BS 8418:2015

BSI Standards Publication

Installation and remote monitoring of detector-activated CCTV systems – Code of practice

bsi.

...making excellence a habit.™

Publishing and copyright information

Published by BSI Standards Limited 2015

ISBN 978 0 580 84981 7

ICS 13.310; 33.160.40

The following BSI references relate to the work on this document:
Committee reference GW/1/10
Draft for comment 14/30293253 DC

Publication history

First published September 2003
Second edition, July 2010
Third (current) edition, January 2015

Amendments issued since publication

Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 42, 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 31 January 2015. It was prepared by Subcommittee GW/1/10, *Closed circuit television (CCTV)*, 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

The Technical Committee recognizes that suppliers of products and services within the scope of BS 8418 might require time to comply with the provisions of BS 8418:2015. For this reason, the provisions of BS 8418:2010 will remain effective for 6 months after the publication date of this British Standard.

This British Standard supersedes BS 8418:2010, which will be withdrawn on 31 July 2015.

Information about this document

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

- The need to carry out a threat assessment and risk analysis and produce an Operational Requirement document to reflect the requirements of BS IEC 62676-4 has been included.
- Clarified the use of portable/mobile systems within the standard.
- Relaxed some of the tamper recommendations and provided a tamper protection/indication table to add clarity to the requirements.
- Included a fault recognition/indication table to provide clarity to the recommendations.
- Decreased the number of event memory recommendations.
- The need for an Uninterruptable Power Supply (UPS) is now determined by threat analysis and risk assessment.
- Signalled the need for a minimum of one data transmission path. Further paths determined by threat analysis and risk assessment.

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

Introduction

Closed circuit television (CCTV) systems, also known as video surveillance systems (VSS), installed and monitored in accordance with this standard are capable of obtaining a response to a confirmed incident from the police (or other responding authority).

The key principles of this standard are to assist in ensuring that the integrity and effectiveness of an installed CCTV system are not compromised. The resilience and quality of the CCTV system need to be maintained at all times and in all environments in which the system is required to work.

When a detector senses an event, images are transmitted to, and displayed at, an RVRC and this is regarded as an activation. Prior to taking action, RVRC operators view these images for a period of time. Under normal circumstances an emergency response is only requested by the RVRC if there is positive evidence in these images of unauthorized access to the secure area and of actual criminal or other untoward activity, i.e. an incident.

1 Scope

This British Standard gives recommendations for the design, installation, commissioning, maintenance, operation and remote monitoring of detector-activated CCTV systems, whether "permanent" or temporary/portable.

This standard applies irrespective of the length of time the CCTV systems are installed and/or whether the equipment can be re-used on another site.

This standard is intended to provide recommendations to the following parties:

a) CCTV companies, on best practice for the design, installation, commissioning, maintenance and operation of detector-activated CCTV systems;

NOTE This includes the installation and maintenance engineers working for the CCTV company.

b) Remote video response centres (RVRCs) monitoring CCTV systems; and

c) customers regarding the management of CCTV systems.

2 Normative references

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

BS 5979:2007, *Remote centres receiving signals from fire and security systems – Code of practice*

BS 7671, *Requirements for electrical installations – IET wiring regulations – Seventeenth edition*

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

BS 7958:2009 [1)], *Closed-circuit television (CCTV) – Management and operation – Code of practice*

[1)] At the time of publication, BS 7958:2009 is under review.

BS 8243:2010+A1:2014, *Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice*

BS 8591:2014, *Remote centres receiving signals from alarm systems – Code of practice*

BS EN 62676-1-1, *Video surveillance systems for use in security applications – System requirement – Part 1-1: General*

BS IEC 62676-4:2014, *Video surveillance systems for use in security applications – Part 4: Application guidelines*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1.1 activation

operation of a CCTV system triggered by an event resulting in the transmission of images to an RVRC

3.1.2 activation delay procedure

procedure involving a delay between an event being detected and an activation occurring

3.1.3 alert

activation where there is not positive evidence in images of unauthorized access to the secure area or of actual criminal activity

3.1.4 alternative power source

power source capable of powering components of the CCTV system for a predetermined time when a prime power source is unavailable

3.1.5 as-fitted document

document in which details of the CCTV system actually installed are recorded

[BS 8243:2010+A1:2014, **3.1.6** (MODIFIED)]

3.1.6 control equipment

equipment for receiving, processing and initiating the onward transmission of data

3.1.7 CCTV company

organization which provides installation and/or maintenance services for CCTV systems

3.1.8 CCTV system

system consisting of camera equipment and/or other image-capture devices, detector(s), monitoring and associated equipment for transmission and controlling purposes

NOTE This might be used for the surveillance of a defined secure area.

