BS 5979:2007

Incorporating
Corrigendum No. 1

BRITISH STANDARD

Remote centres receiving signals from fire and security systems – Code of practice

ICS 13.320

Publishing and copyright information

ISBN 978 0 580 60936 7

The following BSI references relate to the work on this standard:
Committee reference GW/1/11
Draft for comment 06/30133574 DC

Publication history

First published January 1981
Second edition, June 1987
Third edition, December 1993
Fourth edition, December 2000
Fifth (present) edition, September 2007

Amendments issued since publication

Amd. no.	Date	Text affected
Corrigendum No. 1	31 December 2007	Corrections to **5.1.7.2**, **5.1.8.3**, **5.2.1.2**, **5.2.1.3** and **8.3**

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 35 and a back cover.

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 28 September 2007. 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.

The start and finish of textual changes introduced by Corrigendum No. 1 are indicated in the text by tags [C1] ⟨C1⟩. Minor editorial changes are not tagged.

Supersession

This British Standard supersedes BS 5979:2000, which is withdrawn.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

a) references updated;

b) removal of layered security option.

NOTE An ARC that became operational prior to 30 June 2008, and which relied on layered security to achieve compliance with the year 2000 edition of this standard, can continue to use layered security, provided an equivalent standard of protection is achieved compared with the physical means set out in ***5.1.1.3.***

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 in 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.

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.

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 security systems, e.g. intruder, fire, social and closed circuit television (CCTV).

Annex A provides guidance for inspectorates, Annex B contains guidance on remote access to remote centre data systems, Annex C gives a recommended agreement for authorizing filtering.

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 405:1987, *Specification for uncoated expanded metal carbon steel sheets for general purposes*

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

BS 5051-1:1988, *Bullet resistant glazing – Part 1: Specification for glazing for interior use*

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

BS 5306-8:2000, *Fire extinguishing installations and equipment on premises – Part 8: Selection and installation of portable fire extinguishers – Code of practice*

BS 5628-2, *Code of practice for the use of masonry – Part 2: Structural use of reinforced and prestressed masonry*

BS 5839-1:2002, *Fire detection and alarm systems for buildings – Part 1: Code of practice for system design, installation and servicing*

BS 6132:1983, *Code of practice for safe operation of alkaline secondary cells and batteries*

BS 6133:1995, *Code of practice for safe operation of lead-acid stationary batteries*

BS 7858, *Code of practice for security screening of personnel employed in a security environment*

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

BS EN 179:1998, *Building hardware – Emergency exit devices operated by a lever handle or push pad – Requirements and test methods*

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

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

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

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

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 and the following apply.

3.1.1 activity monitor
equipment that automatically monitors the ARC staff for periods of inactivity and automatically creates an audible signal within the ARC in the event of failure to detect activity within a predefined period; if the signal is not acknowledged by the ARC staff within a short, predefined timescale, the equipment automatically raises an alert to a separate, manned location

NOTE The period of inactivity could be due to attack or catastrophe.

3.1.2 alarm company
organization that provides services for I&HAS

NOTE This definition is taken from BS EN 50131-1.

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

NOTE This definition is taken from BS EN 50131-1.

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

3.1.5 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

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

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

3.1.8 audibly confirmed
status in which an incident has been confirmed by a human being at a remote location (normally an ARC) and in which the human being, after having interpreted audio information transmitted from the protected premises, has made a decision that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred

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

3.1.10 confirmed
*NOTE See audibly confirmed (**3.1.8**), visually confirmed (**3.1.33**), or sequentially confirmed (**3.1.27**).*

3.1.11 control equipment
equipment necessary for the setting, unsetting and testing of an IAS and for sending an alarm condition to warning devices and/or signalling equipment

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

3.1.13 deliberately-operated device
a detector that creates an alarm condition as the result of deliberate action by one person

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

NOTE This definition is taken from BS EN 50131-1 as "intrusion detector".

3.1.15 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 option a) of NOTE 1].

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.

3.1.16 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 resistant" given to an element implies that this element fulfils the requirements of the relevant standard fire test.

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 non-combustible
not capable of undergoing combustion under specified test conditions

3.1.19 operations area
that part of an ARC concerned directly with the display of information from the alarm and/or CCTV systems served by the ARC and with the onward transmission of relevant aspects of this information to an emergency service

3.1.20 processor
device that processes the output from one or more sensors to determine whether an alarm condition should be generated

NOTE The processor can be integral with the control equipment.

