SLOVENSKI STANDARD
SIST CLC/R 205-012:1998

01-september-1998

Home and building electronic systems (HBES) - Technical Report 12: Guidelines on requirements for functional safety of products intended to be integrated in a home control system

Home and Building Electronic Systems (HBES) -- Technical Report 12: Guidelines on requirements for functional safety of products intended to be integrated in a home control system

Ta slovenski standard je istoveten z: **R205-012:1997**

ICS:

97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

SIST CLC/R 205-012:1998 **en**

CENELEC

R205-012

REPORT

November 1997

English version

Home and Building Electronic Systems (HBES) Technical Report 12: Guidelines on requirements for functional safety of products intended to be integrated in a home control system

This CENELEC Report has been prepared by the Technical Committee CENELEC TC 205, Home and Building electronic Systems (HBES). It was approved by CENELEC on 1997-10-21.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, 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. R205-012:1997 E

Contents

Introduction

This document gives guidance to the product committees, so that they can specify products using home control systems. It gives guidance on the default actions a device should take when it looses network access, and on the definition of the "safe" state of the product.

As this document is a Report, it uses verb forms such as "should". This does not in any way imply that compliance with such clauses is optional if safety is to be achieved.

1 Scope

The present document provides guidelines to product committees on requirements for Functional Safety of products intended to be integrated in a home control system, as defined in IEC Guide 110. In this report, home control systems are referred to as hcs.

The guidelines also apply to any similar equipment having home and/or building control functions. Any reference in the document to hcs shall be considered to include such similar equipment.

An hcs should comply with the requirements for functional safety indicated in this Report. In addition the individual equipment integrated into an hcs should comply with relevant product safety standards.

2 References

EN 41003	Particular safety requirements for equipment to be connected to telecommunications networks
EN 60950 (mod)	Safety of information technology equipment, including electrical business equipment
EN 41003	Particular safety requirements for equipment to be connected to telecommunications networks
IEC Guide 104	Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions
IEC Guide 105	Principles concerning the safety of equipment electrically connected to a telecommunications network
IEC Guide 110	Home control systems - Guidelines relating to safety
CLC Memorandum 9 ISO/IEC Guide 51	Guidelines for the inclusion of safety aspects in standards
Draft series IEC 1508	Functional safety - safety-related systems
HD 384 series IEC 60364 series	Electrical installation of buildings

3 Definitions and abbreviations

3.1 Definitions

This document makes use of definitions and recommendations from ACOS WG1, as contained in the IEC GUIDE 110:1995-04-26 "home control systems - Guidelines relating to safety".

Functional safety (for a home control system): The ability of a home control system to carry out the actions necessary to achieve and maintain an appropriate level of safety both under normal conditions and when a fault or hazard occurs (see IEC 1508-4).

3.2 Abbreviations

hcs: home control system

4 General guidelines to the product committees

4.1 The hazards

Application of this document is intended to prevent injury or damage due to any of the following hazards which could result from malfunction of failure of an hcs:

- electric shocks
- energy hazards
- fire
- mechanical and heat hazards
- radiation hazards
- chemical hazards

This includes both safety in homes and non industrial buildings, for persons, surroundings, livestock and domestic animals.

4.2 The conditions

The document covers all conditions of normal use and fault conditions.

Foreseeable misuse should be taken into consideration but sabotage, force majeure and intentional damage are excluded.

After abnormal operation or a fault, a device should not interfere with the safety of the hcs and should remain safe for the user in the meaning of the relevant product safety standard. It is not required that the device should still be in full working order.

4.3 Possible protection measures

The following measures are suggested:

- Measures to prevent a home control system from interfering with the safety of a device connected to the hcs.
- Measures to ensure that a malfunction or a failure of a home control system does not impair the safety level of devices integrated into the system.
- Measures to prevent a device integrated into a home control system from interfering with the safety of the hcs, or other devices connected to the hcs.

Some examples of such measures are: appropriate installation of a device, adequate electrical safety of interface modules, control of hcs access, verification of safety critical information, safe mode of a device in the event of a malfunction or a failure of the hcs.

Relevant information should be given within installation or operation manuals (or instruction sheets).

