BS 8591:2014

BSI Standards Publication

Remote centres receiving signals from alarm systems – Code of practice

bsi.

...making excellence a habit.™

Publishing and copyright information

Published by BSI Standards Limited 2014

ISBN 978 0 580 83675 6

ICS 13.320

The following BSI references relate to the work on this document:
Committee reference GW/1/11
Draft for comment 13/30286749 DC

Publication history

First published April 2014

Amendments issued since publication

Date	Text affected

Contents

Foreword *ii*

1 Scope *1*
2 Normative references *1*
3 Terms, definitions and abbreviations *2*
4 Planning *6*
5 Construction and facilities *7*
6 Operation of an alarm receiving centre *14*
7 Records *22*
8 Contingency plan *23*

Annexes
Annex A (informative) Security and technical implications of remote access to remote centre data systems *25*
Annex B (informative) Representation of the typical relationship and communication paths between stakeholders in alarm monitoring and response *27*
Annex C (informative) Filtering actions for fire alarm signals *28*
Annex D (informative) Example form of agreement for authorizing alarm receiving centre to exercise discretion regarding the filtering out of alarm information *30*

Bibliography *32*

List of figures
Figure B.1 – Typical relationship and communication paths between stakeholders in alarm monitoring and response *27*
Figure C.1 – Fire response from ARC to site following receipt of a fire alarm signal *28*

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 34, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 April 2014. It was prepared by Subcommittee GW/1/11, *Remote Centres*, 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

Together with BS EN 50518-1:2010, BS EN 50518-2:2010 and BS EN 50518-3:2011 [1)], this British Standard supersedes BS 5979:2007, which is withdrawn.

Relationship with other publications

This British Standard has been produced following the publication of the BS EN 50518 series of standards, which apply to alarm signals generated from intruder and hold-up alarm systems (I&HAS) only. Alarm signals from other types of alarm systems, i.e. fire, social and closed circuit television systems (CCTV) are not within the scope of the BS EN 50518 series.

BS 5979, *Remote centres receiving signals from fire and security systems – Code of practice*, gives recommendations for the planning, construction and facilities of manned and unmanned remote centres, and for the operation of alarm receiving centres (ARCs) receiving signals from security systems including I&HAS. Consequently, as a result of the publication of the BS EN 50518 series, BS 5979 has been withdrawn.

The withdrawal of BS 5979 has led to the development of this British Standard, which does not include references to the monitoring of I&HAS and is intended to be used in conjunction with the BS EN 50518 series. However, BS 5979 will continue to be used in relation to ARCs that conform to BS 5979.

Information about this document

This British Standard covers the planning, construction and facilities of manned and unmanned centres, and for the operation of ARCs receiving signals from alarm systems other than I&HAS, e.g. fire, social, CCTV, lone worker devices and vehicle tracking.

This standard was written to ensure that any monitored alarm system which required a police response should conform to BS EN 50518 in anticipation that the scope of BS 50518 will be widened to encompass a greater range of systems requiring emergency police response. In order not to conflict with BS EN 50518, requirements for Category II ARCs are generally aligned with BS EN 50518. All ARCs monitoring systems not requiring emergency police response have been put into Category I, acknowledging the lesser requirements for integrity and security of construction, communications, operation and information. This has made it less onerous for non-emergency policy response ARCs to meet the requirements of this standard.

The monitoring of fire detection and fire alarm systems has received substantial review from BS 5979. This has been predominately to recognise the changing environment of social fire alarm monitoring, the review of a number of fatal fires and the need to filter calls to avoid false alarms being passed to the Fire and Rescue Services.

[1)] The 2013 versions of all three parts of the BS EN 50518 series are currently in preparation.

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.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

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 recommendations for the planning, construction and facilities of manned and unmanned remote centres, and for the operation of alarm receiving centres (ARCs), receiving signals from alarm systems, e.g. fire, social, closed circuit television (CCTV), lone worker and vehicle tracking.

This British Standard excludes receiving signals from intruder and hold-up alarm systems (I&HAS).

NOTE See BS EN 50518 series for the monitoring of I&HAS.

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 476 (all parts), *Fire tests on building materials and structures*

BS 5306-3, *Fire extinguishing installations and equipment on premises – Part 3: Commissioning and maintenance of portable fire extinguishers – Code of practice*

BS 5306-8, *Fire extinguishing installations and equipment on premises – Part 8: Selection and positioning of portable fire extinguishers – Code of practice*

BS 5839-1:2013, *Fire detection and fire alarm systems for buildings – Part 1: Code of practice for design, installation, commissioning and maintenance of systems in non-domestic premises*

BS 6132, *Code of practice for safe operation of alkaline secondary cells and batteries*

BS 6133, *Code of practice for safe operation of lead-acid stationary batteries*

BS 7858, *Security screening of individuals employed in a security environment – Code of practice*

BS 8418, *Installation and remote monitoring of detector activated CCTV systems – Code of practice*

BS 8484:2011, *Provision of lone worker device (LWD) services - Code of practice*

BS EN 3-7:2004+A1:2007, *Portable fire extinguishers – Part 7: Characteristics, performance requirements and test methods*

BS EN 12845, *Fixed firefighting systems – Automatic sprinkler systems – Design, installation and maintenance*

BS EN 13501-2, *Fire classification of construction products and building elements – Part 1: Classification using data from reaction to fire tests*

BS EN 50131-1:2006+A1:2009, *Alarm systems - Intrusion and hold-up systems - Part 1: System requirements*

BS EN 50134-3:2012, *Alarm systems – Social alarm systems – Part 3: Local unit and controller*

BS EN 50272-1, *Safety requirements for secondary batteries and battery installations - Part 1: General safety information*

BS EN 50518-1:2010, *Monitoring and alarm receiving centre – Part 1: Location and construction requirements*

BS EN 50518-2, *Monitoring and alarm receiving centre – Part 2: Technical requirements*

BS EN 50518-3, *Monitoring and alarm receiving centre – Part 3: Procedures and requirements for operation*

DD CLC/TS 50134-7:2003, *Alarm systems – Social alarm systems – Part 7: Application guidelines*

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

Other publications

[N1]THATCHAM RESEARCH. *Thatcham category 5 criteria for systems operating centres monitoring and tracking after market/OEM after theft systems with vehicle immobilisation for vehicle recovery*.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this British Standard, the terms and definitions given in BS EN 50131-1:2006+A1:2009 and the following apply.

3.1.1 alarm company
organization that provides services for alarm monitoring

3.1.2 alarm condition
condition of an alarm system, or part thereof, that results from the response of the system to the presence of a hazard

3.1.3 alarm filtering
procedure whereby signalled alarm conditions are intentionally delayed and their status reviewed for the purpose of preventing unnecessary calls to the relevant emergency service or nominated contact by cancelling certain alarm conditions, where such cancellation is authorized by the user

3.1.4 alarm message
message conveyed from an ARC to the relevant emergency service that indicates that an alarm condition has occurred at a protected premises, or which provides supplementary information concerning a previously reported alarm message

3.1.5 alarm receiving centre (ARC)
continuously manned remote centre to which information concerning the status of one or more alarm systems is reported

3.1.6 alarm signal
signal which, upon being received at an ARC or other remote location, identifies a signalled alarm condition

3.1.7 client
person or organization with whom the remote centre has entered into a contract to provide alarm monitoring services

3.1.8 customer
person or organization utilizing the services of an alarm company

3.1.9 detector
device designed to generate an alarm signal or message in response to the sensing of an abnormal condition indicating the presence of a hazard

[SOURCE: BS EN 50518-1:2010, **3.1.6**]

3.1.10 domestic premises
dwellings (see **3.1.11**) and buildings used as sheltered housing (see **3.1.27**)

3.1.11 dwelling
unit of residential accommodation occupied (whether or not as a sole or main residence):

a) by a single person or by people living together as a family;

b) by not more than six residents living together as a single household, including a household where care is provided for residents;

c) by persons who do not live together as a family, but who live in self-contained single-family flats, maisonettes or bedsits within the unit; or

d) as a shared house

NOTE The definitions in c) and d) relate only to some types of house in multiple occupation and specifically exclude hostel type accommodation, for which BS 5839-1 is more appropriate. They can, however, include houses with long-term lodgers.

3.1.12 false alert
signalled alarm condition that (without having been extended to the relevant emergency service) is regarded by the ARC as cancelled, such cancellation having been authorized by the customer

NOTE 1 Such authorization can be either:

a) on a case-by-case basis by use of suitable code words or numbers in accordance with a defined alarm filtering routine; or

b) by prior written agreement.

