SLOVENSKI STANDARD
SIST EN 50131-1:2007/IS2:2011

01-maj-2011

Alarmni sistemi - Sistemi za javljanje vloma in ropa - 1. del: Sistemske zahteve

Alarm systems - Intrusion and hold-up systems - Part 1: System requirements

Ta slovenski standard je istoveten z: EN 50131-1:2006/IS2:2010

ICS:

13.310	Varstvo pred kriminalom	Protection against crime
13.320	Alarmni in opozorilni sistemi	Alarm and warning systems

SIST EN 50131-1:2007/IS2:2011 en

CENELEC

EN 50131-1/IS2

Interpretation 2

EN 50131-1:2006

English version

Foreword

This interpretation of the European Standard EN 50131-1:2006 was prepared by the Technical Committee CENELEC TC 79, Alarm systems. The text of the draft was submitted to the Unique Acceptance Procedure and was approved by CENELEC on 2010-07-09.

This document supersedes EN 50131-1:2006/IS1:2009.

Compared to EN 50131-1:2006/IS1:2009 the only change is the replacement of the 2nd paragraph of 8.5.4 by a new one for clarification's sake.

EN 50131-1:2006, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*, includes many requirements that may not match traditional intrusion systems in some countries. Additionally, standards are written in a style which can make them difficult to understand unless some explanation is given. This interpretation is intended to provide extra information to readers of the standard to assist in its understanding. It should be read in conjunction with the standard.

This interpretation varies in the depth of detail provided. More detail is given for areas that prompted significant questions during the development of EN 50131-1:2006.

This interpretation may also assist translators by clarifying the meaning of the standard.

This interpretation is informative and the standard shall be used to resolve any disputes.

ATTENTION – Numbering of clauses and tables:

In this document (sub)clause and table numbers written in italic (e.g. *Table 7, Subclause 8.3.1*) refer to subclauses and tables in EN 50131-1:2006. Numbers written normally (e.g. Table 2, Subclause 6.1.1) usually refer to this document but, when specifically stated, may refer to other documents.

Contents

Figures

Tables

In Clauses 3 to 9 of this document the section numbering matches the clauses of EN 50131-1:2006.

Only interpreted clauses are given and therefore the numbers are not continuous.

1 About this document

1.1 Scope

This document provides interpretation for the contents of EN 50131-1:2006 only. Other standards, Technical Reports or Technical Specifications in the EN 50131 series or EN 50136 series may be referenced but the interpretation is restricted to the scope and use of EN 50131-1:2006.

1.2 References

The standard that this document interprets is EN 50131-1: 2006, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements.*

Other standards referenced are those listed in the normative references of EN 50131-1:2006.

1.3 Definitions and abbreviations in this document

1.3.1 Definitions

The following definitions apply to terms used in this document that do not appear in EN 50131-1:2006. For other terms refer to EN 50131-1:2006.

1.3.1.1
alarm transmission equipment
equipment which is used primarily for the transmission of alarm messages from the supervised premises transceiver interface to the alarm receiving centre transceiver interface

NOTE This is based on definition 4.5 in EN 50136-1-1:1998. When used in this document it always refers to equipment that is part of the alarm transmission system located at the supervised premises, i.e. the supervised premises transceiver, whether housed separately or within another component of the I&HAS, e.g. the CIE.

1.3.1.2
duress situation
situation in which the I&HAS user is under direct threat and the triggering of an HAS should therefore be hidden from the attacker

1.3.1.3
identifier
physical or logical entity used by a user during authorisation (e.g. numeric code, proximity token, biometric characteristic, etc.)

NOTE The identifier does not necessarily uniquely identify a person.

1.3.2 Abbreviations

This document uses the abbreviations of EN 50131-1:2006 and the following.

ATE	Alarm Transmission Equipment

NOTE The abbreviation ATS (Alarm Transmission System) given in EN 50131-1:2006 is also used for the rating of ATS. In this instance it is followed by a number (e.g. ATS 4). Refer to *8.6*.

2 Brief guide on How to read the standard

2.1 Conventions used in standards (CENELEC Internal Regulations)

When reading standards, it is important to understand the relationship of the sections of the standard and to apply certain conventions. Ignoring these conventions may result in the reader misunderstanding the standard. For full details refer to “CEN/CENELEC Internal Regulations – Part 3: Rules for the structure and drafting of CEN/CENELEC Publications”.

