SLOVENSKI STANDARD
SIST EN 50131-1:1999

01-september-1999

Nadomešča:
SIST ENV 50131-1:1997

Alarm systems - Intrusion systems - Part 1: General requirements

Alarm systems - Intrusion systems -- Part 1: General requirements

Alarmanlagen - Einbruchmeldeanlagen -- Teil 1: Allgemeine Anforderungen

Systèmes d'alarme - Systèmes d'alarme intrusion -- Partie 1: Règles générales

Ta slovenski standard je istoveten z: EN 50131-1:1997

ICS:

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

SIST EN 50131-1:1999 **en**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50131-1

March 1997

ICS 13.320

Supersedes ENV 50131-1:1996

Descriptors: Electric equipment, warning systems, safety devices, intrusion detector, definitions, specifications, classification, environments, performance evaluation, marking

English version

Alarm systems - Intrusion systems
Part 1: General requirements

Systèmes d'alarme
Systèmes d'alarme intrusion
Partie 1: Règles générales

Alarmsysteme - Einbruchmeldeanlagen
Teil 1: Allgemeine Anforderungen

This European Standard was approved by CENELEC on 1996-10-01. 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, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, 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. EN 50131-1:1997 E

Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 79, Alarm systems.

This text of the draft was submitted to the Unique Acceptance Procedure (UAP) and was approved by CENELEC as EN 50131-1 on 1996-10-01.

This European Standard replaces ENV 50131-1:1996.

The following dates was 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) 1997-12-01

EN 50131 will consist of the following parts, under the general title "Alarm systems - Intrusion systems":

- Part 1 General requirements
- Part 2-1 Intrusion detectors - Common requirements
- Part 2-2 Intrusion detectors - Volume detectors
- Part 2-3 Intrusion detectors - Planar detectors
- Part 2-4 Intrusion detectors - Linear detectors
- Part 2-5 Intrusion detectors - Point detectors
- Part 3 Control and indicating equipment
- Part 4 Warning devices
- Part 5 (reserved)
- Part 6 Power supplies
- Part 7 Application guidelines

Table of Contents

		Page
	Introduction	5
1	Scope	5
2	Normative references	6
3	Definitions and Abbreviations	6
	3.1 Definitions	6
	3.2 Abbreviations	11
4	System attributes	11
	4.1 Functionality	11
	4.2 Reliability	12
5	System components	12
6	Security grading	13
7	Environmental classification	14
	7.1 Environmental Class I Indoor	14
	7.2 Environmental Class II Indoor - General	14
	7.3 Environmental Class III Outdoor - Sheltered	14
	7.4 Environmental Class IV Outdoor - General	14
8	Functional requirements	15
	8.1 Detection of intruders and the recognition of faults	15
	8.2 Compatibility	16
	8.3 Operation	16
	8.4 Processing	19
	8.5 Indications	20
	8.6 Notification	23
	8.7 Tamper security	24
	8.8 Interconnections	25
	8.9 Intruder alarm system timing performance	28
	8.10 Event recording	28
9	Power supply	30
	9.1 Types of power supply	30
	9.2 Requirements	30
10	Operational reliability	31
	10.1 Intruder alarm system components	31
11	Functional reliability	31
12	Environmental requirements	31
	12.1 Electromagnetic compatibility	32
13	Electrical safety	32

14 Documentation 32
14.1 Intruder alarm system documentation 32
14.2 Intruder alarm system component documentation 32

15. Marking/Identification 32

Annex A (normative) Special national conditions 33
Annex B (informative) Alarm transmission system performance criteria 34

