BRITISH STANDARD

BS 7992:2002

Code of practice for

Exterior deterrent systems

ICS 13.320

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/2, Installed alarm systems, upon which the following bodies were represented:

Alarms Inspectorate and Security Council
Association of British Insurers
Association of Burglary Insurance Surveyors
Association of Chief Police Officers of England, Wales and Northern Ireland
Association of Security Consultants
British Bankers' Association
British Security Industry Association
Building Research Establishment
Consumer Policy Committee of BSI
Co-opted members
Electrical Contractors' Association
Low Power Radio Association
Metropolitan Police
National Security Inspectorate
Security Facilities Executive
Security Industry Training Organization
Security Systems and Alarms Inspection Board

This British Standard, having been prepared under the direction of the Consumer Products and Services Sector Policy and Strategy Committee, was published under the authority of the Standards Policy and Strategy Committee and comes into effect on 18 January 2002

© BSI 18 January 2002

First published as DD 231 February 2000
Second edition 18 January 2002

The following BSI references relate to the work on this standard:
Committee reference GW/1/2

ISBN 0 580 37449 1

Amendments issued since publication

Amd. No.	Date	Comments

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

Contents

		Page
Committees responsible		Inside front cover
Foreword		ii
1	Scope	1
2	Normative references	1
3	Abbreviations	1
4	Terms and definitions	1
5	System attributes	5
6	System components	10
7	Application guidelines	12
Annex A (informative) Examples of descriptions of the operating characteristics of exterior deterrent systems		16
Bibliography		18

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

Foreword

This British Standard has been prepared by Subcommittee GW/1/2 and supersedes DD 231:1996, which has been withdrawn. It aims to cover a type of intruder alarm system which is not provided for in BS 4737-4.3:1988.

BS 4737-4.3:1988 covers intruder alarm systems in which the balance of the system is located external to any premises and which provide security comparable with that specified in BS 4737-1:1986.

BS 7992 is a new edition of DD 231 and incorporates technical changes only. It does not reflect a full review or revision, which will be undertaken in due course.

Suppliers and installers of security systems have identified a commercial need for systems which normally issue a caution, admonition, or other forewarning before generating a full security alert. Such security systems may be suitable particularly for supervising exposed sites that do not have controls such as barriers or manned patrols to physically restrict public access, and/or for supervising property such as vehicles, machinery, boats, other articles or goods stored within such sites or in the general vicinity of such sites.

BS 4737-4.3 does not include provision for such sites, as it states that there should be at least one soundly constructed barrier or other effective means of restricting access to any exposed supervised site. Moreover, it does not offer guidance regarding systems which incorporate more than one stage or level of security alert (e.g. forewarning, followed by full-warning); and there are other provisions of BS 4737-4.3 that may not be appropriate for such security systems.

Consideration of the above matters has led to the development of this document.

Security systems covered by this British Standard differ in their purpose and mode of operation from those within the scope of BS 4737-1 and BS 4737-4.3. It is not intended that BS 4737-4.3 and this British Standard be regarded as comparable or equivalent. This document is not intended to supersede BS 4737-4.3:1988.

It should be noted that the limited supervision afforded to a building by a security system within the scope of this British Standard is not equivalent to that provided by an intruder alarm system conforming to BS 4737-1. In particular, where comprehensive supervision of a building (or part of a building) is required, an intruder alarm system conforming to BS 4737-1 should be specified and used.

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.

Annexes designated “normative” are part of the body of the standard. Annexes designated “informative” are given for information only. In this standard, Annex A is informative.

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 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.

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

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

© BSI 18 January 2002

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

1 Scope

This British Standard gives recommendations for the planning, equipment and installation of security systems which provide supervision principally to open areas, surroundings of buildings, or property (for example vehicles or machinery) located outdoors and which can provide two or more stages of alert.

Police-calling security systems are not within the scope of this document.

NOTE Although security systems within the scope of this British Standard are intended primarily to supervise areas and/or property that are located outdoors, systems which include supervision of a small office or cabin, or of a room in which the system's own control and indicating equipment is located, are not excluded, provided that such supervision forms only a minor part of the system.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this British Standard. For dated reference, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the publication referred to applies.

BS 3535-1, *Isolating transformers and safety isolating transformers — Part 1: General requirements.*

BS 3535-2, *Isolating transformers and safety isolating transformers — Part 2: Specification for transformers for reduced system voltage.*

BS 4737, *Intruder alarm systems.*

BS 4737-3, *Intruder alarm systems — Part 3: Specifications for components.*

BS 4737-4.1:1987, *Intruder alarm systems — Part 4: Codes of practice — Section 4.1: Code of practice for planning and installation.*

BS 4737-4.2, *Intruder alarm systems — Part 4: Codes of practice — Section 4.2: Code of practice for maintenance and records.*

BS 4737-4.3:1988, *Intruder alarm systems — Part 4: Codes of practice — Section 4.3: Code of practice for exterior alarm systems.*

BS 7150, *Code of practice for intruder alarm systems with mains wiring communication.*

BS EN 60529:1992, *Specification for degrees of protection provided by enclosures (IP code).*