NOTE 2 Communication whereby the customer/user causes (i) a mis-operation signal or (ii) an unset signal to be sent to the ARC affirming that the signalled alarm condition is to be filtered out and not extended to the relevant emergency service are examples of cancellation authorized by the customer [see NOTE 1a)].

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 relevant emergency service.

3.1.13 fire alarm filtering
agreed procedure between the ARC and responsible or authorised person (user) at the premises whereby signalled fire alarm conditions are confirmed or cancelled as fire signals

NOTE Such filtering is not applied to signals from fire alarm systems in residential care premises.

3.1.14 fire resistance
ability of an element of building construction, component or structure to fulfil, for a stated period of time, the required stability, fire integrity and/or thermal insulation and/or other expected duty in a standard fire resistance test

NOTE The designation "fire resisting" given to an element implies that this element fulfils the requirements of the relevant standard fire test.

3.1.15 fire signal
signal intended to indicate the occurrence of a fire

[SOURCE: BS 5839-1:2013, **3.25**]

3.1.16 hold up device
device which, when manually operated, causes an alarm signal or message to be generated

[SOURCE: BS EN 50518-1:2010, **3.1.9**]

3.1.17 mis-operation signal
signal that is definitely and unambiguously identifiable at the ARC as indicating to the ARC that the alarm system has mis-operated and therefore that the alarm signal is to be filtered out and not extended to the relevant emergency service

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 ARC, with the concurrence of the customer.

3.1.18 operations area
that part of an ARC concerned directly with the display of information from the alarm systems monitored by the ARC

3.1.19 police response
emergency police response as defined in the ACPO and Police Scotland policies dependent upon the type of alarm system installed

3.1.20 remote access
restricted facility to view/edit data and/or to create new records from outside the shell of the remote centre

3.1.21 remote centre
location remote from the supervised premises, in which the information concerned with the state of one or more alarm systems is collected either for reporting (i.e. an ARC or a satellite) or for onward transmission

NOTE For the avoidance of doubt, an ATS monitoring centre as defined in BS EN 50136-1 does not come within the definition of remote centre for the purpose of this British Standard.

3.1.22 residential care home
home which provides accommodation and includes nursing care, personal care or personal support, to vulnerable children or adults, but excluding hospitals, schools and sheltered housing

NOTE Such premises include homes for:

- *older people;*
- *children and young people;*
- *people with learning disabilities;*
- *people with drug and alcohol problems;*
- *people with mental health problems;*
- *people with physical and sensory impairment; and*
- *respite and short breaks.*

3.1.23 response agreement
set of instructions agreed between the remote centre and the client as to the actions to be taken in the event of an alarm signal being received

3.1.24 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 ARC

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

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

3.1.25 set
status of an alarm system, or part thereof, in which an alarm condition can be notified

3.1.26 shell
all parts of the boundary of a remote centre including walls, floors, roof or ceiling and including any openings therein

3.1.27 sheltered housing
block or group of dwellings, with each dwelling incorporating its own cooking and sanitary facilities, designed specifically for persons who might require assistance (e.g. elderly people) and where some form of assistance is available at all times

NOTE 1 This does not imply that assistance need be provided on the premises.

NOTE 2 Sheltered housing often includes amenities common to all occupiers, such as lounges and guest rooms.

3.1.28 signalled alarm condition
state of monitoring equipment at an ARC (or other remote location) that indicates that a hazard and/or event or unauthorized interference has occurred at the supervised premises, or is likely to occur

NOTE Once signalled at the ARC as an alarm condition, the event is regarded as a signalled alarm condition even if subsequently filtered out by the ARC personnel as being a false alert not requiring relevant emergency service response.

3.1.29 signalling
initiation of the transmission of an alarm condition from the supervised premises to a remote location

3.1.30 social alarm system (Telecare)
system providing 24 h facilities for alarm triggering, identification, signal transmission, alarm reception, two-way speech communication, reassurance and assistance, for use by persons considered to be at risk

[SOURCE: BS EN 50134-3:2012, **3.1**]

3.1.31 supervised premises
part of a building to which protection is afforded by an alarm system

3.1.32 unset
status of an alarm system, or part thereof, in which an alarm condition cannot be notified

3.1.33 user
person authorized by the customer to operate an alarm system

3.2 Abbreviations

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

ARC – Alarm receiving centre.

CCTV – Closed circuit television.

F&RS – Fire and rescue service.

IAS – Intruder alarm system.

RVRC – Remote video response centre.

4 Planning

4.1 Categorization

The planning for the construction and for the routing of communications services of a remote centre should be determined by the intended categorization of the remote centre, taking into account any foreseeable need for change.

Remote centres should be categorized according to the type(s) of alarm and CCTV signals handled and the consequent requirements for integrity and security of construction, communications, operation and information. The two types of category are:

a) Category I: remote centre handling signals from the following:

- fire alarm systems;
- social alarm systems (Telecare);
- CCTV systems not requiring police response;
- lone worker systems not requiring police response;
- vehicle tracking systems not requiring police response.

b) Category II: remote centre handling signals from category I systems and the following:

- CCTV systems that require police response;
- lone worker systems that require police response;
- vehicle tracking systems that require police response.

NOTE See BS EN 50518 series and BS 8243 for the monitoring of I&HAS.

4.2 Site selection

4.2.1 Remote centres

4.2.1.1 Category I

A remote centre should be located in a building with low risk of fire, explosion, flooding, vandalism and exposure hazards from other buildings.

The building housing the remote centre should be protected against the effects of lightning strike.

*NOTE Appropriate recommendations for the protection of buildings and electronic equipment against lightning strike are contained in BS EN 62305. As an alternative, a remote centre can adopt the recommendations of **8.3** to sustain monitoring facilities at an alternative centre.*

The possibility of gas seepage from or around cables or pipes below ground level should be risk assessed.

4.2.1.2 Category II

ARCs should conform to BS EN 50518.

4.2.2 Alarm receiving centres (ARC)

4.2.2.1 Category I

Displayed information should not be visible from outside the shell of the ARC.

4.2.2.2 Category II

ARCs should conform to BS EN 50518.

4.2.2.3 Satellites

A satellite should be located inside a permanent building. Access to the building (or part of the building) in which the satellite is located should be under the exclusive control of the company operating the ARC to which the satellite is associated.

NOTE For the avoidance of doubt, an ATS monitoring centre as defined in BS EN 50136-1 does not come within the definition of satellite for the purpose of this British Standard.

4.3 Consultation

4.3.1 General

Appropriate consultation should be undertaken with other relevant interested parties, e.g. planning authorities, emergency services, utilities and telecommunication providers.

4.3.2 Telecommunications service

4.3.2.1 General

The telecommunications service provider should be consulted and issues that could jeopardize communication between the telephone exchange(s) and the remote centre should be identified.

Where telecommunications services offering the required levels of availability and security cannot be provided, either an alternative location for the remote centre should be considered or alternative means of providing the required levels of availability and security should be implemented, e.g. diverse routing of services using common technologies such as cables or duplicated services using differing technologies such as cables and RF techniques.

4.3.2.2 Category II ARC

The telecommunications service provider should be consulted with regard to providing electronic detection and physical protection to equipment and access points to cables located in the immediate vicinity of an ARC which, if damaged, could interfere with ARC telecommunications.

4.3.3 Emergency services

The emergency services should be informed of the nature of the risks applicable to the building and its use.

NOTE Where applicable, a familiarization visit could be carried out by local fire crews under Section 7.2(d) of the Fire and Rescue Services Act 2004 [1], and equivalent legislation in Scotland [2] and Northern Ireland [3].

5 Construction and facilities

5.1 Alarm receiving centres

5.1.1 Shell

5.1.1.1 General

The shell and all supporting structures of the ARC should have a fire resistance conforming to BS EN 13501-2, but never less than 30 minutes.

NOTE 1 The application of metal reinforcement can reduce the fire resistance and structural integrity of some construction material.

Cable and service ducts should be sealed where they penetrate walls, floors, etc., to maintain the fire resistance of the ARC.

NOTE 2 Attention is drawn to the Regulatory Reform (Fire Safety) Order 2005 in England and Wales [4] and equivalent legislation in Scotland [5] and Northern Ireland [6].

Fire safety procedures for the building should be such that they cause minimum disruption to the ARC activities.

NOTE 3 Attention is drawn to the Building Regulations 2010 [7], and to the associated guidance given in Approved Document B: Fire Safety [8] and to the LPC design guide for the fire protection of buildings [9].

5.1.1.2 Category I

As a protection to the staff from hazards such as fire and accidental or deliberate vehicle impact, all parts of the shell, excluding the openings, should be of substantial construction.

