BS 8473:2006+A2:2013

BRITISH STANDARD

Intruder and hold-up alarm systems – Management of false alarms – Code of practice

ICS 13.310

Publishing and copyright information

Published by BSI Standards Limited 2013

ISBN 978 0 580 82875 1

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

Publication history

First published as DD 245, 15 January 1998

Second edition, 26 March 2002

First published as BS 8473, 29 September 2006

Amendments issued since publication

Amd. no.	Date	Text affected
16761 Corrigendum No. 1	October 2006	Figure B.1 and Figure B.2 corrected
A1	July 2008	First sentence of **10.7** amended
A2	November 2013	See Foreword

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i and iv, pages 1 to 25 and a back cover.

Foreword

Publishing information

This British Standard was published by The BSI Standards Limited, under licence from The British Standards Institution on 29 September 2006 and came into effect on 31 March 2007. It was prepared by Subcommittee GW/1/2, Installed alarm systems, under the authority of Technical Committee GW/1, Electronic security systems. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

BS 8473:2006+A2:2013 supersedes BS 8473:2006+A1:2008, which is withdrawn.

Information about this document

BS 8473 has been drawn up to assist all parties in the management of false alarms.

False alarms are responsible for absorbing a disproportionate level of resources of the police, the alarm industry, clients and users, and it is in the interests of those concerned that all parties seek to reduce their false alarms to a minimum.

Text introduced or altered by Amendment No. 2 is indicated in the text by tags [A2〉 〈A2]. Text introduced or altered by Amendment No. 1 is not tagged. Minor editorial changes are not tagged.

Use of this document

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

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

BSI permits the reproduction of Annex D, Annex E, Figure F.1 and Figure G.2, on pages 17, 18, 19 and 22 of BS 8473. This reproduction is only permitted where it is necessary for the user to comply with the recommendations in **5.3** and **6.2** during each application of the standard.

Presentational conventions

The word “should” is used to express recommendations of this standard. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

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

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

This page deliberately left blank

1 Scope

This British Standard gives guidance on the management of intruder and hold-up alarm systems (I&HAS), and the management of alarm conditions when they occur in order to reduce the nuisance factor and waste of resources in responding to false alarms.

This document applies to all remotely notified intruder and hold-up alarm systems and also applies to audible only intruder and hold-up alarm systems, except where otherwise stated.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

〉A2〈 BS 8243:2010, *Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of Practice* 〉A2〈

BS EN 50131-1:2006, *Alarm systems – Intrusion systems – Part 1: System requirements*

〉A2〈 BS EN 50518, *Monitoring and alarm receiving centre (all parts)* 〉A2〈

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

DD 243:2004, *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions – Code of practice*

〉A2〈 DD 263: 2010, *Intruder and hold-up systems – Commissioning, maintenance and remote support – Code of Practice* 〉A2〈

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

3 Terms and definitions

For the purposes of this British Standard, the terms and definitions given in BS EN 50131-1, PD 6662 and the following apply.

NOTE Annex A illustrates use of a number of the terms defined. Explanatory diagrams illustrating the relationship between some of the terms defined are shown in Annex B.

3.1 alarm company
organization which provides services for I&HAS

3.2 alarm condition
condition of an I&HAS, or part thereof, which results from the response of the system to the presence of a hazard

3.3 alarm filtering
procedure whereby remotely notified alarm conditions are intentionally delayed at an ARC and their status reviewed for the purpose of

cancelling certain remotely notified alarm conditions, where such cancellation is authorized by the [A2] user [A2] of the I&HAS

3.4 alarm receiving centre
ARC
continuously manned centre to which information concerning the status of one or more I&HAS is reported

[BS EN 50131-1:2006, definition **3.1.6**]

3.5 alarm receiving centre-related false alarm
false alarm attributable to a fault, failure, error, or omission on the part of the ARC responsible for monitoring the I&HAS

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

3.6 client
person or organization utilizing the services of an alarm company for the installation and/or maintenance of an I&HAS

3.7 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 I&HAS or in the equipment supplied by such alarm company

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

[A2] 3.8 duty officer
operator(s) on duty at the RMC responsible for authorizing resets and/or restores of remotely notified I&HAS [A2]

3.9 false alarm
policed alarm condition other than a genuine alarm

3.10 false alert
remotely notified alarm condition, which is regarded by the ARC as cancelled, such cancellation having been authorized by the [A2] user [A2] of the I&HAS

NOTE 1 The following types of communication are examples of cancellation authorized by the [A2] user [A2], whereby the [A2] user [A2] causes:

a) a "mis-operation signal" to be sent to the ARC affirming that the remotely notified alarm condition is to be filtered out and not extended to police; or

b) an "unset signal" to be sent to the ARC affirming that the remotely notified alarm condition is to be filtered out and not extended to police.

NOTE 2 This does not preclude the client giving general or specific standing authority, by prior written agreement, that the alarm company's ARC may designate some alarm signals as void (i.e. cancelled).

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.

3.11 genuine alarm
policed alarm condition which has resulted from:

a) a criminal attack, damage, or attempt at such, upon/to the supervised premises, the alarm equipment or the transmission path carrying the alarm signal; or

b) actions by emergency services in the execution of their duties; or

c) a call emanating from a hold-up alarm system made to summon urgent assistance when an assailant enters a previously defined

area with the obvious intention of harming or threatening any person within that defined area

NOTE Attention is drawn to Table E.1 for guidelines to avoid false activations with hold-up alarms.

3.12 mis-operation signal
signal that is identifiable at the ARC as indicating that the I&HAS has mis-operated and therefore that the remotely notified alarm condition is to be cancelled and regarded as a false alert

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 ARC, with the concurrence of the client.

3.13 [A2] user [A2]
authorized individual using an I&HAS for its intended purpose

3.14 [A2] user [A2]-related false alarm
false alarm attributable to a fault, failure, error or omission on the part of the [A2] user [A2] of the I&HAS

NOTE Examples of [A2] user [A2]-related false alarms are given in Annex C.

3.15 policed alarm condition
remotely notified 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

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

3.17 remotely notified alarm condition
state of monitoring equipment at an ARC (or other remote location) which indicates an alarm condition

NOTE This does not preclude other signals (e.g. unset, set, mis-operation, fault) being received at an ARC.

3.18 restore
procedure of cancelling an alarm, tamper, fault or other condition and returning the I&HAS to a previous condition

NOTE This was previously known as "reset".