Tables

Table 1 : Levels of access 17
Table 2 : Authorisation code requirements 18
Table 3 : Processing of alarm, tamper and fault signals/messages 21
Table 4 : Indication 22
Table 5 : Notification requirements 23
Table 6 : Alarm transmission system performance requirements 23
Table 7 : Tamper detection - Components to include 25
Table 8 : Tamper detection - Forms to be detected 25
Table 9 : Periodic communication between intruder alarm system components 26
Table 10 : Monitoring the availability of interconnections 26
Table 11 : Monitoring of substitution 27
Table 12 : Monitoring of substitution - Timing 27
Table 13 : Monitoring of Interconnections - when monitoring function is to be operational 28
Table 14 : Event recording - Basic functions 29
Table 15 : Event recording - General functions 29
Table 16 : Duration of alternative power supply 30
Table 17 : Alternative power supply - Recharge periods 31

Introduction

This European Standard is a specification for intruder alarm systems installed in buildings, it includes four security grades and four environmental classes.

The purpose of an intruder alarm system is to enhance the security of the supervised premises. To maximise its effectiveness the intruder alarm system should be integrated with appropriate physical security devices and procedures. This is particularly important to higher grade intruder alarm systems.

This Standard is intended to assist insurers, intruder alarm companies, subscribers and the police in achieving a complete and accurate specification of the protection required in particular premises, but it does not specify the type of technology, the extent or degree of detection, nor does it necessarily cover all of the requirements for a particular installation.

All references to the requirements for intruder alarm systems refer to basic minimum requirements and the designers of such installed intruder alarm systems should take into account the nature of the premises, the value of its contents, the degree of risk of intrusion and any other factors which may influence the choice of grade and content of the intruder alarm system.

Requirements for design, planning, operation, installation and maintenance are given in Application Guidelines prEN 50131-7.

This standard is not intended to be used for testing individual intruder alarm system components. Requirements for testing individual intruder alarm system components are given in the relevant component standards.

Intruder alarm systems and intruder alarm system components are graded to provide the level of security required. The security grades take into account the risk level which depends on the type of premises, the value of the contents, and the typical intruder expected.

1 Scope

This European Standard specifies the requirements for intruder alarm systems installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. The standard does not include requirements for exterior intruder alarm systems. These requirements also apply to the components of intruder alarm systems installed in a building which are normally mounted on the external structure of a building.

EXAMPLE : ancillary control equipment or warning devices.

This standard specifies performance requirements for installed intruder alarm systems but does not include requirements for design, planning, installation, operation or maintenance.

These requirements apply to intruder alarm systems sharing means of detection, interconnection, control, communication and power supplies with other applications. The operation of the intruder alarm systems shall not be adversely influenced by the other applications.

Requirements are specified for intruder alarm system components where the relevant environment is classified. This classification describes the environment in which the intruder alarm system 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. General environmental requirements for intruder alarm system components are described in clause 12.

2 Normative references

This European Standard 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 European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

EN 50081-1	1992	Electromagnetic compatibility - Generic emission standard Part 1: Residential, commercial and light industry
EN 50130-4	1995	Alarm systems -- Part 4: Electromagnetic compatibility - Product family standard : Immunity requirement for components of fire, intruder and social alarm systems
prEN 50130-5	*)	Alarm systems -- Part 5 : Environmental test methods
prEN 50131-7	*)	Alarm systems - Intrusion systems -- Part 7: Application guidelines
EN 60073	1993	Coding of indicating devices and actuators by colours and supplementary means (IEC 73:1991)
EN 60950	1992	Safety of information technology equipment, including electrical business equipment (IEC 950:1991, modified)

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this standard, the following definitions apply :

3.1.1 action : (relating to setting and unsetting) - Any deliberate operation or act by the user which is part of the setting or unsetting procedure.

3.1.2 access level : The level of access to particular functions of the intruder alarm system.

3.1.3 active : The state of a detector in the presence of a hazard.

3.1.4 active detector : A detector capable of comparing input signals with pre-defined criteria. (speed/frequency/amplitude/direction) prior to generating an alarm signal or message.

3.1.5 active period : The period during which an alarm signal is present.

3.1.6 alarm : A warning of the presence of a hazard to life, property or the environment.