As an alternative to the fire resistance of the shell set out in **5.1.1.1**, any exterior part of the shell of a Category I ARC should be located so that there is spatial separation sufficient to minimize any potential fire hazard created by neighbouring structures and/or activities.

5.1.1.3 Category II

ARCs should conform to BS EN 50518.

5.1.2 Entrance and exits

5.1.2.1 General

One or more exits providing adequate means of escape in an emergency should be provided utilizing an unlocking device not requiring the use of a key and operable only from within the ARC.

NOTE Such as those given in BS EN 179.

5.1.2.2 Category I

All entrances and exits should be of substantial construction and capable of being made secure.

5.1.2.3 Category II

ARCs should conform to BS EN 50518.

5.1.3 Key transfer hatch

NOTE A transfer hatch or chute may be located in the shell of the ARC.

The hatch/chute should open into a security controlled area. The hatch/chute should be constructed to a standard similar to that of the shell of the ARC. The points of entry should be interlocked to prevent direct access to the ARC being available at any time and the opening and closing actions should be controlled from within the ARC. The outer entrance should open outwards away from the ARC.

Voice communication system(s) should be available from inside the ARC and the outer entry of the hatch/chute.

5.1.4 Glazed areas in the shell

5.1.4.1 Category I

Accessible glazed areas in a Category I ARC should be provided with vandal-resistant glazing (e.g. laminated glass at least 7.5 mm thick or wired glass).

5.1.4.2 Category II

ARCs should conform to BS EN 50518.

5.1.5 Ventilation

5.1.5.1 Category I

Ventilation should be controllable from within the ARC.

5.1.5.2 Category II

ARCs should conform to BS EN 50518.

5.1.6 Services – Category II only

ARCs should conform to BS EN 50518.

5.1.7 Surveillance

5.1.7.1 Category I

Secure means for determining the identity of persons requiring access to the ARC should be provided.

5.1.7.2 Category II

ARCs should conform to BS EN 50518.

5.1.8 Alarm systems

5.1.8.1 Category I

An intruder and hold-up alarm system conforming to PD 6662 (at least grade 2) should be installed which should include at least one hold-up device.

5.1.8.2 Category II

ARCs should conform to BS EN 50518.

5.1.9 Fire detection system

5.1.9.1 Category I and Category II

The whole of the building housing an ARC should be protected by an automatic fire detection system in accordance with at least Category P1/M of BS 5839-1:2013 or by an appropriate automatic fire suppression system, such as an automatic sprinkler system conforming to BS EN 12845. In the event of the automatic fire detection or fire suppression system operating, an alarm signal should be transmitted to another ARC meeting the requirements of this standard or to the F&RS. A fire alarm raised in an ARC should be signalled to the rest of any building in which it is situated and vice versa.

*NOTE Fire alarm design needs to take into account the need for business continuity, see Clause **8**.*

5.1.10 Communications

5.1.10.1 General

All communication cables between the point of entry into the building and the shell should be protected against physical and fire damage. The means of protecting cables from fire might include:

a) routed through areas of low fire risk; or

b) routed through areas protected by automatic fire detection or an automatic fire extinguishing system.

There should be a contract for 24 h emergency maintenance of all telecommunications circuits, the failure of which would affect the monitoring of alarm signals or the extension of alarm signals or the extension of alarm messages to the emergency services.

The ARC should have a minimum of two means of incoming communication for voice and sufficient capacity to cope with peak alarm demand.

Radio communication antennas should be within the shell or otherwise duplicated and/or inaccessible and/or protected against physical attack.

Personal mobile electronic devices, such as telephones, music or data storage devices, pocket PCs and photographic equipment should not be used at or adjacent to the operator's workstation.

5.1.10.2 Outgoing

There should be at least two independent means for outgoing voice communication, which should be dedicated to alarm communications and configured for outgoing calls only.

There should be sufficient communication capacity to enable all operators to make outgoing calls in respect of alarm signals without disconnecting the alarm call requiring that assistance.

In addition, for a Category II ARC, an additional radio communication technology should be installed to permit external communication with a permanently manned control room or another ARC. If radio communication is not practical or reliable, there should be an additional means for outgoing voice communication and configured for outgoing calls only.

5.1.10.3 Incoming

Where satellites connected to an ARC rely on a public switched telephone connection as a communication standby, the ARC should have a minimum of two telephone lines with ex-directory numbers dedicated exclusively for this use.

5.1.10.4 Recording equipment

The ARC should be provided with equipment for the automatic recording of all incoming and outgoing alarm signals, including date and time of receipt, and for the automatic recording of all voice and data communications in and out of the ARC.

5.1.11 Power supplies

5.1.11.1 Category I

5.1.11.1.1 General

The public mains supply should be used as the principal source of electrical power, although reliable alternatives can be used, and a standby power source should be provided as a backup. Changeover to, or from, a standby power supply should not cause the malfunction of equipment. Standby power cables external to the shell should be protected against physical and fire damage. There should be an indication in the operations area of the current source of power.

The mains supply should be such that it is capable of providing sufficient power for the normal load of the ARC and for simultaneously recharging the standby batteries to the required capacity within 24 h.

NOTE Where it can be shown that there is no loss of service delivery performance through transferring all monitoring functions to another alarm receiving centre during a power outage then backup power supplies might not be required. i.e. transfer to take place within UPS battery period.

5.1.11.1.2 Standby power supplies

A standby power supply should be of sufficient capacity for the uninterrupted operation of all communication, signalling, monitoring, recording, essential ventilation and essential lighting equipment, including that required for the necessary surveillance to conform to **5.1.7**, for a period of 24 h based on a demand of 1.5 times the average requirement.

The standby power supply should be either:

a) a standby battery with associated charging equipment (**5.1.11.1.3)**; or

b) a standby generator or generators supported by a standby battery and associated charging equipment (**5.1.11.1.4)**.

Standby batteries and any automatic changeover equipment should be located within the ARC.

5.1.11.1.3 Standby batteries

The standby batteries should be brought into use automatically and immediately if the mains voltage falls below the level required to operate the ARC. The ARC should return to mains power operation and the standby batteries should recharge automatically when the mains voltage is restored to its minimum value.

Standby batteries should be electrically protected by fuses or circuit breakers. Wet cells should be located in a separate battery room with its own ventilation.

Battery installations should conform to either BS 6132, BS 6133 or BS EN 50272-1 as appropriate.

Where a standby generator is provided, the standby battery capacity should be sufficient to power the ARC equipment for at least 4 h based on a demand of 1.5 times the average requirement.

Where a second standby generator is provided, the standby battery capacity should be sufficient to provide the required power for at least 30 min based on a demand of 1.5 times the average requirement.

NOTE Handling and charging batteries might involve flammable or hazardous substances.

5.1.11.1.4 Standby generators

Any generator situated within the shell of the ARC should be separated from the operations areas by sound-resistant construction that would afford a fire resistance conforming to BS EN 13501-2 but never less than 30 min in respect of integrity, insulation and, where relevant, load-bearing capacity, if tested in accordance with BS 476.

All standby generators should be provided with a fuel supply on site sufficient to operate the generator for at least 24 h.

NOTE 1 Charging batteries or storing fuel might involve flammable or hazardous substances.

NOTE 2 Fuel storage is governed by legislation.

All standby generators should have an independent means of starting which should be automatic or controlled from within the ARC when the normal power supply fails. Batteries required for starting a standby generator should be charged by a means that is independent of the operation of the generator.

Any standby generator not installed within the ARC shell should be in a restricted access area.

The area(s) housing generators should be protected by fire alarm and intruder detection systems.

5.1.11.2 Category II

ARCs should conform to BS EN 50518.

5.1.12 Safety equipment

The ARC should be equipped with fire extinguishers, selected, positioned and maintained as recommended in BS 5306-3 and BS 5306-8, for use by trained staff.

The control room should be equipped with at least two portable extinguishers suitable for fires involving electrical equipment. The aggregate rating of all extinguishers in the control room should be at least 26A as defined by BS EN 3-7:2004+A1:2007.

At least two 183B fire extinguishers, as defined by BS EN 3-7:2004+A1:2007, should be readily available for dealing with fires in generator rooms and/or fuel storage areas.

Sufficient extinguishers of an appropriate type should be provided in all other areas.

There should be a supply of torches for emergency use, preferably of the continuously charged type.

5.1.13 Facilities

Toilet and washing facilities should be provided within the ARC. Where cooking facilities are provided they should be separated from the operational area by a construction with a fire resistance conforming to BS EN 13501-2 but never less than 30 min.

