



SLOVENSKI STANDARD
SIST EN 50131-1:2007/A1:2009
01-oktober-2009

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

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

Alarmanlagen - Einbruch- und Überfallmeldeanlagen -- Teil 1: Systemanforderungen

Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les hold-up -- Partie 1:
Exigences système

(standards.iteh.ai)

Ta slovenski standard je istoveten z: EN 50131-1:2006/A1:2009

<https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009>

ICS:

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

SIST EN 50131-1:2007/A1:2009 **en,fr,de**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 50131-1:2007/A1:2009](https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009)

<https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50131-1/A1

May 2009

ICS 13.310

English version

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

Systèmes d'alarme -
Systèmes d'alarme
contre l'intrusion et les hold-up -
Partie 1: Exigences système

Alarmanlagen -
Einbruch- und Überfallmeldeanlagen -
Teil 1: Systemanforderungen

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This amendment A1 modifies the European Standard EN 50131-1:2006; it was approved by CENELEC on 2009-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment 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 amendment 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

Foreword

This amendment to 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 as amendment A1 to EN 50131-1:2006 on 2009-05-01.

The following dates were fixed:

- latest date by which the amendment has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2010-05-01
- latest date by which the national standards conflicting with the amendment have to be withdrawn (dow) 2012-05-01

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 50131-1:2007/A1:2009](https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009)

<https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009>

1 Scope

In the 3rd paragraph, last sentence, **replace** 'operation' by 'functioning'.

In the 4th paragraph, 2nd sentence, **replace** 'operate' by 'function'.

2 Normative references

Replace the 5th reference by the following:

EN 50136-1-1 1998 Alarm systems – Alarm transmission systems and equipment –
Part 1-1: General requirements for alarm transmission systems

Replace the last reference by the following:

EN 61000-6-3 2007 Electromagnetic compatibility (EMC) – Part 6-3: Generic standards –
Emission standard for residential, commercial and light-industrial
environments (IEC 61000-6-3:2006)

3 Definitions and abbreviations

3.1 Definitions

Replace definition 3.1.11 by the following:

3.1.11

alarm transmission system

equipment and network used to transfer information from one or more I&HAS to one or more alarm receiving centres

NOTE Alarm transmission systems exclude local direct connections, i.e. interconnections between parts of an I&HAS which do not require an interface to transform the I&HAS information into a form suitable for transmission.

In definition 3.1.13, **replace** 'system' by 'I&HAS'.

Replace definition 3.1.16 by the following:

3.1.16

authorisation

permission to gain access to the various control functions of an I&HAS

In definition 3.1.17, **replace** 'physical' by 'mechanical'.

In definition 3.1.19, **replace** 'operating' by 'functioning'.

Replace definition 3.1.24 by the following:

3.1.24

event

condition arising from the operation of an I&HAS e.g. setting/unsetting or the functioning of an I&HAS, e.g. alarm signal or message

Replace definition 3.1.25 by the following:

3.1.25

event recording

storage of events arising from the operation e.g. setting or unsetting of an I&HAS or the functioning of an I&HAS for future analysis

Replace definition 3.1.32 by the following:

3.1.32

inhibit

status of a part of an I&HAS in which an alarm condition cannot be notified, such status remaining until the I&HAS or part thereof passes from the set to the unset status

In definition 3.1.33, **replace** 'transmitted' by 'communicated'.

In definition 3.1.41, **replace** 'manually cancelled' by 'cancelled by a user'.

In definition 3.1.44, **replace** 'operation' by 'functioning'.

Replace definition 3.1.50 by the following:

3.1.50

override

intervention, by a user, to permit setting when an I&HAS is not in a normal condition

In definition 3.1.51, **delete** 'a zone of' [SIST EN 50131-1:2007/A1:2009](https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009)

In definition 3.1.54, **add** 'or any part thereof' to end of the definition.

In definition 3.1.55, **replace** 'operating' by 'working'.

Replace definition 3.1.65 by the following:

3.1.65

subsystem

part of an I&HAS located in a clearly defined area of the supervised premises capable of functioning independently of other parts of the I&HAS

Replace definitions 3.1.68 and 3.1.69 by the following:

3.1.68

system components

individual items of equipment which constitute an I&HAS when configured together

3.1.69

supervised premises transceiver

equipment at the supervised premises, including the interface to the I&HAS and the interface to the alarm transmission network

Replace definition 3.1.79 by the following:

3.1.79

unset

status of an I&HAS or part thereof in which an intruder and/or hold-up alarm condition cannot be notified

Replace definition 3.1.82 by the following:

3.1.82

warning device

device that gives an audible alarm in response to a notification

NOTE 1 A warning device may also provide alert indications.