In particular:

- The “Scope” describes the limitations of the standard. In the case of EN 50131-1:2006 for example it states that it does not include “requirements for exterior I&HAS”.
- A term defined in the list of definitions has only the meaning that is written in the list of definitions.
- Normative items are requirements. Informative items are advisory. Any item written as a note is informative.
- Things described as mandatory or written using the word “shall” are required by the standard. Things described as optional or written using the word “may” are not required by the standard but can be included by the I&HAS. If they are included in the I&HAS then they shall comply with any associated requirements.

The terms Permitted (P), Not Permitted (NP) and Not Applicable (NA) appear in the standard. “Permitted” means that the I&HAS may perform the action or include the function. “Not Permitted” means that for the given case the I&HAS shall not perform the action or include the function. “Not Applicable” means that the case should not occur. For example the I&HAS cannot indicate a set status when it is unset (*Table 9*).

In the remainder of this document the section numbering matches the clauses of EN 50131-1:2006.

Only interpreted clauses are given and therefore the numbers are not continuous.

3 Definitions

3.1.9 alarm notification

The use of the term “notification” within the standard also includes the use of warning devices and alarm transmission equipment with the objective of initiating an intervention by a response provider.

3.1.11 alarm transmission system (ATS)

This is one or more sub-systems used to transfer information about the I&HAS to one or more ARC. The standard is primarily concerned with the transfer of information about intrusion and hold-up alarms, fault and tamper conditions. The alarm transmission equipment (ATE) located at the ARC does not form part of the I&HAS. The ATS does not include transmission between components of the I&HAS with the exception of any interface between the CIE and the ATE.

3.1.12 **alert indication**

This only indicates that further indications are available. It gives no information specific to the event that causes it. It also does not imply that any condition causing the “further indication” is still present (see *8.5.3*).

NOTE 2 in *Subclause 8.5.1* clarifies that the alert indication may be suppressed in certain cases such as following triggering of a hold-up device.

The alert indication may have several forms. For example it could be audible and visual until acknowledged by a user and then become visual only, or the audible indication may be present if user response is required more urgently.

3.1.33 **interconnection**

An interconnection is a means of transferring information between I&HAS components. Interconnection does not refer to the system used to transfer information to the ARC (i.e. the ATS). The standard refers to three types of interconnection:

a) specific wired interconnection – an interconnection used solely for the transfer of information used by the I&HAS;

b) non-specific wired interconnection – an interconnection used by the I&HAS but also carrying information for other applications (i.e. any other system, e.g. a lighting control system or another I&HAS);

c) wire-free interconnection – an interconnection that employs a method of spatial transmission (e.g. radio frequency).

3.1.42 **masked**

A movement detector is “masked” when materials are accidentally or deliberately used to prevent the sensor from detecting movement in the intended detection area. This involves interference with the movement detector typically by the use of card, boxes or plates, close to the detector or spray over the surface of the sensor.

This differs from “significant reduction of range” in which the detector is still operational but detection is no longer possible over the whole of the intended detection area because of obstacles placed accidentally or deliberately within that area. The detector has not been directly interfered with but an intruder may move within the intended detection area without being detected.

“Masking” occurs close to the detector (e.g. within 50 mm) whereas “reduction of range” refers to a distance of several metres.

3.1.43 **message**

Each message carried by an interconnection may have a different meaning which is distinguished by the use of “function data”. The “function data” tells the receiver what the message means and provides the status or parameter values. The message may also include “identification” so that the source may be determined and other information for directing the message to a specific device and to determine whether it has been corrupted.

3.1.46 **non-specific wired interconnection**

Refer to the interpretation of *3.1.33* “interconnection” given above.

3.1.48 **notification**

The use of the term “notification” within the standard also includes the use of warning devices and alarm transmission equipment with the objective of initiating an intervention by a response provider.

3.1.49 **operator**

Whereas “user” (refer to *3.1.80*) is a person making use of an I&HAS at any access level (as implied by the definitions of hold-up alarm system, *3.1.28*, and indication, *3.1.31*) an operator is a user at access level 2, 3 or (less likely) 4.

3.1.53 **periodic communication**

“Periodic” means that in a pre-defined period at least one message should occur to ensure the interconnection is operational. A special message may be used to fulfil the timing but any message that is acceptable to the system is suitable.

3.1.61 **significant reduction of range**

Refer to the interpretation of *3.1.42* “masked” given above.

3.1.63 **specific wired interconnection**

Refer to the interpretation of *3.1.33* “interconnection” given above.