5.2 Satellites

5.2.1 Equipment protection

5.2.1.1 General

The equipment in a satellite should be protected against attack or malicious damage in accordance with **5.2.1.2** and **5.2.1.3**.

5.2.1.2 Class A protection

The satellite equipment should be protected by one of the following methods.

a) A building in which the construction of the shell, entrances, exits, glazed openings, inlets and outlets of the satellite and service inlets and outlets should be as recommended for ARCs, although the normal entrance can be a single door and not a lobby with two doors. An IAS should be installed to detect the opening of any door or other access opening and to detect an attack on any door and/or on the shell of the satellite. Alarm conditions should be signalled to an ARC by an ATS Grade 4. If the satellite is capable of being manned, the alarm system should include hold-up devices located within the shell of the satellite. A signal should be transmitted automatically to an ARC whenever any access door to the satellite is not closed and locked.

b) A room of substantial construction, such as 100 mm brick or concrete block or stud partitioning reinforced internally by weld mesh or expanded metal with a maximum mesh size of 100 mm. External walls of the room should meet the shell construction recommendations for a Category II ARC. The room should have the minimum number of entrances and should be without glazed areas. Openings in the shell of the room that are accessible from public areas, such as those for ventilation, should be supervised as recommended for ARCs.

An IAS should be installed incorporating detection to all doors and other access openings by the satellite.

Movement detectors should be incorporated to detect approaches to the satellite equipment. Where satellite equipment is positioned against or attached to a wall of the room, means should be provided to detect an attack on that wall. Alarm conditions should be signalled to an ARC by an ATS Grade 4.

An alarm condition should be signalled whenever any door or other access opening is not closed and locked.

Where a satellite is capable of being manned, the IAS should include at least one hold-up device located within the room.

The satellite equipment should be enclosed in lockable containers constructed from one or more of the following materials:

1) low carbon steel not less than 1.2 mm thick;

2) stainless steel not less than 1 mm thick;

3) material offering durability, security of fixing and resistance to attack by hand-held tools, including burning methods, at least to the same degree as items 1) and 2).

The equipment containers should be firmly secured in position and should be fitted with tamper detection that will operate when the access panel or door is opened by normal means. A signal should be transmitted to the ARC whenever an access panel or door of a container is not closed.

5.2.1.3 Class B protection

The satellite equipment should be located in a room having restricted access. A satellite IAS should be installed in the room for use when it is unoccupied. The system should incorporate detection at all doors or access openings to the room together with movement detector(s) providing an overall field of detection covering all approaches to the satellite equipment. Where satellite equipment is positioned against or attached to a wall of the room, detection should be provided which will signal an alarm prior to the penetration of the wall. If the satellite is capable of being manned, the alarm system should include at least one hold-up device located within the shell of the satellite. The satellite equipment should be enclosed in lockable containers constructed from one or more of the following materials:

a) low carbon steel not less than 1.2 mm thick;

b) stainless steel not less than 1 mm thick;

c) material offering durability, security of fixing and resistance to attack by hand-held tools, including burning methods, at least to the same degree as items a) and b).

The equipment containers should be firmly secured in position and should be fitted with tamper detection that will operate when an access panel or door is opened by normal means. A signal should be transmitted to the ARC whenever an access panel or door of a container is not closed.

5.2.2 Fire alarm

An automatic fire alarm system should be installed conforming to Category P1/M of BS 5839-1:2013 throughout the satellite. A fire alarm condition resulting from a fire within the satellite should transmit an alarm automatically to the ARC. A fire alarm raised in a satellite should be signalled to the rest of any building in which it is situated and vice versa.

5.2.3 Communications

A satellite should have two or more dedicated alarm transmission paths to its ARC for the transmission of alarm signals, supplemented by alternative communication means and/or provision for manning to enable the processing of alarm signals from connected alarm systems in the event that normal communication to the controlling ARC is lost.

Where the satellite has provision for manning, there should be a telephone with an ex-directory number for voice communication.

5.2.4 Power supplies

Power supplies for satellites should meet the recommendations given in **5.1.11**.

Arrangements should exist for a trained engineer to attend a satellite, if required, within 4 h of a fault being detected.

6 Operation of an alarm receiving centre

6.1 Staff selection and training

All ARC staff should be selected and trained according to the level of security of the information to be handled by the ARC. For a Category II ARC, this should be by the security screening process described in BS 7858.

All ARC operators should receive a period of training within the ARC to familiarize them with the routines and practices of operation. There should be a stated minimum period of training to ensure the minimum competence to carry out specified duties, and before the operator is allowed to handle alarms without direct supervision. Further training should be given as necessary for specific subjects, such as new equipment or changes in operational procedure.

6.2 Access

6.2.1 Category I

A written procedure should exist for the granting of entry into, and exit from, the ARC.

Routine access to an ARC should be restricted to authorized staff who have a need to enter on a regular basis.

The number of staff permitted to authorize visitors to an ARC should be restricted and their names included on a list available to the ARC responsible for controlling access.

Use of a key transfer hatch should be restricted to persons named on a list held by the ARC supervisor. The persons should be limited and the names and photographs of these persons should be readily available to those staff responsible for controlling use of the key transfer hatch.

The names and photographs of all authorized staff should be readily available to those staff responsible for controlling access. All visitors should be authorized in advance of the visit and should always be accompanied by an authorized person.

Where provided, remote access to ARC computer systems and data should be restricted and controlled by strict security disciplines. ARC computer equipment should be capable of recognizing any attempt at compromise.

NOTE Further guidance for remote access, providing assistance to third party alarm companies and multi-site companies are given in Annex A.

6.2.2 Category II

ARCs should conform to BS EN 50518.

Use of a transfer hatch should be restricted to persons named on a list held by the ARC supervisor. The persons should be limited and the names and photographs of these persons should be readily available to those staff responsible for controlling the use of the transfer hatch.

Where provided, remote access to ARC computer systems and data should be restricted and controlled by strict security disciplines. ARC computer equipment should be capable of recognizing any attempt at compromise.

NOTE Further guidance for remote access, providing assistance to third party alarm companies and multi-site companies are given in Annex A.

6.3 Operating procedures

6.3.1 All alarm and CCTV systems

NOTE Annex B outlines common lines of communication/the contractual relationship between the ARC, installer/maintainer, users and emergency services.

6.3.1.1 Primary function

The primary function of an ARC should be the handling of alarm and/or CCTV signals, together with other signals relating to the change of status of the alarm and/or CCTV systems, such as setting or unsetting or alarm and fault signals relating to associated alarm transmission systems and any related or subsidiary operations such as keyholding or controlling a security response service.

6.3.1.2 Staffing levels

There should be a minimum of two operators in an ARC at all times, capable of carrying out all operations procedures, at least one of whom should be at their workstation at all times.

Staffing levels should be related to maintenance of the response times given in **6.4** to **6.8**.

Staff in reserve should report for duty within 1 h.

6.3.1.3 Contracts with clients

Clients should be provided with a written contract giving details of the category of the remote centre, the types of system(s) monitored and the fees for the service(s) provided, as appropriate.

As part of this contract, there should be a written response agreement with each client specifying the action(s) to be taken on receipt of an alarm, fault or other signal including mis-operation signal. The response agreement should specify any reports or other information to be provided to the client. The arrangements for contacting a user following a signalled alarm condition should be agreed between the ARC and the client. The client should be given details of the method of communication with the emergency service(s) and the name(s) of the relevant service(s) for their protected premises.

ARCs should provide a monthly report of any alarm system activation to their client in order to aid the client in their management of false alarms.

6.3.1.4 Procedures and work instructions

Clear guidelines on the actions to be taken on the receipt of alarm and/or CCTV signals should be documented in the procedures and work instructions.

All staff should have immediate access to a copy of the procedures and work instructions relevant to their role. Supervisors should ensure that all aspects of the operation are clearly understood and complied with. The procedures and work instructions should include full details of all routine work together with actions to be taken in the event of foreseeable emergencies (see Clause **8**).

As a minimum, the following operational procedures should be documented:

a) access (**6.2**);

b) handling alarms (**6.3.1.4**);

c) complaints (**6.3.1.5**);

d) confidentiality (**6.3.1.8**);

e) information provided to emergency services (**6.3.1.9**);

f) testing of monitored alarm systems (**6.3.1.11**);

g) filtering (**6.4.2**);

h) testing (**6.9**);

i) faults (**6.9.4**); and

j) contingency plans (Clause **8**).

Procedures and work instructions should be kept secure.