3.19 restore management centre
premises where the authorization of the restoring of a remotely notified I&HAS is permitted (see **10.2**)

3.20 satellite
remote centre, normally unmanned, in which the information concerning the state of I&HAS is collected and processed for onward transmission either direct, or via a further satellite, to an ARC

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

3.21 transmission path fault-related false alarm
false alarm directly attributable to a failure of the alarm transmission path(s) between the supervised premises and the ARC

3.22 unconfirmed alarm
signal that has not been designated as audibly confirmed, visually confirmed or sequentially confirmed

3.23 unset signal
signal from an I&HAS indicating that the system has been unset

4 System design

NOTE DD CLC/TS 50131-7 gives guidance for good system design practice.

System design has a substantial bearing on false alarms; therefore all specifiers should take into account the false alarm aspect of system design proposals. Further guidance to assist in designing systems for minimization of false alarms is given in [A2] and BS 8243 [A2].

5 Administration

5.1 General

Each alarm company should appoint a person within the company who is responsible for the performance of intruder and hold-up alarm systems (I&HAS). The appointed person should have a right of direct access to the Chief Executive/Managing Director and have sufficient experience and authority within the company to achieve the objectives of monitoring, analysing and reducing false alarms. In the case of a small company, the Chief Executive/Managing Director may personally undertake this role.

NOTE 1 In this Code of Practice the appointed person is referred to as the Systems Performance Manager (SPM).

NOTE 2 Depending upon the size and regional distribution of the company, it might be necessary to appoint regional managers having corresponding responsibility for the performance of I&HASs within particular regions and reporting to the SPM.

Functional responsibilities for an SPM are given in **5.2.**

5.2 Functions of systems performance manager

The SPM should ensure that the following tasks are carried out effectively in the alarm company.

a) Monitoring of the standards of surveying and installation to ensure that:
   1) industry standards and codes of practice are complied with;
   2) system design proposals meet the requirements of the alarm company's policies;
   3) system design proposals do not result in systems which are likely to generate false alarms;
   4) client documentation is provided in accordance with DD CLC/TS 50131-7 and DD 243 [A2] and/or BS 8243 [A2];
   5) comprehensive training for alarm company staff is maintained;
   6) training for [A2] users [A2] is provided in accordance with DD CLC/TS 50131-7.

b) Maintenance of all contracted systems at intervals in accordance with [A2] DD 263 [A2]. Training for [A2] users [A2] should be offered at each site service interval.

   [A2] *NOTE This includes systems installed in accordance with BS 4737.* [A2]

c) Monitoring of demands for and effectiveness of corrective maintenance in accordance with [A2] DD 263 [A2];

NOTE [A2] *This includes systems installed in accordance with BS 4737.* [A2]

d) Identification of abnormalities and trends likely to lead to false alarms.

e) Monitoring of the alarm company's false alarm management procedure (see Clause **8**).

1) Collection, reporting and analysis of false alarm statistics and their causes.

2) Identification of troublesome systems, equipment and practices.

3) Identification of transmission path problems.

f) Monitoring of client complaints.

g) Monitoring liaison with police security systems offices and maintaining familiarity with their policies.

h) Monitoring evaluation trials on new equipment, with particular reference to false alarms.

i) Ensuring compliance with this British Standard.

j) Working with operational management to obtain a reduction in the incidence of false alarms.

NOTE Attention is drawn to DD 243:2004, ***6.4.2*** *and DD 243:2004,* ***6.4.3*** *which are the preferred methods of unsetting for minimizing the likelihood of false alarms.*

5.3 Checklist of points for preventing false alarms

Alarm companies should pass the information given in Annex D and Annex E to clients to aid in the prevention of [A2] user [A2]-related false alarms.

6 Documentation and training

6.1 For each installation, the alarm company should provide the client representative(s) with sufficient written instructions, reinforced by adequate training, to ensure correct operation can be achieved.

NOTE The client is responsible for ensuring that only competent [A2] *users* [A2] *are permitted to use the I&HAS.*

6.2 The service department should ensure that each service call following notification of an alarm condition is recorded in an appropriate manner, for example by using a corrective maintenance form, identifying false alarms.

Annex F gives an example of a typical corrective maintenance report form. The completed document should be copied to the client.

It is important that the prime cause (see **6.4**) of the false alarm is established and recorded in the corrective maintenance report, as the report forms a source document for the monitoring and categorization of false alarms. The company-wide standard categorization of alarm activations in accordance with Annex G 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 in place for monitoring all remotely notified 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 remotely notified I&HASs, require the ARC 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 remotely notified 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, unconfirmed alarms, and false alerts for monthly analysis.

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

7 Statistics relating to remotely notified I&HAS

An alarm company should compile and collate a record of all remotely notified alarm conditions it receives as follows.

a) Details of all remotely notified alarm conditions should be recorded and categorized as either genuine alarms under several different parameters, unconfirmed alarms, false alarms, or false alerts.

b) Monthly alarm reports should be compiled on an overall company basis, and for each office (see **6.3**), including categorization under appropriate categories (see Annex C), so that common problems can be identified.

c) Figures from the monthly reports should be included in a rolling 12-monthly log, so that a long-term analysis can be made of unconfirmed alarms, false alarms and false alerts.

d) Company-wide statistics should be compiled, as well as statistics relating to each office. Each office should retain copies of the statistics relating to its own area of responsibility which should be made available for inspection.

e) The SPM should oversee the production of the monthly and rolling 12-monthly analyses and ensure that the information is sent to senior executives and others within the alarm company, as appropriate.

8 False alarm management procedure

Alarm companies should have in place a documented process by which the occurrence of false alarms, unconfirmed alarms, and false alerts is identified.

This process should include a means by which any installation giving rise to a false alarm, or more than three unconfirmed alarms and/or false alerts in a rolling 30 day period is identified and reported to the appropriate levels of management for information and action. The aim of the false alarm management procedure is to identify troublesome installations and to overcome the problem before police response is withdrawn.

NOTE 1 Such management systems may be either manual or computer-based. An example of a typical manual process is given in Annex H.

NOTE 2 Attention is drawn to the Policy on police response to security systems *[1] issued by ACPO and the* Security systems policy *[2] issued by ACPOS in Scotland, whereby repeated false alarms could lead to withdrawal of police response.*

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 escalation procedures for their management. This training should be documented and the records retained.

10 Restoring of remote notification I&HASs capable of policed alarm conditions

*NOTE 1 This clause supplements the text that appeared in BS 4737-1:1986, **5.5**, which stated "Following an alarm, a system shall require resetting by means not normally available to the subscriber, except for the resetting of that part of a system which uses deliberately-operated devices only."*

NOTE 2 For systems installed in accordance with BS 4737, the terms "restore" and "restoring" used in this British Standard are treated as being equivalent to "reset" and "resetting" respectively.

