BS 9263:2016

BSI Standards Publication

Intruder and hold-up alarm systems –

Commissioning, maintenance and remote support – Code of practice

bsi.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2016

Published by BSI Standards Limited 2016

ISBN 978 0 580 93636 4

ICS 13.310

The following BSI references relate to the work on this document:
Committee reference GW/1/2
Draft for comment 16/30338904 DC

Publication history

First edition, August 2016

Amendments issued since publication

Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 14, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 August 2016. It was prepared by Subcommittee GW/1/2, *Installed alarm systems*, under the authority of Technical Committee GW/1, *Electronic security systems*. A list of organizations represented on these committees can be obtained on request to their secretary.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Relationship with other publications

This British Standard incorporates maintenance recommendations formerly included in BS 4737, *Intruder alarm systems in buildings*, and is intended to be used in conjunction with PD 6662, *Scheme for the application of European Standards for intrusion and hold-up alarm systems* to provide detail necessary for the implementation of the relevant provisions of DD CLC/TS 50131-7.

As a result of the publication of the BS EN 50131 series, BS 4737-1, BS 4737-2, BS 6799, BS 7042 were withdrawn, but suppliers might wish to continue maintaining intruder alarm systems which conform to these withdrawn standards.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

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

0 Introduction

Commissioning of any intrusion and hold-up alarm system (I&HAS) is vital to ensure the system is fully functional.

Maintenance of an I&HAS is carried out at the client's premises, and could include remote system checks as part of the overall maintenance programme. The purpose of maintenance is to ensure that the system's integrity is maintained and that it is fully functional. Such maintenance prevents minor problems becoming major problems, enables alarm company personnel to correct physical, electrical and electronic faults and allows software updates to take place.

Remote support of I&HAS permits a range of tasks to be carried out from simple capture of system event records or other parameters, through to remote system checks, under manual or automatic control, using the self-diagnostic capabilities of the system. Therefore, analysis of the system to a level similar to alarm company personnel on site might be possible remotely.

1 Scope

This British Standard gives recommendations for the commissioning, on-site corrective and preventative maintenance, remote system checks and remote support of an I&HAS.

This British Standard is applicable to all I&HASs under maintenance, including those installed in accordance with BS EN 50131 (all parts) (see Foreword) and PD 6662.

2 Normative references

The following referenced documents are indispensable for the application 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.

BS 8473, *Intruder and hold-up alarm systems – Management of false alarms – Code of practice*

BS EN 50131-1:2006+A1:2009, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

BS EN 50131-3:2009, *Alarm systems – Intrusion and hold-up systems – Part 3: Control and indicating equipment*

BS EN 50136-1:2012, *Alarm systems – Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems*

DD CLC/TS 50131-7, *Alarm systems – Intrusion and hold-up systems – Part 7: Application guidelines*

PD 6662, *Scheme for the application of European standards for intrusion and hold-up alarm systems*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this British Standard, the terms and definitions given in BS EN 50131-1 and the following apply.

3.1.1 alarm company service technician

individual responsible for commissioning and/or maintenance/service of an I&HAS who has the appropriate competence and training with access to the correct tools and equipment required to professionally carry out their duties

3.1.2 alarm point

one or more detector(s) providing a common signal or message, at the CIE or at the ACE, for the purpose of indication or processing

3.1.3 alternative power source (APS)

power source (e.g. a battery) capable of powering the system for a predetermined period of time when the prime power source (PPS) is unavailable

3.1.4 as-fitted document

document in which details of I&HAS as actually installed are recorded

3.1.5 authentication

secure validation process where the I&HAS and the secure computer exchange a code or codes to confirm their identities before proceeding with a dialogue

3.1.6 client

individual or corporate body responsible for acquiring the I&HAS

3.1.7 dialogue

electronic communication between the I&HAS and a secure computer resulting in an exchange of data

3.1.8 event record

record of events arising from the functioning of the I&HAS

NOTE For example, for analysis.

