SLOVENSKI STANDARD
SIST EN 50131-3:2009

01-oktober-2009

Nadomešča:
SIST EN 50131-6:1999
SIST-TS CLC/TS 50131-3:2004

Alarmni sistemi - Sistemi za javljanje vloma in ropa - 3. del: Kontrolna in indikacijska oprema

Alarm systems - Intrusion and hold-up systems -- Part 3: Control and indicating equipment

Alarmanlagen - Einbruch- und Überfallmeldeanlagen -- Teil 3: Melderzentrale

Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les hold-up -- Partie 3: Equipement de contrôle et de signalisation

Ta slovenski standard je istoveten z: **EN 50131-3:2009**

ICS:

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

SIST EN 50131-3:2009 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50131-3

March 2009

ICS 13.310

Supersedes CLC/TS 50131-3:2003

English version

Alarm systems - Intrusion and hold-up systems - Part 3: Control and indicating equipment

Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les hold-up - Partie 3: Equipement de contrôle et de signalisation

Alarmanlagen - Einbruch- und Überfallmeldeanlagen - Teil 3: Melderzentrale

This European Standard was approved by CENELEC on 2009-02-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 50131-3:2009 E

Foreword

This European Standard 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 as EN 50131-3 on 2009-02-01.

This European Standard supersedes CLC/TS 50131-3:2003.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2010-02-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2012-02-01

EN 50131 will consist of the following parts, under the general title *"Alarm systems – Intrusion and hold-up systems"*:

Part 1	System requirements
Part 2-2	Intrusion detectors - Passive infrared detectors
Part 2-3	Requirements for microwave detectors
Part 2-4	Requirements for combined passive infrared and microwave detectors
Part 2-5	Requirements for combined passive infrared and ultrasonic detectors
Part 2-6	Opening contacts (magnetic)
Part 2-7-1	Intrusion detectors – Glass break detectors (acoustic)
Part 2-7-2	Intrusion detectors – Glass break detectors (passive)
Part 2-7-3	Intrusion detectors – Glass break detectors (active)
Part 3	Control and indicating equipment
Part 4	Warning devices
Part 5-3	Requirements for interconnections equipment using radio frequency techniques
Part 6	Power supplies
Part 7	Application guidelines
Part 8	Security fog device/systems

Introduction

This document is based on the revision of the Technical Specification originally edited by the CENELEC TC 79/WG 3, then submitted to the formal vote and finally approved by CENELEC as CLC/TS 50131-3 on 2003-05-19.

The work done by WG 3 is the result of the comments raised by the National Committees, members of CENELEC and of harmonisation with EN 50131-1:2006 + A1:2009 prepared by TC 79/WG 1; for this reason the reader has to take into account EN 50131-1:2006 + A1:2009, which has to be considered as a “master” document for this EN 50131-3.

Repetition of definitions and requirements contained in EN 50131-1 have been eliminated from this EN 50131-3, in order to minimise conflict in the event of changes to EN 50131-1, except where repetition is deemed essential for the clarity of this document.

Reference has been included to various implications arising from the detector standards. Full detail of the interconnection requirements could be the subject of a future standard.

A number of requirements are contained in this standard for which a formal test procedure can only be written by defining (and hence restricting) the technology by which the requirement is achieved. Accordingly, it has been recognised that such functions can be tested only by agreement between manufacturer and test house, according to documented information relating to how the required functionality has been achieved.

A table to cross reference EN 50131-1 requirements against this EN 50131-3 and tests has been included in Annex D.

Contents

1 Scope

This standard specifies the requirements, performance criteria and testing procedures for control and indicating equipment (CIE) intended for use in intrusion and hold-up alarm systems (I&HAS) installed in buildings. This document also applies to CIE to be used in IAS or HAS.

The CIE may incorporate processing functions of other I&HAS components or its processing requirements may be distributed among such components.

This standard specifies the requirements for CIE installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. These requirements also apply to ACE that are installed inside or outside of the supervised premises and mounted in indoor or outdoor environments.

Where CIE shares means of detection, interconnection, control, communication, processing and/or power supplies with other applications, these requirements apply to I&HAS functions only.