*NOTE 3 This clause supplements PD 6662:2004, **E.3**, PD 6662:2004, Table E.2, and BS EN 50131-1:2006, **8.3.9**.*

10.1 I&HAS configuration

The I&HAS should be configured so that the client and/or owner and/or [A2] user [A2] is unable to set or restore the I&HAS after the following conditions have occurred.

- In the case of [A2] IASs [A2] conforming to DD 243:2002 or subsequent editions of DD 243; a sequentially confirmed alarm condition.
- In the case of [A2] IASs [A2] conforming to a standard that predates DD 243:2002; an intruder alarm condition.
- In the case of I&HASs conforming to PD 6662:2004 at grade 3 or 4; a tamper condition.

NOTE 1 Where parts of an I&HAS can be individually set and unset, this may be applied to each part.

NOTE 2 The need for the I&HAS to be restored occurs when the I&HAS has been unset.

NOTE 3 This does not preclude the transmission of further data during the set period subsequent to transmission of a remotely notified alarm condition.

*NOTE 4 Restoring in conjunction with an RMC is permitted in accordance with Clause **10**.*

[A2] *NOTE 5 Restoration of the 'hold-up' alarm is not subject to remote restoration.* [A2]

10.2 Restore management centres (RMCs)

Only the following premises may be used as RMCs.

a) An ARC conforming to BS 5979 [A2] or BS EN 50518 (all parts) [A2] for the monitoring of I&HASs.

b) A satellite operated and owned by an ARC conforming to BS 5979 for the monitoring of I&HASs.

c) The head office or installing branch of the alarm company that maintains the I&HAS.

d) A secure office for a specific organization's sole use in order to manage the restoring of I&HASs on their own premises.

One RMC may be used during certain hours of the day and another RMC may be used during the remaining hours of the day. At any given time, however, there should not be more than one designated RMC for a particular I&HAS.

The alarm company should ensure that the client has been informed of the correct contact details for the designated RMC at any time.

10.3 Methods of restoring

Restoring of the conditions defined in **10.1** should only be carried out:

a) by the alarm company's service technician at the supervised premises;

b) by the [A2] user [A2] at the supervised premises, acting in conjunction with the RMC and authorized by the RMC, in accordance with **10.4**, **10.8** and **10.9**;

c) remotely by means of electronic signals transmitted from the RMC (the RMC acting in conjunction with the [A2] user [A2] in attendance at the supervised premises) and authorized by the duty officer at the RMC, in accordance with **10.4**, **10.8** and **10.9**.

Codes used by the alarm company service technician for maintenance and testing purposes should not be disclosed to the [A2] user [A2].

NOTE 1 The methods of restoring prohibit an alarm company's service technician from remotely enabling an [A2] user [A2] to restore an I&HAS (for example by quoting to an [A2] user [A2] the anti-code generated by an anti-code generator), except as part of a clearly defined routine involving the duty officer at the RMC and requiring case-by-case authorization from the duty officer at the RMC in accordance with this British Standard.

In the case of **10.3**b) and **10.3**c), the method of restoring the I&HAS should be such that the RMC is able to determine whether the ATS is restored or not.

NOTE 2 For this purpose, information concerning the state of the I&HAS may be given to the duty officer at the RMC in a telephone conversation from the supervised premises.

10.4 Restoring of policed alarm conditions

NOTE This British Standard does not require an ARC (when acting as an RMC) to consult with the alarm company before authorizing a restore. Some alarm companies could require ARCs from which they purchase monitoring services to do this; however this is regarded as a matter for negotiation and agreement between the alarm company concerned and its ARC(s).

If a policed alarm condition has occurred, restoring in accordance with **10.3**b) or **10.3**c) should not be authorized by the RMC unless all the following conditions are satisfied.

a) [A2] User [A2] agreement has been obtained and authorized by an agreed security discipline (normally by suitable code words or numbers).

b) The description of the cause of the remotely notified alarm condition given by the [A2] user [A2] to the duty officer at the RMC is consistent with there being no requirement for a service technician's visit.

c) The duty officer at the RMC has referred to the record of remotely notified alarm conditions (see **10.5**) maintained by the ARC and is satisfied that the I&HAS is not one to which restore is denied in accordance with **10.7**.

10.5 ARC record of remotely notified alarm conditions

The ARC should maintain accurate records of remotely notified alarm conditions in accordance with BS 5979 [A2] and BS EN 50518 (all parts) [A2].

The ARC should inform the alarm company as soon as possible, but at least daily (see **6.3**), of all remotely notified alarm conditions. In the case of remotely notified alarm conditions for which restore has been authorized, the ARC should also inform the alarm company (within the same time period) of the reported cause and of the time that restore was authorized.

10.6 Inter-relationship between the RMC and the ARC

The duty officer at the RMC should have immediate access to the records of remotely notified alarm conditions maintained by the ARC (see **10.5**) and should use these records when deciding whether or not to authorize a restore in accordance with this British Standard.

NOTE Such immediate access might be achieved for example, through the duty officer at the RMC having remote access (see BS 5979) to the computer systems and data of the ARC.

For each alarm condition, the RMC should maintain accurate records of whether restore has been authorized and by whom. The record should identify by name or other suitable means the [A2] user [A2] in attendance at the supervised premises. In order that the RMC can continually satisfy this recommendation, the duty officer at the RMC (if not an ARC) should inform the ARC immediately of all restores authorized by the RMC.

10.7 RMC policy of denying restore

The RMC should deny restore if more than two policed alarm conditions have occurred in the last 12 months.

The RMC may permit a restore if a genuine alarm, or genuine confirmed alarm, has occurred provided the RMC always advises the [A2] user [A2] that insurance cover could be invalidated if a service technician's visit does not take place and the I&HAS is subsequently found not to be in full working order.

When the RMC denies a restore, the alarm company's service technician should visit the supervised premises for the purpose of identifying the cause of the alarm condition, carrying out corrective maintenance/action and ensuring that the I&HAS is in full working order and,

a) in the case of a false alarm due to [A2] user [A2] error, educating the [A2] user [A2] in the operation of the I&HAS, and the avoidance of false alarms. See Annex D;

b) if design faults are noted these are reported to the SPM (see **5.2**) by the next working day.