3 Abbreviations

ACE	ancillary control equipment
ARC	alarm receiving centre
ATE	alarm transmission equipment
ATS	alarm transmission system
CIE	control and indicating equipment
EDS	exterior deterrent system
PAWD	primary audible warning device
RCD	residual current device (current-operated earth-leakage circuit breaker)

4 Terms and definitions

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

4.1
alarm company
organization which provides services for alarm systems

4.2
alarm receiving centre
continuously manned centre to which information concerning the status of one or more alarm systems is reported

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

4.3
alarm system
electrical installation which provides an audible and/or visual warning, and/or a signal to an ARC, in response to the detection of a hazard

4.4
alarm transmission system
equipment and network used to transfer information on the state of one or more alarm systems to one or more ARCs

4.5
automatic dialling equipment
signalling equipment that automatically dials a predetermined telephone number and subsequently transmits a voice message via a switched telephone network

4.6
continuing activity
activity that does not cease promptly after a first-stage warning

4.7
control and indicating equipment
equipment for receiving, processing, controlling and indicating information, and for initiating its onward transmission

4.8
dedicated transmission path
transmission path which is continuously available for the connection of an alarm system to its associated ARC and which does not require switching or setting-up prior to the transmission of individual security alerts

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

4.9
detector
device designed to sense an abnormal condition which indicates a hazard, and to generate a signal or message in response

NOTE A detector may comprise one or more sensors and a processor.

4.10
differ
variation between locks, electronic devices or magnetically coded devices of similar design, which allows each lock or device to be operated only by its own key or code

4.11
digital communicator
signalling equipment that automatically communicates using a switched telecommunications network and exchanges information on the state of the EDS

4.12
end-of-line device
component of a circuit, within an EDS, 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.

4.13
entry/exit route
route for authorized access to the supervised area

© BSI 18 January 2002

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

4.14
exterior deterrent system
security system supervising principally open areas or the surroundings of a building, and which, when in its fully set mode, provides two or more stages of security alert

4.15
external loudspeaker
speaker, not located within a building, equipped to broadcast a recorded voice message

4.16
fault condition
condition of an EDS which prevents the system from functioning normally

4.17
full-warning
ultimate stage of security alert attained by an EDS when the supervised area or supervised property has been subjected to continuing and/or gross activity

4.18
gross activity
any type of trespass that gives rise to full-warning as soon as it is detected by the EDS

NOTE Examples of gross activity are trespass into a large or significant area of the supervised area, trespass deep into the supervised area, or trespass within an article of supervised property.

4.19
latching
state whereby a condition or indication remains until deliberately cancelled

4.20
notification
passing of a security alert, tamper alert or fault condition to warning devices and/or ATSs

4.21
power supply
part of an alarm system which provides power for the EDS or any part thereof

4.22
primary audible warning device
warning device (external or internal) consisting of a sound-producing device which sounds under specified conditions, as recommended in this British Standard for devices that have been so designated

NOTE 1 The term "primary audible warning device" does not apply to a loudspeaker equipped to broadcast a recorded voice message.

NOTE 2 Any audible warning device which has not been designated in the system record as being a PAWD is regarded as not being a PAWD.

4.23
processor
device which processes the output from one or more sensors to determine whether a security alert should be generated

NOTE The processor may be integral with the CIE.

4.24
processor circuit
connection between one or more processors and the CIE, if they are housed in separate containers

4.25
restore
procedure of cancelling a security alert, tamper alert, fault or other condition and returning the EDS to its set condition

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

4.26
security alert
state of any detector, processor or tamper detection device which indicates that activity or unauthorized interference has occurred or is about to occur

NOTE An EDS has two or more stages of security alert.

4.27
security lighting
lighting that is automatically switched on at the supervised area or in the vicinity of the supervised property when a security alert occurs within the supervised area or in or at the supervised property

4.28
sensor
part of a detector which senses a change in condition

4.29
sensor circuit
connection between one or more sensors and a processor

4.30
set
state of an EDS or part thereof in which a security alert can be notified

4.31
shunt lock
door lock incorporating a switching device within the lock case

4.32
signalling
initiating of transmission of a security alert from the supervised area, or from the vicinity of the supervised property, to a remote location

4.33
subscriber
person or organization using the services of an alarm company for the installation of an EDS

4.34
supervised area
area in which a hazard can be detected by an EDS

4.35
supervised property

a) property (for example, vehicles, machinery, boats, goods) which is located within the supervised area

b) property in which a hazard can be detected by the EDS and which is located not more than 500 m outside the boundary of the supervised area or, if there is no supervised area, not more than 500 m from the CIE of the EDS

4.36
system attributes
characteristics of an EDS arising from its design and configuration

4.37
tampering
deliberate interference with an EDS or part thereof

4.38
tamper condition
state of an EDS in which tampering has been detected

 © BSI 18 January 2002

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

4.39
tamper detection
detection of tampering

4.40
tamper protection
methods or means used to protect an EDS or part thereof against tampering

4.41
unset
state of an EDS or part thereof in which a security alert cannot be notified

4.42
user
person authorized to operate an alarm system

4.43
warning device
device which indicates at the supervised area or in the vicinity of the supervised property that a security alert has occurred within the supervised area or in or at the supervised property

NOTE Audible warning devices (external or internal), loudspeakers, stroboscopic lights and floodlights are examples of warning devices.