This standard specifies performance requirements for CIE at each of the four security grades identified in the European Standard EN 50131-1, *"Alarm Systems – Intrusion and hold-up systems – System requirements"*. Requirements are also specified for four environmental classes covering applications for indoor and outdoor locations.

This standard includes mandatory functions, which shall be provided on all CIE for the appropriate security grade, as well as optional functions that may additionally be provided.

This standard does not deal with requirements for compliance with EU regulatory Directives, such as the EMC Directive, Low Voltage Directive, etc. except in that it specifies the equipment operating conditions for EMC susceptibility testing as required by EN 50130-4.

NOTE In this standard reference to the term "I&HAS" is used throughout, except where there is specific need to differentiate between the IAS and HAS portions of a system. The term is intended to include IAS and HAS when such systems are installed separately.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Publication	Year	Title
EN 50130-4	1995	Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
EN 50130-5	1998	Alarm systems - Part 5: Environmental test methods
EN 50131-1 A1	2006 2009	Alarm systems - Intrusion and hold-up systems - Part 1: System requirements
EN 50131-5-3	2005	Alarm systems - Intrusion systems - Part 5-3: Requirements for interconnections equipment using radio frequency techniques
EN 50131-6	2008	Alarm systems - Intrusion and hold-up systems - Part 6: Power supplies
EN 60068-1	1994	Environmental testing - Part 1: General and guidance (IEC 60068-1:1988 + corr. Oct. 1988 + A1:1992)
EN 60068-2-75	1997	Environmental testing - Part 2-75: Tests - Test Eh: Hammer tests (IEC 60068-2-75:1997)
EN 60529		Degrees of protection provided by enclosures (IP code) (IEC 60529)
EN 62262		Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code) (IEC 62262)

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply in addition to those given in EN 50131-1:2006.

3.1.1
acknowledge
action of a user to accept an indication

3.1.2
alarm point
one or more detector(s) providing a common signal or message, at the CIE or at the ACE for the purpose of indication or processing

3.1.3
alarm signal or message
signal or message generated by an alarm point

3.1.4
biometric key
use of biometric characteristic by an authorized user to gain access to restricted functions or parts of a CIE (EXAMPLE: finger print or iris recognition)

3.1.5
conditioning
exposure of the Equipment Under Test (EUT) to environmental conditions in order to determine the effect of such conditions on the EUT

3.1.6
detector
device designed to generate an alarm signal or message in response to the sensing of an abnormal condition indicating the presence of a hazard

3.1.7
digital key
portable device containing digitally coded information used by an authorized user to gain access to restricted functions or parts of a CIE (EXAMPLE: magnetic card, electronic token or similar)

3.1.8
entry route facility
means to ignore signals or messages from specified detectors during unsetting for a specified time period

3.1.9
entry time
time permitted for unsetting procedure where entry route is used

3.1.10
exit route facility
means to ignore signals or messages from specified detectors during setting for a specified period

3.1.11
external power source (EPS)
energy supply external to the I&HAS which may be non-continuous (EXAMPLE: main power supply)

NOTE For Type A and Type B PS only. The EPS is derived as described in EN 50131-6.

3.1.12
fail to set
condition when defined setting procedure has not been completed within a specific time so that I&HAS is left in the “setting mode”

3.1.13
false acceptance rate (FAR)
proportion of biometric verification transactions with wrongful claims of identity that are incorrectly accepted

3.1.14
false rejection rate (FRR)
proportion of biometric verification transactions with truthful claims of identity that are incorrectly denied

3.1.15
interaction
any deliberate operation or act by the user to control or vary the function of the I&HAS

3.1.16
intrusion
entry into the supervised premises by an unauthorised person(s)

3.1.17
logical key
logical information used by an authorized user to gain access to restricted functions or parts of a CIE (EXAMPLE: PIN code, digital key, biometric key)

3.1.18
mechanical key
implement relying solely on physical shape to determine its uniqueness, used by an authorized user to gain access to restricted functions or parts of a CIE

3.1.19
non-I&HAS interface
device external to the I&HAS used to carry out some or all ACE functions (EXAMPLES: Computer, PDA)

3.1.20
operating mode
set, unset, setting and unsetting are the four operating modes