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

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

3.1.23 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 (e.g. an ARC) or for onward transmission

3.1.24 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

3.1.25 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.

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

NOTE This definition is taken from BS EN 50131-1.

3.1.27 sequentially confirmed
status in which confirmation emanates from two or more independent sensors, detectors and/or processors, which are so configured that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred

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

3.1.29 signalled alarm condition
state of monitoring equipment at an ARC (or other remote location) that indicates that intrusion, attempted intrusion or unauthorized interference has occurred at the supervised premises, or is likely to occur

NOTE Once signalled at the remote location 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.

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

3.1.31 unset
status of an IAS or part thereof in which an alarm condition cannot be notified

NOTE This definition is taken from BS EN 50131-1.

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

3.1.33 visually confirmed
status in which confirmation is confirmed by a human being at a remote location (normally an ARC) and in which the human being, after having interpreted a visual image transmitted from the supervised premises, has made a decision that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred

3.2 Abbreviations

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

ARC	Alarm receiving centre.
IAS	Intruder alarm system.
CCTV	Closed circuit television.
RVRC	Remote video response centre.
I&HAS	Intruder and hold-up alarm system.

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 are 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 as follows.

a) *Category I*: remote centre handling signal from fire alarm systems and/or from social alarm systems, and/or from CCTV systems in non-security applications (e.g. traffic flow).

b) *Category II*: remote centre handling signals from IASs and/or from CCTV systems in security applications that require an emergency response (e.g. loss prevention) and/or from fire alarm systems and/or social alarm systems.

4.2 Site selection

4.2.1 Remote centres

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 around cables or pipes below ground level should be given consideration.

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

Preference should be given to locating an ARC in a basement or on an upper floor. Where the ARC is located on a ground floor, access by the general public to the shell of the ARC should be restricted, e.g. by a physical barrier.

The interior of the operations area or equipment room(s) should not be directly visible from outside the shell.

4.2.3 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.

4.3 Consultation

4.3.1 General

Appropriate consultation should be undertaken with other relevant interested parties, for example, planning authorities, utilities, 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 physical and 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 security and emergency procedures of the building housing the remote centre and the response requirements of the appropriate service(s) should be established and documented. This discussion should include consideration of escape routes and emergency exits.

There should be discussion and agreement with the appropriate emergency service(s) responsible for the areas covering the supervised premises. This discussion should include consideration of both primary and secondary means of communication with the emergency services.

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 of not less than 1 h.

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 a fire resistance of at least 1 h.

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

NOTE 2 Attention is drawn to Department of the Environment, Transport and the Regions, Building Regulations *2000 — Approved Document B Fire safety. [1] London: TSO, and to the LPC design guide for the fire protection of buildings [2].*

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, but 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 so located 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

All parts of the shell should be attack resistant.

Examples of acceptable construction are:

1) A solid wall, 215 mm thick, constructed from either brick or dense concrete blocks laid flat;

2) A solid wall, 190 mm thick, constructed from dense aggregate concrete reinforced hollow block, designed in accordance with BS 5628-2;

3) A wall, 190 mm thick, constructed from hollow concrete blocks that have been reinforced with, for example, steel bars or scaffolding tubes;

4) A wall, 150 mm thick, constructed from reinforced concrete cast *in situ.*

5) A wall, not exposed to vehicular attack, reinforced with low carbon steel sheets not less than 1.5 mm thick, of construction that would afford a fire resistance of at least 1 h in respect of integrity, insulation and, where relevant, load-bearing capacity, if tested in accordance with the tests specified in BS 476. Low carbon steel sheets should be welded together and supported by a suitably rigid substructure.

6) Where it is not practical to use these types of construction for floors or ceilings, the existing structure should be reinforced from above, if practicable, by, for example low carbon steel sheets not less than 1.5 mm thick or 100 mm concrete blocks screeded with concrete. Low carbon steel sheets should be welded together and secured by non-returnable screws.

An ARC that became operational prior to 30 June 2008, and which relied on layered security to achieve compliance with the year 2000 edition of this standard, can continue to use layered security, provided an equivalent standard of protection is achieved compared with the physical means set out in this clause.

5.1.2 Entrance and exits

5.1.2.1 Categories I and II

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, such as those in BS EN 179:1998.

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

All entry and exit doors should be of attack resistant construction such as 6 mm low carbon steel or 50 mm hardwood with 1.5 mm low carbon steel sheets securely attached to the outer surface. Hinges, frames, fixings and locking devices should be of substantial construction with a similar resistance to attack.