3.1.67 **supplementary prime power source**

This is a source of power that is similar to the prime power source and does not form part of the I&HAS but is used as an alternative supply for the supervised premises. An example would be a standby generator that automatically starts when the utility company’s AC mains supply is cut.

3.1.80 **user**

Refer to the interpretation of *3.1.49* “operator” given above.

3.1.83 **wire-free interconnection**

Refer to the interpretation of *3.1.33* “interconnection” given above.

3.1.84 **zone**

Although a zone could contain just one detector, the term “zone” is not synonymous with one detector input. A zone is any defined part of the supervised premises. It may include any number of detectors. Examples of zones include: a storey of a building; the perimeter of a building; an outbuilding.

6 Security grading

The security grade should be chosen following a risk assessment. The methods of performing a risk assessment are beyond the scope of EN 50131-1:2006. The examples given in the note are simply guidance. Subclauses 7.1 and 7.2 of CLC/TS 50131-7:2008 describe aspects of risk assessment.

NOTE CEN Technical Committee TC 325 has drafted standards in the CEN/TS 14383 series that guide readers in the subject of risk assessment and grade selection.

7 Environmental classification

EN 50131-1:2006 uses the classification of environmental class given in EN 50130-5:1998. The latter describes how to test components and is for use by manufacturers. Installers and specifiers should select components with an environmental class suitable for the intended installation location. One I&HAS could include components of differing environmental classes. There is no relationship between environmental class and security grade.

8 Functional requirements

8.1 Detection

The requirements related to timing and signal durations are interpreted in *8.9*.

8.1.3 Tamper detection

Tampering may be detected in two ways: by components that include tamper detection as specified in *8.7.2* and as a result of the monitoring of interconnection requirements as specified in *8.8*.

8.1.4 Fault detection

EN 50131-1:2006 does not specify how component faults are detected. Those requirements are given in the component standards.

8.2 Masking and range reduction (also *8.4.5 and 8.4.6*)

Masking and movement detector range reduction detection is required at the grades specified. The methods of passing signals or messages indicating these conditions to components of the system are not specified. *Subclauses 8.4.5* and *8.4.6* permit the processing of these conditions to be performed as if they were either intruder or fault signals or messages. It is permitted to process these conditions as intruder or fault dependent on other circumstances (but this should be clearly described to users and the ARC). For example, a masking detection could be processed as if a fault when unset and as if an intruder when set.

The standard does not prevent additional responses (provided these do not interfere with the mandatory requirements). Examples could include procedures involving “walk tests”, etc.

8.3.1 Access levels

Subclause 8.3.1 and *Table 2* describe the four access levels and give requirements for relationships between them and the functions accessible to them. One important point is that it does not say that an I&HAS has four types of user. The access levels described are simply categorisations. When a function is shown in *Table 2* as “permitted” it does not mean that all users have access to that functionality. The access to a function can be restricted by user type (e.g. a cleaner may not be able to override a condition that prevents setting) or by restriction of a user to part of the IAS (e.g. the store man may be prevented from unsetting a high risk area). Access can also be restricted by circumstances (e.g. a guard patrol may be prevented from unsetting unless an alarm has occurred).

There are other requirements that restrict the access to functions of the system according to the authority granted to the user at that time. For example, *Sublause 8.5* refers to the indications available to different users. *Subclause 8.3.1* also contains many requirements about the access to functions.

In practice, an I&HAS may have many different types of user (e.g. the owner, the installer, a guard, a cleaner, etc.) but to simplify the description the standard uses four categories. The access level relates to the ability of a user at a specific time, however:

- the access levels are not hierarchical (e.g. access level 4 is not superior to access level 2);
- users may have authority to gain access at different access levels.

For example, “level 2 key or codes shall not provide access at level 3 or 4” does not mean that a user cannot have an access level 3 key or code that also permits them access at access level 2.

Access level 1 describes the operational restrictions applicable to a person who does not have any method of gaining authorisation (e.g. a shop customer or an intruder) or a person who has not currently identified himself to the system (e.g. the owner of a system before entering an identity code).

Access level 2 describes the operational restrictions applicable to a typical operator after authorisation by the I&HAS. They may set and unset the system but do not have any authority to change the way it works.

Access level 3 refers to the operational restrictions applicable to a person who has been recognised by the I&HAS and granted a higher level of authority. They should have some technical knowledge or in some way manage the use of the system and should have received sufficient training for this. Typically, this is the installer or maintainer of a system but could also be a manager of the system with the authority to control other users. Only access level 3 users have the authority to open the component housings without causing a tamper condition.

