SLOVENSKI STANDARD
SIST-TS CLC/TS 50131-3:2004

01-marec-2004

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

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

Alarmanlagen - Einbruchmeldeanlagen -- Teil 3: Melderzentrale

Systèmes d'alarme - Systèmes d'alarme intrusion -- Partie 3: Matériel de commande et d'affichage (Centrale d'alarme)

Ta slovenski standard je istoveten z: CLC/TS 50131-3:2003

ICS:

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

SIST-TS CLC/TS 50131-3:2004 **en**

TECHNICAL SPECIFICATION **CLC/TS 50131-3**

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION July 2003

ICS 13.310

English version

Alarm systems – Intrusion systems Part 3: Control and indicating equipment

Systèmes d'alarme– Systèmes d'alarme intrusion Partie 3: Matériel de commande et d'affichage (Centrale d'alarme)

Alarmanlagen – Einbruchmeldeanlagen Teil 3: Melderzentrale

This Technical Specification was approved by CENELEC on 2003-05-19.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Lithuania, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, 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. CLC/TS 50131-3:2003 E

Foreword

The text of this Technical Specification was prepared by the Technical Committee CENELEC TC 79, Alarm systems.

The text of the draft was submitted to the formal vote and was approved by CENELEC as CLC/TS 50131-3 on 2003-05-19.

The following date was fixed:

– latest date by which the existence of the CLC/TS has to be announced at national level (doa) 2003-10-30

_____

Contents

Annexes

Figures

Tables

1 Scope

This Technical Specification specifies the requirements, testing procedures security and environmental performance criteria for control and indicating equipment (CIE) intended for use in intrusion alarm system (IAS) and hold-up alarm systems (HAS) installed in buildings.

This Technical Specification specifies the requirements for CIE installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. These requirements also apply to the components of a CIE which are normally mounted on the external structure of a building. (EXAMPLE: Ancillary control equipment).

This Technical Specification specifies performance requirements for CIE but does not include requirements for design, planning, installation, operation or maintenance.

These requirements apply also to CIE sharing means of detection, interconnection, control, communication and power supplies with other applications.

Requirements are specified for CIE components where the relevant environment is classified. This classification describes the environment in which the CIE component may be expected to operate as designed. 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 Annex A of EN 50131-1. General environmental requirements for CIE components are described in Clause 7.

NOTE In this Technical Specification reference to the term "I&HAS" is used throughout the specification. The term is intended to include IAS and HAS when such systems are installed separately.

2 Normative references

This Technical Specification incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Technical Specification only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

Publication	Year	Title
EN 50130-4	1996	Alarm systems - Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
EN 50130-5	1998	Alarm systems - Environmental test methods
EN 50131-1	1997	Alarm systems - Intrusion systems - General requirements
EN 50131-6	1997	Alarm systems - Intrusion systems - Power supplies
EN 60065	2002	Audio, video and similar electronic apparatus – Safety requirements
EN 60529	1991	Specification for degrees of protection provided by enclosures (IP code)
EN 60950	2001	Information technology equipment – Safety – General requirements

IEC 60068-1 1988 Environmental testing – Part 1: General and guidance

3 Definitions and abbreviations

For the purposes of this specification, the following definitions and abbreviations apply.

3.1 Definitions

3.1.1
acknowledge
action of a user to accept an indication

3.1.2
action
any deliberate operation or act by the user

3.1.3
active period
period during which an alarm signal is present (See Annex A)

3.1.4
alarm
warning of the presence of a hazard to life, property or the environment

3.1.5
alarm condition
condition of an alarm system, or part thereof, which results from the response of the system to the presence of a hazard

3.1.6
alarm notification
passing of an alarm condition to warning devices and/or alarm transmission systems

3.1.7
alarm point
one or more detector(s) grouped together for the purpose of indication or processing

3.1.8
alarm receiving centre (ARC)
continuously manned remote centre to which the information concerning the state of one or more alarm systems is reported

3.1.9
alarm signal
signal generated by a detection device

3.1.10
alarm system
electrical installation which responds to the manual hold-up or automatic detection of the presence of a hazard