3.1.9 closed site

supervised premises entirely surrounded by a securely constructed barrier when the CCTV system is in a set condition

NOTE This is to deter unauthorized access.

3.1.10 customer
person or organization utilizing the services of a CCTV company

3.1.11 data
information in the form of images, audio and other associated, linked or processed information including outputs from detectors

NOTE 1 For example faults, activations, system status.

NOTE 2 This might include specific information regarding an individual.

3.1.12 detector
device that detects an event

NOTE A camera can serve as a detector, e.g. through the process of Video Analytics (VA).

3.1.13 digital key
portable device used for setting and/or unsetting a remotely monitored CCTV system

NOTE Formerly known as Portable ACE or ACE.

3.1.14 digital key reader
fixed equipment that receives signals from a digital key to set and unset a CCTV system

3.1.15 dormant period
period of time in which further activations do not occur

3.1.16 event
activity within a secure area

3.1.17 fault
condition of one or more components or interconnections that prevents the CCTV system or part thereof from operating normally

3.1.18 functional camera
camera with the ability to offer a combination of pan and/or tilt and/or zoom facility

3.1.19 illumination
light that is visible to the camera

3.1.20 incident
activation where there is positive evidence in images of unauthorized access to the secure area or of actual criminal activity requiring intervention

3.1.21 initial activation
first activation that occurs after the CCTV system has been set, or after a previous incident or alert has been closed down during the set period

3.1.22 isolation
status of a detector in which an activation cannot occur, such status remaining until the detector is restored

3.1.23 omission
status of a detector in which an activation cannot occur, such status remaining until the CCTV system is returned to an unset state

3.1.24 open site
supervised premises not entirely surrounded by a securely constructed barrier when the CCTV system is set

3.1.25 operational requirement
key document for system designers, which clearly defines the functions of the CCTV system according to the customer expectations

*NOTE Refer to BS IEC 62676-4:2014, Clause **5** "Operational requirements specifications".*

[BS EN 62676-1-1:2014, **3.1.100** (MODIFIED)]

3.1.26 parked position
position to which a functional camera automatically returns after a preset time or earlier on command

3.1.27 power supply
device that stores, provides and modifies or isolates (electrical) power for a CCTV system or part thereof

3.1.28 prime power source
power source used to support components of a CCTV system under normal working conditions

3.1.29 receiver
equipment which can receive data from wireless and semi-wired detectors

3.1.30 remote video response centre (RVRC)
continually manned remote centre capable of receiving multiple concurrent CCTV images from remote locations for the purpose of interacting with supervised premises to provide security and related services

3.1.31 RVRC operator
person located at the RVRC who is specifically designated, trained and authorized to carry out monitoring of the CCTV system

3.1.32 secure area
area within the supervised premises in which unauthorized access or attempted unauthorized access is intended to be detected

3.1.33 semi-wired detector
wireless detector with a wired power supply

3.1.34 set
state in which a CCTV system, or part thereof, automatically generates an activation in response to an event

3.1.35 supervised premises
site address, agreed by contract, at which there is one or more secure areas

3.1.36 tamper
deliberate interference with a CCTV system or part thereof

3.1.37 uninterruptable power supply
electrical apparatus that provides emergency power to a load when the prime power source fails

3.1.38 unset
state in which a CCTV system, or part thereof, is prevented from generating an activation in response to an event

3.1.39 unwanted activation
avoidable alert

NOTE This can include activations caused by animals and/or vegetation.

3.1.40 user
authorized individual at a supervised premises using a CCTV system for its intended purpose

3.1.41 wireless detector
non-wired detector with an integral power supply

3.2 Abbreviations

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

ESP	emergency service provider
IR	infrared
OR	operational requirement
PIR	passive infrared
RVRC	remote video response centre
UPS	uninterruptible power supply
VSS	video surveillance system

4 CCTV system planning and design

4.1 Planning

4.1.1 Threat assessment and risk analysis

A threat assessment and risk analysis should be performed in accordance with BS IEC 62676-4:2014, **4.2.1**, prior to CCTV system design and to assist in understanding the purpose of the system.