4.4 General measures

For the hcs products, the following should apply:

- The existing measures and protection concepts incorporated in e.g. EC Directives and product standards need to be taken into account.
- No part of home control system should rely upon unconfirmed safety-critical information. This applies equally to new and modified systems (extensions, changes of configuration). (From IEC-ACOS GUIDE 110, clause 4.2.1).

- The network or any other part of a home control system should not impair the safety of a device; all safety aspects of e.g. EC Directives and the product standard of the device should be complied with. Similarly, connection of an application device should not interfere with the safety of the home control system. (After: IEC-ACOS GUIDE 110, clause 4.2.2).

- If a device relies upon an hcs for its safe operation but cannot verify correct function of the relevant parts of the hcs, the device should maintain an appropriate level of safety independent of the hcs. (After: IEC-ACOS GUIDE 110, clause 4.2.3).

- An order or series of orders (even if incorrect or unexpected) received via the hcs should not lead to a hazard or damage the hcs product or the equipment controlled by the hcs. These orders may cause the product not to operate at all or not to operate properly -for example by entering a "default" mode, provided it is in a safe mode.

- The manufacturer and/or installer should apply the relevant safety standards to the installation of hcs, in particular IEC 60364 (containing the rules for the erection and design of electrical installations), so as to ensure safety and proper functioning for the use intended.

It is to be noted that the above recommendations can easily be taken into account by a manufacturer of a product, integrating a hcs access, that has a well-defined function (for example dish-washer, toaster...).

The above recommendations should not present difficulties for product manufacturers skilled in the design and production of conventional forms of domestic appliances and similar equipment, that are appliances and equipment without hcs access,

Integration of a hcs access adds electrical safety issues, which have to be complied with, but does not add new classes of potential safety hazards. In this case, the manufacturer is expected to know about the existing safety measures for a non-hcs connected device, in order to ensure its safety.

As an example, an oven integrating a hcs access may be unexpectedly switched on, either over the hcs or locally by a child; this has to be taken into account by the manufacturer the same way. The integration of the hcs access does not create a new hazard; only another way of exposing an existing hazard; that of unintended operation.

5 Guidelines referring to installation

The above recommendations may not be sufficient in such cases where the geographical distribution or the combination of the device with other devices may lead to potential functional safety hazards.

For example, a light in a staircase may lead to safety hazard if unexpectedly switched off. Similarly a device used to switch on or off an electrical line or plug, operating independently of the kind of load connected, may generate additional safety hazards, depending on what equipment is using the line or plug.

In these cases, the manufacturer should draw the attention of the installer and/or the user to the installation and usage conditions and requirements:

- Installation of products should be made according to the manufacturer's user and installation manuals; these manuals should provide guidance for the installation, configuration, extension and maintenance of such systems so that potential safety problems are avoided.

- Installation of an hcs does not alter or diminish the need to comply with existing regulations and guidelines. After the installation of a home control system or any hcs-connected device, the electrical installation should still comply with the latest regulations and state of art. This should be stated in the product instructions.

- Relevant safety requirements apply to the connection of a home control system to a public services network if the home control system includes an access point to such networks.

If the system is to be installed in a building where some national or regional safety requirements applies, the behaviour of the system should comply with these requirements. In case of fault, the system should default to a safe mode compatible with those requirements.

6 Case by case suggested requirements

6.1 Message types

A primary consideration of safety relates to the messages sent on an hcs. The messages on an hcs may be intended to do one of a number of things:-

1) Convey either information or instructions to a device; for example "it is 22C in the bedroom" or "turn off the kitchen heater". The messages are generally about the real world, that is the world outside the hcs, and are intended to have an immediate effect on the actions of other devices. These are the most common form of messages on an hcs.

2) Change the state of a device by rendering either the whole or parts of the device inoperable -taking it on-line or off-line.[1]

3) Modify the performance of a device; for example "don't report temperature changes smaller than 1C" or "send an alarm if the temperature of the swimming pool is below 16C". These messages modify the future performance of the system. These may be regarded as configuration messages since they modify the way in which the target device is configured.