NOTE 2 Such indications should be easily distinguishable from those related to the notification of an alarm condition.

Replace definition 3.1.84 by the following:

3.1.84

zone

area of the supervised premises where an intrusion, attempted intrusion, or the triggering of a hold-up device may be detected by an I&HAS

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

3.2 Abbreviations

Add the following after the last abbreviation:

SPT - supervised premises transceiver
<https://standards.iteh.ai/catalog/standards/sist/ec0d99b3-4481-49cf-b25c-b725057d8a30/sist-en-50131-1-2007-a1-2009>

6 Security grading

Add the following paragraph before NOTE 1:

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 grade in question, the requirements for any higher grade (as identified by the manufacturer) shall apply.

8 Functional requirements

Table 1 – Faults

Replace ‘Other faults’ by ‘Other faults’^b.

Add the following after table footnote ^a:

^b Other faults as specified in components standards.

8.3.1 Access levels

Replace the paragraph after the note by the following:

Access at level 3 shall be prevented unless either

- a) access has been permitted by a user with level 2 access, or
- b) in grades 1, 2 and 3 I&HAS, access at level 3 may be provided without authorisation by a level 2 user providing
 - 1) the user to be given access at level 3 is at the supervised premises and accesses the CIE locally, and
 - 2) the I&HAS is unset, and
 - 3) in grade 1 I&HAS notification is given by a warning device when the access at level 3 is granted,
 - 4) in grades 2 and 3 notification is given by a warning device and remotely, i.e. by an ATS, when the access at level 3 is granted.

Access at level 4 shall be prevented until access has been authorized by a user with level 2 access and by a user with level 3 access.

Table 2 – Levels of access

Replace by the following table:

Functions	Access levels			
	1	2	3 ^a	4 ^b
Setting	NP ^e	P	P	NP
Unsetting	NP	P	P	NP
Restore I&HAS	NP	P	P	NP
Verify I&HAS functions	NP	P	P	NP
Interrogate event log	NP	P	P	NP
Inhibit/isolate/override ^c	NP	P	P	NP
Add/change individual authorisation codes	NP	P ^d	P ^d	P ^d
Add/delete level 2 users & codes	NP	P	P	NP
Add/change site specific data	NP	NP	P	NP
Change/replace basic programme	NP	NP	NP	P
Key: P = Permitted NP = Not permitted.				
NOTE 1 The inclusion of the functions shown in this table does not imply that provision of such functions in I&HAS is mandatory.				
NOTE 2 This table specifies access levels for each function; further conditions, applicable to each function, are specified elsewhere in this standard.				
NOTE 3 Requirements relating to user access are not intended to restrict methods of initialisation of user access at the time that the CIE is first powered-up (e.g. the existence of default or single use access codes).				
^a Only when authorised at level 2. ^b Only when authorised at level 2 and level 3. ^c Depending on the grade. ^d An individual is only permitted to change his/her own user code. ^e Permitted only in grade 1, see 8.3.4.				

Table 3 – Authorisation code requirements

Replace twice 'Physical' by 'Mechanical'.

8.3.4 Setting

Add the following after the last sentence:

In grade 1 I&HAS users at access level 1 may start setting (e.g. by a pushbutton) provided that this setting process may also be cancelled before completion by a user at access level 1 and means to start setting is located inside the supervised premises.

NOTE Starting of setting of the system by users at access level 1 should be used with caution.

Table 5 – Overriding of prevention of setting conditions

Replace 'ATE' by 'ATS' in table footnote ^b.

8.3.8.2 Unsetting – as specified in 8.3.7 b)

Replace the 3rd paragraph by the following:

When an intruder alarm condition occurs during the unsetting procedure the alarm condition shall be notified by a warning device or indicated. When remote notification is included in the intruder alarm system, the alarm condition shall not be remotely notified until the indicator or warning device has functioned for a minimum of 30 s and the entry timer has expired.

Renumber the two existing notes into NOTE 1 and NOTE 2 respectively.

Table 6 – Restoring

Replace by the following table:

	Grade 1	Grade 2	Grade 3	Grade 4
Intruder	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
Hold-up	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
Tamper	Access level 2 or 3	Access level 2 or 3	Access level 3	Access level 3
Fault ^a	Access level 2 or 3	Access level 2 or 3	Access level 3	Access level 3
Prime power source fault	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
ATS fault	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
Masking	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
Significant reduction of range	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3	Access level 2 or 3
^a Except prime power source and ATS faults.				

8.3.10 Inhibit

Replace 'operation' by 'functioning'.

8.3.11 Isolate

In the 1st line, delete 'the operation of'.