3.1.21
open by normal means
opening of the equipment housing by the procedure defined by the manufacturer

3.1.22
Personal Identification Number (PIN Code)
code used by an authorised user to gain access to restricted functions or parts of a CIE (example, numeric or alphanumeric)

3.1.23
soak
an attribute of an alarm point such that signals or messages that normally create notifications are prevented from doing so, but continue to be recorded in the event log

3.1.24
storage device (SD)
device which stores energy (EXAMPLE: a battery)

3.1.25
Supervised Premises Transceiver (SPT)
this document uses the definition of EN 50131-1:2006

3.1.26
test condition
condition of an alarm system in which the normal functions are modified for test purposes

3.1.27
user input
command generated by a deliberate user action

3.1.28
user input device
device used for user input (EXAMPLES: ACE, physical lock with electrical contacts)

3.2 Abbreviations

For the purposes of this European Standard the following abbreviations are used:

ACE Ancillary control equipment
APS Alternative power source
ARC Alarm receiving centre
ATS Alarm transmission system
CIE Control and indicating equipment
EPS External power source
EUT Equipment under test
FAR False acceptance rate
FRR False rejection rate
HAS Hold-up alarm system
IAS Intrusion alarm system
I&HAS Intrusion and hold-up alarm system
PDA Personal digital assistant
PIN Personal identification number
PS Power supply
SD Storage device
SPT Supervised premises transceiver
WD Warning device

4 Equipment attributes

4.1 General

CIE shall include attributes for the reception of signals and/or messages, processing the information, notification and indication as appropriate. The detailed requirements are provided in Clause 8.

NOTE If a function is provided that is optional for a particular grade and a claim of compliance is made, it shall meet the applicable requirements for the grade for which compliance is claimed (if any are given). If there are no specifications for the function at the grade in question, the requirements for any higher grade (as identified by the manufacturer) shall apply.

Compliance with this standard shall be demonstrated by assessment of Clause 4 through to Clause 10 and the application of the tests of Clause 11.

Annex D provides a cross reference between the requirements of EN 50131-1 and the requirements and tests of this standard.

4.2 Functionality

Functions additional to the mandatory functions specified in this standard may be included in I&HAS providing they do not influence the correct operation of the mandatory functions.

Where provided, these additional functions shall not affect compliance with the requirements of this standard, except as permitted by EN 50131-1:2006, 8.3.13.

It is permitted for the CIE to include functionality for special purposes that would render the I&HAS non-compliant with EN 50131-1. The manufacturer's documentation shall include a warning to this effect.

If use of a function(s) or combination of functions within the CIE would result in the installed I&HAS not being compliant with EN 50131-1 or being compliant at a lower security grade (EXAMPLE: function(s) reducing the security of the I&HAS) the manufacturer shall, either:

a) detail the configuration(s) which are compliant with EN 50131-1;

or

b) detail the function(s) or combination of functions that would result in the installed I&HAS not being compliant with EN 50131-1.

The manufacturer shall document the fact that compliance labelling should be removed or adjusted if non-compliant configurations are selected.

5 CIE construction

The CIE may be in a single housing or be distributed in multiple housings and may be combined with other I&HAS components.

Provision shall be made to allow adequate fixing of the housing to the mounting surface.

Use of equipment not part of the I&HAS may be used to carry out ACE functions (EXAMPLE: computer, PDA) if the conditions specified in Annex C are met.

6 Security grade

The CIE and ACE shall be declared to comply with one of four security grades (with grade 1 being the lowest and grade 4 being the highest) and shall meet all the requirements of that grade.

The requirements for the performance of the CIE will vary depending upon its grade. Any testing will be carried out according to the grade declared in the CIE documentation and marking.

7 Environmental performance

7.1 Requirements

CIE and ACE shall be suitable for use in at least one of the environmental classes defined in EN 50131-1.

When the requirements of the four environmental classes are inadequate, due to the extreme conditions experienced in certain geographic locations, special national conditions are given in EN 50131-1:2006, Annex A.

7.2 Environmental and EMC tests

EN 50130-4 specifies EMC susceptibility tests relevant to I&HAS components. The operating conditions for these tests are specified in Table 32 of this standard.