The normal entrance to an ARC should be via two doors separated by a lobby with the doors interlocked to prevent both being open at the same time. The doors and the lobby area should be for the exclusive use of the ARC. Entry to the lobby and ARC should be controlled from within the ARC by separate physical actions. Egress from the ARC should be controlled from within the ARC. Egress from the lobby may be controlled from within the ARC or the lobby. Where egress from the lobby is controlled from within the lobby a means of surveillance of any person in the vicinity outside the entrance door should be available inside the lobby.

More than one normal entrance to the ARC is permissible provided each entrance conforms and operating procedures exist which ensure that only one entrance is in use at any one time. All doors should open outwards from the ARC.

The entrance lobby floor area should normally not exceed 6 m^2 and should have a means for the surveillance of any person in the lobby area from within the ARC. However, where building constraints exist, the lobby may have a larger floor area provided that the surveillance facilities are such that no part of the lobby is out of the view of ARC staff.

Where a facility to open both entrance doors from the outside is provided to deal with an emergency within an ARC, this should be achieved by means of a high security locking system, the keys or combination code of which should be kept in a burglary resistant safe or vault to which access is restricted to a list of nominated persons. This safe or vault should be located in a secure area, separate from the ARC, and should be supervised by an alarm system conforming to PD 6662 signalling to the ARC when the safe or vault is open.

NOTE 1 This could be a secure manned centre operating a keyholding service.

Supervision of the area where the safe or vault is located should be by means of an alarm system conforming to PD 6662 and communicating to the ARC.

NOTE 2 In the case of a remote centre commissioned prior to 1 January 2006, existing alarm systems can be used.

5.1.3 Key transfer hatch

Where provided, a key transfer hatch should not exceed 20 000 mm^2 in cross-sectional area.

If constructed in the shell wall of the ARC, the outside of the key transfer hatch should be in a restricted access area. The inner and outer doors and frames of any key transfer hatch facility should be of substantial construction, such as 6 mm low carbon steel or equivalent. Hinges, fixings and locking devices should also be of substantial construction with a similar resistance to attack. The doors should be interlocked to prevent direct access being available at any time and their actions should be controlled from within the ARC. Barrel type systems can be used; otherwise the outer door should open outwards.

When constructed in the internal lobby wall a key transfer hatch can include only one door. This door should be interlocked with the outer door to the internal lobby to prevent both the outer lobby door and the key hatch doors being opened at the same time. Opening of the key transfer hatch door should be controlled from within the ARC. The door, frame, hinges and locking devices should be of the same substantial construction as if they were located in the shell wall.

Voice communication system(s) should be available between the operations area of the ARC and the outer entrance door, the lobby area and at the key transfer hatch.

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

Glazed areas in the shell of a Category II ARC should be kept to a minimum, with no individual area exceeding 1.5 m^2. Where provided, glazing in the shell should be non-openable.

Any glazed area in the shell together with its frame and fixings should have substantial resistance to physical attack and all glazing should have a resistance to firearms conforming to BS 5051-1:1988, class S86/G2. All glazing not in accordance with BS 5051-1:1988, class S86/G2 should be raised to this level by secondary glazing, e.g. by the addition of polycarbonate sheeting of an appropriate thickness.

5.1.5 Ventilation

5.1.5.1 Category I

Ventilation should be controllable from within the ARC.

5.1.5.2 Category II

Ventilation systems serving an ARC should be independent from those of the rest of the building (when the building in which the ARC is located is shared) and controlled from within the ARC. All vents should be protected with air-tight flaps which can readily be closed either manually from inside the ARC or automatically in the event of suspicion that gas or smoke is being drawn into the ARC.

Ventilation inlet or outlet openings in the shell exceeding 20 000 mm^2 should be supervised internally against attempts at entry by means of an appropriate detection device connected to the IAS of the ARC. In addition, such openings should be protected by one of the following:

a) an expanded steel mesh screen (see BS 405) with each opening in the mesh not larger than 150 mm^2. The screen should be welded to a substantial steel frame which should be securely bolted through to the shell of the ARC at intervals not exceeding 100 mm;

b) solid low carbon steel bars, of diameter not less than 19 mm, spaced not more than 125 mm apart between centres.

5.1.6 Services – Category II only

Service cables or pipes breaching the shell of an ARC should not exceed 20 000 mm^2 in cross-sectional area.

The clearance around a cable or pipe should not exceed 1.5 mm. Where clearance around a cable or pipe exceeds 1.5 mm, it should be filled with material of equivalent specification to that of the shell.