5 System attributes

5.1 General

5.1.1 The EDS should include attributes for the detection of intruders, processing of information and notification of security alerts, and the means to operate the EDS.

On first detecting activity within the supervised area (or within or near the supervised property), an EDS does not normally give full-warning, but issues a caution, admonition, or other forewarning (e.g. actuation of security lighting and/or of a recorded voice message by loudspeaker) to deter persons from continuing a trespass.

Normally, provision is also made for giving a local audible warning and/or summoning assistance if persons fail to heed the forewarning(s) and continue their trespass.

Provision may also be made for giving a full-warning without delay, if gross activity is identified.

There may be intermediate stages of security alert between the initial warning and full-warning.

If detected activity within the supervised area (or within or near the supervised property) ceases promptly after first-stage warning, or at any subsequent stage, the security system normally reverts to its quiescent watchful state.

Typical stages of security alert provided by a security system within the scope of this document are as follows:

— first-stage warning: security lighting;
— second-stage warning: recorded voice message broadcast by loudspeaker;
— third-stage warning: sounding of audible warning device;
— full warning: signalling to an ARC.

Other configurations are possible.

5.1.2 To ensure the optimum reliability of the EDS, the following should be considered:

a) environmental suitability: measures to ensure that the EDS functions correctly and reliably under given environmental conditions;

b) operational reliability: measures to ensure the simple and correct operation of the EDS;

c) functional reliability: the selection of EDS components according to their suitability for the required application.

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

5.2 Components

An EDS should include the following components:

a) CIE, which may be incorporated in any other system component;

b) one or more detectors and/or one or more sensors with associated processor(s);

c) one or more PAWDs;

d) one or more power supplies, which may be combined with other system components or may be housed separately.

Additionally, an ATS may be incorporated.

Systems incorporating an ATS may be configured so that the PAWD sounds only as described in **6.5.5**.

Systems incorporating an external loudspeaker may be configured so that the PAWD sounds only in the event of a tamper condition.

5.3 Environmental suitability

To ensure the correct performance of the system, components should be suitable for use in the environment in which they are required to operate.

The influence of environmental conditions should not change the state of the EDS, nor damage system components nor substantially change system performance.

5.4 Functions

5.4.1 *Detection of intruders and recognition of faults*

5.4.1.1 *General*

The EDS should include means for the detection of intruders and of tampering, and for the recognition of faults.

Other events may be detected, provided that this does not adversely affect the detection of intruders and tampering, and the recognition of faults.

Detectors should be configured so that any failure to communicate with the CIE within the required time period should be treated as a tamper signal.

When a detector relies upon the interruption of an interconnection to create an intruder or tamper signal, the intruder signal should be different from a tamper signal.

NOTE 1 This includes instances where the interconnection passes directly through a mechanical or magnetic switch (contact) or through the relay of a detector or a tamper switch (contact).

When an interconnection is extended to form an intruder detector or tamper detector, the resulting signal should be treated as an intruder or tamper signal.

NOTE 2 In this case, the CIE effectively forms part of the detector, as the CIE is directly monitoring that part of the interconnection which is acting as a detector. (An example is continuous wiring.) Means provided to adjust the field of view of a detector should be made inaccessible to unauthorized personnel. Alternatively there should be means to detect unauthorized adjustment. In this case, unauthorized adjustment should be treated as tampering. Care should be taken to minimize the risk of accidental adjustment.

5.4.1.2 *Intruder detection*

An EDS should only include detectors which are suitable for the environment and application. A detector can incorporate more than one form of technology; for example, passive infra-red and microwave or ultrasonic.

Individual detectors may be logically grouped so that the generation of one or more intruder signals or messages from one or more detectors is necessary to generate a security alert.

An individual detector may be configured so that more than one activation is necessary to generate an alarm signal or message.

Detectors can be classified as follows:

a) simple change of state devices; for example, mechanically or magnetically operated devices;

b) active detection devices, i.e. devices which include active components; for example, movement or vibration detectors.

Active detection devices should provide individual means to confirm that they are operational.

 © BSI 18 January 2002

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

5.4.1.3 *Recognition of faults*

The system should be able to recognize the following faults:

a) primary power fault;

b) primary cell fault (where fitted);

c) fault in the CIE;

d) fault in the ATS (where provided).

Other faults may be recognized, provided that this does not adversely affect the recognition of faults a) to d).

5.4.2 ***Operation***

5.4.2.1 *Design*

The EDS should be designed so that the possibility of operator error during setting or unsetting is minimized. Partial setting or unsetting may be possible.

5.4.2.2 *Authorization*

NOTE The owner of the EDS has the absolute authority over the system. This authority may be delegated to others.

Access to the system should be restricted by the use of physical keys which provide a degree of security not less than that provided by a key-operated switch of 200 differs, or by means of logical keys which provide a degree of security equivalent to that of a key-operated switch of 10,000 differs.

In order to isolate or bypass any sensor, detector or processor circuit while the system is in the set mode, it should be necessary to operate a shunt lock of not less than 200 differs, or other means offering an equivalent degree of security.

The CIE or ACE may incorporate a programmed timeswitch, provided that the means of changing the programme is protected by a degree of security not less than that afforded by a key-operated switch of 200 differs.

