

Code of practice for

Management of false alarms

ICS 13.310

Committee responsible for this Draft for Development

The preparation of this Draft for Development was entrusted by Technical Committee GW/1, Electronic security systems, to Sub-Committee 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 Limited
- Consumer Policy Committee of BSI
- Electrical Contractors' Association
- Metropolitan Police
- National Security Inspectorate
- Security Facilities Executive
- Security Industry Training Organization
- Security Systems and Alarms Inspection Board

This Draft for Development, having been prepared under the direction of the Consumer Products and Services Sector, was published under the authority of the Standards Policy and Strategy Committee and comes into effect on 26 March 2002

© BSI26 March 2002

First published
15 January 1998
Second edition
26 March 2002

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

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 37231 6

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
1 Scope	1
2 Normative references	1
3 Definitions	1
4 System design	3
5 Administration	3
6 Documentation	4
7 Statistics relating to remote signalling alarm systems	4
8 False alarm management procedure	4
9 Diagnosis of false alarms	5
10 Resetting of remote signalling systems	5
Annex A (informative) Typical steps in the transmission and filtering of alarm conditions	8
Annex B (informative) Progress of an alarm condition	8
Annex C (informative) Examples of false alarms	10
Annex D (informative) Guidelines for designing to minimize false alarms	11
Annex E (informative) Functions of systems performance operatives	11
Annex F (informative) Preventing false alarms: 10 points to remember	13
Annex G (informative) Corrective maintenance report form	14
Annex H (normative) Recommendations for the recording of signalled alarm conditions	15
Annex J (informative) Attendance on false alarms	17
Annex K (informative) Resetting of remote signalling systems	19
Table J.1 — Action to be taken following attendance on subscriber error	17
Table J.2 — Action to be taken following attendance on non-subscriber errors	18
Figure B.1 — Progress of an alarm condition	9
Figure G.1 — Example of corrective maintenance report form	14
Figure H.1 — Flow diagram illustrating the compilation of monthly reports on signalled alarm conditions	16
Figure K.1 — Model flowchart for the resetting of remote signalling systems	19
Bibliography	20

Foreword

This Draft for Development was prepared by Sub-Committee GW/1/2. It supersedes DD 245:1998 which is withdrawn.

DD 245 has been drawn up to assist alarm companies in the management of false alarms, which is recognized as essential to establishing and maintaining good relations with police, insurers and subscribers.

False alarms are responsible for absorbing a disproportionate level of resources of the police, the alarm industry and subscribers, and it is in the interests of all concerned that each alarm company should seek to reduce its false alarms to a minimum.

Compliance with this and other relevant codes of practice, together with the selection of high standard equipment and regular maintenance, will ensure that false alarms are kept to a minimum level.

Note that the recommendations in DD 245:2002 are not in full alignment with the recommendations of DD 243:2002. This misalignment will be considered during the next review of DD 245:2002.

As a code of practice, this Draft for Development 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.

This Draft for Development is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

A review of this Draft for Development will be carried out not later than 2 years after its publication. Notification of the start of the review period, with a request for the submission of comments from users of this Draft for Development, will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received, the responsible BSI Committee will judge whether the Draft for Development can be converted into a British Standard or what other action should be taken.

Observations which it is felt should receive attention before the official call for comments will be welcomed.

These should be sent to the Secretary of BSI Technical Committee GW/1/2 at BSI, British Standards House, 389 Chiswick High Road, London W4 4AL.

Compliance with a Draft for Development 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 20, an inside back cover and a back cover.

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

1 Scope

This Draft for Development applies to all remote signalling intruder alarm systems. This Draft for Development also applies to audible only intruder alarms, except where otherwise stated.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this Draft for Development. For dated references, 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 4737-1:1986, *Intruder alarm systems in buildings — Part 1: Specification for installed systems with local audible and/or remote signalling*.

BS 4737-4.4.2:1986, *Intruder alarm systems in buildings — Part 4: Codes of Practice — Section 4.2: Code of practice for maintenance and records*.

BS 5979:2000, *Code of practice for remote centres receiving signals from security systems*.

BS 7042:1988, *Specification for high security intruder alarm systems in buildings*.

BS EN 50131-1:1997, *Alarm systems — Intrusion systems — Part 1: General requirements*.

PD 6662:2000, *Scheme for the application of European Standards for intruder alarm systems*.

3 Definitions

For the purposes of this standard the definitions in BS EN 50131-1, BS 4737-1, BS 7042, PD 6662 and the following apply.