EN 50130-5 describes environmental test methods relevant to I&HAS components. The tests applicable are specified in Table 32 of this standard.

NOTE Other environmental aspects, covered by EU Regulatory Directives, are outside the scope of this standard.

8 Functional requirements

8.1 Inputs

Depending on the grade of the CIE and ACE, means shall be provided to receive signals or messages from detectors, hold-up trigger devices and information from user input devices as specified in the following subclauses.

NOTE 1 This standard does not specify details of interconnections or the format of these signals or messages. Details of possible means of transfer of the information are included in some of the component standards within the EN 50131 series.

NOTE 2 Some system components may require up to 180 s to initialise before normal functionality is available (EXAMPLE: detectors).

8.1.1 Intruder detection

The CIE shall provide the means to receive signals or messages from intruder detectors.

8.1.2 Hold-up device

When a CIE provides hold-up facilities, means shall be provided to receive signals or messages from hold-up devices.

8.1.3 Tamper

The CIE shall provide the means to receive tamper signals or messages.

8.1.4 Fault

Dependent on the grade, CIE shall include means to recognize the fault conditions as specified in EN 50131-1:2006, Table 1 and in addition those faults shown in Table 1.

Table 1 - Recognition of additional fault conditions

Faults	Grade 1	Grade 2	Grade 3	Grade 4
Battery change required [a]	M	M	M	M
Power output fault b [b]	Op	Op	M	M
Monitoring of processing	Op	Op	M	M
M = Mandatory Op = Optional [a] = applies to type “C” PS only as defined in EN 50131-6. [b] = as in EN 50131-6:2008, 4.2.5.				

8.1.5 User input

The CIE shall provide the means to receive information from user input devices (EXAMPLE: a keypad or switch).

8.1.6 Masking

The CIE shall provide the means to receive masking signals or messages, according to grade.

The CIE shall process masking signals or messages when the system is set and optionally when unset.

8.1.7 Movement detector range reduction

The CIE shall provide the means used to receive reduction of range signals or messages, according to grade.

NOTE The means to convey movement detector reduction of range signals or messages from detectors may not permit differentiation from masking events. See detector standards.

8.1.8 Non-I&HAS inputs

When a CIE receives signals or messages or other information not necessary to meet the requirements of this standard (EXAMPLE: monitoring of non-I&HAS equipment), this shall not affect the ability of the CIE to meet the requirements of this standard.

8.2 Outputs

Notification output requirements are detailed in 8.6

The CIE may need to provide output signals or messages to interface with other I&HAS components, as required by other relevant component standards. The installation documentation shall identify which configurations are available.

EXAMPLES:

a) indication enable for detector or other component;

b) set/unset status information for detector, security fog device, etc.;

c) to trigger audible or visual alarm confirmation equipment;

d) to trigger security fog devices, etc.;

e) to enable functional test mode of detector;

f) to trigger remote self-test of detector or other component;

g) to restore detectors or other devices.

NOTE If the restore involves removal of power from detectors, up to 180 s should be allowed for the detector to resume normal operation (see EN 50131-2-series).

Output signals or messages may additionally be provided to interface to equipment outside of the I&HAS (EXAMPLE: lighting).

8.3 Operation

The CIE shall provide the means necessary to enable authorized users to access the functions of the CIE. Access to these functions shall be restricted by access levels and corresponding authorisations according to 8.3.1 and 8.3.2 (EXAMPLE: by using a keypad or lock).

8.3.1 Access levels

Access to the functions of a CIE shall be restricted according to the requirements of EN 50131-1:2006, 8.3.1. If the CIE includes security functions additional to those identified in EN 50131-1:2006, Table 2 the access levels necessary to operate those functions shall be specified by the manufacturer. Access levels for any non-security functions shall be specified in the manufacturer's documentation.

Access at level 3 shall be authorized by access level 2 such that:

a) access remains authorized until manually removed,

or

b) access requires authorization for each occasion it is used.

Access at level 4 shall be authorized by access level 2 and 3 for each occasion it is used.

If level 3 access is granted without level 2 authorisation, as permitted by EN 50131-1:2006, 8.3.1, the internal warning device shall be time limited, either to a fixed time quoted by the manufacturer or until silenced by the level 3 user.