



DPC: 24/30471656 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 26 July 2024

Origin: European

Latest date for receipt of comments: 18 September 2024

Project No. 2023/00634

Responsible committee: GW/1 Electronic security systems and products

Interested committees:

Title: Draft BS EN 50131-2-8 BS Alarm systems - Intrusion and hold-up systems. Part 2-8: Intrusion detectors. Shock detectors.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 18 September 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Miss Beverley Webb (BSI)

Direct tel: 0208 996 7061

E-mail: beverley.webb@bsigroup.com

Full document details: 24/30471656 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

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

1	Contents	Page
2	European foreword	4
3	Introduction	5
4	1 Scope	6
5	2 Normative references	6
6	3 Terms, definitions and abbreviations	6
7	3.1 Terms, definitions.....	6
8	3.2 Abbreviations	7
9	4 Functional requirements	7
10	4.1 General	7
11	4.2 Event Processing	8
12	4.3 Detection.....	9
13	4.4 Immunity to false alarm sources	11
14	4.5 Operational requirements	11
15	4.6 Tamper security	12
16	4.7 Electrical requirements	14
17	4.8 Environmental classification and conditions	15
18	5 Marking, identification and documentation	16
19	5.1 Marking and/or identification.....	16
20	5.2 Documentation	16
21	6 Testing	16
22	6.1 General	16
23	6.2 General test conditions	16
24	6.3 Basic Detection Test.....	17
25	6.4 Performance tests.....	18
26	6.5 Detection and immunity tests.....	20
27	6.6 Low shock integration attack detection performance test	22
28	6.7 Switch-on delay, time interval between signals and indication of detection	23
29	6.8 Adjustment of detection sensitivity.....	23
30	6.9 Self-tests	23
31	6.10 Tamper security	24
32	6.11 Electrical tests.....	26
33	6.12 Environmental classification and conditions	27

34 6.13 Marking, identification and documentation 29

35 **Annex A (normative) Dimensions and requirements of the standardized interference test magnets ... 30**

36 **A.1 Normative references 30**

37 **A.2 Requirements..... 30**

38 **Annex B (normative) General Testing Matrix 33**

39 **Annex C (informative) Example list of small tools..... 35**

40 **Annex D (normative) Mounting substrate..... 36**

41 **Annex E (normative) Verification of detection performance and false alarm immunity..... 37**

42 **Annex F (informative) Low shock integration attack test carousel 40**

43 **Annex G (normative) Immunity to small objects hitting the mounting surface..... 41**

44 **Bibliography..... 43**

45

46 **European foreword**

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

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

50 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)

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

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

53 — Reworked the document structure in general;

54 — Reworked the requirements and test sections in general;

55 — Redefined the detection performance requirements and test methods;

56 — Redefined the immunity requirements and test methods;

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

58 Introduction

- 59 This document is a European Standard for shock detectors used as part of an Intrusion and Hold-up Alarm
60 System (I&HAS) installed in buildings. It includes four security grades and four environmental classes.
- 61 The purpose of a shock detector is to detect the shock or series of shocks due to a forcible attack through a
62 physical barrier (for example doors or windows).
- 63 The shock detector must provide the necessary range of signals or messages to be used by the rest of the
64 I&HAS.
- 65 The number and scope of these signals or messages will be more comprehensive for systems that are specified
66 at the higher Grades.
- 67 This document is only concerned with the requirements and tests for the shock detectors. Other types of
68 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.				

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

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.			

4.3 Detection

4.3.1 Detection performance

4.3.1.1 General

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 shock detector may include means of adjustment to suit different types of installation.

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

The shock detector shall generate an intrusion alarm signal or message when a simulated structure penetration 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.

- 177 The adjustment may be performed locally either by;
- 178 — means that are enclosed within the shock detector housing. e.g. pots, jumpers or links
- 179 or
- 180 — a method that does not involve opening the shock detector housing, provided that a tamper signal or
- 181 message is generated before the adjustment is completed, e.g. NFC token.