6.3.1.5 Complaints procedure

The ARC operating company should have a clearly defined, published procedure for the receipt and handling of complaints. Clients should be given details of the person to contact if they wish to complain about any aspect of the service.

The address, telephone number and job title of the person to be contacted should be provided, together with the preferred method of communication.

6.3.1.6 Audit

The ARC manager should ensure all procedures are carried out correctly and that a documented audit of all procedures is undertaken at periods not exceeding 12 months.

6.3.1.7 Personnel safety monitoring

The safety and security of the ARC personnel should be automatically monitored at a maximum of 60 min intervals. In case of non-response to the safety and security check within 60 s, an alarm should be automatically extended to another ARC.

6.3.1.8 Confidentiality

When appropriate, documented procedures to authenticate the exchange of confidential information between the ARC and the customer should be agreed with the client.

NOTE 1 Authentication can be achieved by use of passwords or codes.

NOTE 2 Examples of confidential information include changes to setting or unsetting times, the cancelling of alarm conditions, and the names and addresses of users.

NOTE 3 Attention is drawn to the Data Protection Act [10].

6.3.1.9 Information provided to emergency services

The ARC should have documented procedures for identifying and for wording the information required by each response service.

6.3.1.10 Transmission faults

The user should be informed of any transmission fault as soon as practicable. Agreement should be reached with the client as to the course of action regarding the notification of the appropriate emergency service.

Recurrent and/or intermittent transmission faults should be the subject of discussions with the client on the action required from the ARC upon receipt of a transmission fault signal.

A record of all transmission faults and their duration should be maintained by the ARC and should be reviewed for action daily.

6.3.1.11 Testing of monitored alarm systems

The ARC should have a documented procedure for accepting an oral request to place a monitored alarm system on test by a user, client or installing/maintaining company, whereby alarm signals will not be passed to the emergency services and/or nominated contact(s) during the period of the test. The procedure should be agreed with the client.

As a minimum, the procedure should include that the person making the request confirms:

a) the site identification code; and

b) a previously agreed passcode (except for fire alarm systems).

The ARC procedures should revert to their original status after the test period has elapsed. The time period allowed for the system to remain on test should not be greater than 8 h.

6.4 Fire alarm systems

*COMMENTARY ON **6.4**.*

The ARC and ARC operator are part of the critical path between a fire being detected and a rescue or extinguishment of the fire taking place. Any delay in the receipt of a call, information gathering, passing the call to the F&RS and passing appropriate information to the F&RS service might delay the F&RS response or contribute to an inappropriate response being made and therefore could put occupants and fire-fighters lives at risk.

6.4.1 General

Fire alarm signals should be given priority and should be clearly distinguishable from other alarm indications, at least by visual means.

There should be an agreement with each F&RS to which fire alarm signals are to be passed.

NOTE 1 An ideal method of providing address details to the F&RS comprises of a unique reference number (URN).

Action should be taken by an operator to initiate communications with the control room of an appropriate emergency service or, if applicable (see **6.4.2**), to commence a filtering procedure within 30 s for 90% of signals received, and within 90 s for 98.5% of signals received.

NOTE 2 Alarm filtering can commence at any time within the times given above.

Fire alarm signals should normally be passed without delay and without the application of filtering procedures, except in the case of domestic premises. Filtering should normally be applied to all signals received from domestic premises, particularly where facilities exist to establish direct speech communication with residents (e.g. via a social alarm system).

Filtering should apply in the following instances:

a) if no contact with the protected premises can be established, the filtering process should cease and action should be taken to contact the F&RS without any further delay within 30 s; or

b) once voice communication with an occupant(s) has been established, action should be taken to contact the F&RS within a maximum of 60 s, unless the ARC has been informed unambiguously that the signal is a false alert.

The ARC should review with their client on a monthly basis all systems that have been taken off a contractual requirement to contact the F&RS temporarily (e.g. because of false alerts) to confirm the status of the systems and the ARC should keep records of these reviews.

NOTE 3 The above recommendations are predicated on the assumption that the contract with the client will require that the F&RS are summoned in the event of a fire signal that is not a false alert. This is not necessarily the case. A contract can require that only other actions are taken, such as contact with key-holders; in such cases, it is not expected that the ARC will contact the F&RS on receipt of an alarm signal, regardless of the circumstances.

NOTE 4 Refer to Annex C for the contacting site flow diagram.

NOTE 5 Electronic transmission of alarm signals between the ARC and the F&RS is permitted providing a written agreement exists between the two parties.

There should be a requirement for a written report to be made, describing the circumstances and action taken, in all cases where the time between receipt of a signal and transmission of information to the F&RS exceeds 180 s.

6.4.2 Filtering

Following the receipt of a fire alarm, the ARC should call the F&RS if:

a) there is no filtering in place;

b) where filtering is in place and there is no contact with anyone on site within 30 s (see **6.4.1**);

c) filtering is in place and a person on site confirms that there is a fire; or

d) a person on site authorizes the F&RS to be called.

Other than in the case of domestic premises (for which filtering should always be applied), filtering procedures should only be implemented by the ARC if requested, in writing, by the client. There should be an agreed written procedure between the ARC and the client. The agreed procedure should determine the arrangements for review, confirmation or cancellation (filtering) of signalled fire alarm conditions.

NOTE Annex D provides an example form of agreement for authorizing ARCs to exercise discretion regarding filtering.

The ARC should review any filtering procedures every 12 months with the client.

Filtering procedures should be documented and readily accessible to ARC operators and should clearly record the agreed maximum filtering period.

Filtering should not be applied to signals from fire alarm systems in residential care premises.

6.4.3 Fire signals transmitted automatically via social alarm systems

*COMMENTARY ON **6.4.3**.*

In sheltered housing, early attendance of the F&RS in the event of fire can be important. Where a social alarm system is installed in premises, such as sheltered housing (but also independent dwellings for vulnerable people), it is appropriate for fire signals to be relayed to the same location as alarm signals from the social alarm system. However, in the first instance, it is not usually appropriate to summon the F&RS on receipt of a fire signal at an ARC.

Where the operator has the opportunity to verify the call through two-way speech, this should be done prior to contacting the F&RS. If a fire is confirmed, the F&RS should be contacted immediately.

The line to the occupant and the F&RS should be kept open until the call is closed by the arrival of fire crews on the scene or at the request of the F&RS control officer.

The ARC should have procedures and facilities, agreed with the F&RS, to transfer the call to the F&RS by conference call or some other means in order so that the F&RS can, if necessary, give fire survival guidance directly to an occupant. If technology precludes the availability of facilities to transfer the call to the F&RS, operators at the ARC should be competent to provide this guidance; during the incident, guidance should be given in consultation with the F&RS control operator.

Any further information gained, such as the exact location and condition of the occupant, other persons involved and the exact location and cause of the fire, should be transferred to the F&RS.

NOTE It might be advantageous to include a second operator to speak to the occupant or F&RS.

If the fire detection and fire alarm system is integrated with the social alarm system and both systems share a single communications link to an ARC, fire alarm signals should be distinguishable from other signals. Handling of one or more non-fire alarm signals at the ARC should not delay the display of a fire alarm signal received at the ARC (whether from the same premises as the non-fire alarm signal(s) or from different premises).

6.5 Social alarm systems

Specific operating procedures for ARCs handling signals from social alarm systems are given within Section 8 of DD CLC/TS 50134-7:2003.

NOTE 1 Where there is conflict between DD CLC/TS 50134-7:2003 and this British Standard, it is expected that the recommendations of this British Standard will take precedence.

NOTE 2 Further information on social alarm monitoring can be found in the TSA Code of Practice [11].

6.6 CCTV system monitoring

6.6.1 Detector activated remotely monitored CCTV systems conforming to BS 8418

RVRCs monitoring detector activated CCTV systems installed to BS 8418 should conform to those sections of BS 8418 relating to RVRCs.

NOTE Such systems are eligible for Police Unique Reference Numbers.

6.6.2 CCTV systems not conforming to BS 8418

NOTE 1 CCTV systems other than BS 8418 CCTV systems are not eligible for police response under the security systems policy issued by ACPO. [2)]

Where video monitors at an ARC continually display images from a CCTV system, there should always be at least one operator on duty to control the CCTV system and to evaluate the information in images received.

NOTE 2 It is permissible for one operator to control and evaluate the information in images from more than one CCTV system provided this is agreed in writing in contracts with clients.

Where video monitors at an ARC display images normally only in response to the detection of an event, action should be taken by an operator to commence evaluation of the information in images received within 90 s for 80% of cases and within 180 s for 98.5% of cases, unless otherwise agreed in writing with the client.