3.1.9 frequently used detector

detector expected to operate during the occupation of the supervised premises

3.1.10 information security

protection of information exchanged between a secure computer and the I&HAS

3.1.11 prime power source

power source used to support the I&HAS under normal operating conditions

3.1.12 remote location

premises of an alarm company or an alarm receiving centre (ARC) from where it is possible to initiate and/or process remote system checks and/or remote support

3.1.13 remote service personnel

personnel carrying out remote support by operating the secure computer controlling a dialogue

NOTE This operation might be automated.

3.1.14 remote support

carrying out some or all the control and indicating equipment (CIE) functions of an I&HAS from a secure computer

3.1.15 remote system check

electronic check of the status of an I&HAS from a secure computer as part of preventative maintenance

3.1.16 secure computer(s)

computer(s) at a remote location used to access remote servicing or support functions, which are not accessible without applying security measures, to ensure unauthorized persons cannot gain access to data

*NOTE See **4.3** for authorization recommendations.*

3.1.17 site visit

attendance at the supervised premises by an alarm company service technician

3.1.18 soak test

status of a part of an I&HAS from which an alarm condition is recorded in the event log but is intentionally prevented from being notified

*NOTE See also BS EN 50131-3:2009, **8.3.9**.*

3.1.19 supervised premises

part of a building and/or area in which an intrusion, attempted intrusion, or the triggering of a hold-up device can be detected by an I&HAS

3.1.20 system configuration

site specific data required for correct functioning of the I&HAS

3.1.21 user

person authorized to operate an I&HAS

3.2 Abbreviations

For the purposes of this British Standard, the following abbreviations apply.

ACE	Ancillary Control Equipment
ARC	Alarm Receiving Centre
APS	Alternative Power Source
ATE	Alarm Transmission Equipment
ATS	Alarm Transmission System
CIE	Control and Indicating Equipment
DVM	Digital Volt Meter
HD	Hold-up Device
I&HAS	Intrusion and Hold-up Alarm System

ISDN	Integrated Services Digital Network
PPS	Prime Power Source
PS	Power Supply
PSTN	Public Switched Telephone Network
WD	Warning Device

4 Security of communications for remote support and remote system checks

4.1 General

Remote system checks or remote support should be carried out through a secure computer at a remote location.

When used for remote support and/or remote system checks, the interfaces to a secure computer should meet the requirements of BS EN 50131-3:2009, Annex C.

4.2 Initialization of connection

Initialization of connection between an I&HAS and a secure computer should be carried out by one of the following methods.

a) Automatic: The I&HAS initiates a dialogue:

   1) in response to a system event;

   2) at a pre-programmed time for scheduled remote system checks.

b) Manual, on site: A user or alarm company service technician manually initiates a connection from the I&HAS to a secure computer for the purposes of remote support or remote system checks.

c) Manual or automatic, remote: Remote service personnel manually initiate a connection from a secure computer to the I&HAS or the secure computer initiates the connection automatically for the purposes of remote support or remote system checks.

   Use of the manual or automatic remote at Grade 3 should only be permitted if one of the following safeguards is in operation:

   1) information security measures are in place in accordance with **4.5**; or

   2) initialization of connection is confirmed by a user or alarm company service technician on site;

      *NOTE 1 Use of this method at Grade 4 is only permitted if information security measures are in place (see **4.5**).*

d) Manual, remote with PSTN or ISDN ring-back: Remote service personnel manually initiate a connection from a secure computer to the I&HAS. On receipt of the incoming call, the I&HAS drops the connection and initiates an automatic dial-back call to the secure computer so that remote support or remote system checks can be carried out.

NOTE 2 Initialization is not complete until authentication of communication has successfully taken place, regardless of the method used.

NOTE 3 Different methods of initialization can be used on different occasions or for different purposes.

4.3 Authorization

*COMMENTARY ON **4.3***

Access to the I&HAS for the purpose of remote system checks or remote support requires authorization to access the communications software running on the secure computer.

Authorization should conform to the access level requirements of BS EN 50131-1:2006+A1:2009, **8.3.1** and **8.3.2**.

Remote service personnel accessing the communications software running on the secure computer should be uniquely identifiable in the audit trail (e.g. by use of individual PIN codes).

Management procedures should be in place at the secure location to ensure that:

a) if PIN codes are used for access to the communications software running on the secure computer, the codes are changed at regular intervals;

b) remote service personnel log out of the communications software running on the secure computer before allowing others to use it or leaving it unattended; and

c) access to the secure computer/communications software is promptly barred to personnel leaving employment.