5.4.2.3 *Setting and unsetting*

For an EDS (with or without ATS) in which setting and unsetting are not carried out in conjunction with an ARC or remotely, initiation of the setting or unsetting of the EDS or part thereof should be effected by means of either the CIE or ACE.

For an EDS in which setting and unsetting are carried out in conjunction with an ARC there should be an audible or visual indication at the supervised area, or in the vicinity of the supervised property, that the agreed setting procedure is being followed and has been successfully completed. There should be an audible or visual indication at the supervised area, or in the vicinity of the supervised property, that an unsetting procedure agreed with the ARC is being followed and has been successfully completed.

5.4.2.4 *Restoring*

Following activation, any part of the EDS, including the ATS, should be restored, either automatically or by means of a signal transmitted from an ARC, to its pre-activation quiescent watchful condition, so that it is able to generate and/or signal a further security alert.

Following restoring after a security alert, no indication need be given during unsetting procedures.

5.4.2.5 *Inhibit and isolate operations*

The EDS may include a means of inhibiting or isolating individual functions or groups of functions. Access to this should be restricted to users by the means described in **5.4.2.2**. A programmable timeswitch may be used to inhibit the functioning of certain parts of the security system while in the set mode, but it should not be possible to use the timeswitch to fully set or unset the EDS.

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

5.4.3 *Processing*

5.4.3.1 *Full-warning condition*

An EDS should be so configured that in full-warning a PAWD (see **6.4**) sounds, and/or remote signalling in accordance with **6.5** is triggered.

Techniques should be employed, wherever possible, to confirm a full-warning condition; for example, by the comparison, summation or other analysis by the CIE of information generated within a defined interval of time:

a) by more than one sensor or detector;

b) by the repeated triggering of a single sensor or detector.

Full-warning should be generated if gross or continuing activity is detected. If activity sufficient to generate a first-stage warning continues unabated, the EDS should generate full-warning within 2 min of generation of the first-stage warning.

5.4.3.2 *Tamper signals*

When the system is unset, any tamper condition should cause an immediate audible warning at the CIE, at the supervised premises or in the vicinity of the supervised property. This warning should sound until it is cancelled manually by a key-operated switch of 200 differs or by another means that provides an equivalent degree of security.

NOTE The means for cancelling the tamper alarm may be incorporated in the means used for initiating the setting of the system, e.g. a multi-position, key-operated switch.

When the system is set, any tamper condition should create a full-warning.

5.4.4 *Indications*

Indications should be given in one central location convenient for the user. Indications may also be provided at other locations. Indication may be audible, visual, or both.

5.4.5 *Notification*

Notification of conditions should depend on the type of condition and on the status of the EDS. Notification may be by a warning device, remotely powered or self-powered, or by an ATS.

An ATS may signal either to an ARC or to a local console as part of a subscriber/zone monitoring facility.

In systems including two or more warning devices, the warning devices should be interconnected so that any tamper condition in any warning device should cause all other warning devices to operate without delay.

Notification may be supplemented by means such as loudspeakers or mains driven sirens, provided that the use of such devices does not prevent the correct operation of the PAWDs.

Where an ATS is supplemented with a warning device, there may be a delay not exceeding 10 min in operating the warning device. The operation of the warning device may be inhibited if the notification by the ATS is confirmed by the ARC or other receiving facility during this period. If a fault which affects all available ATS transmission paths is detected, any such delay should be automatically eliminated.

Audible warning devices should operate for a minimum of 30 s unless a shorter period is demanded by local legislation. The maximum operating period for an audible warning device should be 20 min. There should be a facility to permit the use of a visible warning device to supplement the audible warning device.

Audible warning devices may be located inside or outside the supervised areas determined by the user.

5.4.6 *Tamper security*

5.4.6.1 *Tamper protection*

All terminals and means of mechanical and electronic adjustment should be located within the component housing.

Housings should be sufficiently robust to prevent undetectable access to internal components.

The means of access to internal elements of CIE, ACE and warning devices should be secured with a minimum of two screws or bolts, or alternatively by a mechanical lock.

The means of access to detection devices should be secured by a minimum of one screw or by an equivalent fastener requiring a tool.

 © BSI 18 January 2002

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

5.4.6.2 *Tamper detection*

Means should be provided to detect tampering with system components. System components located outside the supervised area should be provided with a higher degree of tamper detection than those installed inside the supervised area.

Tamper detection should be incorporated in the following system components:

a) CIE/ACE;

b) PAWDs;

c) loudspeakers;

d) detection devices;

e) processors;

f) junction boxes;

g) ATE;

h) power supplies.

Tamper detection should be active in both the set and unset modes.

The following forms of tampering should be detected:

1) opening by normal means;

2) removal from mounting (excluding loudspeakers and junction boxes);

3) interference with externally sited PAWDs;

4) change of detector orientation;

5) masking of movement detectors.

The PAWD should sound in the event of an electrical change to its connection(s) to the CIE, or if its tamper detection operates.

5.4.6.3 *Monitoring of interconnections*

Interconnections should allow communication between system components within the time periods specified for the installation.

Interconnections between system components may be of the following types:

a) specific wired links;

b) non-specific wired links;

c) wire-free links.

