TECHNICAL REPORT

ISO/IEC TR 14762

First edition
2001-01

Information Technology – Home Control Systems – Guidelines for functional safety

Reference number
ISO/IEC TR 14762:2001(E)

TECHNICAL REPORT – TYPE 3

ISO/IEC TR 14762

First edition
2001-01

Information Technology – Home Control Systems – Guidelines for functional safety

PRICE CODE H

For price, see current catalogue

CONTENTS

INFORMATION TECHNOLOGY – HOME CONTROL SYSTEMS – GUIDELINES FOR FUNCTIONAL SAFETY

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 through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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

The main task of IEC and ISO technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where, for any other reason, there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when the technical committee has collected data of a different kind from that which is normally published as an International Standard, for example ‘state of the art’.

Technical reports of types 1 and 2 are subject to review within three years of publication to decide whether they can be transformed into International Standards. Technical reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC 14762, which is a technical report of type 3, was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This document which is purely informative is not to be regarded as an International Standard. Comments on the content of this document should be sent to IEC Central Office.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

INTRODUCTION

This technical report 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 loses network access, and on the definition of the “safe” state of the product.

Verb forms such as “should” are used because a technical report is informative and should not contain requirements. However, if safety is to be achieved, compliance with the statement is compulsory.

INFORMATION TECHNOLOGY – HOME CONTROL SYSTEMS – GUIDELINES FOR FUNCTIONAL SAFETY

1 Scope

This technical report gives guidelines for functional safety of electrically-controlled devices intended to be integrated in a home control system (HCS), as defined in IEC Guide 110. These guidelines also apply to similar equipment having home and/or building control functions. Any reference to HCS includes similar equipment, such as sensors and activators for security and energy management.

1.1 User environment

This technical report is concerned with the safety of persons, surroundings, livestock and domestic animals. It includes personal protection against electric shock, effects of excessive temperature, radiation, explosion, implosion, mechanical stability and moving parts, as well as protection against fire. It covers safety both in homes and non-industrial buildings. (See IEC Guide 104.)

This technical report specifies requirements intended to ensure safety for the user and layperson who may come into contact with the equipment and, where specifically stated, for service personnel (see clause 1 of IEC 60950).

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.

1.2 Hazards

Application of this technical report is intended to prevent injury or damage due to any of the following hazards that could result from malfunction or failure of an HCS:

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

Included is safety in homes and non-industrial buildings for persons, surroundings, livestock and domestic animals.

1.3 Conditions

This technical report covers all conditions of normal use and fault conditions.

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

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

1.4 Possible protection measures

The following measures are suggested:

- measures to prevent an HCS from interfering with the safety of a device connected to the HCS;
- measures to ensure that a malfunction or a failure of an HCS does not impair the safety level of devices integrated into the system;
- measures to prevent a device integrated into an HCS 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).

2 Reference documents

IEC Guide 104, *The preparation of safety publications and the use of basic safety publications and group safety publications*

IEC Guide 110, *Home control systems – Guidelines relating to safety*

IEC Guide 112:2000, *Guide on the safety of multimedia equipment*

IEC 60065:1998, *Audio, video and similar electronic apparatus – Safety requirements*

IEC 60364 (all parts), *Electrical installation of buildings*

IEC 60950, *Safety of information technology equipment*

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

3 Definitions and abbreviations

3.1 Definitions

For the purpose of this technical report the definitions of IEC Guide 110 apply as well as the following definition.

3.1.1
functional safety (for a home control system)
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 61508-4]

3.2 Abbreviations

HCS: home control system

4 General guidelines for the product committees

For HCS products, the following applies.

- The existing measures and protection concepts incorporated in regulations and product standards need to be taken into account.
- No part of a home control system should rely upon unconfirmed safety-critical information. This applies equally to new and modified systems (extensions, changes of configuration). (IEC Guide 110, 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 regulations 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. (IEC Guide 110, 4.2.2.)
- If a device relies upon an HCS for 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. (IEC Guide 110, 4.2.3.)
- An order or series of orders (even if incorrect or unexpected) received via the HCS should not result in 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 by integrating an HCS access that has a well-defined function (for example dish-washer, toaster, etc.).

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 do not include HCS access.

Integration of an HCS access adds electrical safety requirements that 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 the safety of this device.