4.4 Authentication of communication

Before data is exchanged between the secure computer and the I&HAS, authentication of communication should be achieved by the successful exchange of codes held by the I&HAS and the secure computer.

Codes used in authentication of communication should have at least one million differs, be generated in a non-sequential manner and be unique for each secure computer.

NOTE Codes can be allocated by alarm company personnel or generated automatically by the equipment at the first connection.

4.5 Information security

Where information security measures are required [see **4.2** c)] these should conform to BS EN 50136-1:2012, **6.8.1** and Table D.6.

Information security measures should be as follows:

a)	Grade 1 and 2	I0
b)	Grade 3	I2
c)	Grade 4	I3

NOTE Where "I" is the information security measure.

5 Inspection, functional testing and commissioning

The installed system should be inspected and functionally tested to ensure that it operates correctly and in accordance with the system design proposal and the installation plan where applicable, including any agreed changes.

Commissioning of the I&HAS should be in accordance with Annex A. The results should be recorded using a checklist similar to Table A.1.

Where the I&HAS conforms to BS EN 50131 (PD 6662 scheme), commissioning should be in accordance with DD CLC/TS 50131-7, incorporating the checks given in Annex A.

6 Preventative maintenance

6.1 General

Where alarm company personnel discover faults, the client should be informed as soon as practicable and agreement reached as to the corrective action to be taken. The alarm company should, where possible, correct any faults during the maintenance. Where this is not possible, any prior agreed corrective action should be taken as soon as practicable.

6.2 On-site maintenance

Where practicable, the service technician should ensure that the I&HAS is fully tested. Parts of the system that could not be fully tested should be recorded on the maintenance record, together with the reasons for their omission and the signature of the client or representative.

A record of checks and work carried out should be either given to the client at the time of maintenance or provided within 10 days.

NOTE This record can be in electronic form if acceptable to the client.

Preventative maintenance carried out at a site visit should be in accordance with Annex B, **B.2**.

6.3 Remote system checks

6.3.1 General

There should be a written agreement with the client detailing the frequency of remote system checks.

Preventative maintenance carried out by remote system checks should be in accordance with Annex B, **B.3**, taking account of the specific details itemized in **6.3.2**.

NOTE 1 Where an I&HAS has a limited number of detectors that would be expected to activate during the normal occupation of the supervised premises, it might be more appropriate to consider on-site maintenance in preference to remote checks.

Confirmation that remote system checks have been carried out should be given to the client within 10 days.

NOTE 2 This record can be in electronic form if acceptable to the client.

Remote system checks should not generate false alarms.

If the remote system checks are carried out whilst the I&HAS or any part of it remains set, the I&HAS should continue to function normally.

A dialogue should not prevent conformity to BS EN 50131-1:2006+A1:2009, **8.9.2**, and with BS EN 50136-1.

6.3.2 Application of Annex B.3

When applying remote system checks in accordance with Annex B, **B.3**, the following checks should be carried out.

a) Review of the event record

   At least 40 events of the I&HAS event record should be reviewed. Any fault(s) found, or evidence that the system is not setting/unsetting correctly, should be reported to the user/client.

b) Check accuracy of CIE clock

The CIE clock should be checked for the correct date and time, and adjusted if necessary.

c) Check of soak test/isolation

The remote system check should be used to identify any detectors that are on soak test or programmed as isolated. If any such detectors are found for which there is no prior agreement with the user/client, the user/client should be either informed or any agreed action carried out.

NOTE Detectors are not normally on soak test for more than 14 days.

d) Prime power source (PPS)/alternative power source (APS)

The remote system check should identify that the PPS is available, that the APS is charging (if applicable) and that the APS is capable of powering the I&HAS if a PPS failure occurs. If any faults are found, the user/client should be informed.

e) Detectors

The remote system check should show the activity of detectors expected to operate during the normal occupation of the supervised premises. There should be a written agreement with the client detailing the frequently/non-frequently used detectors.

NOTE This might be detailed in the as-fitted document.

Subsequent changes should be managed in accordance with **8.1**.

f) Alarm transmission system (ATS)

The ATS should be checked to ensure it is operating correctly. Where multiple transmission paths are provided, they should all be tested. This should be done in conjunction with the ARC, e.g. by using ARC logs to verify correct receipt of these test signals, and should not create a false alarm.

6.4 Frequency

Frequency of preventative maintenance should be in accordance with Table 1.

Preventative maintenance should take place during the sixth calendar month (twelfth calendar month for annual visits) after the month of commissioning or of the previous preventative maintenance.

NOTE For example, a system commissioned in January is to have preventative maintenance scheduled in July and the following January. Preventative maintenance carried out during the calendar month immediately prior to or after the due month can be regarded as having been carried out on time.

Late preventative maintenance should not be used as the basis for scheduling subsequent preventative maintenance.

Table 1 **Minimum frequency of preventative maintenance**

Grade	Number of visits
BS 4737[A)] WD only	one site visit per year
BS 4737[A)] remote signalling	two site visits per year or one site visit plus one remote system check per year[B)]
BS 7042[A)]	two site visits per year or one site visit plus one remote system check per year[B)]
BS EN 50131 (PD 6662), Grade 1, 1T[C)]	one site visit per year or a site visit every two years and a remote system check in intermediate years
BS EN 50131 (PD 6662), Grade 2 X[C)]	one site visit per year
BS EN 50131 (PD 6662), Grade 2 notification options A, B, C and D	two site visits per year or one site visit plus one remote system check per year
BS EN 50131 (PD 6662), Grade 3	two site visits per year or one site visit plus one remote system check per year
BS EN 50131 (PD 6662), Grade 4	two site visits per year

[A)] See Foreword.

[B)] Substitution of one site visit per year with a remote system check is permitted only if the equipment permits compliance with all the relevant requirements of this document.

[C)] Grades 1, 1T and 2X are not suitable for police calling systems.

7 Corrective maintenance

An emergency service facility should be available to the client/user at all times. The client should be given the contact details of the alarm company's emergency service facility.

The emergency service facility should be located and organized so that the alarm company's representative can attend the supervised premises as soon as practicable but at least within four hours or before the I&HAS is required to be set, whichever is the longer. This period could be extended with installations on offshore islands and those with local audible alarms only. However the extended period should be agreed in writing by the client and subject to the approval of any insurer involved. The period can also be extended at the client's request, which should be recorded.

NOTE 1 Remote support can be used preliminary to, or as part of, corrective maintenance.

NOTE 2 DD CLC/TS 50131-7 refers to corrective maintenance as "repair".

8 Remote support

8.1 General

Where remote support is to be provided, specific approval should be obtained from the client.

A dialogue should not prevent conformity to BS EN 50131-1:2006+A1:2009, **8.9.2**, and with BS EN 50136-1.

The user/client should agree any change to an I&HAS that is implemented remotely, at the time of the change or by prior arrangement. A record of all such changes should be maintained by the alarm company, and made available to the client as required.

8.2 Use of remote support functionality

Whilst the use of all remote support functions by the alarm company, or ARC under contract to the alarm company, is subject to agreement between the client/alarm company and (where applicable) insurer, specific functions should be subject to the conditions/restrictions detailed in Table 2.

NOTE Use of all functions is subject to the access level requirements of BS EN 50131-1:2006+A1:2009, Table 2. Only those functions that might be used by the client/user when operating the I&HAS at the supervised premises can be made available to the client/user remotely.

Table 2 **Remote support function**

Function	Conditions/restrictions
Set/unset I&HAS (or part thereof)	By alarm company/ARC only at specific request of client/user
Perform restore remotely	In accordance with BS EN 50131-1 and BS 8473
Change other site-specific parameter	Not whilst I&HAS (or relevant part) is set
Apply/remove inhibit to alarm point or I&HAS function	With permission of client/user but not whilst I&HAS (or relevant part) is set
Apply/remove isolation to alarm point or I&HAS function	With permission of client/user but not whilst I&HAS (or relevant part) is set
Apply/remove soak test to alarm point	With permission of client/user but not whilst I&HAS (or relevant part) is set
Test WD	With permission of client/user but not whilst I&HAS (or relevant part) is set
Activate/silence WD	By alarm company/ARC only at specific request of client/user

NOTE This table does not imply that all of the facilities mentioned are provided in the system.

9 Documentation, audit trail and records

Records of all maintenance, temporary disconnections and remote support carried out, and any corrective measures taken or required, should be made and retained for a minimum period of 15 months after the site visit, remote system check or remote support to which it refers, so that a full audit trail is available of work performed at site and from each secure computer.

The records should include:

a) the date and time;

b) detailed records of the checks undertaken and the results;

c) details of any changes made to system configuration;

d) the identity of personnel carrying out the work;

e) identification of the secure computer used in any dialogue;

f) details of any temporary disconnection including date, time and reason for the disconnection and subsequent reconnection;

g) the identity of the user/client authorizing such changes/disconnections; and

h) monthly and annualized performance records of all preventative maintenance.

NOTE See also Annex B.

Annex A (normative) Commissioning of an I&HAS

As a minimum, commissioning of an I&HAS should be in accordance with Table A.1.

Table A.1 **Commissioning recommendations**

Actions	Tick when checked	Remarks
Check that the I&HAS has been installed and configured in accordance with the system design proposal (any deviations agreed in writing with the customer)		
Check the I&HAS conforms to current industry standards and is to a high standard of workmanship		
Check that all interconnections are clearly labelled at the CIE, power supply units, expanders, remote key pads and junction boxes		
Log resistance of detection interconnections or check continuity of bus wired interconnections		
Check every detector for correct operation through to the CIE		
Check that all batteries in CIE/PS(s) are marked with the date of installation		
Log the current drawn by all power supplies with the I&HAS in quiescent and alarm states		
Remove the mains supply and check that the battery voltage of all equipment is within the specified limits and the I&HAS operates normally		
Check that there is adequate standby battery capacity to meet the requirements of the applicable standard the system was installed to		
Check the operation of all WDs on system activation and when the hold-off voltage is removed from any self-powered device		
Check the operation of all tamper devices		
Check the area or volume of coverage of movement/vibration detectors including alignment of active beam detectors and any anti-masking or range reduction facilities (as appropriate)		
Check the entry/exit route(s) for correct operation and record entry/exit times		
Set system. Operate detection device(s) to check the resulting alarm condition(s) are notified correctly		
Test correct operation of all ATS paths (where fitted) for correct receipt of signals at the ARC		
If remote system checks or remote support is to be used, check correct synchronization of site-specific parameters between the I&HAS and secure computer		
Show the customer the extent of the detection coverage and correct operation of the I&HAS including the operation of detectors and the use of HDs		
Check that all documentation is correctly completed and customer documentation is left on site. Communication procedures with the ARC (if any) should be explained		
Obtain customer signature acknowledging receipt and correct operation of key/codes to the I&HAS		
Check that all surplus materials are removed from site and the premises left in a tidy condition		

NOTE The table is a suggested template for use. Other methods of recording the information can be used.

Annex B (normative) Preventative maintenance checks

B.1 General

Preventative maintenance should be in accordance with **B.2** (site visit) or **B.3** (remote system checks) and documented in accordance with Clause **9**.

B.2 Site visit

On-site preventative maintenance checks (inspection and test) should include the following:

a) ensure that the installed system meets the as-fitted document;

b) tamper detection;

NOTE 1 Check at least one tamper for correct operation through to the CIE.

c) setting and unsetting;

NOTE 2 Offer user(s) refresher system operation training, if required.

d) entry and exit procedures;

e) power supplies, including any APS;

NOTE 3 See Annex C.

f) functioning of detectors and HDs;

g) environmental conditions for adverse effects;

h) operation of WDs;

NOTE 4 Operation of self-powered WDs includes removal of hold-off voltage.

i) operation of ATS (all paths);

j) visual inspection for potential problems (electrical and physical).

The equipment should be correctly reinstated after testing.