Interconnections should be monitored to ensure that the means of communication between system components are continuously available, and also to detect tampering and to recognize faults which affect the operation of the EDS.

Failure of communication between system components should be detected within 10 s.

5.4.6.4 *Ancillary equipment*

Ancillary equipment located outside the supervised premises should have appropriate tamper protection and detection.

5.5 Power supply

5.5.1 The recommendations of **5.5.2**, **5.5.3** and **5.5.4** apply to all items of power supply equipment (including those fitted as an integral part of any CIE, sensor or detector, and those for dedicated transmission path signalling equipment), with the exception of power supplies for:

a) PAWDs;

b) security lighting;

c) sensors and detectors using wire-free links;

d) signalling equipment (other than for dedicated transmission path signalling equipment).

5.5.2 Where a public mains electricity supply is continuously available at the supervised area or in the vicinity of the supervised premises, the EDS should have at least two sources of power. The prime source, used when the system is operating normally, should be the primary mains electricity supply. The alternative source should be capable of supporting the system for a predetermined period if the prime source fails. A change-over between the prime source and the alternative source should not trigger a security alert.

NOTE It is accepted that mains-operated security lighting cannot be supported by an alternative power source consisting of storage devices.

An alternative power source should be capable of powering the system for at least 12 h of normal operation when the prime source of power is unavailable.

The alternative power source should be brought automatically into use immediately the mains voltage falls below the level necessary to ensure that the output voltage is sufficient to operate the EDS. When mains voltage is restored to its minimum rated value, the system should revert to mains power and any stand-by battery should recharge automatically.

5.5.3 When the prime source is reinstated, the power supply should have sufficient capacity to support the normal load of the EDS and simultaneously to recharge any stand-by battery to the required capacity within 24 h.

NOTE For the purpose of calculating battery capacity, normal operation of an EDS may be regarded as the condition in which the system is fully set but no-one is present within the supervised area or in or close to the supervised property.

5.5.4 Where no public mains electricity supply is available, the system may be powered by storage devices (batteries).

The period of time for which the battery provides for the normal load of the system should be stated in the system documentation, and should indicate the period in security alert mode that has been allowed for in calculating the overall period.

5.6 Operational reliability

CIE should be clearly and unambiguously marked, and logically arranged so as to minimize the possibility of operator error.

5.7 Functional reliability

System components should be selected for their compatibility and suitability for the required application and likely environmental conditions.

5.8 Documentation

Documentation relating to the EDS should be concise, complete and unambiguous. Information on maintenance, servicing and operation should be provided. The information should be sufficient to ensure the reliable functioning of the EDS.

Instructions relating to the operation of the system should be designed to minimize the possibility of operator error.

6 System components

6.1 Enclosures

Enclosures for components should be constructed from materials offering durability, security of fixing and resistance to attack.

6.2 Control and indicating equipment

6.2.1 CIE should be located within the supervised area (if any) or in a secure building.

6.2.2 CIE and processors which are not located within a building should be contained within a lockable enclosure providing a degree of protection of IP55 in accordance with BS EN 60529.

NOTE To comply with the recommendations of **6.1** and **6.2.2**, it is permissible to use a double enclosure, the inner casing constructed from materials which are durable, securely fixed and resistant to attack, the outer casing providing a degree of protection of IP55. Alternatively, a single enclosure which combines all these attributes may be used.

6.2.3 Processors should be enclosed with the CIE, or within separate enclosures.

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

 © BSI 18 January 2002

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

6.2.4 Timeswitches should be regarded as part of the CIE, and in respect of their location, housing and tamper protection should comply with the recommendations applicable to CIE. Timeswitches should be provided with a battery back-up such that their operation is not affected by a mains power failure of up to 12 h duration.

If a timeswitch fails, the EDS should remain in or revert to its fully set mode.

6.3 Sensors and detectors

Sensors and detectors should conform to the relevant Section(s) of BS 4737-3.

Sensors and detectors which are not located within a building or enclosed within supervised property should be contained within enclosures providing a degree of protection of IP53 in accordance with BS EN 60529.

6.4 Warning devices

The PAWD should conform to the requirements for warning devices given in the relevant Parts of BS 4737 except where this British Standard makes a recommendation to the contrary.

NOTE Audible warning devices which are supplementary to the PAWD need not conform to BS 4737.

External loudspeakers need not be housed.

6.5 Alarm transmission systems

6.5.1 The ATS equipment and its connection to the transmission path should be located within the supervised area or in a secure building in the vicinity of the supervised property.

6.5.2 ATS equipment which is not located within a building should be contained within a lockable enclosure providing a degree of protection of IP55 in accordance with BS EN 60529.

6.5.3 Automatic dialling equipment, digital communicators and dedicated transmission path equipment should conform to the relevant Parts of BS 4737, except where this British Standard makes a recommendation to the contrary.

6.5.4 ATS should include the facility to override any attempt to block the transmission path by “ringing in” or “dialling out”. Otherwise, the transmission path should be configured for “outgoing calls only”, or an ex-directory line should be used.

6.5.5 If an EDS is configured so that it is possible for a security alert condition to be signalled to a remote location without a PAWD having sounded, the transmission path should be monitored. If a fault, “off-hook” or “ringing-in” is detected and the ATS is unable to transmit, at least one PAWD should sound within a period of 30 s after the presentation of any security alert condition which was intended to have been signalled to a remote location.