NOTE Annex A illustrates use of a number of the terms defined. An explanatory diagram illustrating the relationship between some of the terms defined is shown in Annex B.

3.1

alarm company

organization prepared to provide, install and maintain an intruder alarm system

3.2

subscriber

person or organization utilizing the services of an alarm company for the installation and/or maintenance of an intruder alarm system

3.3

alarm condition

state of any detector, processor or tamper detection device which indicates that intrusion, attempted intrusion or unauthorized interference has occurred or is about to occur

3.4

alarm receiving centre (ARC)

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

3.5

signalled alarm condition

state of monitoring equipment at the alarm receiving centre (or other remote location) which indicates that intrusion, attempted intrusion or unauthorized interference has occurred at the protected premises or is about to occur

NOTE Once signalled at the alarm receiving centre as an alarm condition, the event is regarded as a signalled alarm condition even if subsequently filtered out by the alarm receiving centre personnel as being a false alert not requiring police response (or response by another emergency response authority).

3.6

mis-operation signal

signal that is unambiguously identifiable, at the alarm receiving centre, that the alarm system has mis-operated and therefore that the signalled alarm condition is to be filtered out and not extended to the police

NOTE The designation of a particular type of signal as a mis-operation signal is therefore a matter for agreement between the alarm company and the alarm receiving centre, with the concurrence of the subscriber.

3.7

unset signal

signal from an intruder alarm system indicating that the system has been unset

3.8

alarm filtering

procedure whereby signalled alarm conditions are intentionally delayed at the alarm receiving centre and their status reviewed with a view to preventing unnecessary calls to the police by cancelling certain signalled alarm conditions, where such cancellations are authorized by the subscriber

NOTE Attention is drawn to the *Policy on police response to security systems* [1] issued by the Association of Chief Police Officers (ACPO) of England, Wales and Northern Ireland. It is essential to maintain adequate security disciplines in relation to the use of code words or numbers and to have in place working practices which ensure that events are duly policed at the expiry of the permitted time delay, unless they have been proved to be false alerts.

3.9

false alert

signalled alarm condition which (without having been extended to the police or other emergency response authority) is regarded by the alarm receiving centre as cancelled, such cancellation having been authorized by the subscriber

NOTE 1 Such authorization is either:

- a) on a case-by-case basis, by use of suitable code words or numbers, in accordance with a defined filtering routine; or
- b) by prior written agreement.

NOTE 2 The following types of communication are examples of cancellation authorized by the subscriber (see NOTE 1a), whereby the subscriber causes:

- a) a “mis-operation signal”; or
- b) an “unset signal”, to be sent to the alarm receiving centre affirming that the signalled alarm condition is to be filtered out and not extended to police.

NOTE 3 False alerts are not regarded as false alarms. False alarms are events that have not been successfully identified and filtered out, and have therefore been notified to the police.

3.10

policed alarm condition

signalled alarm condition which (after any defined time delay for completion of alarm filtering, if applicable) has not been classified as a false alert and which therefore has been duly extended to the police

NOTE In the case of an alarm system which signals directly to the police (i.e. not via an alarm receiving centre) every signalled alarm condition is a policed alarm condition.

3.11

false alarm

policed alarm condition which has not resulted from:

- a) a criminal attack, damage, or attempt at such, upon/to the protected premises, the alarm equipment or the line carrying the alarm signal; or
- b) actions by emergency services in the execution of their duties; or
- c) a call emanating from a personal attack system made with good intent

NOTE 1 Activation of detectors without apparent damage or entry to the premises is considered a false alarm unless proved otherwise.

NOTE 2 False alerts are not regarded as false alarms; by definition false alerts are events that have been successfully identified and filtered out without having been notified to the police.

3.12

genuine alarm

policed alarm condition other than a false alarm

3.13**company-related false alarm**

false alarm attributable to a fault, failure, error, or omission on the part of the alarm company which installed or maintains the alarm system or in the equipment supplied by such alarm company

NOTE Examples of company-related false alarms are given in Annex C.

3.14**subscriber-related false alarm**

false alarm attributable to a fault, failure, error or omission on the part of the subscriber of the alarm system

NOTE Examples of subscriber-related false alarms are given in Annex C.

3.15**line fault-related false alarm**

false alarm directly attributable to a fault, failure, error or omission on the part of the carrier of the alarm signalling (e.g. the firm operating the public switched telephone network) between the protected premises and the remote location (e.g. alarm receiving centre), or in the transmission line or equipment of such carrier

NOTE Separate records of line fault-related false alarms are kept for RedCARE®¹⁾ systems and for systems other than RedCARE®¹⁾.