10.8 Restoring of false alerts

If a false alert has occurred, restoring may be authorized in accordance with the conditions set out in **10.3**b) when the following conditions are satisfied.

a) The [A2] user [A2] has requested a restore via live voice communication (e.g. telephone conversation) with the duty officer at the RMC.

b) [A2] User [A2] agreement has been obtained and authorized by an agreed security discipline (normally by suitable code words or numbers).

c) The description of the cause of the remotely notified alarm condition given by the [A2] user [A2] to the duty officer at the RMC is consistent with there being no requirement for a corrective maintenance visit.

10.9 Restoring of false alerts remotely by the RMC

If a false alert has occurred, restoring in accordance with **10.3**c) should not be authorized by the RMC unless all the conditions set out in either a) or b) are satisfied.

a)

1) The [A2] user ⟨A2⟩ has requested a restore via live voice communication (e.g. telephone conversation) with the duty officer at the RMC.

2) [A2] User ⟨A2⟩ agreement has been obtained and authorized by an agreed security discipline (normally by suitable code words or numbers).

3) The description of the cause of the remotely notified alarm condition given by the [A2] user ⟨A2⟩ to the duty officer at the RMC is consistent with there being no requirement for a corrective maintenance visit.

b)

1) The RMC is an ARC conforming to BS 5979 [A2] or BS EN 50518 (all parts) ⟨A2⟩ for the monitoring of I&HASs [see **10.2**a)].

2) A signal indicating cancellation of the remotely notified alarm condition authorized by the [A2] user ⟨A2⟩ has been received by the ARC within 120 s of the remotely notified alarm condition having been received by the ARC.

3) There is a mechanism in place at the ARC to guarantee, on a case-by-case basis for each remotely notified alarm condition that has been cancelled, that action has not been taken and will not be taken by the ARC to establish communications with the police control room.

4) There is a written agreement between the alarm company and the ARC to the effect that restoring in accordance with **10.3**c) under the conditions given in **10.9**b)1), **10.9**b)2) and **10.9**b)3) may be carried out by the ARC.

*NOTE It is a matter for agreement between the alarm company and the ARC, with the concurrence of the client and/or owner, as to what signal(s) are to be regarded by the ARC as indicating cancellation of the remotely notified alarm condition authorized by the [A2] user ⟨A2⟩ (see **3.6** and **3.9**).*

Annex A (informative) Typical steps in the transmission and filtering of alarm conditions

NOTE This example relates to an I&HAS with remote notification requiring police response and signalling via an ARC at which signals are filtered by means of a cancellation procedure.

A.1 Initiation

An alarm condition occurs at the supervised premises.

A.2 Signalling

The alarm condition is remotely notified to an ARC.

A.3 Receipt by the ARC

Once received by the ARC the alarm condition is then termed a remotely notified alarm condition.

A.4 Filtering

Remotely notified alarm conditions are delayed at the ARC prior to being extended to the police. The purpose of this intentional time delay is to allow an opportunity for false alerts to be identified and filtered out at this stage, by means of a cancellation procedure.

This need not apply to remotely notified alarm conditions originating from [A2] IAS [A2] using the unsetting [A2] methods [A2] described in DD 243:2004, **6.4.2**, [A2] **6.4.3** and **6.4.6** [A2].

A.5 Policing

NOTE Certain remotely notified alarm conditions such as unconfirmed alarm conditions, are not extended to the police.

If after elapse of the intentional filtering delay a remotely notified alarm condition has not been proved to be a false alert, it is presumed that it could be genuine and the call is extended to the police. Once the police have been notified, the remotely notified alarm condition is then termed a policed alarm condition (see **3.14**).

A.6 Analysis

Each policed alarm condition is subsequently classified as either a genuine or a false alarm. False alarms are further classified according to cause, as described in this British Standard.

Annex B (informative) Progress of an alarm condition

Figure B.1 shows the progress of a typical alarm condition for I&HAS which are not capable of generating confirmed alarms. Figure B.2 shows the progress of a typical alarm condition for I&HAS which are capable of generating confirmed alarms capable of generating.