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

5 Guidelines referring to installation

The above recommendations may not be sufficient in 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 a 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 the equipment that 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 done 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 the 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 a network.

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

6 Case by case requirements

6.1 Message types

A primary consideration of safety relates to the messages sent on an HCS. The messages on an HCS are intended to do one of a number of things as listed below.

a) Convey either information or instructions to a device; for example, "it is 22 °C 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 forms of messages on an HCS.

b) Change the state of a device by rendering either the whole or parts of the device inoperable, for example, taking it off-line.[1)]

c) Modify the performance of a device; for example, "don't report temperature changes smaller than 1 °C" or "send an alarm if the temperature of the swimming pool is below 16 °C". 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.

---

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 safe operation.

d) Modify the source or destination of messages; for example “in the 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)]

e) 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 that affects the functional safety of an HCS system is the openness of the system, 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 categorize systems as follows.

a) 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.

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

c) 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, the greater the exposure to inappropriate messages and the higher the probability that, at some time during the lifetime of the system, such messages will occur.

It is also likely that the probability of receiving an inappropriate message will rise during the lifetime of a system as the density of installed systems increases. In fact, 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 be applied to the messaging. This level of security should take into account a future increase in the density of installed systems.

---

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 technical report, “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.

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

6) Infrared (IR) signalling is one of these media, 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.

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 a separate level of security provided that the manner in which the connection or extension is achieved offers 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 for traffic lights where the simultaneous illumination of the green light on two sides of an underground garage entrance presents obvious risks.

In the latter case, the problem is aggravated by the presence of moving cars, and it appears that, in general, motion and heat are two of the many elements that are likely to constitute safety hazards with respect to HCS installations.

Therefore two cases can be defined:

a) safe products in a safe environment (for example: a lamp and the related switch in an application where a fault has no serious consequence);

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

6.4 Safety requirements

Table 1 lists possible requirements and methods of meeting them.

Table 1 – Possible requirements and methods of meeting them

Requirements	Ways to meet them
Avoid inadvertent operation of devices in the house via external signals	Limit external operations – to what has been explicitly authorized by the occupant, for example, 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 access code) Simple code, 4 digit (OK for closed medium, insufficient for open medium, since it is transmitted) Longer code Encryption, and/or authentication
Verify identity of the target device + verify identity of the “downloader”	For example, “certified piece of software”

6.5 Case dependent requirements

6.1, 6.2 and 6.3 deal with three orthogonal factors affecting the functional safety of HCS systems, i.e.:

a) nature of the message and the consequences of that message, considered at five levels;

b) degree to which the system is exposed to risk by the "openness" of the system, categorized into three levels;

c) severity of the potential hazard.

These can be related in a three-dimensional matrix, but given the limitations of paper and printing processes, the third dimension uses respectively standard and italic fonts for safe and unsafe applications. The standard text is left justified, while the text in italics is right justified. See table 2 for this matrix.

Table 2 – Factors affecting the functional safety of HCS systems

Message→ **Openness↓**	**1** **Normal operation messages**	**2** **On/Off**	**3** **Configuration parameters**	**4** **Network management**	**5** **Download of software**
Closed	No requirements *No requirements*	No requirements	*Identify target* *+ some tool or procedure*	Verify identity of the target *Idem,* *plus check consistency of the address / the rest of this group address* → *installation verification ?* → *or design of products with pre-programmed addresses*	Verify identity of the target *Trusted software* *Verify identity of both parties*
Semi-open	Avoid inadvertent operation: → sufficient range of addresses, house codes,... *Idem*			Idem *Idem*	Idem + some verification of source identity *Idem*
Completely open	Avoid inadvertent operation: → sufficient range of addresses, house codes,... *Idem,* *+ authentication*			Idem *Idem,* *+ identify source*	Idem + some verification of source identity *Idem (perhaps more complex verification in this case)*
NOTE Standard font: Safe devices in safe applications *Italic font: Unsafe devices and/or unsafe applications*					

Annex A

Some examples

The following examples are taken from various fields, and describe potential issues and ways to solve them. They may be used by product committees to stimulate ideas for their own domains. They have not been checked nor approved by the relevant product committees, who may well have different recommendations for their specific products.

NOTE Q: Question; A: Answer

A.1 Example 1: Oven

Q: Can an oven or cooking range be switched on from a distant point via the HCS?