4.1.2 Operational requirement (OR)

The CCTV company should ensure that an Operational Requirements document is generated in accordance with BS IEC 62676-4:2014, **5.2** and **5.3**, which clearly defines the needs, justifications and purpose of the CCTV system. The OR document should take account of the threats identified, and inform the design of the CCTV system as well as provide a mechanism for producing a technical specification and test procedures.

*NOTE The Operational Requirements could be included within the System Design Proposal. See **4.2**.*

4.1.3 Temporary and/or portable systems

Where temporary and/or portable systems are used, they should conform to all of the recommendations in this standard.

4.2 CCTV system design proposal

4.2.1 The CCTV company should agree a CCTV system design proposal, based on the OR, with the customer.

4.2.2 The CCTV system design proposal should include:

a) diagram(s) showing the:

1) position of all cameras, detectors and their planned fields of view;

NOTE 1 See Annex A for diagrams for positioning detectors.

2) extent of the secure area;

3) designated location of parked vehicles and other movable objects or materials that could compromise the effectiveness of the CCTV system;

NOTE 2 These might be identified during the site survey or initial discussions with the customer.

4) actual dimensions on drawings that are not drawn to scale.

b) type, location, mounting height and brief technical specification of cameras and lenses;

c) type, location, mounting height, direction, range and brief technical specification of detectors;

NOTE 3 This should include information regarding dormant periods after activation.

d) identity of functional camera presets which are associated with detectors and the identity of the detectors with which they are associated;

e) identity of fixed cameras associated with detectors and the identity of detectors;

f) type and locations of audio devices;

g) the data transmission path(s) used by the CCTV system, with details of the party(ies) responsible for their implementation and their continuing provision and maintenance;

h) artificial illumination required, with details of the party(ies) responsible for its implementation and maintenance;

i) location and brief technical specification of components such as controls, power supplies and storage devices; and

j) services for which the customer is responsible with details of the user responsibilities for correct operation of the CCTV system.

NOTE 4 See Annex B for the factors affecting design requirements when creating a CCTV system design proposal.

4.3 Detector selection, positioning and configuration

4.3.1 General

Except in cases where it would be inappropriate, the detection areas should fall within the field(s) of view of the CCTV camera(s) so that the causes of activations can be viewed (for diagrams regarding the positioning of detectors, see Annex A).

NOTE 1 Examples of cases where it would be considered inappropriate to have a camera covering a detection area are where a movement detector is installed inside public toilets with the associated camera(s) covering any possible entry/exit points, or where a movement detector is installed inside a private dwelling with any associated camera(s) covering any possible entry/exit points.

Where detectors include outputs for transmitting information about the status of the detector to the control equipment and/or RVRC, agreement should be made between the RVRC, the CCTV company and the customer regarding the expected response at the RVRC [see **8.1**h)].

NOTE 2 Examples of detector status could include health check or fault condition.

4.3.2 Detector selection

4.3.2.1 Detectors should be chosen to meet the OR of the CCTV system and minimize unwanted activations.

NOTE See Annex C for types of technology used in detection equipment. See Annex A for examples of movement detector positioning.

4.3.2.2 Where detector technology incorporates a dormant period after activation, measures should be put in place to prevent this from compromising the security of the CCTV system. This dormant period should be clearly referred to in the system design proposal [see **4.2.2**c)].

NOTE Such measures might include a procedure being put in place for an RVRC operator to continue viewing specified cameras until the dormant period is over.

4.3.2.3 Detectors should be selected that are capable of covering the detection range required for the purpose of the CCTV system.

4.3.3 Detector position

4.3.3.1 Detectors should be positioned so that events within the secure area result in activations. This might require the area to be divided into multiple detection zones.

NOTE It is important to consider the on-site related factors given in Annex B as these can influence the position and correct use of detectors.

4.3.3.2 Where a detector faces a boundary, it should be positioned so that movement outside the secure area is not detected (see Figure A.2 and Figure A.3).

NOTE It is advisable to position detector(s) facing away from the boundary or to use dual technology or a second device to limit unwanted alarms in cases where boundaries adjoin roads, playgrounds, public footpaths etc.