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

Surveillance facilities should be provided so that approaches to the building in which the ARC is located can be monitored. Adequate lighting should be provided for the type of surveillance used. All surveillance equipment should be ⟦C1⟩ protected ⟨C1⟧ against adverse weather conditions and other environmental hazards.

Facilities should be provided to enable ARC staff to identify visitors before permitting them to enter the entrance lobby and to view any activity therein (see **5.1.2.3**). Surveillance facilities should be provided to enable ARC staff to identify personnel using any key transfer hatch.

It should be possible for ARC staff to view the outside of the ARC, the emergency exit(s) and any adjacent communications junctions or cabinets, particularly where these are accessible to the public.

NOTE The use of switching and split screen facilities for the ARC CCTV system is acceptable.

5.1.8 Alarm systems

5.1.8.1 Category I

An ARC IAS should be installed which should include a deliberately-operated device. In single-manning situations (see **6.3.1.2**), an activity monitor should be provided.

5.1.8.2 Category II

An ARC I&HAS should meet the requirements of PD 6662 (at least Grade 3) and the means of notification should meet the requirements of one of the notification options for a Grade 4 I&HAS.

NOTE Systems installed prior to 2006 might still be marked as BS 4737 or BS 7042, which were appropriate standards until 2005.

An ARC IAS should be installed and should incorporate detectors that respond to forcible attack upon the shell, doors, appropriate ventilation openings and key transfer hatches. The IAS should include deliberately-operated devices installed at the normal operating positions, key transfer hatches, entrance(s) and emergency exit(s). An alarm condition should be signalled whenever any of the following conditions are met:

a) both entry doors are open at the same time; or

b) an emergency exit is open; or

c) if entry has been initiated by an emergency procedure.

The alarm condition should be notified to another ARC meeting the requirements of Category II of this standard.

Any alarm condition other than that given from a deliberately-operated device should create an indication in the ARC and should be signalled automatically if not acknowledged by the ARC staff within 60 s. Alarm conditions originating from deliberately-operated devices should be signalled without delay.

If delayed signalling is required to enable verification, this should apply only to those alarm conditions created by automatic detectors in areas subject to surveillance.

An ARC should have detection systems for carbon monoxide and smoke, which will give warning to the ARC staff prior to the levels reaching a concentration necessitating evacuation.

5.1.8.3 Both categories

The whole of the building housing an ARC should be protected by an automatic fire detection system in accordance with Category P1/M of BS 5839-1:2002 or by an automatic sprinkler system (see NOTE 1). In the event of the automatic fire detection or sprinkler system operating, an alarm signal should be transmitted to another ARC meeting the requirements of this standard or to the fire and rescue service. 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 1 In the case of a remote centre commissioned prior to 15 July 2003 (when BS 5839-1:1988 was withdrawn), automatic fire detection systems to BS 5839-1:1988 (withdrawn) were used. Existing detection systems do not need to be upgraded.

NOTE 2 In the case of a remote centre commissioned prior to 1 January 1994, if the remote centre is located in a multiple occupancy building and agreement cannot be obtained for the installation of automatic fire detection in areas of the building outside the control of the remote centre operator, the fire resistance of the shell and supporting structure should be capable of protecting against fire spread and building collapse for a prolonged duration, taking into account the likely fire load in the other areas of the building.

NOTE 3 Where an ARC is located in a semi-detached or terraced unit within a property, each semi-detached or terraced unit can be regarded as a separate building if there is full fire separation between units. Typically, full fire separation is not achieved unless the party wall extends above the roof, though the criteria vary according to the roofing materials used.

5.1.9 Communications

5.1.9.1 General

All communication cables between the point of entry into the building and the shell should be protected against physical and fire damage. Means of protecting cables from fire are as follows:

a) routed through areas of low fire risk; or

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

c) cables of standard or enhanced fire resistance (see BS 5839-1:2002, **26**).

NOTE BS 5839-1 contains recommendations for protection of circuits that are required to maintain their integrity during a fire.

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.

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.

5.1.9.2 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.

In addition, for a Category II ARC, a radio communication facility 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.

5.1.9.3 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.

5.1.9.4 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 origin, and for the automatic recording of all voice and data communications in and out of the ARC.

5.1.10 Power supplies

5.1.10.1 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.

5.1.10.2 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 (**5.1.10.3)**; or

b) a standby generator or generators supported by a standby battery and associated charging equipment (**5.1.10.4)**.

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

5.1.10.3 Standby batteries

The standby batteries should be brought into use automatically immediately 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 or BS 6133 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.