3.16**prime cause**

first event in the series of events which has led directly to the alarm condition

3.17**reset management centre**

manned premises where the authorization of the resetting of remote signalling intruder alarm systems is permitted (see 10.2)

3.18**satellite**

remote centre, normally unmanned, in which the information concerning the state of alarm and/or CCTV systems is collected and processed for onward transmission either direct, or via a further satellite, to an alarm receiving centre

NOTE 1 The junction point of alarm system signalling circuits is not regarded as a satellite.

NOTE 2 An alarm receiving centre is classified as a satellite if, during periods without manning, alarms are transmitted through to another alarm receiving centre.

4 System design

System design has a substantial bearing on false alarms; all specifiers should therefore have regard to the false alarm aspect of proposed design specifications.

Further guidance and information to assist in designing systems for minimization of false alarms is given in Annex D.

5 Administration

The alarm company should define, within its areas of management responsibility, the position (job title) responsible for all aspects of alarm system performance.

The size and scope of the above responsibility should be commensurate with the individual company's structure but should be so designed as to produce an escalating level of operation/involvement up to and including the chief executive/managing director.

NOTE 1 Annex E shows typical functional responsibilities for operatives having responsibility for systems performance.

NOTE 2 A checklist of points to remember for preventing false alarms is given in Annex F.

¹⁾ RedCARE® is a trade name owned by British Telecommunications plc., BT Head Office, 71 Newgate Street, London EC1A 7JA. This information is given for the convenience of users of this standard and does not constitute an endorsement by BSI of the product named. Equivalent products may be used if they can be shown to lead to the same result.

6 Documentation

6.1 For each installation, the subscriber should be provided with sufficient instructions to ensure correct operation is achieved with a minimum occurrence of false alarms.

6.2 Each service department should ensure that each service call following the notification of an alarm condition is recorded in an appropriate manner identifying false alarms.

Annex G gives an example of a typical corrective maintenance report form. The document should be produced in duplicate (one copy for the firm and one for the subscriber); it is suggested that the document is produced on two-part NCR (no carbon required) paper.

It is important that the prime cause (see **6.4**) of the false alarm is established and recorded in this report, as the report will form a source document for the monitoring and categorization of false alarms. The company-wide standard categorization of alarm activations in accordance with Annex H should be used on the corrective maintenance report form.

6.3 Each office at which corrective maintenance call-out requests are received and recorded should have a system for monitoring all signalled alarm conditions and all other alarm conditions (e.g. local audible) reported to the alarm company.

The monitoring system may be manual or computerized but, as a minimum, it should:

- a) form the source document for the identification of troublesome systems and the analysis of recurring defects;
- b) in the case of remote signalling alarm systems, require the central monitoring station to report daily;
NOTE In the case of Saturdays, Sundays and public holidays, the report may be delayed to the following office day.
- c) provide a register of all signalled alarm conditions and of all other alarm conditions (e.g. local audible) that have been reported to the alarm company, and discriminate between genuine alarms, false alarms, and false alerts;
- d) provide for the analysis of monthly alarm condition statistics.

6.4 In all documentation and reports, the prime cause of the false alarm should be reported, not its effect.

7 Statistics relating to remote signalling alarm systems

Each alarm company should compile and collate a record of signalled alarm conditions relating to remote signalling alarm systems, as follows.

- a) Details of all signalled alarm conditions should be recorded and categorized as either genuine alarms under several different parameters, as false alarms, or as false alerts.
- b) Monthly alarm reports should be compiled on an overall company basis, and for each office (as referred to in **6.3**), including categorization under appropriate categories, so that common problems can be identified.
- c) Figures from the monthly reports should be included in a rolling twelve-monthly log, so that a long-term analysis can be made of false alarms.
- d) Company-wide statistics should be compiled, as well as statistics relating to each 'office'. Each office should have available copies of the statistics relating to its own area of responsibility.
NOTE These statistics relating to the area of responsibility of an office should be held available at the relevant office for inspection.
- e) The executive identified in accordance with clause **5** as having responsibility for all aspects of alarm systems, performance should be responsible for overseeing the production of the monthly and rolling twelve-monthly analyses and for ensuring that the information is sent to senior executives and others within the firm, as appropriate.

8 False alarm management procedure

Each alarm company should have in place a documented process by which the incidence of false alarms is identified.

This process should include a means by which any installation giving rise to a high incidence of false alarms is identified and reported to the appropriate levels of management for information and action.