SLOVENSKI STANDARD
SIST-TS CLC/TS 50131-2-8:2012

01-junij-2012

Alarmni sistemi - Sistemi za javljanje vloma in ropa - 2-8. del: Javljalniki vloma - Javljalniki udara

Alarm systems - Intrusion and hold-up systems - Part 2-8: Intrusion detectors - Shock detectors

Alarmanlagen - Einbruchmeldeanlagen - Teil 2-8: Anforderungen an Erschütterungsmelder

Systèmes d'alarme - Systèmes de détection d'intrusion - Partie 2-8: Indicateur de choc

Ta slovenski standard je istoveten z: CLC/TS 50131-2-8:2012

ICS:

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

SIST-TS CLC/TS 50131-2-8:2012 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50131-2-8

April 2012

ICS 13.320

English version

Alarm systems - Intrusion and hold-up systems - Part 2-8: Intrusion detectors - Shock detectors

Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les hold-up - Partie 2-8: Détecteurs d'intrusion - Détecteurs de chocs

Alarmanlagen - Einbruchmeldeanlagen - Teil 2-8: Anforderungen an Erschütterungsmelder

This Technical Specification was approved by CENELEC on 2012-01-23.

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, Bulgaria, Croatia, 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, Turkey and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. CLC/TS 50131-2-8:2012 E

Contents

Page

Foreword

This document (CLC/TS 50131-2-8:2012) has been prepared by CLC/TC 79 "Alarm systems".

This document was circulated for voting in accordance with the Internal Regulations, Part 2, Subclause 11.3.3.3.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Introduction

This document is a Technical Specification for shock detectors used as part of intrusion alarm systems installed in buildings. It includes four security grades and four environmental classes.

The purpose of a shock detector is to detect the shock or series of shocks due to a forcible attack through a physical barrier (for example doors or windows) and provide the necessary range of signals or messages to be used by the rest of the intrusion and hold-up alarm system.

The number and scope of these signals or messages will be more comprehensive for systems that are specified at the higher grades.

This Technical Specification is only concerned with the requirements and tests for the shock detectors.

1 Scope

This Technical Specification is for shock detectors installed in buildings to detect the shock or series of shocks due to a forcible attack through a physical barrier (for example doors or windows).

It provides for security Grades 1-4 (see EN 50131-1), specific or non specific wired or wire-free detectors and uses Environmental Classes i-iv (see EN 50130-5).

This Technical Specification does not include requirements for detectors intended to protect for example vaults and safes from penetration attacks from e.g. drilling, cutting or thermal lance.

This Technical Specification does not include requirements for shock detectors intended for use outdoors.

A detector shall fulfil all the requirements of the specified grade.

Functions additional to the mandatory functions specified in this Technical Specification may be included in the detector, providing they do not adversely influence the correct operation of the mandatory functions.

This Technical Specification does not apply to system interconnections.

2 Normative references

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

EN 50130-4:2011, *Alarm systems — Part 4: Electromagnetic compatibility — Product family standard: Immunity requirements for components of fire, intruder and social alarm systems*

EN 50130-5:2011, *Alarm systems — Part 5: Environmental test methods*

EN 50131-1, *Alarm Systems — Intrusion systems and hold-up systems — Part 1: System requirements*

EN 50131-6, *Alarm systems — Intrusion systems and hold-up systems — Part 6: Power supplies*

EN 60068-1:1994, *Environmental testing — Part 1: General and guidance (IEC 60068-1:1988 + A1:1992 + corrigendum Oct. 1988)*

EN 60068-2-75:1997, *Environmental testing — Part 2-75: Tests — Test Eh: Hammer tests (IEC 60068-2-75:1997)*

IEC 68-2-52:1984, *Environmental testing — Part 2: Tests — Test Kb: Salt mist, cyclic (sodium, chloride solution)*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms, definitions and abbreviations given in EN 50131-1 and the following apply.