6.6 Power supply equipment

6.6.1 *General*

Power supply equipment should be located within the supervised area or in a secure building.

Power supply equipment which is not located within a building should be contained within a lockable enclosure providing a degree of protection of IP55 in accordance with BS EN 60529.

Power supply equipment should conform to the relevant Parts of BS 4737, except where this British Standard makes a recommendation to the contrary.

Where the prime power source is the public mains electricity supply, it should be permanently connected (i.e. not by plug and socket) via a fused outlet, situated adjacent to the CIE and incorporating a safety isolating transformer which conforms to BS 3535-1 and, if relevant, BS 3535-2.

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

6.6.2 *Security lighting*

The electrical protection against overload and/or earth-leakage afforded to circuits supplying mains-operated security lighting controlled by an EDS should be so designed and configured that a fault or overload in the security lighting circuit does not cause failure of the mains supply to any other part of the EDS or to any other final sub-circuit of the electrical installation. Similarly, a fault or overload in any other final sub-circuit of the electrical installation should not cause failure of the mains supply to the security lighting. For example the security lighting may be fed from a separate fuse or over-current circuit breaker at the final distribution board. If RCDs are used, a separate RCD should be provided for the security lighting circuit.

NOTE Security lighting which is powered from the mains electricity supply via a step-down transformer is regarded as mains-operated.

6.7 Interconnections

6.7.1 *General*

Interconnections, including wiring, jointing and flexible interconnections, should conform to the relevant Parts of BS 4737, except where this British Standard makes a recommendation to the contrary.

Interconnections between the main CIE and its separate power supplies (if any) should be mechanically protected.

Any cable containing wires that supply an external loudspeaker should be electrically protected such that, on severance of the cable, a tamper condition is created.

Junction boxes which are not located within a building should provide a degree of protection of IP55 in accordance with BS EN 60529.

6.7.2 *Wire-free interconnections*

Wire-free interconnections should provide the following:

a) transmission of a signal when a sensor or detector has detected activity, or transmission of other signals from the CIE as appropriate, such as signals to warning devices;

b) local or remote annunciation of a low voltage or high impedance condition of a transmitter battery before it becomes incapable of supporting 3 days' normal operation in addition to the generation of the fault signal;

c) capability for the communication channel in use to be monitored so that the presence of any continuous blocking or interfering signals which are present for more than 30 s and which could prevent the reception of legitimate signals are detected, and a fault indication is generated at the receiver. It is necessary to agree the action to be taken when this indication is generated.

Consideration should be given to providing indicators (at the receiver) to show which of the transmitters has operated.

6.7.3 *Mains wiring communication*

Mains wiring communication should provide the features recommended in BS 7150 for a class 3 system.

7 Application guidelines

7.1 System design

7.1.1 *System planning*

The planning of an EDS should follow the relevant recommendations given in clause **3** of BS 4737-4.1:1987.

In determining the operational characteristics of an EDS, it is important to have due regard for environmental considerations, and particularly for minimizing noise nuisance.

The existing and potential environmental conditions at the supervised area and in the vicinity of the supervised property should be taken into consideration when planning the type of system to be installed. Reference should be made to clause **3.2** of BS 4737-4.3:1988, for examples of environmental conditions that may cause problems with exterior security systems.

The detailed inspection of a site, with particular reference to local conditions, is essential in order to select the most appropriate form(s) of detection and to minimize the potential for false security alerts.

 © BSI 18 January 2002

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

7.1.2 *Sensors and detectors*

General guidance on the use of various types of sensors and detectors in exterior situations is given in clause **5.2** of BS 4737-4.3:1988. However, it should be noted that the first paragraph of **5.2.2.1** of BS 4737-4.3:1988 is not appropriate to exterior deterrent systems covered by this British Standard.

Sensors and detectors monitoring a supervised area should be so configured or so grouped as to allow ready identification of any part of the supervised area that has suffered trespass.

Sensors and detectors monitoring specific articles of supervised property should be so configured or so grouped as to allow ready identification of the specific sensor or detector that has been triggered.

For linear fence-mounted or similar boundary-type detectors, the length of a detection zone should not exceed 100 m, and each zone should have latching indication.

Where buried or vibration-sensitive detectors are used, care should be taken to ensure that zones do not cross differing materials of construction or geological strata.

7.1.3 *Documentation prior to installation*

The design specification should include a prominent notice to the following effect, which should be in capital letters at least 2.4 mm in height and not smaller than the lettering used for the main body of the design specification.

> THIS SECURITY SYSTEM IS NOT INTENDED TO BE AN INTRUDER ALARM CONFORMING TO BS 4737.
>
> IT IS AN EXTERIOR DETERRENT SYSTEM AND IT IS INTENDED MAINLY FOR SUPERVISING OPEN (i.e. UNFENCED) AREAS (SUCH AS FORECOURTS) OR PROPERTY STORED IN SUCH OPEN AREAS.
>
> THIS EXTERIOR DETERRENT SYSTEM IS INTENDED TO COMPLY WITH THE RECOMMENDATIONS OF BS 7992, PUBLISHED BY THE BRITISH STANDARDS INSTITUTION.
>
> IMPORTANT NOTE. THE POLICE SERVICE IS NOT NORMALLY WILLING TO ACCEPT OR RESPOND TO SECURITY ALERT SIGNALS ORIGINATING FROM EXTERIOR DETERRENT SYSTEMS OF THIS TYPE.