6.7 Signals from lone worker devices

The ARC should conform to BS 8484:2011, Clause **6**.

6.8 Signals from after-theft systems with vehicle immobilization for vehicle recovery

The ARC should conform to Thatcham Requirements [N1] for system operating centres monitoring Category 5 after-theft systems with vehicle immobilization for vehicle recovery.

NOTE Attention is drawn to the BS EN 15213 series on after-theft systems for the recovery of stolen vehicles.

[2)] See <http://www.acpo.police.uk> [last viewed 20 February 2014].

6.9 Testing

6.9.1 General

Documented procedures should exist for the regular testing of all equipment required for the operation of the ARC. Equipment having internal clocks should be synchronized with the World Time Clock at least every 24 h.

NOTE World Time Clock is a universal time-keeping utility providing the most accurate time by synchronizing with atomic time servers and displaying local time and date in any location around the world.

6.9.2 Daily tests

The following equipment should be checked for correct functioning on a daily basis and the results recorded:

a) alarm receiving equipment (RCT);

b) annunciation equipment (AE);

c) communications systems (see **5.1.10**); and

d) all incoming and outgoing communication lines (see **5.1.10**).

6.9.3 Weekly tests

The following equipment should be checked for correct functioning on a weekly basis and the results recorded:

a) alarm systems of the ARC (see BS EN 50518-1:2010, Clause **6**);

b) electrical power supplies (see BS EN 50518-1:2010, Clause **7**); and

c) emergency lighting equipment.

6.9.4 Fault procedures and reporting

Any item of equipment involved in the receipt, display or onward transmission of an alarm signal, including power supplies, should have a standby facility and procedure that can be brought into use either automatically or by an ARC operator within 1 h from the moment the existence of the fault becomes known to the operator.

A documented procedure should exist for the repair of equipment mentioned in **7.2**. This procedure should include a time frame for the commencement of the fault report, which should not exceed 15 min of discovery.

6.10 Recovery from equipment failures

*COMMENTARY ON **6.10**.*

*This subclause is intended to cater for reasonably foreseeable equipment failures but not catastrophic failure of a major part of an ARC; this is covered in Clause **8**.*

6.10.1 Category I

Any item of equipment involved in the receipt, display or onward transmission of an alarm signal, including power supplies, should have a standby facility or procedure that can be brought into use either automatically or by an ARC operator within 1 h from the moment the existence of the fault becomes known to the operator.

The ARC should be provided with adequate spares for all receiving, processing and display equipment that is common to more than one connected system. Arrangements should exist for a trained engineer to attend an ARC, if required, within 4 h of a fault being detected.

6.10.2 Category II

Remote centres should conform to BS EN 50518-2:2010 Clause **7**.

7 Records

NOTE Attention is drawn to the Data Protection Act [10].

7.1 Client records

Client records for each system connected to an ARC should be readily available to operators. Client records may be written or stored in electronic memory, in which case they should be available for print-out on demand. Client records should be kept for the duration of the contracts plus two years.

Client records should contain the following information:

a) name, address and telephone number of the client, with an allocated reference number and details of any special arrangement or circumstances concerning the customer;

b) names and telephone numbers of key-holders;

c) the appropriate emergency service to be contacted or other agreed action(s) to be undertaken, when an alarm condition occurs;

d) agreed setting/unsetting times where appropriate; and

e) the types of signals to be monitored.

Records of all monitored events should be kept for not less than two years after the event to which they refer.

7.2 Logs

A log should be maintained recording all routine testing, maintenance and emergency servicing to ARC equipment. The log should be kept for a minimum of three years.

7.3 Performance analysis

The ARC should maintain an analysis of its performance in terms of the response time to incoming signals (see **6.4** to **6.8**). Performance figures should be calculated on a monthly basis as a minimum. The figures should be kept for a minimum of three years.

7.4 Voice communications

All telephone communications to and from an ARC should be recorded with their time and date, should be kept for at least three months and should be capable of being replayed. Telephone communications of incidents relating to social alarms should be kept for at least two years.

Voice communications that are the subject of enquiry raised with the ARC should be retained until the conclusion of the enquiry.

7.5 Data communications

All data communications to and from the ARC should be recorded with their time and date, should be kept for at least two years, and should be capable of being printed and/or displayed.

NOTE RVRC image and data retention times are referred to in BS 8418.

7.6 Audits

A record of all audits (see **6.3.1.6**) should be retained for at least three years from the date of their performance.

7.7 Security

All records should be stored securely and backup procedures instituted for electronically stored data.

7.8 Disposal

All records of a confidential nature should be disposed of in a secure manner when no longer required, e.g. by shredding.

8 Contingency plan

8.1 General

There should be a documented contingency plan for dealing with the event of an ARC and/or its satellite(s) being put out of action. The contingency plan should cater for any reasonably foreseeable abnormal occurrence with the potential to cause degradation or loss of service at an ARC. The actions to be taken should be clearly defined covering both technical and/or other emergencies. The contingency plan should include:

a) a means whereby the appropriate emergency services can be informed immediately;

b) provision for manning satellite stations that do not automatically divert to an alternate ARC in order to identify any systems which have gone into alarm condition and to inform the emergency services and users of those supervised premises in alarm condition;

c) a means for informing clients;

d) contact details of contractors and service providers able to undertake reinstatement whilst the service is maintained;

e) the means by which services will be continued or restored; and

f) a review period of not less than six months, performed by the management.

8.2 Hazard examples

Examples of hazards that should be considered when writing the contingency plan include:

a) complete failure of processing capability;

b) faults in, or damage to, site utilities, communications equipment or communications circuits;

c) fire, including exposure to fire in adjoining and adjacent properties;

d) flood or other water incursion, e.g. from the bursting of pipe systems;

e) storm and lightning damage, including lightning induced over-voltages carried on public electricity supplies and telephone lines;

f) vehicle impact, including rail vehicles and aircraft;

g) malicious damage;

h) criminal attack, bomb threats or other duress situations; and

i) abnormal levels of activity or staff shortages.

8.3 Reinstatement of monitoring services

Where an envisaged incident involves loss of monitoring services, plans should be made to reinstate operations on site or to transfer to an alternative site conforming substantially to either this British Standard for Category I or for Category II, BS EN 50518 or BS 5979 within a maximum of 28 days of the loss of monitoring.

NOTE 1 It is expected that monitoring services will resume in a much shorter time frame. The 28 days refers to the time for the alternative premises to conform to the recommendations of this British Standard or the BS EN 50518 series.

Where satellites might be required to be manned during an emergency, procedures should exist to enable relevant personnel to be contacted immediately and to have the satellite staffed within a time limit of 4 h.

NOTE 2 The recommendations of this subclause are not intended to apply to CCTV schemes, such as town centre CCTV schemes, which are reliant upon fixed, physical communication paths, e.g. fibre optic cables.

8.4 Staff procedures associated with contingency plan

The ARC manager should ensure that staff are instructed in the procedures associated with the contingency plan. In particular, the shift supervisor should be familiar with all procedures and, in the event of having to instigate any of the evacuation actions, should be able to advise the staff accordingly.

All staff should receive instruction in the location and use of all fire and first aid equipment provided at the ARC. The procedures to be adopted in the event of partial or complete loss of service from an ARC and/or any associated satellite(s) should be defined, including a procedure for the operational security of client records.

A detailed action plan should be provided covering both the controlled evacuation of non-essential staff, in the event of a small emergency which might be dealt with using local resources, and the evacuation of all personnel if the shift supervisor so determines. The plan should include the procedures for re-entry and/or recovery following an incident.

Operators should receive necessary training in the procedures associated with contingency plans. Contingency plans should be rehearsed at intervals not exceeding six months by simulating a damage incident. Warning of such a rehearsal should not be given to management and staff other than any provisions necessary to avoid loss of service to clients/customers.

Records should be kept of actions taken during the rehearsal as part of the normal activity log; the contingency plan should be reviewed and if necessary amended, taking account of the results of the rehearsal. Records should be kept for a minimum of three years.

Annex A (informative) Security and technical implications of remote access to remote centre data systems

A.1 General

ARC operators are reminded of other standards relating to the security of information management systems, e.g. BS ISO/IEC 27002:2005, BS ISO/IEC 17799:2005/BS 7799-1:2005.

A.2 Levels of access

While remote access to remote centre data systems can be made as secure as a client requires, at least two levels of security are recommended.

a) *Remote access level 1*: the client logs on to the operating system which allows access only to the application program.

b) *Remote access level 2*: a different passcode is then required to gain access to the application level.

