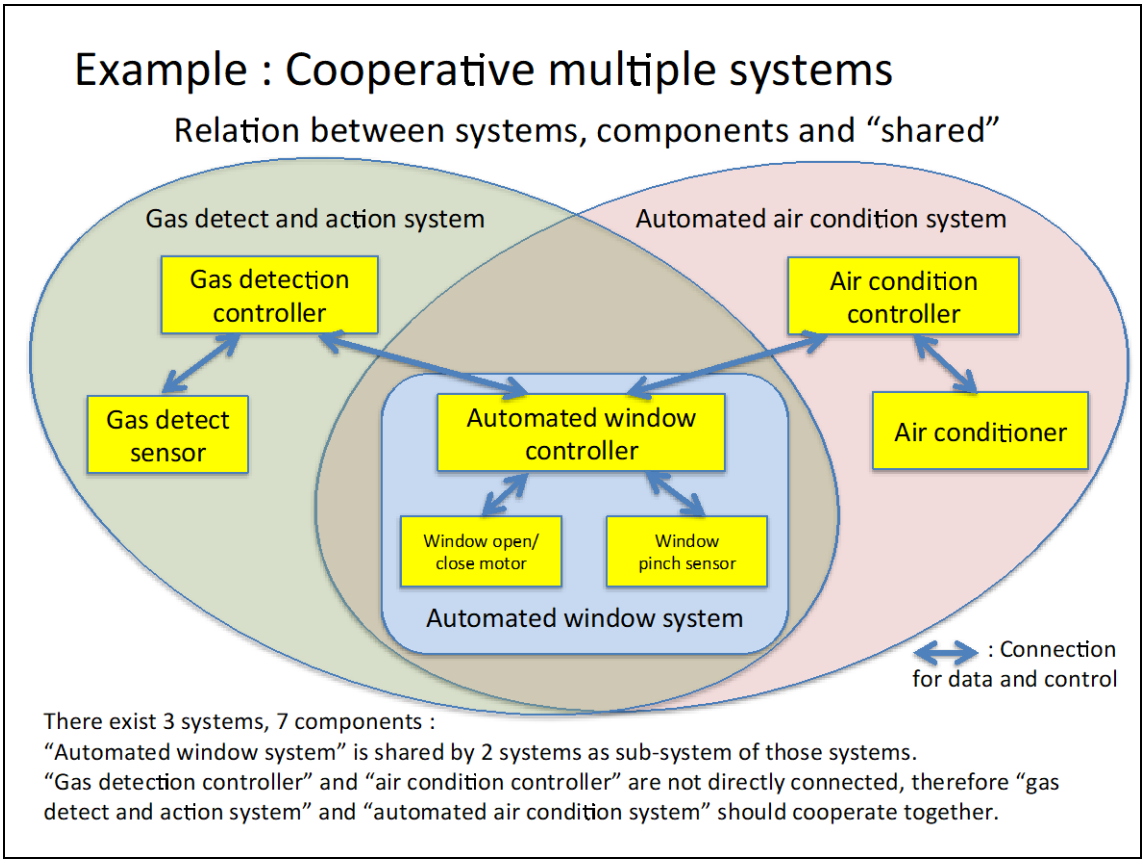

Figure 1 – Cooperative multiple systems

Documents
Document Sharing Hub
Full document details: 25/30509480 DC

COOPERATIVE MULTIPLE SYSTEMS IN CONNECTED HOME ENVIRONMENTS -- FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC SAFETY-RELATED SYSTEMS -- AAL ASPECTS

Part 1: General requirements for design and development

1 Scope

IEC 63168 series specifies AAL specific functional safety requirements of electrical/electronic (E/E) safety-related systems for cooperative multiple systems that are operated together in a connected home environment.

The AAL specific functional safety requirements are:

– AAL specific Safety Integrity Level (SIL) definitions that account for different types of AAL users; and

– a risk assessment procedure using the AAL specific SIL.

These cooperative multiple systems may be installed and operated by AAL users, including operators who are not fully trained.

The requirements are specified in accordance with the principles of the basic standard for functional safety, IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems), and the other related standards including ISO/IEC 14762 (Information technology -- Functional safety requirements for Home and Building Electronic Systems (HBES)) and IEC 63044 series (Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)).

This part of IEC 63168 specifies general requirements for design and development of cooperative multiple systems in connected home environment.

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 60050-871:2018, *International electrotechnical vocabulary – Part 871: Active assisted living (AAL)*

ISO 25119-1:2010, *Tractors and machinery for agriculture and forestry –Safety-related parts of control systems – Part 1: General principles for design and development*

ISO 26262-1:2011, *Road vehicles – Functional safety – Part 1: Vocabulary*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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

audit

examination of an implemented process

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

[SOURCE: ISO 26262-1:2011, 1.5]

3.2

connected home environment

home environment that provides a home network (IEV 732-10-01) to ensure that devices within the home can communicate to one another and to devices outside the home

3.3

cooperative multiple systems

systems that operate while affecting each other

3.4

electrical and/or electronic system
E/E system

system that consists of electrical and/or electronic elements, including programmable electronic elements

EXAMPLE Power supply; sensor or other input device; communication path; actuator or other output device.