182 Where the adjustment is performed locally it shall not be possible to gain such access without generating a

183 tamper signal or message or causing visible damage.

184 **4.4 Immunity to false alarm sources**

185 **4.4.1 General**

186 When the shock detector is configured to meet the detection requirements it shall also have sufficient immunity

187 to false alarm sources without any further adjustment to the settings of the shock detector.

188 **4.4.2 Immunity to Small objects hitting the mounting surface**

189 To reduce the probability of the shock detector generating a false alarm condition upon multiple small impacts

190 onto the mounting surface. Example: hail stones, sand, gravel, or debris blown by the wind.

191 The shock detector shall not detect the small objects hitting the mounting surface when the value listed in Table 4

192 is presented to the shock detector at a rate of $(2\ 100 \pm 10)$ % impacts over 2,5 min.

193 **4.4.3 Standard Immunity**

194 To ensure the shock detector does not generate a false alarm condition upon a single impact onto the mounting

195 surface, for example, normal opening or closing of a door or when a system is set or a letterbox is opened/closed

196 through the delivery of letters. The detector shall not generate an intrusion alarm signal or message when the

197 values of Table 4 are presented.

198 **4.5 Operational requirements**

199 **4.5.1 Time interval between intrusion signals or messages**

200 Shock detectors using wired interconnections shall be able to provide an intrusion alarm signal or message not

201 more than 15 s after the end of the preceding intrusion alarm signal or message.

202 Shock detectors using wire free interconnections shall be able to provide an intrusion alarm signal or message

203 after the end of the preceding intrusion alarm signal or message within the following times:

- Grade 1 300 s
- Grade 2 180 s
- Grade 3 30 s
- Grade 4 15 s

204 **4.5.2 Switch on delay**

205 The shock detector shall meet all functional requirements within 180 s of the power supply reaching its nominal

206 voltage as specified by the manufacturer.

4.5.3 Self-tests

4.5.3.1 Local Self-test

According to Table 1, the shock detector shall provide the ability to perform a local self-test which is intended to provide confidence that the shock detector is able to meet its basic performance requirements e.g. able to detect.

The results of the local self-test shall be notified according to Table 2. If a fault condition is detected on the detection technology when a self-test is performed, the self-test shall be processed as a failed test.

The local self-test may be part of a continuous monitoring process or shall be performed as a specific function at least once every 24 h.

If normal operation of the shock detector is inhibited during a local self-test, the time for which the shock detector is inhibited shall be limited to a maximum of 30 s in any period of 2 h.

The following information shall be provided to the test house:

1. How to create a fault condition on the detection technology e.g. short the sensor signal output to ground
2. If the local self-test inhibits the shock detector, evidence that the inhibition is within the timing requirements.

4.5.3.2 Remote Self-test

According to Table 1, the shock detector shall provide the ability to perform a remote self-test which is intended to provide confidence that the shock detector is able to meet its basic performance requirements e.g. able to detect.

When the shock detector receives a signal or message to perform a remote self-test, the shock detector shall start the remote self-test within 10 s.

The shock detector shall complete a remote self-test within 30 s and return to normal operation.

The results of the remote self-test shall be notified according to Table 2.

Should an intrusion condition be detected when the remote self-test is being performed, the shock detector shall not notify an intrusion alarm signal or message.

If an independent signal or message is used to notify a remote self-test pass, then it is permitted to notify an intrusion alarm signal or message during the remote self-test.

If a fault condition is detected on the detection technology when a remote self-test is performed, the remote self-test shall be processed as a failed test.

The following information shall be provided to the test house:

1. How to create a fault condition on the detection technology e.g. short the sensor signal output to ground.
2. How long the self-test takes to initiate and complete.

4.6 Tamper security

4.6.1 General

The tamper security requirements for each grade of shock detector are shown in Table 5. The requirements apply to the shock detector and its individual components (e.g. multiple sensors).