5.1.10.4 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 of at least 1 h 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.

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

5.1.11 Safety equipment

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

At least two 183B fire extinguishers, as defined by BS EN 3-7:2004, 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.

5.1.12 Staff facilities

Toilet and washing facilities should be provided within the ARC. Facilities for the preparation of food and drink should be provided, and should be located within the ARC. Where a cooking appliance is provided, it should be separated from the operations area by a construction with a fire resistance of not less than 30 min.

NOTE readers are reminded of the Workplace (Health and Safety and Welfare) Regulations [3].

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 the recommendations for either class A or class B protection as specified in **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 a dedicated transmission path. If the satellite is capable of being manned, the alarm system should include deliberately-operated 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 a dedicated transmission path.

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 deliberately-operated 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 deliberately-operated 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:

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 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 type P1 of BS 5839-1:2002 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 one 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. The choice between these alternatives should be related to the number of alarm system connections as follows:

a) for less than 16 alarm systems connected, a dedicated alarm transmission path only;

b) for 16 to 64 alarm systems connected, a dedicated alarm transmission path and either an alternative communication means or provision for manning;

c) for more than 64 alarm systems connected, a dedicated alarm transmission path and both an alternative communication means and provision for manning.

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 **5.1.10**.

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 stated a minimum period of training appropriate 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

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.

For Category II ARCs, 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. All entry/exit movements for a Category II ARC, including movements of authorized staff, should be logged.

Where provided, remote access to ARC computer systems and data of both Category I and Category II ARCs 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 B.

6.3 Operating procedures

6.3.1 All alarm and CCTV systems

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

Except for those ARCs handling signals only from social alarm systems, 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 work station at all times.

Staffing levels should be related to maintenance of the response times given in **6.4** to **6.7**.

Staff in reserve should report for duty within 30 min in an emergency for single manned ARCs and 1 h for others.

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 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 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 management and the emergency service. The client should be given details of the method of communication with emergency service(s) and the name(s) of the relevant service(s) for their protected premises.

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**).

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 is undertaken at periods not exceeding six months.

6.3.1.7 Counter duress

To help identify duress risks against operators of Category II ARCs or their families, there should be a manually initiated exchange of agreed messages between ARCs at hourly intervals. Where these messages are exchanged by verbal contact, there should be either:

a) a system of code words or numbers and a separate duress code word; or

b) a simple audible signal at hourly intervals which will automatically send out an alarm if it is not acknowledged within 1 min or if the ARC staff carry out an agreed duress procedure.

6.3.1.8 Confidentiality

When monitoring IASs and when considered appropriate to other types of systems, e.g. CCTV, procedures should be established to authenticate the exchange of confidential information between the ARC and the customer. Details 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, names and addresses of users.

6.3.1.9 Information provided to emergency services

The ARC should have 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.

6.4 Intruder and hold-up alarm systems

6.4.1 Handling of alarms

6.4.1.1 General

For intruder and hold-up alarm systems (I&HAS) designed to generate confirmed alarm conditions, see DD 243.

6.4.1.2 Performance criteria

*COMMENTARY ON **[6.4.1.2]** refer also to Annex C, Form of agreement for authorizing alarm receiving centre to exercise discretion regarding the filtering out of alarm information.*

Unless otherwise agreed in writing with the client, action should be taken to establish communications with the control room of an appropriate emergency service, or to commence a filtering procedure, within the following times of receipt of the alarm signal at the ARC:

a) for hold-up alarm conditions: 30 s for 80% of signals received and 60 s for 98.5% of signals received;

b) all other alarm conditions: 90 s for 80% of signals received and 180 s for 98.5% of signals received.

Alarm signals/conditions to which alarm filtering is required to be applied should be subject to an intentional delay of not more than 120 s (120 s being the maximum alarm filtering delay) before being extended to the police, as an opportunity for the alarm to be designated as a false alert and therefore cancelled as part of the alarm filtering routine.

Alarm filtering can commence at any time within the times given in b). The maximum overall alarm handling times are therefore 210 s for 80% of signals received and 300 s for 98.5% of signals received. In the remaining 1.5% of cases it is permissible for the maximum overall alarm handling times to be longer than 300 s, though obviously the times should always be kept to a minimum.

