SLOVENSKI STANDARD
oSIST prEN 50131-2-8:2024

01-september-2024

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

Ta slovenski standard je istoveten z: **prEN 50131-2-8**

ICS:

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

oSIST prEN 50131-2-8:2024 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50131-2-8

July 2024

ICS 13.320

Will supersede EN 50131-2-8:2016

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 draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2024-10-11.

It has been drawn up by CLC/TC 79.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CENELEC 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 CEN-CENELEC Management Centre has the same status as the official versions.

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, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Project: 76632

Ref. No. prEN 50131-2-8 E

Contents

Page

European foreword

This document (prEN 50131-2-8) has been prepared by Technical Committee CLC/TC 79 “Alarm systems”, the secretariat of which is held by BSI.

This document is currently submitted to the Enquiry/ Primary Questionnaire.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

This document will supersede EN 50131-2-8:2016 and all of its amendments and corrigenda (if any).

prEN 50131-2-8:2024 includes the following significant technical changes with respect to EN 50131-2-8:2016 :

— Reworked the document structure in general;

— Reworked the requirements and test sections in general;

— Redefined the detection performance requirements and test methods;

— Redefined the immunity requirements and test methods;

— Clarified wording wherever necessary to avoid misunderstanding and to optimize for reading.

Introduction

This document is a European Standard for shock detectors used as part of an Intrusion and Hold-up Alarm System (I&HAS) 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).

The shock detector must provide the necessary range of signals or messages to be used by the rest of the I&HAS.

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

This document is only concerned with the requirements and tests for the shock detectors. Other types of detectors are covered by other documents identified as in the EN 50131-2 series.

1 Scope

This document 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 specifies four security Grades 1-4 (in accordance with EN 50131-1), specific or non-specific wired or wire-free shock detectors and uses environmental Classes I-IV (in accordance with EN 50130-5).

This document does not include requirements for detectors intended to detect penetration attacks on safes and vaults for example by drilling, cutting or thermal lance.

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

A shock detector needs to fulfil all the requirements of the specified grade.

Functions additional to the mandatory functions specified in this document can be included in the shock detector, providing they do not adversely influence the correct operation of the mandatory functions.

This document does not deal with requirements for compliance with regulatory directives, such as EMC-directive, low-voltage directive, etc., except that it specifies the equipment operating conditions for EMC-susceptibility testing as required by EN 50130-4.

This document 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, *Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems*

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

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

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

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, definitions

3.1.1
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 I&HAS

3.1.2
gross attack
large single shock due to an impact on the supervised material, e.g. impact generated by a sledge hammer on a concrete surface

3.1.3
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

3.1.4
masking
interference with the shock detector input capability, which prohibits the triggering of the shock detector (e.g. disabling the shock detector with an external magnet)

3.1.5
sealed detector
type of detector construction, whereby there is no direct access to the internal components or connections, e.g. a “potted” unit usually supplied with integral connecting cable

3.1.6
shock
sudden transient acceleration e.g. caused by a mechanical impact as a result of a forcible attack through a physical barrier

3.1.7
shock detector
combination of one or more shock sensor(s) and an analyser, which provides signalling or messaging to the I&HAS

3.1.8
shock sensor
element which detects the mechanical energy caused by sudden transient acceleration and which produces a signal for further analysis

3.1.9
shock test
operational test, during which a shock detector is activated by using the standard triggering method in a controlled environment

3.2 Abbreviations

CIE	Control and Indicating Equipment
EMC	Electro Magnetic Compatibility
I&HAS	Intrusion and Hold-up Alarm System

4 Functional requirements

4.1 General

A shock detector consists of one or more shock sensor and an analyser, which may either be in the same housing, or in separate housings. Furthermore, the analyser can be integrated into another component of the I&HAS (for example the CIE).

4.2 Event Processing

Shock detectors shall process the events in accordance with Table 1.