A: Yes, if “distant” is within the same kitchen.

Q: What if “distant” is on the other side of the apartment and somebody has put something flammable in the oven in the meantime? What if “distant” means over the phone? Shouldn’t this be forbidden?

A: Time-switching of ovens has been available for years; there is no difference between a clock on the oven and a distant order.

Q: There is still a difference, because the person setting the clock on the oven can also check what is inside the oven.

A: Then a ”remote switch-on enable” button on the oven would be a solution: it would have to be set before the oven can be switched on from a distance and automatically reset when the door is opened. You do not need this button to be set in advance to switch the device off from a distance. The oven would still need to comply with all the intrinsic safety standards that apply to traditional ovens.

Q: This does not solve the problem for the cooking range as there is no door to control access.

A: Remote control of a cooking range should be limited to a few meters, and within the same room.

It may be necessary to allow for only one binding for the control device (as opposed to monitoring). If only one binding for control is allowed, it is easier to ensure that it has been done properly and with full knowledge of the installation and commissioning phase. More bindings may be allowed for monitoring (for example, to show usage, or to measure energy consumption).

A.2 Example 2: Devices presenting a high potential risk of hazard

Some devices may be considered by their manufacturer as presenting a particularly high risk of hazard. These devices usually require the presence of a local operator.

Q: Is it only allowed to switch on such a device when it is in sight?

A: Yes, if this is the product committee requirement.

Q: Does this prevent the integration of HCS access?

A: Not necessarily: infrared HCS access requires the presence of the operator within visible distance of the device, and can therefore be used within the requirement to be in sight of the device.

Q: But a gateway between another medium and this infrared connection may allow operation by a distant operator.

A: Commands transmitted over a gateway from another medium to the infrared connection should then be identified as “non-locally-originated” (or not transmitted at all) to avoid problems.

A.3 Example 3: Mains plugs, socket-outlets and circuits

Mains plugs operated via an HCS, mains socket-outlets operated via an HCS, and mains circuits operated via an HCS in the distribution board are

- useful, because they allow connection of classical devices to “HCS mains plugs” or “HCS mains socket-outlets” or “HCS mains circuits,” since all brown and white goods manufacturers will not be able to offer a full range of HCS products in the first phase,
- potentially hazardous, because they allow connection of any type of device. These devices therefore can be activated with functions that are *a priori* unknown to the manufacturer or installer of the plug (or socket-outlet or mains circuit).

Installation rules already allow socket-outlets that are controlled by remote switches usually located in the same room. “Add-ons” for socket-outlets that are time-switched or remote controlled (via power lines or radio frequency) are also available in do-it-yourself shops. This kind of device generates the same kind of safety hazard as HCS-operated plugs or socket-outlets.

The generic answer is that the installer and the user are responsible. A possible idea would be to impose a configuration and commissioning tool that clearly separates the different mains circuits (lighting, heating ...). Another possible idea would be a new plug and socket-outlet standard for remote controlled appliances. This socket-outlet would not accept traditional plugs; the new plug would fit both old and new sockets. The new plug would then be fitted only to appliances that are safe for remote control and these could be plugged into the old or new sockets depending on whether the user wants local or remote control.

A.4 Example 4: Water temperature adjustment

It is generally understood that the maximum temperature of a domestic hot water storage cylinder should be limited (to about 60 °C) to avoid the risk of accidental scalding. Clearly, the user of the system may wish to set a lower set-point if considered appropriate, and that set-point should therefore be user-accessible. The heater unit might include software or hardware to prevent the user from setting a temperature greater than 60 °C. This might be inappropriate in cases when

a) the heater also has industrial uses requiring a higher set-point, or

b) the particular installation has other mechanisms to prevent scalding, such as thermostatic mixers on all taps and shower-heads.

What mechanisms might be appropriate to allow the installer to set the upper limit on installation but prevent the user subsequently increasing that upper limit? For example, might a special tool be needed to set a temperature greater than 60 °C? In the absence of an adjustment by the installer, what should be the default value for the upper temperature limit?

Bibliography

ISO/IEC Guide 51, *Guidelines for the inclusion of safety aspects in standards*

IEC 62151:2000, *Safety of equipment electrically connected to a telecommunication network*

EN 41 003, *Particular safety requirements for equipment to be connected to telecommunications networks*