In adverse and unforeseen circumstances (for example, severe weather conditions or extended power failures) affecting alarm monitoring at an ARC, the processing of alarms by the ARC might very occasionally become delayed. It is permissible under these circumstances for alarms to be held in the alarm filtering delay for longer than 120 s and for the alarm to be cancelled if a mis-operation signal or an unset signal is received during the extended alarm filtering delay, provided such extensions to alarm filtering delays are kept to a minimum. There should be an indication at the ARC, available to the ARC supervisor, of the number of alarms held in the filtering delay so as to facilitate best use of operators and the contacting of staff in reserve (see **8.2** (i)).

6.4.1.3 Authorization of cancellation of intruder alarms

Cancellation of a remotely-notified intruder alarm condition should be individually authorized by the customer, case-by-case in accordance with a defined alarm filtering routine, whereby the user or the IAS communicates with the ARC (using suitable code words or numbers) affirming that the IAS has mis-operated and that the alarm is to be filtered out.

NOTE 1 Communication whereby the user or the IAS causes a mis-operation signal to be sent to the ARC, affirming that the IAS system has mis-operated and therefore that the signalled alarm condition is to be filtered out, is an example of cancellation individually authorized by the customer.

NOTE 2 Communication whereby the user or the IAS causes an unset signal to be sent to the ARC, affirming that the IAS has been unset and therefore that the signalled alarm condition is to be filtered out, is an example of cancellation individually authorized by the customer.

NOTE 3 This does not preclude the customer giving general or specific standing authority, by prior written agreement, that the alarm company's ARC can designate some alarm signals as void (i.e. cancelled).

6.4.1.4 Authorization of cancellation of hold-up alarms

The customer can give general or specific standing authority, by prior written agreement, that the alarm company's ARC can apply filtering techniques to hold-up alarm signals from specific premises.

6.4.1.5 Method of alarm filtering

If, prior to the police being informed, the ARC receives a signal that is identifiable to the ARC as being a mis-operation signal or a signal that is identifiable to the ARC as indicating that the alarm system is unset, then the ARC can (and normally in the absence of any contrary indications should) designate the alarm condition as being a false alert, and regard the alarm condition as cancelled, without extending any alarm message to the police.

NOTE 1 It is a matter between the parties whether or not users are to be called in the event of a false alarm.

*NOTE 2 During alarm filtering it is permissible for the ARC to attempt to contact the user at the supervised premises and/or other users by telephone and/or to receive incoming telephone calls from the users with a view to obtaining duly authenticated authorization (using suitable code words or numbers) by live voice for the alarm condition to be designated as a false alert and therefore cancelled without any alarm message being extended to the police. Such practices are to be regarded as optional (i.e. additional to the method described here in **6.4.1.5** and/or for contractual agreement.)*

6.4.1.6 Informing the police

When the police are to be informed, the ARC should observe the protocols given below.

The ARC should make only one successful call to the police (relating to an alarm signal or series of alarm signals received from particular protected premises), except where there is good reason for making more than one call.

Examples of exceptions are given as follows.

a) If an alarm has been reported to the police, but subsequent information enables the ARC to designate the alarm as being cancelled (and cancellation has been authorized by the customer in accordance with **6.4.2**, **6.4.1.4**), then a second call to the police should be made informing them that the alarm is now cancelled, and that police attendance is therefore not now required.

b) If initial attempts to contact users fail, then a second (or subsequent) call to the police should be made, informing them of this.

In all cases where a second (or subsequent) call is made to the police, the ARC should state clearly to the police that further information is being given regarding an alarm that has previously been reported, and should quote the police incident reference.

6.4.2 Transmission fault handling

*NOTE 1 The following recommendations apply in addition to the recommendations listed in **6.3.1.10**.*

Unless otherwise agreed with the client in writing, where a transmission fault, or interruption, is received from an alarm system which is in the unset condition, the ARC operator should endeavour to contact the user at the supervised premises and/or another user to establish the likely cause. The emergency service should not be informed unless responses from these contacts give cause for concern.

Unless otherwise agreed with the client in writing, where a transmission fault, or interruption, is signalled from an automatic alarm system in the set condition, the emergency service should not be informed unless the fault is sustained for more than 60 s**.**

NOTE 2 These recommendations do not apply to deliberately-operated alarm systems installed in accordance with BS 4737-2 and might not apply to other systems as agreed with the emergency service.

6.4.3 Monitoring of setting and unsetting

Where monitoring of the setting and unsetting of an alarm system, including CCTV with detection, is required, the latest times for setting and the earliest times for unsetting each day should be agreed in writing with the client and recorded. Where arrangements are made to permit variations to be notified, this should be done by an agreed confidential exchange (see **6.3.1.8**) and changes should be recorded. Unless otherwise agreed, all setting and unsetting times should be recorded for monitored systems. There should be an unambiguous presentation of setting and unsetting signals in the ARC. It should not be necessary for the operator to derive such signals by the interpretation of alarm or transmission fault signals.