4.3.3.3 Detectors should be selected and positioned in such a way that when looking horizontally across an area in an east-west plane they are not adversely affected by the rising or setting of the sun. Where necessary, secondary detectors, covering the same area as the associated primary detectors should be oriented in a different position and paired with the primary detectors.

4.3.4 Detector configuration

4.3.4.1 When configuring detectors, manufacturer's recommendations should be followed to prevent their incorrect operation.

4.3.4.2 Multiple detectors that cover different areas should not be connected to a single input unless individually identified by the RVRC, e.g. detectors identified by individual internet protocol (IP) addresses.

NOTE This is particularly relevant when a functional camera is directed to multiple preset locations dependent on the detector or an area where an event is taking place. In these circumstances it is important that the detector indicates independently at the RVRC, otherwise there is no method of determining that two incidents might have occurred in short succession.

4.4 Camera positioning and configuration

NOTE Attention is drawn to the Data Protection Act [1], the Human Rights Act [2], the Protection of Freedoms Act [3] and the Surveillance Camera Code of Practice [4].

4.4.1 General

4.4.1.1 Cameras should be positioned so that the areas of coverage of detectors can be viewed (see **4.3.1**).

4.4.1.2 When displayed on the screen, the size of a person should conform to BS IEC 62676-4:2014, **6.7** in relation to the intended task (i.e. identification, recognition, observation or detection), the minimum requirement being detection.

4.4.1.3 The entry/exit route to the secure area should either be viewed by a fixed camera or a functional camera in its parked position.

4.4.1.4 Where functional cameras are the sole means of viewing the field of detection, they should be treated as multi-position fixed cameras through

defined presets, rather than treated as infinitely variable devices. The area to be viewed by each camera in its defined preset positions should be clearly identified. Any camera views, or items within camera views, specified by the customer as needing to be carefully monitored should be checked to make sure that their requirement is met. If a camera is required to survey a large area, the area should be divided into a series of discrete adjacent zones, each corresponding to a stored defined preset position. It should not be possible for an intruder travelling at 2 m/s to pass out of the field of detection before the camera can be moved to view the area.

*NOTE It is important to check that at each of its defined preset positions the zoom setting still conforms to (**4.4.1.2**).*

4.4.1.5 Where functional cameras using preset positions in association with detectors are deployed, access to alter such preset positions should be restricted to the CCTV company and/or the RVRC. Adjustable preset positions may be utilized but only where there are no associated detectors.

4.4.1.6 Wherever possible, cameras should not overlook public areas.

NOTE For areas not intended to be the subject of surveillance; privacy masking may be used to prevent inadvertent viewing.

4.4.1.7 Installed control equipment should be able to withstand prevailing environmental conditions.

NOTE Further information on environmental test methods can be found in BS EN 50130-5.

4.4.1.8 Cameras should be uniquely identified using a name/label which is displayed with or within the camera view at the RVRC and which corresponds to the name/label shown on the supervised premises plan [see **6.1**c) and **9.1.2**] for the relevant camera view.

4.4.1.9 The rising and setting of the sun should be taken into account when positioning cameras across an area in an east-west plane so that their performance is not adversely affected.

NOTE It is advisable, in instances where there might be adverse effects, to pair secondary cameras and detectors with primary cameras and detectors.

4.4.1.10 The secondary cameras and detectors should be oriented in a different plane to that of the primary cameras and detectors.

4.4.2 Illumination

4.4.2.1 Intended fields of view of the cameras throughout the supervised premises should be illuminated (see **4.2.2,** h) and Annex D. When natural illumination is inadequate for CCTV images to be used for the intended purpose at the RVRC (see **4.4.1.2**), artificial illumination should be provided.

4.4.2.2 As a minimum, CCTV system detection areas should be illuminated to allow the RVRC to identify the cause of the activation (see **10.5**).

4.4.2.3 Camera fields of view should be illuminated so that it is possible for an RVRC operator to verify the presence or absence of a human form (see **4.4.1.2**) upon display of an image at the RVRC.

NOTE This applies to all displayed images, including pre-alarm.

4.4.2.4 Artificial illumination that is provided should be maintained in accordance with the manufacturer's recommendations.

4.4.2.5 Known artificial illumination faults should be rectified as soon as practicable and in accordance with the documented agreement in **8.3**.