Figure B.1 **I&HAS not capable of generating confirmed alarms**

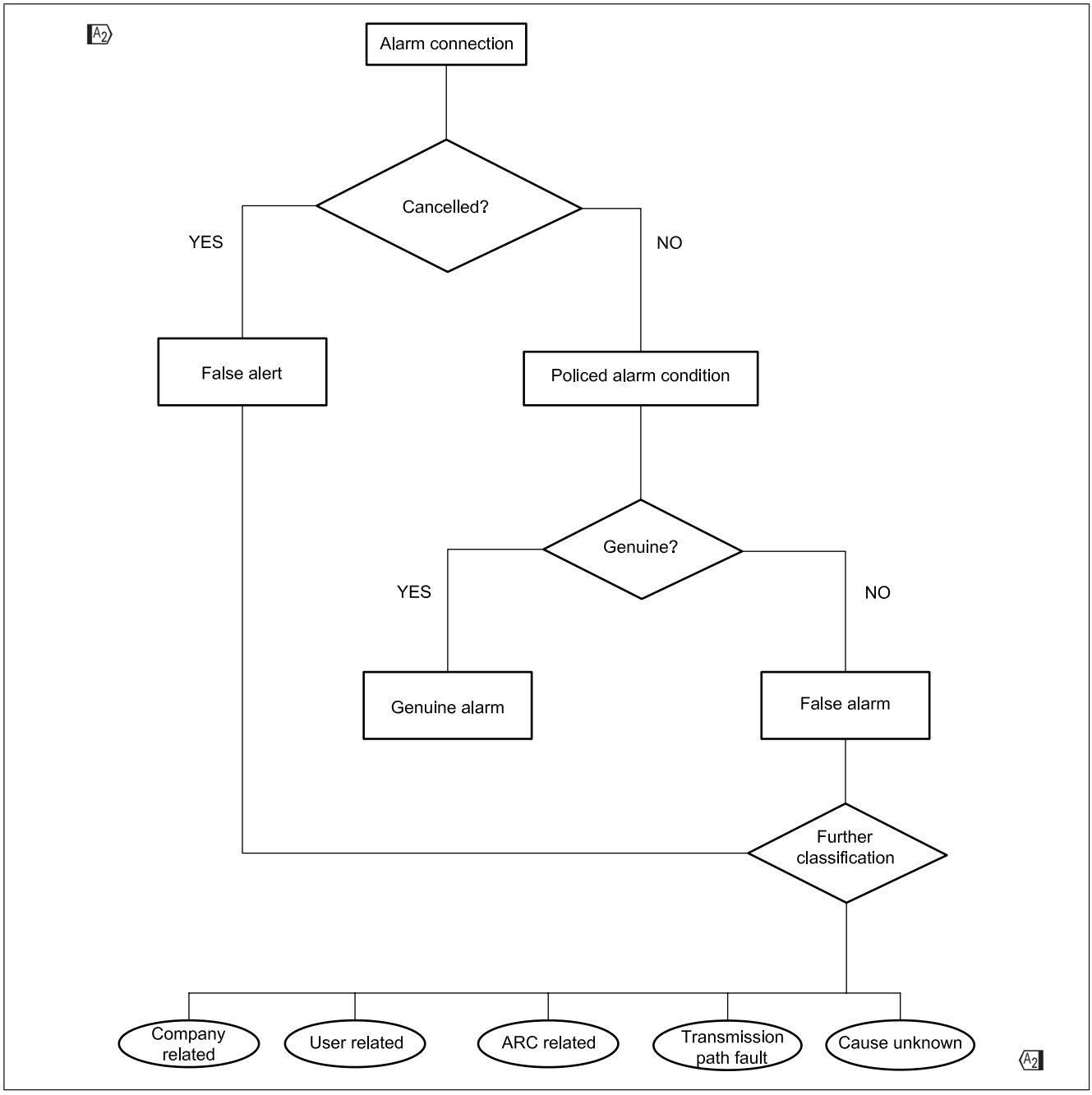
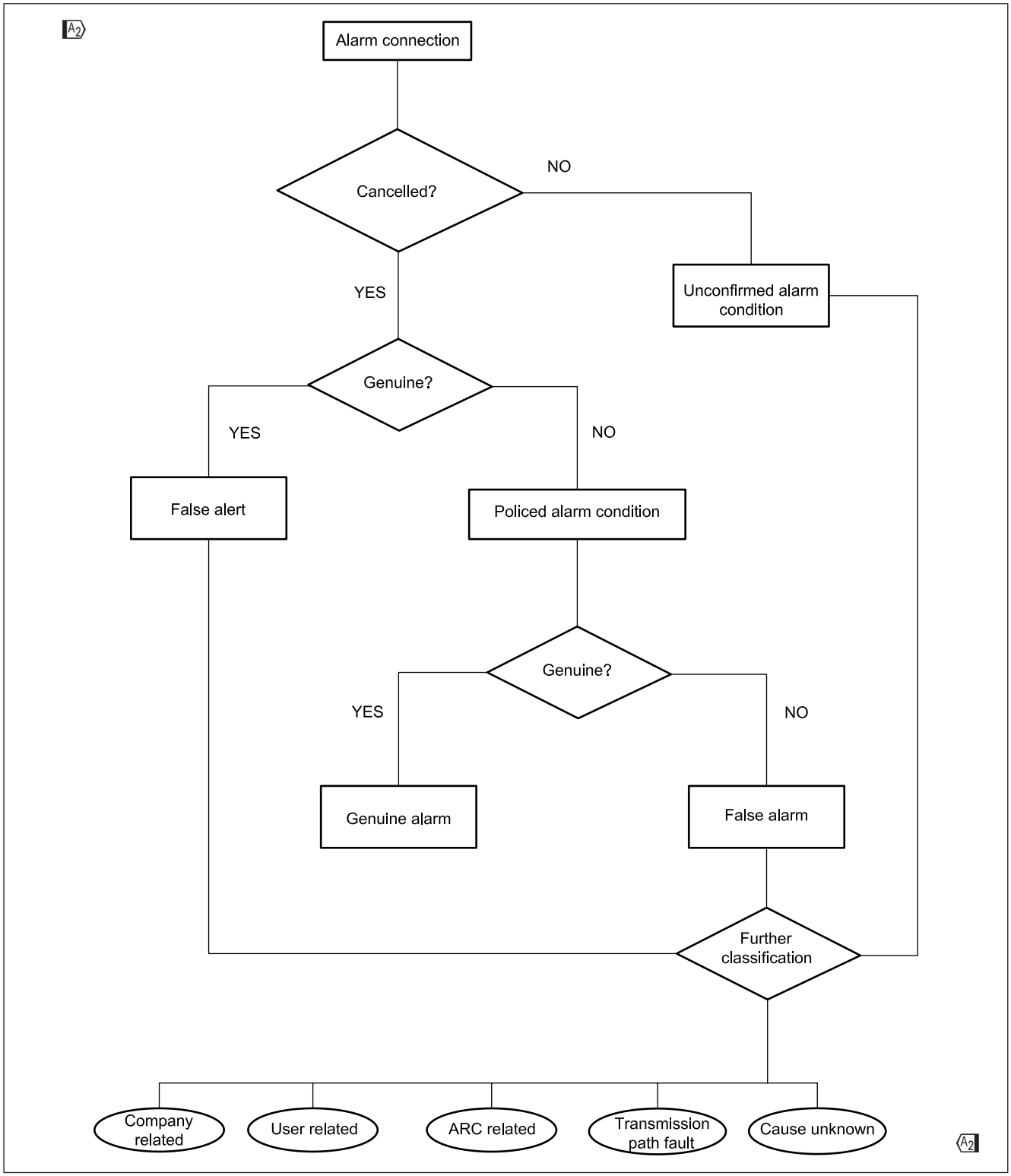


Figure B.2 **I&HAS capable of generating confirmed alarms**



Annex C (informative) Examples of false alarms

C.1 Company-related false alarms

*NOTE Incorrect siting, coverage, range or choice of detector would fall under **C.1.1, C.1.2** and **C.1.3**.*

C.1.1 System design

Any false alarm attributable to incorrect design of the alarm installation or the faulty application of detection devices; includes any false alarm attributable to electrical interference or transients from which the I&HAS should be immune, such as mains transients, effects of electrical storm, CB or radio interference; also includes the effects of mains power failure and activations caused by rodents, insects, birds, bats, etc.

C.1.2 System installation

Any false alarm attributable to poor workmanship (except as covered by **C.1.3**).

C.1.3 System maintenance/repair

Any false alarm attributable to lack of preventative maintenance or to poor workmanship in carrying out repairs during breakdown calls.

C.1.4 Procedural failure

Any false alarm attributable to failure to put an I&HAS onto test when carrying out maintenance or repair.

C.1.5 Control equipment

Any false alarm directly attributable to an electrical or mechanical failure of control equipment which cannot be attributable to any other category, and which would result in repair or replacement of the control equipment or any part of the control equipment.

C.1.6 Movement detectors

Any false alarm directly attributable to an electrical or mechanical failure of a movement detector, which cannot be attributed to any other category and which would result in the repair or replacement of the movement detector or of any part of the movement detector.