6.4.3.1 Setting

Where an alarm system has not been set by the latest time agreed for this with the client, the ARC should endeavour to contact the user at the supervised premises and/or another user to establish the cause of this.

6.4.3.2 Unsetting

Where an alarm system is unset before the earliest time agreed for this with the client, the user/customer should be informed without delay.

Premature unsetting signals might be indicative of an alarm system management problem in which the emergency service should not be involved. Either the agreed unsetting time should be complied with by establishing improved control or it should be revised to accord with actual practice.

6.5 Fire alarm systems

6.5.1 General

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

Fire alarm signals should normally be passed without delay and without the application of filtering procedures.

Action should be taken by an operator to establish communications with the control room of an appropriate emergency service, or, if applicable (see **6.5.2**), to commence a filtering procedure, within 30 s for 90% of signals received.

NOTE Automatic transmission of alarm signals between the ARC and the emergency services 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 fire brigade exceeds 180 s.

6.5.2 Filtering

Filtering procedures should be implemented if required by the emergency fire service.

Where filtering procedures are considered essential, the following recommendations should be followed:

a) Filtering procedures should be applied to fire alarm systems on the written instruction of the alarm company (if different from the ARC operator) and the client/customer, confirming that consultation has taken place with the relevant emergency fire service.

b) When such procedures are implemented, they should be documented and readily accessible to ARC operators from within the ARC and should clearly record the agreed maximum filtering period.

6.6 Social alarm systems

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

6.7 CCTV system monitoring

6.7.1 Detector activated remotely monitored CCTV systems complying with BS 8418

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

NOTE Such systems are eligible for Police Unique Reference Numbers.

6.7.2 CCTV systems not complying with 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 http://www.acpo.police.uk

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.

6.8 System availability

6.8.1 Equipment checks

6.8.1.1 Daily checks

The following equipment should be checked for correct operation at least once every 24 h and the results recorded:

a) communication receivers;

b) timing, recording and logging equipment;

c) visual and audible displays of alarm signals;

d) all incoming and outgoing communications equipment.

6.8.1.2 Weekly checks

The following equipment should be checked for correct operation at least once every seven days and the results recorded:

a) standby power supplies and automatic change-over equipment;

NOTE Testing is to continue on normal load for a minimum period of 15 min, or the minimum running time recommended by the manufacturer if this is longer.

b) emergency lighting equipment including torches;

c) the ARC alarm systems.

6.8.2 Recovery from equipment failures

NOTE 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****.*

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.

7 Records

NOTE Attention is drawn to the Data Protection Act [4].

7.1 Client records

Client records for each security 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 3 years.

Client records should contain the following information:

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

b) names and telephone numbers of users;

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;

e) the types of signals to be monitored.

Records of all monitored events should be kept for not less than 3 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.

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 **6.7**). Performance figures should be calculated on a monthly basis as a minimum.

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 12 months.

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 12 months, and should be capable of being printed and/or displayed.

NOTE RVRC image and data retention times are referred to 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.

Records essential to the maintenance of services to clients should be duplicated and stored in fire-resistant cabinets or in secure areas either on or off site.

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.

NOTE Attention is drawn to the Data Protection Act [4].

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;

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 (see **6.8**);

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, for example, 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;

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 complying substantially with BS 5979 within a maximum of 28 days of the loss of monitoring.

Where satellites may 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.

Remote centres contracted to handle signals from IASs conforming to BS 7042:1988 should additionally have the ability to sustain monitoring at an alternative wholly independent remote centre which meets the recommendations for Category II, without interruption of service.

NOTE 1 Examples of suitable arrangements providing availability of back-up monitoring are:

a) signalling networks wherein monitoring is performed by more than one remote centre at all times or can be performed at an alternative site by automatic switching, with the routing of communication circuits independent of each remote centre;

b) connection of the protected premises to two independent remote centres by independently routed signalling circuits.

[C1] *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, for example fibre optic cables.* [C1]

8.4 Staff procedures associated with contingency plan

It should be the responsibility of the ARC manager to 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.