The text commencing “IMPORTANT NOTE” may be omitted at the discretion of the installation company if the design specification does not include provision for any form of ATS.

7.2 Installation

7.2.1 *General*

The EDS should be installed in accordance with the manufacturer’s instructions and the relevant recommendations of BS 4737-4.1.

Equipment enclosures should be firmly secured in position.

Batteries should be connected by means consistent with the design of the battery terminals. All batteries should be marked with their date of installation.

The PAWD should be so located as to minimize the possibility of inadvertent damage and to discourage wilful interference. It should be securely mounted on a rigid surface.

Unless the PAWD is fitted within a secure building, it should be located not less than 3 m from the ground, on a suitable building or on a free-standing pole or post.

7.2.2 *Wiring*

Attention is drawn to BS 7671 (IEE Wiring Regulations).

Particular care should be taken with regard to protective earthing and bonding.

Particular care should be taken to electrically segregate wiring which carries mains voltage from wiring which carries extra-low voltages, and to electrically separate circuits operating at these different voltages.

Attention is drawn to the need for any relay or contactor having a coil operating at safety extra-low voltage (SELV) and contacts connected to mains voltage to be designed and intended for such use. The relay or contactor should provide full class II insulation (double insulation or reinforced insulation) between the coil and contacts such that, even under fault conditions, mains voltage cannot become superimposed on the SELV.

If mains supply voltage from two separate circuits (or from two or more phases of a multi-phase supply) is fed to any item of equipment, or taken into any enclosure containing electrical equipment, appropriate safeguards against electric shock should be provided, including a warning notice. The warning notice should state that more than one supply (and/or phase) is taken into the equipment and should draw attention to the need to isolate all supplies (and/or phases) before working on the equipment.

7.3 Commissioning and hand-over

7.3.1 *General*

The commissioning and hand-over of the EDS should be in accordance with the relevant recommendations of **4.7** of BS 4737-4.1:1987.

At hand-over, the alarm company should give a practical demonstration of the operating procedures.

The subscriber should ensure that those using the supervised area and supervised property are familiar with and observe the agreed procedures.

7.3.2 *Operational instructions*

The setting, unsetting and operating procedures should be clearly and legibly set out and provided to the subscriber in a form suitable for display on or adjacent to the CIE.

7.3.3 *Operational checks*

Following installation, the operation of, and the coverage provided by, the system should be checked by on-site testing appropriate to the sensing/detection principles employed. The testing should include simulated trespass and simulated attack.

Sensing/detection coverage should be evaluated to establish that no areas of unwanted coverage exist. Depending upon the complexity of the system, further system tests and inspection of the site should be carried out after installation, and corrections made to the system for any change in conditions.

7.4 System record

Upon completion of the installation of the EDS, a system record should be made. This should include the following information:

a) the name and address of the subscriber;

b) the name and address of the supervised area, or (if there is no supervised area) of the vicinity in which the supervised property is situated;

c) the type and location of each permanently-wired detector, and the type and location of each permanently-wired sensor and processor.

Where wire-free sensors or wire-free detectors are employed, the type of sensor or detector should be stated, together with a description of the part (comprising not more than five sensors or detectors: see **7.5.2**) of the EDS to which it is dedicated. If a processor requires more than one input to generate a security alert condition, the details of such inputs should be given. The record should identify any sensor or detector that requires additional independent verification of a security alert condition before this condition can be signalled;

d) the type and location of CIE and power supplies;

e) details of those circuits which the subscriber or ARC has the facility to shunt or isolate, and of any shunting or isolation facilities provided for warning devices or signalling equipment;

f) the type and location of each warning device;

g) the identification of any equipment with wire-free or mains communicating links;

h) details of any delays or duration limitations associated with signalling and warning devices;

i) the type and location of signalling equipment;

j) the type and location of end-of-line devices;

k) any designated entry/exit route(s) (if applicable);

l) details of necessary site discipline and maintenance, and of system limitations with respect to these;

© BSI 18 January 2002

Licensed copy: Vocational Training Council, Vocational Training Council Version correct as of 18/10/2017

m) the name, address and telephone number of the ARC to which the EDS is connected (if applicable);

n) a description of the operating characteristics of the EDS, identifying each stage of security alert and specifying (with times, where appropriate) the typical event and/or sequence of events which leads to each of these stages. Examples of descriptions are given in Annex A;

o) a recommendation that the user make on-site checks at appropriate intervals, to ensure that natural changes in environmental conditions or inadequate site discipline and maintenance have not adversely affected operation or coverage.

NOTE The system record may include drawings, preferably using the symbols given in BS 4737-5.2.

A copy of the system record should be provided to the subscriber.

All documentation referring to the EDS should be kept in a place which is accessible only to authorized persons.

7.5 Maintenance

7.5.1 *Preventive maintenance*

Preventive maintenance visits to the protected premises should be made by a representative of the maintenance company during or before the twelfth calendar month following the month of commissioning or of the previous preventive maintenance visit.