C.1.7 Other electrical/electronic devices

Any false alarm directly attributable to an electrical or mechanical failure of any electrical or electronic device, other than one listed above, which cannot be attributed to any other category, and which would result in the report or replacement of the electrical or electronic device or of any part thereof.

C.1.8 Non-electrical/electronic device

Any false alarm directly attributable to an electrical or mechanical failure but which cannot be attributed to any other category and which would result in the repair or replacement of the failed item.

C.2 [A2] User-related [A2] false alarms

NOTE Advice on the prevention of false alarms is given in Annex D and Annex E.

C.2.1 Insecure premises

Any false alarm attributable to the condition of doors, windows and other openings into the supervised premises.

NOTE Openings might or might not be supervised by I&HAS detectors but are sited within the I&HAS supervised area.

C.2.2 [A2] User [A2] error

Any false alarm attributable to actions by untrained or inadequately trained [A2] users [A2] of the I&HAS.

C.2.3 Wrong entry procedure

Any false alarm attributable to action by the [A2] user [A2] which differs from the operational instructions given to the client on the correct course of actions to follow when entering the supervised premises.

C.2.4 Wrong exit procedure

Any false alarm attributable to any deviation by the [A2] user [A2] from the operational instructions given to the client on the correct course of actions to follow when leaving the supervised premises.

C.2.5 Twenty-four hour equipment

Any false alarm attributable to the deliberate or accidental operation of continuously (24 hour) operated detectors/devices on the I&HAS.

C.2.6 Irregular opening/closing

Irregular opening/closing is any false alarm attributable to the opening/closing of premises outside of the periods agreed with the installing/maintaining alarm company.

NOTE For systems installed in accordance with DD 243 the police would not be notified of irregular opening or closing of the premises outside the agreed time schedules.

C.3 ARC-related false alarms

Examples of ARC related false alarms include the following.

- Human error.
- Policing a system while system is on test.
- Failing to put system on test.
- Policing unconfirmed alarms from confirmed systems.
- Passing of incorrect information to police.
- ARC equipment failure.

Annex D (normative) Preventing false alarms: points to remember

D.1 The intruder alarm system (IAS) is to be operated only by persons who have been correctly trained. If there is uncertainty about the correct operational procedures the alarm company should be contacted.

D.2 Before leaving the premises check that all doors and windows are physically secured. A walk around the supervised area is the only effective way of doing this properly.

D.3 Ensure that detection devices are not obstructed. In particular be careful that infrared beams and movement detectors are not obstructed by stock or other items.

D.4 If movement detectors are used do not introduce sources of heat, movement or sound into the area supervised by these detectors without informing the alarm company.

D.5 Always follow the entry/exit procedure agreed with the alarm company. Entry through any door other than the one designated should be physically prevented. Switching off the IAS is always the first task on entry.

D.6 Before entry, ensure that the means necessary to enter the premises and unset the IAS are known and available in a secure manner to the [A2] user [A2].

D.7 Inform the alarm company of any alterations to the premises which could affect the IAS. Do not permit people other than employees of the alarm company to make changes to the IAS. Place system on test when building alterations are taking place.

D.8 Treat the IAS with care. Wiring and detection devices can be accidentally damaged or moved. If this occurs inform the alarm company immediately.

D.9 After a false alarm check the system carefully and, if possible, note the cause of activation. Inform the alarm company of the believed cause of the activation immediately.

D.10 Make sure regular maintenance checks are carried out by the alarm company and that you have the correct contact details for the alarm company and ARC. Remember that excessive false alarms can result in police response being withdrawn.

D.11 Most IAS require a mains electricity supply. If the electricity supply to your system is disconnected for more than 4 h contact the alarm company.

Annex E (normative) Hold-up alarms [A2] and hold-up alarm confirmation [A2]

E.1 A hold-up device should only be operated to summon urgent assistance when an assailant enters a previously defined area with the obvious intention of harming or threatening any person within that defined area.

E.2 The hold-up device is for the personal safety of staff on the premises. Misuse results in the loss of police response to this facility. The guidelines given in Table E.1 assist in the avoidance of false activations.

Table E.1 **Guidelines to avoid false activations**

Incident	Recommended action	Notes
A threat of current or imminent physical danger to staff on the premises	Press the hold-up device	This is the intended function of a hold-up device or "personal attack" button
Theft of property or fraud with the suspects still on the premises, e.g. petrol station "drive-offs", credit card fraud, shoplifting, etc.	Dial 999 and give details (unless to do so would provoke an attack in which case activate hold-up device)	The hold-up alarm should not normally be used for this type of incident
Theft of property or fraud with the suspects no longer on the premises	Contact local police by non-emergency means	If the suspects have left, then the incident is no longer an emergency
Incident outside the premises	Dial 999 and give details (unless to do so would provoke an attack in which case activate hold-up device)	The hold-up device is specific to the premises

NOTE The use of the hold-up device provides the police with very limited information. A phone call can help with details of a crime such as descriptions, etc.

[A2] **E.3** With the introduction of hold-up confirmation, there may be a requirement to operate two different hold-up devices, or perhaps one device that requires two different methods of operation. Users should familiarise themselves with these devices and ensure their staff are trained in their operation to ensure they are used correctly.

NOTE BS 8243 provides requirements for hold-up confirmation. Further information should be sought from your alarm company. [A2]

E.4 The system might have a duress code facility, if this is not required please ask the alarm company to remove it.

E.5 If the hold-up device is a single push device contact the alarm company and request a dual push device.

NOTE PD 6662:2004, Annex A states that single push devices are not permitted on any PD 6662 alarms.

E.6 Always contact the alarm company if any electrical or building work is being carried out which could result in cable or equipment damage.

E.7 Put labels on the hold-up devices to identify them, e.g. "POLICE HOLD UP".

E.8 Do not attempt to remove the hold-up device from its mounting.

E.9 Hold-up devices in domestic environments should be out of reach of small children.

E.10 Portable hold-up devices should be accounted for at all times and [A2] users [A2] properly trained in their use.

Annex F (informative) Corrective maintenance report form

An example of a corrective maintenance report form is shown in Figure F.1.