4) Modify the source or destination of messages; for example "in future send details of the temperature in the bedroom to the heater in the kitchen". These are generally referred to as network management messages since they change the "shape" of the network.[2]

5) Modify the performance of the device by down-loading new application code.[3]

The messages are listed above in increasing order of their potential impact on functional safety. Reconfiguring the source and destination of communication can clearly create hazards. For example, managing the network so that the left-hand door of a garage door opener is no longer listening to its own safety system but to that of the adjacent right-hand door can create serious hazards.

6.2 Physical medium openness

The second issue which affects the functional safety of an hcs system is its openness, and particularly the degree to which accidental or deliberate access can be gained to the physical media of that system to issue any of the messages listed above. Again, listing in order of increasing hazard, we can categorise systems as:

1) **Closed.**[4] Entirely contained within one building or other secure entity and operating only on closed media such as twisted-pair, coaxial cable or fibre-optics. In such a system, all messages must have originated within the local environment and a higher degree of trust may (perhaps) be placed in such messages. Physical intrusion is not considered in this document.

---

1 These messages should not prejudice the safety of a system since it should not be necessary to rely on the functioning of all network devices for such safe operation.

2 In some systems network management may be performed automatically with little or no human intervention, so called "plug & play" or manually by setting switches in devices to set their addresses.

3 Potentially lethal if that code is, for example, insufficiently tested and the device is safety critical.

4 In this document, 'closed' or 'open' refer to physical connection or susceptibility to the outside world and not to Intellectual Property Rights or the fact that a specification is proprietary or not.

2) **Semi-open.** A system which, although within one building or other secure entity, uses an open transmission media such as powerline signalling or radio to carry some or all of its messages. Such as system may be prone to accidental interference or deliberate attack[5] from other systems operating in the vicinity since the signalling media chosen has no hard physical limits.[6] Examples of such accidental interference have been experienced for power line signalling systems.

3) **Completely open.** A system including potentially unrestricted access to other communication channels such as telephone, Ethernet, CATV or Internet. In such a case, the signalling range is effectively unbounded and messages or instructions could be received from almost anywhere in the world.

The more open a system is, the greater its exposure to inappropriate messages and the higher probability that, at some time during the system's lifetime, such messages will occur.

It also appears likely that the probability of reception of an inappropriate message will rise during that lifetime as the density of installed systems increases. The first power line system installed in a block of apartments is unlikely to experience problems until the second, third, and subsequent, systems arrive.

Consequently it follows that the greater the degree of openness of a system, the higher the level of security that should applied to the messaging, and that level of security should take account of a future increase in the density of installed systems.

A system originally installed as a closed system may subsequently be extended by the addition of an open or semi-open segment. When making such an extension the impact on the existing system should be considered. This does not mean that the security of the whole system should necessarily be upgraded to a level appropriate for an open or semi-open system (and for the application running on that system). It may be that each section might retain its own level of security provided that the manner in which the connection or extension is achieved provides the appropriate protection. This is analogous to the use of a "firewall" between corporate computing networks and the Internet.

6.3 Degree of hazard of devices and applications

The third dimension to the problem is the degree of risk associated with the device receiving the message. Under normal conditions light bulbs, and even electricity supplies, may fail and a lamp lighting (or failing to light) when intended should not create a significant safety hazard. However this is not true of traffic lights where the simultaneous illumination of the green lamp on two sides of underground garage entrance has obvious risks.

In the latter case the problem is exacerbated by the presence of motion, in this case that of the cars, and it appears that, as a generality, motion and heat are two of the elements that are likely to constitute safety hazards with hcs installations.

We can therefore define two cases:

1) safe products in safe environment (for example: a lamp and its switch, in an application where a fault has no serious consequence)

2) unsafe products, or products in unsafe environment (for example: a cooking range, or a lamp and its switch, in an application where a fault may have serious consequences)

---

5 This document excludes considerations of sabotage and intentional damage when that sabotage or damage originates within the building. However external sabotage or damage by remote access should be preventable by suitable design.

6 Strictly this includes infrared (IR) signalling, but the effective range is much lower than radio or power line signalling and it is normally confined to line-of-sight signalling. The opportunities for problems caused by sources outside the building are therefore much lower. Problems are more likely to arise from the use of IR for other purposes within the building.