[SOURCE: ISO 26262-1:2011, 1.31]

3.5

element

system or part of a system including components, hardware, software, hardware parts, and software units

[SOURCE: ISO 26262-1:2011, 1.32]

3.6

exposure

duration of time and frequency in which an individual is in a situation in which the potential hazard exists

[SOURCE: ISO 25119-1:2010, 3.14]

3.7

failure

termination of the ability of an item to perform a required function

[SOURCE: ISO 25119-1:2010, 3.15]

3.8

fault

state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

[SOURCE: ISO 25119-1:2010, 3.16]

3.9

functional safety

system that performs in a way that does not present an unreasonable risk of injury to residents, visitors or bystanders

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

3.10

functional safety requirement

requirement for a safety-related function of the E/E system

3.11

harm

physical injury

[SOURCE: ISO 25119-1:2010, 3.24]

3.12

hazard

potential source of harm

[SOURCE: ISO 25119-1:2010, 3.25]

3.13

hazard analysis and risk assessment

method to identify and categorize hazardous events of items and to specify safety goals and H-SILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk

3.14

hazardous event

combination of a hazard and a hazardous situation

3.15

hazardous situation

circumstance in which a person is exposed to a hazard or hazards, exposure to which can have immediate or long-term effects

[SOURCE: ISO 25119-1:2010, 3.26]

3.16

home environment

environment within a home, including the totality of appliances [e.g. household technology, home network, furnishings]

[SOURCE: IEC 60050-871:2018, 871-03-02]

3.17
H-SIL decomposition
apportioning of safety requirements redundantly to sufficiently independent elements, with the objective of reducing the H-SIL of the redundant safety requirements that are allocated to the corresponding elements

3.18
Item
system or array of systems to implement a function at connected home environment level, to which IEC 63168 is applied

3.19

lifecycle

entirety of phases from concept through decommissioning of the item

[SOURCE: ISO 26262-1:2011, 1.72]

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

3.20

modification

authorized alteration of an item

[SOURCE: ISO 26262-1:2011, 1.75]

3.21

operating mode

perceivable functional state of an item or element

[SOURCE: ISO 26262-1:2011, 1.81]

3.22

review

examination of a work product, for achievement of the intended work product goal, according to the purpose of the review

Note 1 to entry: Reviews can be supported by checklists.

[SOURCE: ISO 26262-1:2011, 1.98]

3.23

risk

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

[SOURCE: ISO 26262-1:2011, 1.99]

3.24

risk analysis

combination of the specification of the limits of the machine, hazard identification and risk estimation

[SOURCE: ISO 25119-1:2010, 3.40]

3.25

risk assessment

overall process comprising risk analysis and risk evaluation

[SOURCE: ISO 25119-1:2010, 3.41]

3.26

risk evaluation

judgment on the basis of risk analysis as to whether a given risk is tolerable

[SOURCE: ISO 25119-1:2010, 3.42]

3.27

safety activities

activity performed in one or more subphases of the safety lifecycle

3.28

safety culture

policy and strategy used within an organization to support the development, production and operation of safety-related systems

[SOURCE: ISO 26262-1:2011, 1.107]

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

3.29

safety goal

description of how a given hazard is to be avoided

Note 1 to entry: It is the top level safety requirement, derived from the hazard analysis and risk assessment.

Note 2 to entry: The existence of several safety goals for one item is possible.

[SOURCE: ISO 25119-1:2010, 3.44]

3.30

safety integrity level for connected home environment
H-SIL

one of four levels to specify the item's or element's necessary requirements of IEC 63168 and safety measures to apply for avoiding an unreasonable residual risk, with an alphabet from A representing the least stringent level to D the most stringent level

3.31
safety lifecycle
necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of product design and finishes when all of the E/E safety-related systems and other risk reduction measures are no longer available for use [SOURCE: IEC 61508-4:2010, 3.7.1]

3.32

safety manager

role filled by the person responsible for the functional safety management during the item development

[SOURCE: ISO 26262-1:2011, 1.109]

3.33

safety plan

plan to manage and guide the execution of the safety activities (1.104) of a project including dates, milestones, tasks, deliverables, responsibilities and resources

[SOURCE: ISO 26262-1:2011, 1.112]

3.34

severity

measure of the most likely degree of harm to an endangered individual

[SOURCE: ISO 25119-1:2010, 3.47]

3.35

subphases

subdivision of a stage in the safety lifecycle that is specified in a distinct clause

3.36

system

set of elements that relates at least a sensor, a controller and an actuator with one another

Note 1 to entry: The related sensor or actuator can be included in the system, or can be external to the system.

Note 2 to entry: An element of a system can also be another system.

[SOURCE: ISO 26262-1:2011, 1.129]

Documents
Document Sharing Hub

Full document details: 25/30509480 DC

3.37

work product

output of a design or development activity

[SOURCE: ISO 25119-1:2010, 3.57]

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply

SOP start of production

SRS safety related system

5 Overall safety Management

5.1 Objectives

For development of safe E/E system product in connected home environment, developers should consider safety impacts on the cooperative multiple systems throughout the product life cycle to be developed. The contents to be considered include hazard analysis and risk assessment on the cooperative multiple systems. Since users of E/E system products include young people and elderly people, and the scope of influence exerted by the cooperative multiple systems includes visitors and neighbours, developers may conduct system analysis for safety based on use case as necessary.

NOTE 1 See IEC 63168-2 to know the examples of hazard analysis and risk assessment.

NOTE 2 See Annex A to know the examples of system analysis for safety based on use case.

The main objective, set out in this clause, is to define the responsibilities of the persons, departments and organizations responsible for each phase during the overall safety lifecycle or for activities within the various phases. This relates to both the activities necessary to ensure the required level of functional safety for the item, and to the confirmation measures endorsing that level of functional safety. Another objective is to define management activities during the complete safety lifecycle.

The E/E system should be designed and constructed so that the principles of risk analysis, risk assessment and an iterative process for the design of safety-related components of control systems are taken fully into account (see Figure 2).

Documents
Document Sharing Hub

Full document details: 25/30509480 DC