3.1.7 alarm receiving centre : A continuously manned centre to which information concerning the status of one or more alarm systems is reported.

3.1.8 alarm company : An organisation which provides services for alarm systems.

*) Under consideration

3.1.9 alarm condition : A condition of an alarm system, or part thereof, which results from the response of the system to the presence of a hazard.

3.1.10 alarm notification : The passing of an alarm condition to warning devices and/or alarm transmission systems.

3.1.11 authorisation codes : Physical or logical keys which permit access to intruder alarm system functions.

3.1.12 alarm system : An electrical installation which responds to the manual or automatic detection of the presence of a hazard.

3.1.13 alarm transmission system : Equipment and network used to transfer information concerned with the state of one or more alarm systems to one or more alarm receiving centres.

NOTE : Transmission systems exclude local direct connections, i.e. interconnections between parts of an alarm system which do not require an interface to transform the alarm system information into a form suitable for transmission.

3.1.14 alternative power source : A power source capable of powering the system for a predetermined time when a prime power source is unavailable.

3.1.15 ancillary control equipment : Equipment used for supplementary control purposes.

3.1.16 application : An alarm system (intrusion & holdup, social alarm, CCTV, access control, fire or another TC 79's application) or any other system outside of this TC 79 scope (heating, air cooling, lighting..)

3.1.17 authorisation : The permission to gain access to the various functions of an intruder alarm system.

3.1.18 operating programme : The software, firmware and/or hardware of control and indicating equipment supplied by the manufacturer which provides the means by which the processing of signals or messages can be configured by an installer or user.

3.1.19 communication : The transmission of messages and/or signals between intruder alarm system components.

NOTE : The transmission of a signal may include the continual passing of an electrical current through a switch or relay forming the interface between intruder alarm system components. It is not necessary to change the status of any such switch or relay. Due to the nature of data communication the transmission of a message may require deliberate initiation, e.g. in response to a poll or at specified time intervals, this initiation may or may not require the change of status of a switch or relay.

3.1.20 condition/mode/state : The state of an alarm system or part thereof.

3.1.21 control and indicating equipment : Equipment for receiving, processing, controlling, indicating and initiating the onward transmission of information.

3.1.22 dedicated transmission path : A transmission path which is continuously available for the connection of an alarm system to its associated alarm receiving centre and which does not require switching or setting up prior to the transmission of individual alarm events.

3.1.23 detector : A device designed to generate an intruder signal or message in response to the sensing of an abnormal condition indicating the presence of a hazard.

3.1.24 detector masking : The condition whereby the performance of a detector is impaired.

3.1.25 entry/exit route : The route by which authorised entry or exit to the supervised area may be achieved.

3.1.26 event : Conditions arising from the operation of the intruder alarm system e.g. setting/unsetting, alarm.

3.1.27 event recording : The storage of events arising from the operation of the intruder alarm system e.g. for analysis.

3.1.28 failure of communication : The inability to pass a message or signal between intruder alarm system components.

3.1.29 fault condition : A condition of an alarm system which prevents the intruder alarm system or parts thereof from functioning normally.

3.1.30 fault signal/message : Information generated due to the presence of a fault.

3.1.31 inhibit : The status of a part of an alarm system in which an alarm condition cannot be notified.

3.1.32 intruder alarm system : An alarm system to detect and indicate the presence, entry or attempted entry of an intruder into supervised premises.

3.1.33 interconnection : The means by which messages and/or signals are transmitted between intruder alarm system components.

3.1.34 interference : The corruption of signals and/or messages passing between intruder alarm system components.

3.1.35 intruder alarm condition : A condition of an alarm system, or part thereof, which results from the response of the intruder alarm system to the presence of an intruder.

3.1.36 intruder signal or message : information generated by an intruder detector

3.1.37 isolation : The status of a part of an alarm system in which an alarm condition cannot be notified, such status remaining until manually cancelled.

3.1.38 latching : A state applying to a condition or indication which remains until deliberately cancelled.

3.1.39 local interconnection for alarm transmission : The interconnection between an alarm system and an alarm transmission system and between an alarm receiving centre receiver and annunciation equipment.

3.1.40 message : Series of signals routed by a network which include identification, function data and the various means for providing its own integrity, immunity and proper reception.

3.1.41 monitoring : The process of verifying that interconnections and equipment are functioning correctly.

3.1.42 non-specific wired interconnection : An interconnection conveying information pertaining to two or more applications.

3.1.43 normal condition : The state of an intruder alarm system where no conditions exist which would prevent the setting of the intruder alarm system.

3.1.44 notification : The passing of an alarm, tamper or fault condition to warning devices and/or alarm transmission systems.

3.1.45 override : The deliberate cancellation of an operational requirement.

3.1.46 power supply : That part of an alarm system which provides power for the intruder alarm system or any part thereof.

3.1.47 prime power source : The power source used to support the intruder alarm system or part thereof under normal operating conditions.

3.1.48 response authority : The designated authority with responsibility for attending the supervised premises following an alarm and taking the appropriate action.

3.1.49 restore : The procedure of cancelling an alarm, tamper, fault or other condition and returning the intruder alarm system to a previous condition.

3.1.50 self-powered device : A device incorporating its own power sources.

3.1.51 sensor: That part of a detector which senses a change in condition.

3.1.52 set : The status of an alarm system or part thereof in which an alarm condition can be notified.

3.1.53 signal : Variable parameters by which information is conveyed.

3.1.54 site specific data : Information relating to the configuration of a particular intruder alarm system.

EXAMPLE : processing parameters.

3.1.55 specific wired interconnection : An interconnection conveying information pertaining to one application.

3.1.56 standby period : The period during which the alternative power source is capable of supporting the intruder alarm system.

3.1.57 message substitution : The intentional or unintentional creation of alternative messages between intruder alarm system components which prevent the correct operation of the intruder alarm system.

3.1.58 component substitution : The replacement of intruder alarm system components with alternative devices which prevent the intruder alarm system operating as designed.

3.1.59 subsystem : That part of an intruder alarm system located in a clearly defined part of the supervised premises capable of independent operation.

3.1.60 supervised premises : That part of a building and/or area in which a hazard may be detected by an alarm system.

3.1.61 supplementary prime power source : An energy source capable of supporting the intruder alarm system for extended periods, without affecting the standby period of the alternate power source.

3.1.62 system attributes : The characteristics of an intruder alarm system arising out of its design and configuration.

3.1.63 system components : The individual items of equipment which make up an intruder alarm system when configured together.

3.1.64 tamper : Deliberate interference with an intruder alarm system or part thereof.

3.1.65 tamper alarm : An alarm generated by tamper detection.

3.1.66 tamper condition : A condition of an alarm system in which tampering has been detected.

3.1.67 tamper detection : The detection of deliberate interference with an alarm system or part thereof.

3.1.68 tamper protection : Methods or means used to protect an alarm system or part thereof against deliberate interference.

3.1.69 tamper security : Methods or means used to protect an alarm system or part thereof against deliberate interference and the detection of deliberate interference with an alarm system or part thereof.

3.1.70 tamper signal or message : Information generated by a tamper detector.

3.1.71 test condition : The condition of an alarm system in which the normal functions are modified for test purposes.

3.1.72 transmission path : A communication route used to convey notification information.

3.1.73 unset : The status of an intruder alarm system or part thereof in which an alarm condition cannot be notified.

3.1.74 user : A person authorised to operate an alarm system.

3.1.75 user identification : Access to an intruder alarm system by means which enable an operator to be identified.

3.1.76 warning device : A device that gives an alarm or an alert.

3.1.77 wire-free interconnection : An interconnection conveying information between intruder alarm system components without physical media. The interconnection may convey information pertaining to two or more applications.

3.1.78 zone : An assessed area where abnormal conditions may be detected.