Inspection and testing should be carried out in accordance with the recommendations of BS 4737-4.2.

7.5.2 *Corrective maintenance*

To facilitate the tracing of faults, there should be effective means of identifying troublesome or faulty equipment. It should be possible to trace a fault down to a part of the EDS comprising not more than one detector. Fault-finding instruments should be capable of monitoring the performance of the EDS for a period of several hours and of producing a performance record such that a fault is traceable to a part of the system comprising not more than one detector.

NOTE It is not necessary for the means of tracing troublesome or faulty equipment to be permanently incorporated in the EDS or permanently available at the supervised area or property. The fault-finding instruments may be normally held by the alarm company, provided that they are available as necessary.

An emergency service should be available at all times. The subscriber should be kept informed of the address and telephone number of the maintenance company's emergency service.

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

Licensed copy: Vocational Training Council, Version correct as of 18/10/2017

Annex A (informative)
Examples of descriptions of the operating characteristics of exterior deterrent systems

A.1 Permanently-wired system

EXAMPLE

The *ABC Lighting-Linked Deterrent System 3000* offers "round the clock" supervision for forecourts and similar unfenced areas, by detecting intrusion into the site and initiating a sequence of security alerts. These include high-power lighting, low-key audible and visual signals, and ultimately the sounding of a siren.

As soon as the *System 3000* detects that someone is on the site, the low-key sounder will be heard and the "trespasser" light for the relevant zone will be illuminated at the system's control equipment.

Additionally, during hours of darkness, the high-power lights for that zone will be automatically switched on. (During daylight hours, operation of the lighting is automatically suppressed.)

If staff are legitimately working on the site, the operation of the low-key sounder for a selected zone (or zones) can be suppressed.

If a trespasser remains active within a zone for longer than a preset period of time when the *System 3000* is in the "full alert" mode, a recorded voice message is broadcast by loudspeaker, as a caution to the trespasser.

If the trespasser ignores the loudspeaker message and continues activity on the site, then the floodlights will flash. The siren and the blue strobe (i.e. stroboscopic light) are also triggered.

As an optional extra, a signal can be transmitted (via the public switched telephone network or via a radio network) to an off-site alarm receiving centre, for keyholder response. After the trespasser has left the zone, and following a further predetermined period, the siren will stop, the lights will be extinguished, and the *System 3000* will automatically revert to its original watchful state.

The precise operating characteristics vary according to the amount of movement within the site that is detected by the sensors of the *System 3000*. However, the following are typical, (assuming that the trespassers remain continually active on the site):

— typical time from first detecting trespass to commencement of recorded voice message: 1 min;

— typical time from first detecting trespass to triggering of siren and blue stroboscopic light (accompanied during hours of darkness by flashing of high-power lighting): 2 min.

A.2 Wire-free system

EXAMPLE

The *XYZ Wireless 4000 Deterrent System* offers "round the clock" supervision for specific assets (e.g. motor vehicles) located on forecourts and similar unfenced areas, by detecting vibration of, and/or movement within, these items of supervised property, and initiating a security alert appropriate to the interference detected. The security alerts available include high-power lighting, low-key audible and visual signals, and ultimately the sounding of a siren.

As soon as the system, when activated, detects interference with an asset (e.g. vibration caused by someone trying to steal vehicle wheels or to break glass) the low-key sounder will sound and the "trespasser" light will be illuminated at the system's control equipment.

If a second case of interference is detected within 60 s of the first, a recorded voice message is broadcast by loudspeaker, as a caution to the trespasser.

If the trespasser ignores the loudspeaker message and continues to interfere with supervised property, then the siren and the blue strobe (i.e. stroboscopic light) are also triggered.

As an optional extra, a signal can be transmitted (via the public telephone network or via a radio network) to an off-site alarm receiving centre, for keyholder response.

© BSI 18 January 2002

If an internal violation (movement within a motor vehicle) is detected, the siren and blue strobe are automatically triggered, (together with the optional remote communication facility, if provided).

After the trespasser has ceased interfering with the supervised items of property, and following a further predetermined period, the siren will stop, the lights will be extinguished, and the *Wireless 4000* will automatically revert to its original watchful state.

Typical time from cessation of detected interference and activity at the supervised property to all lights being extinguished and all sounders silent: 1 min.

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

Bibliography

BS 4737-1:1986, *Intruder alarm systems — Part 1: Specification for installed systems with local audible and/or remote signalling.*

BS 4737-5.2:1998, *Intruder alarm systems — Terms and symbols — Recommendations for symbols for diagrams.*

BS 7671:2001, *Requirements for electrical installation — IEE Wiring Regulations — Sixteenth edition.*

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

© BSI 18 January 2002

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017

blank

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: 020 8996 9000. Fax: 020 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: 020 8996 9001. Fax: 020 8996 7001. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: 020 8996 7111. Fax: 020 8996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: 020 8996 7002. Fax: 020 8996 7001. Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI.

This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained.

If permission is granted, the terms may include royalty payments or a licensing agreement. Details and advice can be obtained from the Copyright Manager. Tel: 020 8996 7070.

BSI
389 Chiswick High Road
London
W4 4AL

Licensed copy: Vocational Training Council, Vocational Training Council, Version correct as of 18/10/2017