3.1 Terms and definitions

3.1.1
shock
sudden transient acceleration or deceleration e.g. caused by a mechanical impact as a result of a forcible attack through a physical barrier

3.1.2
incorrect operation
physical condition that causes an inappropriate signal or message from a shock detector

3.1.3
masking
interference with the shock detector input capability, which prohibits the triggering of the shock detector (e.g. disabling the detector with an external magnet)

3.1.4
shock test
operational test, during which a shock detector is activated by using the standard triggering method in a controlled environment

3.1.5
shock detector
combination of one or more shock sensor(s) and an analyser, which provides signalling or messaging to the Intruder & Hold Up alarm system

3.1.6
shock sensor
element which detects the mechanical shock energy and produces a signal for further analysing

3.1.7
analyser
physical unit or processing capabilities used to process the signal(s) produced by one or more shock sensor(s) and provides a signal or message to the intruder & Hold Up alarm system

3.1.8
mass inertia
physical underlying principle which will be used for sensing a shock e.g. a weighted or piezo transducer sensor

3.1.9
gross attack
large single shock due to a impact on the supervised material, e.g. impact generated by a sledge hammer on a concrete surface

3.1.10
low shock integration attack
series of low level shocks, due to a number of impacts on the supervised material integrating over a certain time, e.g. impacts generated by chiselling on a concrete surface

3.1.11
standard immunity window
framed window, which will be used for all immunity tests, where a framed window is required, according to Annex D.

3.2 Abbreviations

CIE Control & Indicating Equipment

EMC Electro Magnetic Compatibility

4 Functional requirements

4.1 General

A shock detector consists of a shock sensor and an analyser, which may either be in the same housing, or in separate housing. Furthermore the analyser can be integrated into another component of the Intruder & Hold Up alarm system (for example the CIE).

4.2 Event Processing

Shock detectors shall process the events shown in Table 1. Shock detectors shall generate signals or messages as shown in Table 2.

Table 1 – Events to be processed by grade

Event	Grade			
	1	2	3	4
Intrusion	M	M	M	M
Tamper Detection	Op	M	M	M
Masking Detection				
Magnetic Masking	Op	Op	M	M
Detection of penetration of sensor housing	Op	Op	Op	M
Removal from the mounting surface [a]	Op	Op	M	M
Low Supply Voltage – wire free devices	M	M	M	M
Low Supply Voltage – wired devices	Op	Op	Op	M
Total Loss of Power Supply [b]	Op	M	M	M
Local Self Test [c]	Op	Op	Op	M
Remote Self Test [c]	Op	Op	Op	M

Key
M = Mandatory, Op = Optional

[a] Mandatory for wire-free at grades 2, 3 and 4; mandatory for all surface mounted grade 3 and 4 types, optional for wired surface mounted grades 1 and 2. Not required for wired, concealed flush mounted types grade 3.

[b] Mandatory for wire-free at all grades. Only required if power is for normal local operation, e.g. purely switch based solutions do not fall under this requirement; however if signal processing (except if it is the CIE itself) is required to process the output of the sensor, such an event shall be generated. No generation of a message or signal is required when the condition is detected by the CIE due to system design, e.g. bus based systems.

[c] Only required if signal processing is used to generate any signal or message, e.g. purely mechanical based solutions do not fall under this requirement. No generation of a message or signal is required when the condition is detected by the CIE due to system design, e.g. bus based systems.

Table 2 – Generation of Signals or Messages

Event	Signals or Messages		
	Intrusion	Tamper	Fault
No Event	NP	NP	NP
Intrusion	M	NP	NP
Tamper	NP	M	NP
Masking*	M	Op	M
Removal from the mounting surface	NP	M	NP
Low Supply Voltage	Op	Op	M
Total Loss of Power Supply**	M	Op	Op
Local Self Test Pass	NP	NP	NP
Local Self Test Fail	NP	NP	M
Remote Self Test Pass	M	NP	NP
Remote Self Test Fail	NP	NP	M

Key
M = Mandatory

NP = Not Permitted

Op = Optional

* An independent signal or message may be provided instead.

NOTE 1 This permits two methods of signalling a masking event: either by the intrusion signal and fault signal, or by a dedicated masking signal or message. Use of the intrusion signal and fault signal is preferable, as this requires fewer connections between CIE and shock detector. If multiple events overlap there will be some signal combinations that may be ambiguous. To overcome this ambiguity it is suggested that shock detectors should not signal 'intrusion' and 'fault' at the same time except to indicate masking. This implies that the shock detector should prioritise signals, e.g. 1 Intrusion, 2 Fault, 3 Masking.

** Alternatively Total loss of Power Supply shall be determined by loss of communication with the shock detector.

NOTE 2 When, in Table 1, an event may optionally generate signals or messages, they shall be as shown in this table.

NOTE 3 It is accepted that a bus system may send out dedicated signals or messages and does not necessarily have to follow the mapping of Table 2, provided that all of the required events are signalled.