Figure F.1 **Model form for recording corrective maintenance**

<table>
<tr><td colspan="6">CORRECTIVE MAINTENANCE REPORT</td></tr>
<tr><td colspan="3">Customer Name .....
Address .....
.....</td><td colspan="3">Date ..... Serial No .....
Location, e.g. office, stores, etc .....
..... Spec No .....</td></tr>
<tr><td colspan="3">Reported fault .....
Type of Notification: x2 Remotely Powered WDs

Self-powered WD Main ATS Additional ATS

Specify make of ATS .....</td><td colspan="3">Circuit No .....
Circuit Location .....
Device Type .....
Device Model .....</td></tr>
<tr><td>Cause of callout
1. GENUINE ALARM</td><td>2. COMPANY RELATED</td><td>3. [A2⟩ USER ⟨A2] RELATED</td><td>4. ARC RELATED</td><td>5. TRANSMISSION PATH RELATED</td><td>6. CAUSE UNKNOWN</td></tr>
<tr><td colspan="6">Further detail and action taken
.....
.....
.....
.....
.....
.....</td></tr>
<tr><td colspan="3">.....
.....
.....
.....
.....

Further Action Required .....
.....
.....
.....</td><td colspan="3">Restore Yes/No .....
Method of Restoring .....
Charge Yes/No .....
Amount £.....
Time Arrival ..... Depart .....
Time Taken..... Travel Time .....

Materials : Cost £.....
Used .....
.....</td></tr>
<tr><td colspan="6">The System has been left in full working order apart from the items and/or disconnections listed below:
.....
.....
.....
.....</td></tr>
<tr><td colspan="3">Technician's Initials

Customer's Signature</td><td colspan="3">Office Use Time

Initials</td></tr>
</table>

Annex G (normative) Recommendations for the recording of remotely notified alarm conditions

G.1 The statistical analysis of remotely notified alarm conditions relating to remotely notified I&HASs (see Clause **7**) should be in accordance with Annex G (an example flow diagram of the compilation of statistics is given in Figure G.1).

G.2 Each alarm company should adopt a company-wide standard terminology for categorizing remotely notified alarm conditions, to enable the compilation and analysis of statistics, as a means of identifying trends and as an aid to the management of false alarms and the identification of their cause. A model form for recording remotely signalled/notified alarm conditions is given in Figure G.2.

G.3 As a minimum, alarm activations should be categorized as one of the following:

a) genuine alarm;

b) company-related alarm;

c) [A2] user [A2]-related alarm;

d) ARC-related alarm;

e) transmission path fault-related alarm;

f) cause-unknown alarm.

Every attempt should be made to ascertain the cause of alarms in order to minimize the number of alarms categorized as cause-unknown alarms.

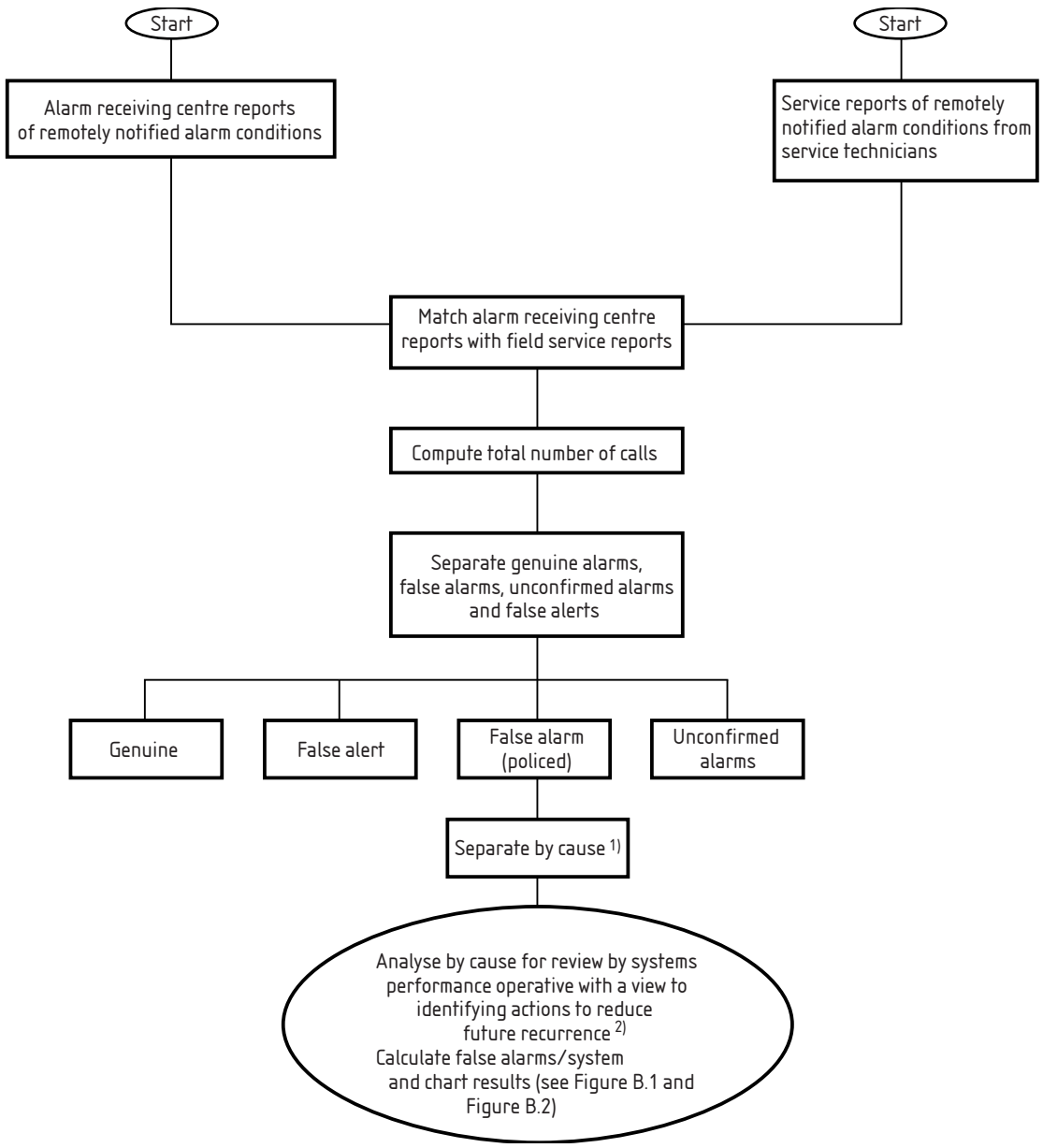
NOTE Further subdivision can be useful for the alarm company's own purposes and analysis; additional forms of categorization (e.g. by age of system) can yield useful information.

G.4 A record of false alerts and unconfirmed alarms should also be maintained and those that do not result in a service technician call-out.