3.1.11
alarm transmission system (ATS)
system used to transfer information between one or more alarm systems and one or more alarm receiving centres

3.1.12
alternative power source (APS)
power source capable of powering the system for a predetermined time when a prime power source (PPS) is unavailable

3.1.13
ancillary control equipment (ACE)
equipment used for supplementary control purposes

3.1.14
conditioning
exposure of a specimen to environmental conditions in order to determine the effect of such conditions on the specimen

3.1.15
control and indicating equipment (CIE)
equipment for receiving, processing, controlling, indicating and initiating the onward transmission of information

3.1.16
detector
device designed to generate an alarm signal in response to the sensing of an abnormal conditions indicating the presence of a hazard

3.1.17
entry route facility
means to ignore signals or messages from specified detectors during unsetting for a specified time period

3.1.18
event recording
storage of events arising from the operation of the I&HAS components

3.1.19
exit route facility
means to ignore signals or messages from specified detectors during setting for a specified period

3.1.20
external power source (EPS)
energy supply external to the IAS which may be non-continuous, used as the prime power source in type A and type B power supply

3.1.21
fault condition
condition of an alarm system which prevents the system or parts thereof from functioning normally

3.1.22
fault signal or message
information generated due to the presence of a fault

3.1.23
hold-up alarm system (HAS)
alarm system providing the means for a user to deliberately generate a hold-up alarm condition

3.1.24
hold-up device
device which when triggered causes a hold-up alarm signal or message to be generated

3.1.25
indication
information (in audible, visual or any other form) provided to assist the user in the operation of an I&HAS

3.1.26
inhibit
status of a part of an alarm system in which an alarm condition cannot be notified, such status is cancelled when the CIE is unset (EXAMPLE: intruder alarm, tamper alarm, etc.)

3.1.27
interconnections
means by which signals and/or messages are transmitted between I&HAS components

3.1.28
intruder alarm condition
condition of an alarm system, or part thereof, which results from the response of the I&HAS to the presence of an intruder

3.1.29
intruder detector
device that generates an alarm condition in response to intrusion or attempted intrusion, or to deliberate action by the subscriber

3.1.30
intrusion
entry into the protected premises by an unauthorised person(s)

3.1.31
intrusion and hold-up alarm system (I&HAS)
combined intruder and hold-up alarm system

3.1.32
isolation
status of a part of an alarm system in which an alarm condition cannot be notified, such status remains until deliberately cancelled (EXAMPLE: intruder alarm, tamper alarm, etc)

3.1.33
logical key
code (EXAMPLE: numeric or alphabetic) entered by an authorized user to gain access to restricted functions or parts of a CIE

3.1.34
message
series of signals routed by a network which includes identification, functional data and the means to provide its own integrity, immunity and proper reception

3.1.35
monitoring
process of verifying that the interconnections and equipment are functioning correctly

3.1.36
normal condition
state of an I&HAS where no conditions exist which would prevent the setting of the system

3.1.37
notification
passing of alarm, tamper, hold up or fault conditions to warning devices and/or alarm transmission systems

3.1.38
operating mode
set, unset, setting and unsetting are the four operating modes

3.1.39
override
intervention by a user to permit setting when a fault condition exists

3.1.40
physical key
implement used by an authorised user to gain access to restricted functions or parts of a CIE (mechanical key, magnetic card, electronic token or similar)

3.1.41
power supply (PS)
device that stores, provides and also modifies or isolates (electrical) power for an alarm system or part thereof. The two basic parts of a PS are the Power Unit (PU) and the storage device (EXAMPLE: battery)

3.1.42
power unit (PU)
device that provides and also modifies or isolates (electrical) power for an IAS or part thereof, and for the storage device if required

3.1.43
prime power source (PPS)
power source used to support the I&HAS or part thereof under normal operating conditions

3.1.44
restore
procedure of cancelling an alarm, tamper, fault or other condition and returning the I&HAS to the previous condition

3.1.45
set
status of an alarm system or part thereof in which an alarm condition can be notified