Access to the application software can be granted by means of a log on identification code together with a passcode of not less than eight characters. After 15 min of inactivity, the client is automatically logged off the system and connection to level 1 terminated. Reconnection requires the log on procedure to be carried out from the beginning. Client access by telephone to a remote centre is no different to a manual system.

A.3 Access to the system

At the remote centre, it is recommended that the hardware and software responsible for processing the remote access be kept separate from the hardware and software responsible for processing the alarm signals, apart from any necessary communication link. This could be achieved by the use of a front-end processor.

The equipment at the remote centre that is used to communicate with remote access clients is then connected to a computer which is separate from the ones that are used to process alarm signals. To prevent unlawful access to the system, the remote centre might consider disconnecting the client for at least 1 h following three unsuccessful attempts to gain access to the system.

A.4 Authorization for facilities

A.4.1 General

Only access to data relating to each client's respective, specific contract with the remote centre is permitted.

A.4.2 View only

All data relating to the specific contract that is covered by the use of a given password is to be made available for viewing by remote access except for passwords, security codes and emergency service telephone numbers.

A.4.3 Edit

Provide a different log on passcode to access the edit facility to that of the view only function and after 5 min of inactivity, terminate access. The following are not to be edited:

a) the response agreement;

b) the relevant emergency service unique reference number (URN);

c) the archive history; and

d) suspension of service.

A.4.4 Creation of a new record

The creation of a new record is separate from that of view only or edit. Creation of a new client record can be undertaken remotely, but it is only to be brought online under the control of the remote centre.

A.4.5 Confirmation of changes made

Remote centre operators are advised to verify to the best of their ability the edited changes. To protect against the risk of unauthorized changes, and to protect against the risk of invalid data being held on the computer, confirmation of changes are to be forwarded to the person/organization with whom the remote centre has a contract. This can be by paper or electronic means (e.g. email).

A.5 Placing a system on test

The facilities for placing a system on test are not to be made available at access level 1. It is important that a differentiation is made between a test and the suspension of the monitoring service. Suspension of service would normally be the responsibility of the remote centre under instruction from the client

Tests would normally be for the purposes of fault diagnosis, or routine maintenance. An engineer or client is required to enter both his/her own passcode and the site identification code in order to gain access to the system. Tests are to be conducted for no longer than 4 h.

It is recommended that the remote centre data revert to its original status after 4 h. The client/engineer would be required to log on again if testing is to be continued.

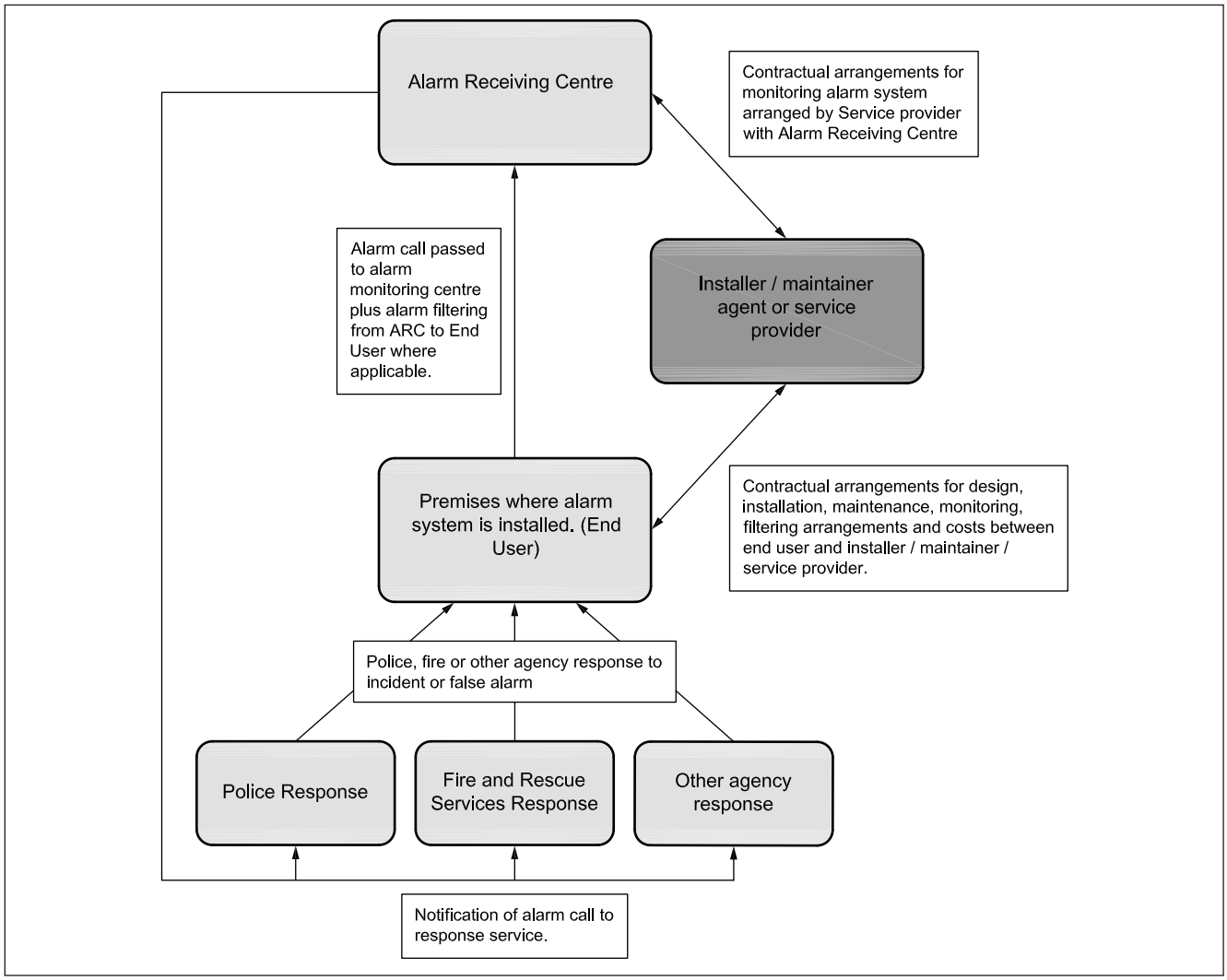
A.6 Password management

Means are to be provided to audit, validate and/or delete unused, withdrawn or otherwise unauthorized usernames and passwords.

Annex B (informative) Representation of the typical relationship and communication paths between stakeholders in alarm monitoring and response

Many parties are involved in the supply, use and response of alarm systems. The following diagram shows the various stakeholders and their lines of communication/contractual relationships.

Figure B.1 **Typical relationship and communication paths between stakeholders in alarm monitoring and response**



Annex C (informative)

Filtering actions for fire alarm signals

Fire alarm signals can normally be passed without delay and without the application of filtering procedures, except in the case of domestic premises (see **6.4.1**).

Certain fire alarm signals received at the ARC might require filtering in an attempt to verify if the signal is genuine or false. Time is critical when responding to fire alarms therefore any attempts to filter are to be kept to a minimum.

The following diagram gives guidance on actions and timing when filtering fire alarm signals ("AFAs").

Figure C.1 **Fire response from ARC to site following receipt of a fire alarm signal**