G.5 The statistics should be reviewed by the SPM for I&HASs performance, with a view to identifying actions to reduce the future incidence of false alarms.

G.6 To achieve good false alarm management, it is essential that every effort is be made to match all RMC reports with field service reports.

Figure G.1 **Flow diagram illustrating the compilation of monthly reports on remotely notified alarm conditions**



1) Separation by cause might have to be done by the originator of the report.

2) It is only positively identified prime causes of alarm conditions that are categorized.

Figure G.2 **Model form for recording remotely signalled/notified alarm conditions**

REPORT OF SIGNALLED/NOTIFIED ALARM CONDITIONS for month of……..……..Year.20….. (REMOTE SIGNALLING/NOTIFICATION ALARM SYSTEMS ON POLICE RESPONSE ONLY)		
NAME OF ALARM COMPANY		
NAME AND LOCATION OF ALARM CO. CONTACT PERSON		
No. of remotely signalled/notified alarm conditions from DD 243 systems “POLICED” during the calendar month		A
No. of remotely signalled/notified alarm conditions from OTHER (non-DD 243) systems “POLICED” during the calendar month		B
TOTAL no. of remotely signalled/notified alarm conditions “POLICED” during the calendar month (A + B = C)		C
No. of GENUINE ALARMS from all systems during the calendar month		D
No. of FALSE ALARMS “POLICED” from all systems during the calendar month (C – D = E)		E
ANALYSIS OF FALSE ALARMS “POLICED”		
No. of COMPANY-RELATED false alarms “policed” during the calendar month		F
No. of [A2] USER-RELATED [A2] false alarms “policed” during the calendar month		G
No. of ARC-RELATED false alarms “policed” during the calendar month		H
No. of TRANSMISSION PATH-RELATED false alarms “policed” during the calendar month (faults “policed” due to single and dual path failures)		J
No. of CAUSE UNKNOWN false alarms “policed” during the calendar month		K
TOTAL NO. OF ALARM SYSTEMS WITH REMOTE SIGNALLING/NOTIFICATION		L
“POLICED” FALSE ALARMS PER SYSTEM PER MONTH (E / L = M)		M
ANNUALIZED: “Policed” false alarms per system per annum (12 × M = N), during this calendar month		N
ROLLING TWELVE-MONTHLY LOG: Add “N” for this month to “N” for each available previous month, up to a maximum of 11 previous months (i.e. max. of 12 months). Divide the result by the total number of months included in the calculation (i.e. where full year’s figures are available, divide by 12; if only 3 months’ figures are available, divide by 3).		O
“POLICED” FALSE ALARMS per system per annum (P), during the ..... month period ended on the last day of this calendar month.		P

Annex H (normative) Attendance on false alarms

H.1 General

The actions to be taken following the notification of a false alarm are based on the principle of greater involvement of management, rather than relying on the technical staff alone, at an early stage in false alarm repeat occurrences.

In this way, a higher level of technical skills can be directed towards problem installations to ensure prompt and accurate fault diagnosis, to be followed by the correct remedial solution.

H.2 Attendance following activation

H.2.1 Following the notification of an alarm activation a service technician should attend the premises concerned and should:

a) review the event log and ensure that a copy is retained on the client's file by the alarm company;

b) determine any previous alarm activations;

c) determine the reason for the current alarm activation in accordance with **H.2.2**, and record the findings;

d) carry out repair or remedial work to ensure that a reoccurrence of the alarm activation is unlikely.

H.2.2 After the occurrence of a false alarm, inspections and all necessary tests, as appropriate, should be carried out, by the service technician, on the following.

a) The A2 user's A2 operational procedure, including securing of supervised premises, setting of the system and whether all persons involved with setting and unsetting the system are fully conversant with the procedures.

b) The supervised premises, for any change of use or structural changes, electrical supplies or work which could affect the alarm system.

c) Any possible sources of environmental interference, e.g. heating systems, automatic lighting control, radio frequency interference and build up of dust and cobwebs, etc.

d) The correct operation of the system, in particular:

   1) control and indicating equipment;

   2) power supplies, including standby batteries and voltages at the detectors and WDs;

   3) movement detectors, by walk tests, ensuring that the ranges are properly set and that adverse environmental influences are not inside fields of detection;

   A2 4) Shock (Vibration) detectors and Glass Break detectors to ensure their sensitivity are still correctly set; A2

   5) beam interruption detectors, ensuring that beams are not likely to be obstructed;

   6) magnetic contacts, ensuring that supervised doors and windows are physically secure when closed;

7) interconnecting wiring and connections for correct functioning;

8) warning devices; ensuring correct operation including self-actuation;

9) alarm transmission systems; ensuring correct operation to the ARC;

10) all tamper circuit connections;

11) equipment related to exit/entry routes including final exit/first entry locks, readers and switches;

12) PACE for correct operation and battery life.

H.2.3 If the alarm activation can be determined to have been an [A2] user [A2] error and is likely to reoccur, it might be necessary to adopt another method of unsetting such as the method described in DD 243:2004 [A2] and BS 8243 [A2].

Bibliography

Standard references

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

BS 4737-1:1986, *Intruder alarm systems in buildings – Part 1: Specification for installed systems with local audible and/or remote signalling*[1)]

BS 4737-4.2:1986, *Intruder alarm systems in buildings – Part 4: Codes of Practice – Section 4.2: Code of practice for maintenance and records*[2)]

Other references

[1] ASSOCIATION OF CHIEF POLICE OFFICERS OF ENGLAND, WALES AND NORTHERN IRELAND. *Policy on police response to security systems*. London: Association of Chief Police Officers of England, Wales and Northern Ireland, 2005.

[2] ⟩A2⟩ POLICE SCOTLAND. *Policy on police response to security systems*. ⟨A2⟩ Glasgow: Association of Chief Police Officers in Scotland, ⟩A2⟩ April, 2013 ⟨A2⟩.

1) Withdrawn on 1 December 2003
2) Withdrawn on 1 June 2005.

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: +44 (0)20 8996 9000 Fax: +44 (0)20 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: +44 (0)20 8996 9001
Fax: +44 (0)20 8996 7001 Email: orders@bsigroup.com

You may also buy directly using a debit/credit card from the BSI Shop on the Website http://www.bsigroup.com/shop.

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: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

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: +44 (0)20 8996 7002
Fax: +44 (0)20 8996 7001 Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsigroup.com/BSOL.

Further information about BSI is available on the BSI website at http://www.bsigroup.com.

BSI Group Headquarters
389 Chiswick High Road,
London W4 4AL, UK
Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

Copyright