Annex A (informative) Notes for guidance of inspectorates

When interpreting the recommendations of this British Standard code of practice, an inspectorate should have regard for the following underlying objectives.

a) A remote centre should have the capability of reliably communicating alarm and other related information between supervised premises and the designated emergency service without unreasonable delay.

b) The reliability of the monitoring service should be ensured by the provision of an adequate number of competent personnel supported by the necessary domestic facilities.

c) The remote centre should be resistant to damage by foreseeable events, e.g. fire, flood, severe weather conditions and malicious damage, that might occur within the remote centre or in the surrounding area.

d) The monitoring service should be resilient to disruption by foreseeable events that might affect the remote centre or the transmission network.

e) Remote centres handling signals from IASs should be equipped with intruder detection and other appropriate surveillance systems. ARCs should be physically resistant to criminal attack to protect operational personnel for the period of time required to transmit a call for assistance.

The decisions reached by any independent inspectorate with regard to the issue of a certificate of compliance for its own purposes can form a basis for the recording and promulgation of established precedents, but these do not constitute a formal interpretation of the British Standard, which remains solely under the authority of the BSI committee responsible for BS 5979.

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

B.1 General

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

B.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 should be employed.

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

b) *Remote access level 2*: a different pass code 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 pass code of not less than eight characters. After 5 min of inactivity the client should be automatically logged off the system and connection to level 1 terminated. Reconnection should necessitate that the log-on procedure has to be carried out from the beginning. Client access by telephone to a remote centre is no different to a manual system (see **6.2** and **6.3.1.8**).

B.3 Access to the system

At the remote centre, the hardware and software responsible for processing the remote access should be 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 for receiving signals from remote access clients should be connected to a computer which is separate from the ones that are used to process alarm signals. To prevent unlawful access to the system, procedures should be set up by the remote centre to disconnect the client for at least 1 h following three unsuccessful attempts to gain access to the system.

B.4 Authorization for facilities

B.4.1 General

Access should only be permitted to data relating to each client's respective, specific contract with the remote centre.

B.4.2 View only

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

B.4.3 Edit

Access to the edit facility should only be available by means of a different log-on pass code to that of view only, and access should be terminated after 5 min of inactivity. It should not be possible to edit:

a) the response agreement;

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

c) the archive history;

d) suspension of service.

B.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 should only be brought on-line under the control of the remote centre.

B.4.5 Confirmation of changes made

Remote centre operators should 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 should be forwarded to the person/organization with whom the remote centre has a contract. This can be by paper or electronic means (e.g. e-mail).

B.5 Placing a system on test

The facilities for placing a system on test should not be 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. It should only be possible to place a system on test remotely if it is known that the system is unset.

Tests would normally be for the purposes of fault diagnosis, or routine maintenance. An engineer or client should enter both his/her own pass code and the site identification code in order to gain access to the system. Tests should be for no longer than 2 h.

The remote centre data should revert to its original status after 2 h. The client/engineer would be required to log on again if testing is to be continued.

B.6 Password management

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

Annex C (normative) Form of agreement for authorizing alarm receiving centre to exercise discretion regarding the filtering out of alarm information

C.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 (see **6.4.1.2**) unless there exists a prior written agreement between the alarm company and the customer, 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 that they should 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, for example: 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?

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

C.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.

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

BS 8418:2003, *Installation and remote monitoring of detector activated CCTV systems – Code of practice*

BS 8473, *Intruder and hold-up alarm systems – Management of false alarms – Code of practice*

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

BS EN 50132-7, *Alarm systems – CCTV surveillance systems for use in security applications — Part 7: Application guidelines*

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 EN ISO 11064-1, *Ergonomic design of control centres – Part 1: Principles for the design of control centres*

BS EN ISO 11064-2, *Ergonomic design of control centres – Part 2: Principles for the arrangement of control suites*

BS EN ISO 11064-3, *Ergonomic design of control centres – Part 3: Control room layout*

BS EN ISO 11064-4, *Ergonomic design of control centres – Part 4: Layout and dimensions of workstations*

BS EN ISO 11064-6, *Ergonomic design of control centres – Part 6: Environmental requirements for control centres*

BS EN ISO 11064-7, *Ergonomic design of control centres – Part 7: Principles for the evaluation of control centres*

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

Other documents

[1] GREAT BRITAIN Building Regulations 2000 — Approved Document B Fire safety. London: The Stationery Office.

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

[3] GREAT BRITAIN Workplace (Health and Safety and Welfare) Regulations 1992. London: The Stationery Office.

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

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@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

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

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111.
Fax: +44 (0)20 8996 7048. Email: info@bsi-global.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@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

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

Copyright

389 Chiswick High Road
London
W4 4AL