There may be access level 4 users. These are people who can significantly alter the operation of the system beyond simply changing configurable variables. Typically, this would be via a software upgrade of the CIE. The implication of this access level is that a special method exists to achieve this. It is not simply the replacement of a memory device by an installer because that could be performed by a user at access level 3.

Other requirements of the standard may restrict the ability of users according to security grade or circumstances. The requirements modifying *Table 2* are listed here:

Subclause 8.3.6 / Table 5	At higher grades some conditions cannot be overridden by users at access level 2
Subclause 8.3.9 / Table 6	At higher grades some conditions cannot be restored by users at access level 2
Subclause 8.3.11	Isolation is not permitted by access level 2 users on grades 3 and 4 I&HAS

8.3.2 Authorisation

Examples of “logical key” include a user code entered on a keypad, and an electronic card used with a proximity reader or a magnetic stripe card.

The authorisation stated in *8.3.2* applies in all cases when a user requires access to functions (whether it is for unsetting, viewing the event record, or changing site specific data, etc.). In each grade the number of differs can be the same for access levels 2, 3 and 4. *Subclause 8.3.4* permits all I&HAS to be set (but only set) using the number of differs of grade 1.

EN 50131-1:2006 requires that the functions listed in *Table 2* are restricted by use of authorisation techniques. There are three aspects to the authorisation:

1. the use of authorisation codes or equivalent means (as per *8.3.2*);
2. access to functions for users at access level 3 requires an access level 2 user to grant them permission;
3. access to functions for users at access level 4 requires access levels 2 and 3 users to grant them permission.

The standard does not specify when, or for how long permission is granted. Permission may be required on each attempt at authorisation, may be granted for a certain duration (e.g. for the next 8 hours), or for an indefinite period. This is however a standard for systems. It does not give procedural requirements. Therefore, the requirement is that the I&HAS is an integral part of the granting of permission (i.e. written authorisation is not sufficient).

Individuals use functions at certain access levels. Access levels are not attributes of the person. All users are considered to be using the system at access level 1 at certain times and, according to the authority granted to them, can then operate the system using alternative access levels. How this is achieved is not stated.

8.3.8.2 Unsetting

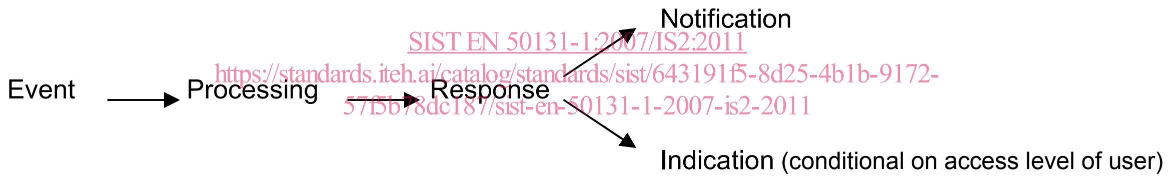
When this clause applies, remote notification (i.e. the transmission of messages to an ARC) is, depending on the sequence of events, possibly delayed by 30 s. If intrusion detection occurs after the end of the unsetting period (entry timer) but before the end of the 30 s delay, then the 30 s delay may be cancelled and ATS messages sent immediately.

8.3.9 Restoring

In *Table 6*, “Access levels 2 or 3” means that either access level may restore the I&HAS in accordance with the requirements of *8.3.9*. “Access level 2” means that the I&HAS should allow for one or more access level 2 users to restore the condition. Note that it is not mandatory to permit all access level 2 (or 3) users to have the ability to restore the I&HAS.

Subclauses 8.4, 8.5 and *8.6* - Processing, indications and notification

The three subjects of processing, indications and notification are very closely linked. Although the standard divides these items into three clauses they are related. For example, the requirements for “what” is notified are in *8.4, Processing*, rather than in *8.6* (which describes forms of notification). This interpretation views the system as being “event-driven”. That means that the processing begins as the result of an event and the outputs (notification and indication) are the result of the processing.



The requirements are detailed in the standard by the use of *Tables 7, 8, 9* and *10*. Figure 1 shows the relationship between these tables and the CIE. For simplicity of explanation this interpretation assumes that the processing functions of the CIE are centralised (this is the typical case) but distributed processing is permitted by the standard.