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	Op	Op	M	M
Low Supply Voltage [c]	Op	Op	M	M
Total Loss of Power Supply [a]	Op	M	M	M
Local self-test [b]	Op	Op	M	M
Remote self-test [b]	Op	Op	Op	M
M = Mandatory Op = Optional				
[a] Total loss of power supply does not apply for message-based shock detectors. [b] Not required for non-processing shock detectors, e.g. purely mechanical. [c] For Shock detectors using Type C power supplies the requirements of EN 50131-6 apply.				

142 Shock detectors shall generate signals or messages as shown Table 2.

143 **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 [a]	M	Op	M
Low Supply Voltage	Op	Op	M
Total Loss of Power Supply [b]	M	Op	Op
Local Self-Test Pass [a]	NP	NP	NP
Local Self-Test Fail	NP	NP	M
Remote Self-Test Pass [a]	M	NP	NP
Remote Self-Test Fail	NP	NP	M
M = Mandatory NP = Not Permitted Op = Optional			
This permits two methods of signalling a masking: either by the intrusion signal and fault signal, or by a dedicated masking or message. Use of the intrusion signal and fault signal is preferable, as this requires fewer connections between CIE and the 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 prioritize signals, e.g. 1 Intrusion, 2 Fault, 3 Masking. When, in Table 1, an event may optionally generate signals or messages, they shall be as shown in this table.			
[a] An independent signal or message may be provided instead. [b] Total loss of Power Supply does not apply for message-based shock detectors.			

144 ## 4.3 Detection

145 ### 4.3.1 Detection performance

146 #### 4.3.1.1 General

147 The shock detector shall be designed to distinguish between environmental shocks and shocks resulting from a
148 physical attack which may be intended to penetrate the structure. The shock detector may include means of
149 adjustment to suit different types of installation.

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

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

153 **Table 3 — Detection performance**

Detection performance	Grade			
	1	2	3	4
Detection				
Gross attack detection	M	M	M	M
Low shock integration attack detection	Op	Op	Op	M
Immunity				
Immunity to Small objects hitting the mounting surface	M	M	M	M
Standard Immunity	M	M	M	M

154 **Table 4 — Detection and immunity values**

Requirement	Peak acceleration (g)	Mass (grams)
Gross attack detection	≥ 70	111
Low shock integration attack detection	≥ 50	14
Standard Immunity	≤ 30	33
Immunity to Small objects hitting the mounting surface	≤ 20	4

155 #### 4.3.1.2 Gross attack detection

156 To ensure the shock detector can generate an alarm condition upon a single impact onto the mounting surface.
157 Example: attempting to break through a door by kicking or use of a hammer.

158 The shock detector shall generate an intrusion alarm signal or message within 10s when the value listed in
159 Table 4 is presented to the shock detector.

160 #### 4.3.1.3 Low shock integration attack detection

161 To ensure the shock detector can generate an alarm condition upon a multiple lower-level impacts onto the
162 mounting surface. Example: use of tools such as a chisel to remove material from a wall to create an opening.

163 The shock detector shall detect the low shock integration attack when the value listed in Table 4 is presented to
164 the shock detector 10 times with a gap of 2 s between each impact.

165 The shock detector shall generate an intrusion alarm signal or message within 28 s of the first impact.

166 ### 4.3.2 Indication of detection

167 Shock detectors at Grades 3 and 4 that include processing capabilities shall provide an indicator at the shock
168 detector to indicate when an intrusion alarm signal or message has been generated.

169 At Grades 3 and 4 this indicator shall be capable of being enabled and disabled remotely at access level 2.

170 Shock detectors which are solely powered by the energy resulting from the impact or a series of impacts do not
171 require an indicator.

172 ### 4.3.3 Adjustment of detection sensitivity

173 If the shock detector includes means to adjust the detection sensitivity, this may be performed remotely and/or
174 locally.

175 The adjustment may be performed remotely, provided it is only available at access level 3. e.g. via the CIE or
176 message based system.