4.3 Detection

4.3.1 Detection performance

4.3.1.1 Generalities

The shock detector shall be designed to distinguish between environmental shocks and shocks resulting from a physical attack which may be intended to penetrate the structure. The means for achieving this may be adjustable to suit varying circumstances.

The operating parameters of the shock detector shall be verified as specified by the manufacturer.

The manufacturer shall clearly state in the product documentation, any special limitation concerning installation e.g. area of coverage etc.

The shock detector shall generate an intrusion signal or message when a simulated structure penetration is performed at all grades.

4.3.1.2 Verification of gross attack detection performance

This test will verify the detection performance for sensitivity and area of coverage, according to the supported conditions claimed by the manufacturer for a gross attack.

There are minimum performance requirements for gross attack detection which need to be fulfilled by the shock detector according to Table G.1.

Furthermore, the manufacturer can specify other performance requirements, which need to be verified by testing against the performance specifications provided by the manufacturer.

The manufacturer shall specify the lowest and the highest detection level of the supported area of coverage on a specified material for an impact defined at a certain energy level according to Table G.1. Each of the specified lowest and highest detection levels will be tested.

4.3.1.3 Verification of low shock integration attack detection performance

This test will verify the detection performance for sensitivity and area of coverage according to the supported conditions claimed by the manufacturer for a low shock integration attack.

This test only applies, if the manufacturer claims his product supports this feature

There are minimum performance requirements for low shock integration attack detection which need to be fulfilled by the shock detector according to Table G.1.

Furthermore, the manufacturer can specify other performance requirements, which will be verified by testing against the performance specifications provided by the manufacturer.

The manufacturer shall specify the lowest and the highest detection level of the supported area of coverage on a specified material for an impact defined at a certain energy level as specified in Table G.1. Each of the specified lowest and highest detection levels will be tested.

4.3.2 Indication of detection

Powered shock detectors at Grades 3 and 4 that include processing capabilities shall provide an indicator at the detector to indicate when an intrusion signal or message has been generated. Self-powered shock detectors (e.g. detectors which rely on the energy resulting from the impact or a series of impacts) do not require such an indicator.

At Grades 3 and 4 this indicator shall be capable of being enabled and disabled remotely at Access Level 2.

4.4 Immunity to false alarm sources

4.4.1 General

The detector shall have sufficient immunity to false alarm sources if the following requirements have been met:

No intrusion signal or message shall be generated as a result of the false alarm sources according to each individual test clause.

If not defined in the individual test section differently, for this clause the tests will be performed on the standard immunity test window as defined in 3.1.10, wherever a monitored object is required.

4.4.2 Immunity to Small objects hitting a framed window

The detector shall not generate an intrusion signal or message when small objects such as hail, sand, gravel etc. hit the outside of the monitored surface, when set to the chosen sensitivity level required to pass the gross attack detection performance test. The tests are described in 6.7.2.

4.4.3 Immunity to Hard objects hitting a framed window

The detector shall not generate an intrusion signal or message when hard objects (e.g. handlebars of a bicycle) hit the outside of the monitored surface, when set to the chosen sensitivity level required to pass the gross attack detection performance test. The tests are described in 6.7.3.

4.4.4 Immunity to Static pressure

The detector shall not generate an intrusion signal or message when permanent pressure changes applied to the monitored surface, when set to the chosen sensitivity level required to pass the gross attack detection performance test. The tests are described in 6.7.4.

4.4.5 Immunity to Dynamic pressure

The detector shall not generate an intrusion signal or message when dynamic pressure changes (due to wind, etc.) applied to the monitored surface, when set to the chosen sensitivity level required to pass the gross attack detection performance test. The tests are described in 6.7.5.

4.4.6 Standard Immunity Test

The detector shall not generate an intrusion signal or message when for each standard installation material (glass plate, wooden plate & concrete plate as defined in Annex A), a minimum force will be issued at a given distance from the detector, when set to the chosen sensitivity level required to pass the gross attack detection performance test. The tests are described in 6.7.6.

4.5 Operational requirements

4.5.1 Time interval between intrusion signals or messages

Shock detectors using wired interconnections shall be able to provide an intrusion signal or message not more than 15 s after the end of the preceding intrusion signal or message.

Shock detectors using wire free interconnections shall be able to provide an intrusion signal or message after the end of the preceding intrusion signal or message within the following times: