

Specification for

High security intruder alarm systems in buildings

UDC [696.6:654.924.3:.006.02]

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents

AVA

Document Sharing Hub

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Furniture and Household Equipment Standards Committee (FHM/-) to Technical Committee FHM/45, upon which the following bodies were represented:

- Association for Payment Clearing Services
- Association of British Insurers
- Association of Burglary Insurance Surveyors
- Association of Chief Police Officers of England and Wales
- Association of Metropolitan Authorities
- British Retailers' Association
- British Security Industry Association
- British Telecommunications plc
- Construction Security Advisory Service
- Consumer Policy Committee of BSI
- Department of the Environment (Property Services Agency)
- Electrical Contractors' Association
- Electrical Contractors' Association of Scotland
- Electrical Installation Equipment Manufacturers' Association (BEAMA Ltd.)
- Electricity Supply Industry in England and Wales
- Electronic Engineering Association
- Home Office
- Home Office Crime Prevention Centre
- Independent Associated Alarm Installers Ltd.
- Institution of Electrical and Electronics Incorporated Engineers
- Lloyd's Syndicates Survey Department
- Metropolitan Police
- Ministry of Defence
- National Association of Goldsmiths of Great Britain and Ireland
- National Supervisory Council for Intruder Alarms
- Post Office
- Royal Institute of British Architects
- Telecommunication Engineering and Manufacturing Association
- Tobacco Advisory Council
- Eine and Spirit Security Liaison Ltd.

The following bodies were also represented in the drafting of the standard, through subcommittees and panels:

- Building Societies Association
- Business Equipment and Information Technology Association
- Coopted member

This British Standard, having been prepared under the direction of the Furniture and Household Equipment Standards Committee, was published under the authority of the Board of BSI and comes into effect on 30 September 1988

© BSI 01-1999

The following BSI references relate to the work on this standard:
Committee reference FHM/45
Draft for comment 87/40338 DC

ISBN 0 580 16825 5

Amendments issued since publication

Amd. No.	Date of issue	Comments

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
1 Scope	1
2 Definitions	1
3 System requirements	4
4 Operational requirements	6
5 Detectors	7
6 Control equipment	9
7 Power supply equipment	10
8 Warning devices	10
9 Remote signalling equipment	12
10 Additional facilities	13
11 Claims of compliance	15
Appendix A Sound level test for audible warning devices	16
Figure 1 — Suggested method of suspension	17
Figure 2 — Method of measurement	18
Publications referred to	Inside back cover

Foreword

This British Standard has been prepared under the direction of the Furniture and Household Equipment Standards Committee. It has been published in response to requests for an enhanced level of security requirements for intruder alarm systems beyond those of BS 4737 and appropriate to the protection of premises, articles and/or operations of especial value or of a sensitive nature.

The value of any risk to which protection by an alarm system complying with this standard is appropriate is not quantified, since this will be dependent upon the view taken of the seriousness of any loss, which will differ in individual circumstances. Where the consequences of intrusion into, and/or loss from, premises are considered by a customer or an insurance company to be such as to require greater security than that provided by a system complying with BS 4737, the requirements of this standard are appropriate.

The standard provides the general requirements considered necessary for high security intruder alarm systems for premises, with some additional requirements for specific types of premises or activity such as cash-handling. It is intended to assist customers, insurers, alarm companies and the police in achieving a complete and accurate specification of the protection required in a particular location, but does not specify the extent or degree of protection nor does it necessarily cover all of the requirements for a particular installation.

Attention is drawn to the Institution of Electrical Engineers' *Regulations for Electrical Installations* (15th edition, 1981).

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 18, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

1 Scope

This British Standard specifies requirements for the construction, installation and operation of high security intruder alarm systems installed in buildings and in facilities at the shell thereof. Such systems consist of one or more detectors, one or more items of control equipment, one or more audible warning devices and the necessary signalling devices and power supply equipment.

This standard also applies to those systems in which the only detectors are deliberately-operated devices, i.e. “bandit” or “hold-up” alarm systems, and systems which use wire-free connections for deliberately-operated devices.

NOTE The titles of the publications referred to in this standard are listed on the inside back cover.

2 Definitions

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

2.1 General terminology

2.1.1

intruder alarm system

an electrical installation to detect and indicate the presence, entry or attempted entry of an intruder into protected premises

2.1.2

protected premises

that part of a building to which protection is afforded by an intruder alarm system

NOTE In a high security alarm system this may include facilities installed at the shell of cash-handling premises such as night safes and A.T.M.s (see 2.1.4).

2.1.3

cash-handling premises

a building or part of a building wherein the handling and/or transfer of currency takes place as a major part of the business of the occupier

NOTE Examples of cash-handling premises include banks, building societies and post offices.

2.1.4

automated teller machine (A.T.M.)

equipment enabling a customer to obtain banking services, principally the dispensing and/or receipt of cash, without teller assistance

2.1.5

shell

all parts of the boundary of a premises, i.e. walls, floor, roof, and including any openings therein

2.1.6

secure area

an area, within the protected premises, with an enhanced level of physical protection

NOTE Examples of secure areas include strong-rooms and vaults.

2.1.7

threshold

the approaches, internally within the protected premises, to a secure area

2.1.8

zone

one or more detector or processor circuits which may be set and/or unset together for an identifiable area or section of the protected premises

2.1.9

customer

an individual or organization utilizing the services of an alarm company for the installation of an intruder alarm system

2.1.10

alarm company

an organization prepared to provide and install an intruder alarm system

2.1.11

remote centre

premises, remote from those in which the alarm systems are fitted, in which the information concerning the state of alarm systems is collected for display or for onward transmission

NOTE This may be the customer's own facility.

2.1.12

entry route

the designated route between the outside of the protected premises and the control equipment, used when unsetting the system

2.1.13

exit route

the designated route between the control equipment and the outside of the protected premises, used when setting the system

2.1.14

alarm condition

the state of any detector, processor or tamper detection which indicates that intrusion, attempted intrusion or unauthorized interference has occurred

2.1.15

fault condition

a condition of any part of an intruder alarm system which has to be eliminated to restore correct operation

2.1.16
set

the state of an intruder alarm system, or part thereof, in which an alarm condition can be sent to warning devices and/or signalling equipment

2.1.17
unset

the state of an intruder alarm system, or part thereof, in which an alarm condition cannot be sent to warning devices and/or signalling equipment

NOTE Some circuits, such as those used for tamper detection or deliberately-operated devices, may remain in the set condition whilst the alarm system is apparently unset.

2.1.18
reset

the process of removing an alarm or fault condition thereby enabling a system to be set and including the act of setting

2.1.19
latching

a description applying to a condition which remains until deliberately removed

2.1.20
tamper detection

a means for the disclosure of the existence of unauthorized interference with a component of an installed intruder alarm system

2.1.21
shunting

the bypassing of a sensor, detector or processor circuit or part thereof

2.1.22
isolation

the exclusion of sensor, detector or processor circuits forming a recognizable zone

2.2 Equipment terminology**2.2.1**
sensor

a device which senses a change which could be caused by the intrusion or attempted intrusion by one or more persons but does not determine whether an alarm condition should be generated

2.2.2
sensor circuit

the connection between one or more sensors and a processor

2.2.3
detector

a device that generates an alarm condition in response to intrusion or to attempted intrusion, or to deliberate action

NOTE The term “detector” includes deliberately-operated devices (see 2.2.14).

2.2.4
coincidence detector

a detector requiring outputs from two or more sensors to generate an alarm condition

2.2.5
double-knock detector

a detector requiring two consecutive outputs from a single sensor to generate an alarm condition

2.2.6
dual technology detector

a detector requiring outputs from two sensors using differing detection principles to generate an alarm condition

2.2.7
video motion detector

a detector generating an alarm condition in response to a change in the signal from one or more closed-circuit television cameras

2.2.8
audio detector

a detector generating an alarm condition in response to sound

2.2.9
listening channel

a communications link for the routine monitoring of sounds at a protected premises and/or the transmission of those occurring during an alarm condition

2.2.10
sensitivity

the performance of a detector in terms of the level of activity, i.e. noise, movement, etc., required for the generation of an alarm condition by the detector

2.2.11
detector circuit

the connection between one or more detectors and the control equipment of an intruder alarm system

2.2.12
processor

a device which processes the output from one or more sensors to determine whether an alarm condition should be generated

NOTE A processor may be integral with control equipment.

2.2.13**processor circuit**

the connection between one or more processors and the control equipment, if they are housed in separate containers

2.2.14**deliberately-operated device**

a detector that creates an alarm condition as the result of deliberate action by one person

2.2.15**protective switch**

a detector associated with a movable part, such as a door or window, and generating an alarm condition when the movable part is opened

2.2.16**power supply equipment**

equipment providing power for the operation of an intruder alarm system or any component thereof

2.2.17**control equipment**

equipment necessary for the setting, unsetting and testing of an intruder alarm system and for sending an alarm condition to warning devices and/or signalling equipment

2.2.18**ancillary control equipment**

equipment, connected to the control equipment, used for completion of the setting procedure and/or for the initiation of the unsetting procedure and/or for circuit indication

2.2.19**programmer**

automatic equipment providing preset time windows during which the manual performance of setting or unsetting operations is allowed

2.2.20**end-of-line device**

a component of a circuit, within an intruder alarm system, which provides a potential difference across the circuit at a point where that circuit apparently terminates

NOTE Typical end-of-line devices include batteries, resistors and transformers.