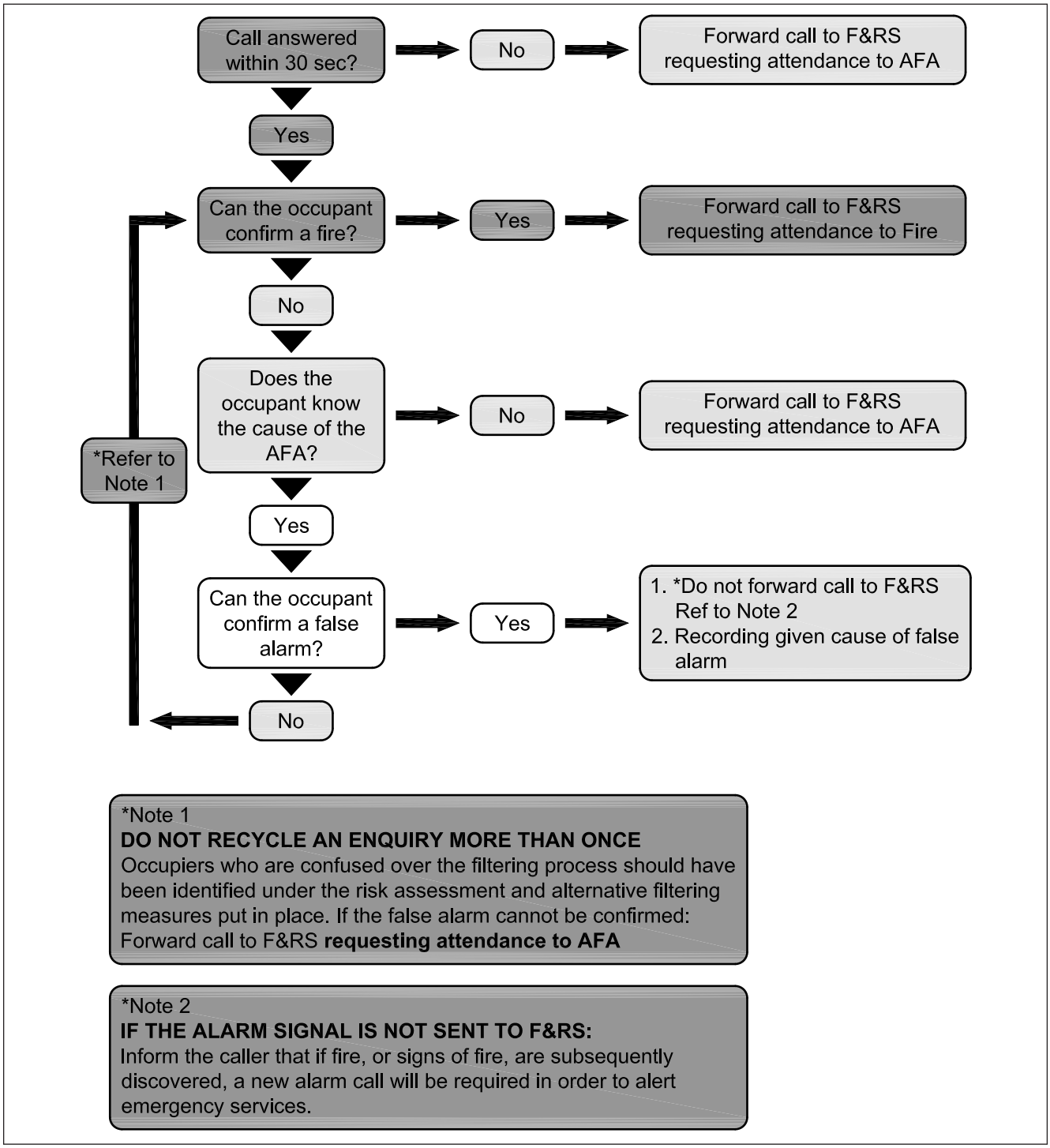


Figure C.1 **Fire response from ARC to site following receipt of a fire alarm signal**

NOTE 1 This Figure is taken from the CFOA's Code of Practice – Best Practice for Summoning a Fire Response via Fire Alarm Monitoring Organisations and is published with the kind permission of the Chief Fire Officers' Association.

NOTE 2 Filtering procedures are determined and vary by fire authority.

Annex D (informative) Example form of agreement for authorizing alarm receiving centre to exercise discretion regarding the filtering out of alarm information

D.1 The alarm company should not give the ARC a standing authorization or standing instruction to the effect that alarm signals can be cancelled by the ARC unless there exists a prior written agreement between the alarm company and the customer, with such written agreement:

a) being signed by the customer;

b) including a statement whereby the customer confirms that:

   1) they have received a copy of the "system record";

   2) they have received a copy of the alarm filtering policy of the ARC;

   3) they have received a copy of a summary of the operational instructions adopted by the ARC; and

   4) they accept the alarm filtering policy of the ARC;

c) including (or alternatively having been preceded by) a written notice advising the customer to consult with their insurers before entering into an agreement giving authorization for an ARC to exercise discretion regarding the filtering-out of alarm information;

d) clearly stating whether or not alarm information that has been filtered-out in accordance with the agreement (without having been extended to the emergency authority) is to be notified to the customer and (if it is to be so notified) when the customer/user is to be called (e.g. at the time of receipt of the alarm information, or during normal working hours).

NOTE It is the responsibility of the alarm company to ensure that the authorizations, instructions and other alarm monitoring arrangements between the alarm company and the ARC do not conflict with any agreement entered into between the alarm company and the customer, and it is recommended that alarm companies take particular care to check that their monitoring arrangements do not permit the ARC to cancel alarm information in circumstances which have not been accepted by the customer.

The agreement should state exactly how the discretion is to be used, e.g. does it apply only to the first occasion in a set period, or to more than one occasion in a set period and, if the first has not been responded to, what are the circumstances under which an alarm message is to be extended to the emergency authority, even though not confirmed?

D.2 The ARC should have clear and comprehensive operational instructions readily available to ARC operatives, setting out the steps in the handling of alarm information that is subject to the agreement. The operational instructions should clearly indicate the decision points and the decision criteria.

*NOTE **D.1**b) 3) requires a summary of these operational instructions to be supplied by the alarm company to the customer.*

D.3 Where a decision not to extend alarm information to the emergency authority is taken by an ARC operative, the receipt of that alarm information should nevertheless be recorded by the ARC. The circumstances relating to the decision should also be recorded and along with the name or other identifier of the operative who made the decision.

D.4 Where a decision not to extend information to the emergency authority is taken automatically by the pre-programmed ARC equipment, the receipt of that alarm information should nevertheless be recorded by the ARC. The circumstances relating to the decision should also be recorded, or alternatively

the details of the program controlling the automatic ARC equipment, sufficient to allow identification of the reasons for the alarm information having not been extended to the emergency authority.

Bibliography

Standards publications

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

BS 8243, *Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice*

BS EN 179, *Building hardware – Emergency exit devices operated by a lever handle or push pad, for use on escape routes – Requirements and test methods*

BS EN 15213-1, *Intelligent transport systems – After-theft systems for the recovery of stolen vehicles – Part 1: Reference architecture and terminology*

BS EN 15213-2, *Intelligent transport systems – After-theft systems for the recovery of stolen vehicles – Part 2: Common status message elements*

BS EN 15213-3, *Intelligent transport systems – After-theft systems for the recovery of stolen vehicles – Part 3: Interface and system requirements in terms of short range communication system*

BS EN 15213-4, *Intelligent transport systems – After-theft systems for the recovery of stolen vehicles – Part 4: Interface and system requirements in terms of long range communication system*

BS EN 15213-5, *Intelligent transport systems – After-theft systems for the recovery of stolen vehicles – Part 5: Messaging interface*

BS EN 50136-1, *Alarm systems - Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems*

BS EN 62305-1, *Protection against lightning – Part 1: General requirements*

BS EN 62305-2, *Protection against lightning – Part 2: Risk management*

BS EN 62305-3, *Protection against lightning – Part 3: Physical damage to structures and life hazard*

BS EN 62305-4, *Protection against lightning – Part 4: Electrical and electronic systems within structures*

BS ISO/IEC 27002:2005/BS 7799-1:2005, *Information technology – Security techniques – Code of practice for information security management*

BS ISO/IEC 17799:2005/BS 7799-1:2005, *Information technology – Security techniques – Code of practice for information security management*

CEN/TS 15213-6, *Road transport and traffic telematics – After-theft services for the recovery of stolen vehicles – Part 6: Test procedures* [3)]

Other documents

[1] GREAT BRITAIN. The Fire and Rescue Services Act 2004. London: The Stationery Office.

[2] GREAT BRITAIN SCOTTISH PARLIAMENT. Fire (Scotland) Act 2005. London: The Stationery Office.

[3] GREAT BRITAIN. The Fire and Rescue Services (Northern Ireland) Order, 2006. London: The Stationery Office.

[4] GREAT BRITAIN. The Regulatory Reform (Fire Safety) Order 2005 (FSO). London: The Stationery Office.

[3)] Part 6 awaits final evaluation and ratification as an EN and until such time remains a valid part of this EN as CEN/TS 15213-6:2011.

[5] SCOTLAND. Fire Safety (Scotland) Regulations, 2006. London: The Stationery Office.

[6] NORTHERN IRELAND. The Fire Safety Regulations (Northern Ireland), 2010. London: The Stationery Office.

[7] GREAT BRITAIN. Building Regulations 2010 – Approved Document B Fire Safety. London: The Stationery Office.

[8] NBS. Approved Document B: Fire Safety. Newcastle: RIBA Enterprises Ltd., 2013.

[9] LPC. The LPC design guide for the fire protection of buildings 2000. Gloucestershire: Fire Protection Association.

[10] GREAT BRITAIN. Data Protection Act 1998. London: The Stationery Office.

[11] TSA. Code of Practice 2009. Wilmslow: Telecare Services Association.

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™