



BSI Standards Publication

Alarm systems — Intrusion and hold-up systems

Part 2-8: Requirements for shock detectors

National foreword

This British Standard is the UK implementation of EN 50131-2-8:2025. It supersedes BS EN 50131-2-8:2016, which will be withdrawn on 31 August 2028.

The UK participation in its preparation was entrusted to Technical Committee GW/1, Electronic security systems and products.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 26448 7

ICS 13.320

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Alarm systems - Intrusion and hold-up systems - Part 2-8: Requirements for shock detectors

Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les hold-up - Partie 2-8: Exigences relatives aux détecteurs de chocs

Alarmanlagen - Einbruch- und Überfallmeldeanlagen - Teil 2-8: Anforderungen an Erschütterungsmelder

This European Standard was approved by CENELEC on 2025-07-15. 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 CEN-CENELEC Management Centre 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 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.



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

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

A.2	Requirements.....	30
Annex B (normative)	General testing matrix	33
Annex C (informative)	Example list of small tools.....	35
Annex D (normative)	Mounting substrate.....	36
Annex E (normative)	Verification of detection performance and false alarm immunity.....	37
Annex F (informative)	Low shock integration attack test carousel	39
Annex G (normative)	Immunity to small objects hitting the mounting surface.....	40
Bibliography.....		42

European foreword

This document (EN 50131-2-8:2025) has been prepared by Technical Committee CLC/TC 79 “Alarm systems”.

The following dates are fixed:

- latest date by which this document has to be (dop) 2026-08-31
implemented at national level by publication of
an identical national standard or by
endorsement
- latest date by which the national standards (dow) 2028-08-31
conflicting with this document have to be
withdrawn

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

EN 50131-2-8:2025 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.

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

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

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 are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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*

EN 60404-5, *Magnetic materials - Part 5: Permanent magnet (magnetically hard) materials - Methods of measurement of magnetic properties (IEC 60404-5)*

EN 60404-14, *Magnetic materials - Part 14: Methods of measurement of the magnetic dipole moment of a ferromagnetic material specimen by the withdrawal or rotation method (IEC 60404-14)*

EN 60404-8-1, *Magnetic materials - Part 8-1: Specifications for individual materials - Magnetically hard materials (IEC 60404-8-1)*

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

EXAMPLE 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

EXAMPLE 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

EXAMPLE disabling the shock detector with an external magnet

3.1.5**sealed shock detector**

type of detector construction whereby there is no direct access to the internal components or connections

EXAMPLE 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(s) 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 shall 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.

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

Table 4 — Detection and immunity values

Requirement	Peak acceleration (g)	Test spheres	
		Mass (grams)	Diameter (mm)
Gross attack detection	70 (−0 %/+10 % tolerance)	111	30
Low shock integration attack detection	50 (−0 %/+10 % tolerance)	14	15
Standard immunity	30 (−10 %/+0 % tolerance)	33	20
Immunity to small objects hitting the mounting surface	10 – 18 (0 % tolerance) (with 60 % over 15g)	4	12

4.3.1.2 Gross attack detection

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

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

4.3.1.3 Low shock integration attack detection

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

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

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

4.3.2 Indication of detection

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

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

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

4.3.3 Adjustment of detection sensitivity

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

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

The adjustment may be performed locally either by;

- means that are enclosed within the shock detector housing. e.g. pots, jumpers or links
- or
- a method that does not involve opening the shock detector housing, provided that a tamper signal or message is generated before the adjustment is completed, e.g. NFC token.

Where the adjustment is performed locally it shall not be possible to gain such access without generating a tamper signal or message or causing visible damage.

4.4 Immunity to false alarm sources

4.4.1 General

When the shock detector is configured to meet the detection requirements it shall also have sufficient immunity to false alarm sources without any further adjustment to the settings of the shock detector.

4.4.2 Immunity to small objects hitting the mounting surface

To reduce the probability of the shock detector generating a false alarm condition upon multiple small impacts onto the mounting surface. Example: hail stones, sand, gravel, or debris blown by the wind.

The shock detector shall not detect the small objects hitting the mounting surface when the value listed in Table 4 is presented to the shock detector at a rate of $(2\ 100 \pm 10 \%)$ impacts over 2,5 min.

4.4.3 Standard immunity

To ensure the shock detector does not generate a false alarm condition upon a single impact onto the mounting surface, for example, normal opening or closing of a door or when a system is set or a letterbox is opened/closed through the delivery of letters. The detector shall not generate an intrusion alarm signal or message when the values of Table 4 are presented.

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 alarm signal or message not more than 15 s after the end of the preceding intrusion alarm signal or message.

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

4.5.2 Switch on delay

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