2.2.21**shunt lock**

a door lock incorporating a switching device within the lock case

2.2.22**differ**

the variation between locks, electronic devices or magnetic coded devices of similar design which allows each lock or device to be operated only by its own key or code

2.2.23**lock switch**

a switch actuated by a door lock such that its state changes when the lock is opened or closed

2.2.24**door switch**

a switch actuated by a door such that its state changes when the door is opened or closed

2.2.25**shunt switch**

a switch operated by a key, combination or other secure means

2.2.26**security camera**

a device providing visual images for the purposes of detection, surveillance and/or suspect recognition

2.3 Warning device terminology**2.3.1****warning device**

a device that gives an indication at the protected premises that an alarm condition has occurred within the protected premises

2.3.2**external audible warning device**

a sound-producing device located outside the protected premises

2.3.3**internal audible warning device**

a sound-producing device located within the protected premises

2.4 Signalling terminology**2.4.1****signalling**

the transmission of information regarding the status or change of status of an alarm system from the protected premises to a remote location

2.4.2**digital communicator**

signalling equipment that automatically communicates using a switched telephone network to exchange encoded information on the state of the alarm system

2.4.3**dedicated transmission path**

a continually available communications link which does not require to be established for the transmission of information concerning the state of an alarm system

NOTE This includes communications links which require an initial switching operation to select one of a number of alternative paths and those in which alarm system data are superimposed on an existing communications channel.

3 System requirements

3.1 Components

All systems shall have the following components.

- a) *Detectors*: one or more detectors and/or one or more sensors with associated processors complying with clause 5.

NOTE Detectors using operating principles not specified in clause 5 may additionally be included in a system provided that the system complies with this standard and that their use is agreed in writing between the customer and the alarm company. Where a relevant specification exists in Part 3 of BS 4737 a detector should comply with this.

- b) *Control equipment*, complying with clause 6.
- c) *Power supply equipment* complying with clause 7.
- d) *Audible warning devices*: one or more audible warning devices complying with 8.2 or 8.3.
- e) *Signalling*: one or more dedicated transmission paths with a standby digital communicator complying with clause 9.

3.2 General requirements

3.2.1 Housing. Where required by the appropriate clauses of this British Standard, equipment shall be enclosed in one or more separate containers, each of which shall be constructed from one or more materials from the following list:

- a) low carbon steel not less than 1.2 mm thick;
- b) stainless steel not less than 1 mm thick;
- c) material offering durability, security of fixing and resistance to attack by hand-held tools, including burning methods, at least the equal of the foregoing.

The equipment container(s) shall be firmly secured in position and shall be fitted with tamper detection, which will operate when the lid or access panel is opened by the normal means and when the container is removed from its mountings. The position of a tamper detection switch shall not be discernible from the outside of the container.

The connection between separated containers shall be mechanically and electrically protected.

3.2.2 Tamper detection. The operation of tamper detection shall generate an alarm condition. When the system is unset, any such alarm condition shall cause an audible indication which shall sound until it is inhibited manually by a means affording a degree of security not less than that provided by a key-operated switch of 1 000 differs.

NOTE 1 This may be incorporated in the same means used for initiating the setting of the system, e.g. by the use of a multiposition, key-operated switch.

NOTE 2 Where required, tampering during the unset period may additionally be signalled.

During any period when operation of the audible indication is inhibited, a visible indication shall be given at the control equipment, and the system shall not set.

When the system is set, an alarm condition resulting from the operation of tamper detection shall be signalled.

The zone in which tamper detection has been activated shall be indicated at the control equipment.

3.2.3 Operating procedures. The agreed setting, unsetting and operating procedures shall be clearly and legibly set out and given to the customer.

NOTE 1 The procedures are the subject of agreement between the alarm company and the customer.

When the system is handed over the alarm company shall give a practical demonstration of the operating procedures.

NOTE 2 It is the customer's responsibility to ensure that occupants of the protected premises are familiar with and observe the agreed procedures. Where appropriate, occupants should be made aware of the location of any deliberately-operated device(s).

3.2.4 Documentation. Upon completion of installation of the alarm system, the alarm company shall prepare a system record which shall include the following information:

- a) the name and address of the protected premises;
- b) the name and address of the customer;
- c) the type and location of each detector and the type and location of each sensor and processor. If a processor requires more than one input to generate an alarm condition, the details of such inputs shall be given;
- d) the type and location of control equipment and power supplies;
- e) details of those circuits which the customer or remote centre has the facility to shunt or isolate and any shunting or isolation facilities provided for warning devices or signalling equipment;
- f) the type and location of each warning device;