

Code of practice for Management of false alarms

ICS 13.310

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

Committees responsible for this Draft for Development

The preparation of this Draft for Development was entrusted to Technical Committee GW/1, Electronic security systems, upon which the following bodies were represented:

- Association of British Insurers
- Association of Chief Police Officers of England and Wales
- Association of Security Consultants
- British Security Industry Association
- British Telecommunications plc
- Consumer Policy Committee of BSI
- Department of the Environment (Building Research Establishment)
- Electrical Contractors' Association
- Fire Brigades Union
- National Approval Council for Security Systems
- Security Facilities Executive
- Security Systems and Alarms Inspection Board

This Draft for Development, having been prepared under the direction of the Sector Board for Consumer Products and Services, was published under the authority of the Standards Board and comes into effect on 15 January 1998

© BSI 1998

Amendments issued since publication

Amd. No.	Date	Text affected

The following BSI reference relates to the work on this standard:
Committee reference GW/1

ISBN 0 580 28977 X

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
1 Scope	1
2 References	1
3 Definitions	1
4 System design	2
5 Administration	2
6 Documentation	2
7 Statistics relating to remote signalling alarm systems	3
8 False alarm management procedure	3
9 Diagnosis of false alarms	3
10 Resetting of remote signalling systems	3
Annexes	
A (informative) Typical steps in the transmission and filtering of alarm conditions	5
B (informative) Progress of an alarm condition	5
C (informative) Examples of false alarms	7
D (informative) Guidelines for designing to minimize false alarms	7
E (informative) Functions of systems performance operatives	8
F (informative) Preventing false alarms: 10 points to remember	8
G (informative) Corrective maintenance report form	10
H (normative) Recommendations for the recording of signalled alarm conditions	11
J (informative) Attendance on false alarms	13
K (informative) Resetting of remote signalling systems	15
Tables	
J.1 Action to be taken following attendance on subscriber error	13
J.2 Action to be taken following attendance on non-subscriber errors	14
Figures	
B.1 Progress of an alarm condition	6
G.1 Example of corrective maintenance report form	10
H.1 Flow diagram illustrating the compilation of monthly reports on signalled alarm conditions	12
K.1 Model flowchart for the resetting of remote signalling systems	15
List of references	Inside back cover

Foreword

This Draft for Development has been prepared by Technical Committee GW/1. It 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.

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 *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 at BSI Head Office, 389 Chiswick High Road, London, W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 16, an inside back cover and a back cover.

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 References

2.1 Normative references

This Draft for Development incorporates, by dated reference, provisions from other publications. These normative references are made at the appropriate places in the text and the cited publications are listed on the inside back cover. For dated references, only the cited edition applies; any subsequent amendments to or revisions of the cited publication apply to this Draft for Development only when incorporated in the reference by amendment or revision.

2.2 Informative references

This Draft for Development refers to other publications that provide information or guidance. Editions of these publications current at the time of issue of this standard are listed on the inside back cover, but reference should be made to the latest editions.

3 Definitions

For the purposes of this standard the following definitions 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 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.

3.3 signalled alarm condition

State of monitoring equipment at a central station (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 central station as an alarm condition, the event is regarded as a signalled alarm condition even if subsequently filtered out by the central station personnel as being a false alert not requiring police response (or response by another emergency response authority).

3.4 false alert

Signalled alarm condition which (without having been extended to the police or other emergency response authority) is regarded by the central station as cancelled, such cancellation having been authorized by the subscriber by use of suitable code words or numbers in accordance with a defined filtering procedure.

3.5 filtering

Intentional delay of signalled alarm conditions at the monitoring station prior to being passed on to the police or other emergency response authority, in order to allow opportunity for false alerts to be identified.

NOTE. Attention is drawn to the *Intruder alarm policy* (IAP) [1] issued by the Association of Chief Police Officers (ACPO) in England and Wales, which calls for filtering procedures to be adopted in certain circumstances. The two commonly used filtering procedures are 'abort' and 'verification'.

A normal abort procedure is for the central station personnel to wait for a defined interval of time (typically 90 s) between receiving the signalled alarm condition and extending the call to the police to allow the subscriber an opportunity to abort the alarm condition by contacting the remote centre (whether by speech telephone or by transmitting electronically an abort code).

A normal verification procedure is for the central station personnel, upon receipt of a signalled alarm condition, to telephone the protected premises with a view to obtaining the appropriate verification. If verification is not obtained within a defined period of time, a call is made to the police (or other appropriate emergency response authority).

Whichever procedure is adopted, 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.

3.6 policed alarm condition

Signalled alarm condition which (after allowing any defined time delay for completion of a filtering procedure (if applicable) has not been classified as a false alert and which therefore has been duly communicated to the police.

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

3.7 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.

3.8 genuine alarm

Policed alarm condition other than a false alarm.

3.9 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.

3.10 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.

3.11 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. remote monitoring centre), or in the transmission line or equipment of such carrier.

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

3.12 prime cause

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

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.

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.

¹⁾ Trade name owned by British Telecommunications plc.

- 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 alarm is identified and reported to the appropriate levels of management for information and action.

NOTE 1. Such management systems may be either manual or computer-based. (An example of a typical manual process is given in annex J.)

NOTE 2. Attention is drawn to the *Intruder alarm policy* issued by the Association of Chief Police Officers (ACPO) in England and Wales [1], whereby repeated false alarms may lead to withdrawal of police response.

NOTE 3. An aim of the false alarm management procedure should be to identify troublesome installations and to overcome the problem before any warning letter is issued by the police.

9 Diagnosis of false alarms

Each alarm company should provide personnel involved in the execution and management of corrective maintenance with training in both the means to identify false alarms and the necessary reporting procedures for their management. This training should be documented.

10 Resetting of remote signalling systems

NOTE. Attention is drawn to **6.5e** of BS 5979 : 1993.

10.1 In addition to this clause, **5.5** of BS 4737 : Part 1 : 1986 and **3.4** of BS 4737 : Section 4.2 : 1986 should also apply.

10.2 Following reception by a central monitoring station of a signalled alarm condition, it should not be possible to reset the signalling system of the originating alarm system until that signalling system has been reset at the protected premises.

NOTE. This does not preclude the transmission of further data subsequent to transmission of a signalled alarm condition.

10.3 Resetting as required by **10.2** should be carried out at the protected premises:

- a) by the alarm company's service technician, in accordance with **3.4.1** of BS 4737 : Section 4.2 : 1986; or
- b) by the subscriber (acting in conjunction with the central station and authorized by the central station), in accordance with **3.4.2** of BS 4737 : Section 4.2 : 1986; or
- c) remotely by means of electronic signals transmitted from the central station (the central station acting in conjunction with the subscriber in attendance at the protected premises) and authorized by the central station in accordance with **3.4.2** of BS 4737 : Section 4.2 : 1986.

NOTE. Item b) permits use by a central station (under controlled conditions) of an anti-code generator, whereby a code derived from the alarm system is keyed in to the generator and causes generation of an anti-code which when keyed in to the alarm system enables the signalling system to be reset.

10.4 Resetting procedures should be such that a subscriber is not enabled to reset the signalling system other than in accordance with **10.3b**.

NOTE. This prohibits an alarm company's service technician from remotely enabling a subscriber to reset a remote signalling system (for example by quoting to a subscriber the anti-code generated by an anti-code generator), except as part of a clearly defined routine involving the duty officer at the central station and requiring case by case authorization from the duty officer at the central station.