3.1.46
signal
variable parameters by which information is conveyed

3.1.47
soak
an attribute of a zone or 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. The soak attribute can be manually or automatically removed

3.1.48
stand-by period
defined time for which a power supply shall supply energy to the components of the alarm system in the event of failure of the EPS

3.1.49
storage device
device which stores energy (EXAMPLE: a battery)

3.1.50
storage failure
inability of a storage device to maintain the output voltage above the minimum value, in the event of a failure of the EPS

3.1.51
supervised premises
that part of a building in which a hazard may be detected by an alarm system

3.1.52
tamper alarm
alarm generated by tamper detection

3.1.53
tamper condition
condition of an alarm system, resulting from the detection of tampering

3.1.54
tamper detection
detection of deliberate interference with an alarm system or part thereof

3.1.55
tamper protection
methods or means used to protect an alarm system or part thereof against deliberate interference

3.1.56
test condition
condition of an alarm system in which the normal functions are modified for test purposes

3.1.57
triggering
deliberate operation of a hold-up device

3.1.58
unset
status of an IAS or part thereof in which an intruder alarm condition cannot be notified

3.1.59
user
person authorised to operate an alarm system

3.1.60
user input
command generated by a deliberate user action

3.1.61
warning device
device that gives an alarm or an alert

3.1.62
wire-free interconnection
interconnection conveying information between I&HAS components without physical media. The interconnection may convey information pertaining to two or more applications

3.1.63
zone
an assessed area where abnormal conditions may be detected

3.2 Abbreviations

3.2.1 **ACE:** Ancillary control equipment

3.2.2 **APS:** Alternative power source

3.2.3 **ARC:** Alarm receiving centre

3.2.4 **ATE:** Alarm transmission equipment

3.2.5 **ATS:** Alarm transmission system

3.2.6 **CIE:** Control and indicating equipment

3.2.7 **EPS:** External power source

3.2.8 **HAS:** Hold-up alarm systems

3.2.9 **IAS:** Intrusion alarm system

3.2.10 **I&HAS:** Intruder and hold-up alarm system

3.2.11 **PIN:** Personal identity number

3.2.12 **PPS:** Prime power source

3.2.13 **PS:** Power supply

3.2.14 **PU:** Power unit

3.2.15 **SD:** Storage device

3.2.16 **WD:** Warning device

4 Equipment attributes

4.1 General

Control and indicating equipment shall include attributes for the detection of input status, processing the information, notification and indication as appropriate. The detailed requirements for the following attributes are provided in Clause 8.

4.2 Functionality

Control and indicating equipment shall include the following functions:

4.2.1 Inputs

The ability to receive and recognize intrusion, tamper and fault signals or messages. Other signals and messages can be received and recognized. Such inputs shall not affect any mandatory requirements of this specification.

4.2.2 Operation

The operation function is to enable the CIE to respond to automatic or manual user instructions (EXAMPLE: set, unset, inhibit, isolate).

4.2.3 Processing

The processing function is to enable the CIE to process signals and messages from detectors and hold-up devices, to process tamper and monitoring functions and respond to user instructions.

4.2.4 Outputs

To give information to the user and to provide notification and/or indication of alarm or fault or tamper conditions.

4.2.5 Tamper security

To enable the CIE to resist tampering using physical means and to provide electrical, electronic or other means to detect tampering.

4.2.6 Monitoring

To monitor, according to the grade, that the CIE and the interconnections are operating correctly.

In the event of a fault condition being detected, the CIE shall provide an indication and/or notification.

5 CIE structure

The CIE can be distributed in multiple housings or be in a single housing, and may be combined with other IAS components.

Other applications or functions not specified in this specification may be provided; such applications or functions shall not affect any requirements given within this specification.

6 Security grade

The CIE requirements shall be divided into four security grades, with grade 1 being the lowest and grade 4 being the highest.

The requirements for the performance of the CIE will vary depending upon its stated grade and will be tested according to the grade in the CIE documentation and marking.

Security grades 1 to 4 shall be in accordance with the descriptions in EN 50131-1.