B.3 Remote system checks

Remote system checks should include the following:

a) interrogate event record and take appropriate corrective action;

NOTE 1 This might require a site visit.

b) where applicable, check the system has been set and unset;

NOTE 2 This can be taken from the event record.

c) check no adverse tamper or fault conditions exist on the system where the system has this capability;

d) check any alarm circuits that are on soak test;

e) check any alarm circuits that are inhibited/isolated;

f) ensure time and date of clock are correct, update if required;

g) check PPS is available;

h) check health of any APS;

i) check that "frequently used" detectors are operating;

j) check operation of ATS (all paths).

Annex C (informative) Calculation of standby battery capacity

C.1 General

To calculate the battery capacity, it is necessary to take two current readings:

a) the current when there is no alarm present. This is known as the quiescent current; and

b) the current when in alarm with all WDs and ATE activated. This is known as the alarm current.

NOTE 1 The two different readings are required as the standby battery needs to be capable of providing power for the required duration including two periods when the system is in a full alarm condition.

*NOTE 2 Each alarm period can have WDs activated for 15 min. (see BS EN 50131-1:2006+A1:2009, **8.6**)*

C.1.1 Example of time period required in quiescent and alarm condition

If the required standby period is 12 h, as required at Grade 2, then the battery needs to be capable of providing sufficient power for 11.5 h at the quiescent current +0.5 h (2 × 15) min at full alarm current.

NOTE 1 If the standby period was 24 h then the time periods would be 23.5 h quiescent and 0.5 h in alarm.

The battery capacity can then be calculated as follows:

$$C = 1.25 \times [(I1 \times T1) + (I2 \times T2)]$$

where:

C	minimum capacity of battery in Ampere hours (Ah)
1.25	ageing factor (this represents a 25% deficit in battery life over the expected life of the battery)
I1	Quiescent current (A)
T1	Quiescent standby time (h)
I2	Alarm current (A)
T2	Alarm standby time (h)

NOTE 2 This calculation assumes that the control equipment and associated PSUs are type A (as described in BS EN 50131-1:2006+A1:2009), i.e. mains supply, and an alternative power source recharged by the control equipment/ PSU, where the alternative power source is a lead acid battery.

C.1.2 Example of battery calculation

A Grade 2 intruder alarm system with a quiescent current of 250 mA, alarm current of 750 mA (from above the standby period is 12 h with an assumed period of 30 min in alarm condition):

Quiescent load =
I1 × T1
= 0.25
× 11.5 = 2.875 Ah

Alarm load =
I2 × T2
= 0.75 × 0.5 = 0.375 Ah

$$C = 1.25 \times (2.875 + 0.375)$$
$$C = 1.25 \times 3.25$$
$$\mathbf{C = 4.06\ Ah}$$

The next highest available battery is to be used.

C.2 Measuring current on a I&HAS

C.2.1 Example measurement

An example of how to measure the quiescent current and alarm current of a typical intruder control panel is given in **C.2.2** and **C.2.3**.

C.2.2 Quiescent current (non-alarm condition)

C.2.2.1 Using a suitable test meter, such as a digital volt meter (DVM), set the meter to read DC Amps (select a high range such as 10 A).

C.2.2.2 Disconnect the positive charge lead from the battery terminal (normally a push on receptacle).

C.2.2.3 Connect the DVM in series between the positive battery terminal and the disconnected battery lead.

C.2.2.4 Disconnect the mains supply to the control panel.

C.2.2.5 The total current drawn by all equipment supplied by the control panel PSU is displayed on the DVM.

NOTE Typical readings could be between 0.2 A (200 mA) and 0.5 A (500 mA).

C.2.3 Alarm current (alarm condition)

Repeat the procedure in **C.2.2** with the system in full alarm state, e.g. with WDs sounding and ATE signalling.

NOTE A typical reading could be between 0.4 A (400 mA) – 0.7 A (700 mA).

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 4737 [1)], *Intruder alarm systems in buildings*

BS 6799[1)], *Code of practice for wire-free intruder alarm systems*

BS 7042[1)], *Specification for high security intruder alarm systems in buildings*

Further reading

BS 7671, *Requirements for electrical installations – IET Wiring Regulations*

BS 8243, *Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice*

BS EN 50131-5-3, *Alarm systems – Intrusion systems – Part 5-3: Requirements for interconnections equipment using radio frequency techniques*

[1)] Withdrawn.

This page deliberately left blank

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.