NOTE 1 Until the fault is rectified and accepted as such by the RVRC, the secure area affected by the failure of artificial illumination might not be capable of being monitored by the RVRC.

*NOTE 2 It might be desirable to have an agreement (see **8.3**) between the RVRC, CCTV company and/or customer as to the checks to be made to ensure the correct operation of the artificial illumination.*

NOTE 3 It is advisable to implement a process for reporting artificial illumination failure back to the RVRC.

4.4.2.6 Wherever possible, artificial illumination sources should not be positioned to directly face cameras as this might impede the clarity of CCTV images.

4.4.2.7 Illumination should be positioned so as to minimize potential problems with image degradation.

NOTE Illumination that surrounds and/or is close to the camera lens, might lead to image degradation for example, due to insect infestations and unwanted reflections.

4.4.2.8 If clocks are used to control the artificial illumination, they should be adjusted in accordance with the British summer time (BST) time change. These adjustments should be the responsibility of the RVRC, the customer or the CCTV company, as agreed contractually [see **8.1**c)].

NOTE It is desirable for the RVRC to be able to control artificial illumination within the secure area.

4.5 Audio challenge

Installed audio challenge facilities should be clearly audible, without undue distortion, and within the area of coverage of the relevant detectors as indicated in the system design proposal. Audio challenges during the set state should be initiated by the RVRC only.

NOTE 1 Audio challenges may consist of pre-recorded or live voice operation.

NOTE 2 Attention is drawn to Clean Neighbourhoods and Environment Act 2005 [5], the ACPO Policy on Police Response to Security Systems [6] and the Police Scotland Security Systems Guidance [7].

4.6 CCTV system performance and integrity

4.6.1 Activation performance

Except where activation delay procedures exist (see **9.2**), an activation(s) should be set up to initiate within 1 s of an event being detected.

4.6.2 Data transmission system

The data transmission system should be capable of sending continuous live video until the RVRC operator terminates the connection.

Compression required for transmission should not compromise the image presented to the RVRC operator (see **4.4.1.2**).

4.6.3 Detector omission

4.6.3.1 Detectors should only be omitted temporarily. The minimum frequency (number/time) of activations occurring before a detector is omitted should be agreed in writing between the customer, the CCTV company and the RVRC [see **8.1**f)]. Omitted detectors should be restored automatically when a CCTV system is returned to an unset state.

NOTE Detector omission might, for example, be the consequence of a high number of unwanted activations.

4.6.3.2 Detector omission should be authorized or rejected in accordance with **9.4**. Wherever practicable, technology should be implemented to automatically calculate the frequency of excessive activations and notify the RVRC operator.

4.6.3.3 Detector omission should be recorded in a log maintained at the supervised premises [see **4.6.10**h)] and/or RVRC [see **10.3**f)]. As a minimum this log should detail the time and date that the detector is omitted, whether this is automated or manual, the name or ID of the user/RVRC operator and, either the time and date when it is restored, or the duration of the omission.

4.6.3.4 The procedure for detector omission should not involve fully unsetting the CCTV system or blocking the connection to the RVRC.

4.6.4 Detector isolation

4.6.4.1 Detectors should be isolated according to the written agreement between the customer, the CCTV company and the RVRC [see **8.1**f)] to take account of special circumstances in which prolonged periods of activity within the detector's coverage area render it necessary, or where detector omission(s) has failed to resolve an excessive number of unwanted activations.

NOTE Special circumstances can be, for example, periods of time in which builders are known to be accessing a part of the supervised premises or occasions when a vehicle or goods within the detector's coverage area would cause unwanted activations.

4.6.4.2 Isolated detectors should only be restored following agreement between the customer, the CCTV company and the RVRC [see **8.1**f)].

4.6.4.3 Detector isolation should be logged at the RVRC [see **10.3**g)] and/or in the event log at the supervised premises. As a minimum logging should include the time and date that the detector is isolated, the name or ID of the person who isolated it and, either the time and date when it is restored, or the duration of the isolation.

4.6.4.4 The procedure for detector isolation should not include fully unsetting the CCTV system or blocking the connection to the RVRC.

4.6.5 Video integrity

Camera signals between the camera and control equipment should be monitored for video loss in accordance with Table 2. If the video loss does not automatically restore within 30 s, it should be recorded in the event log at the premises. The system should ensure that video loss is clearly indicated locally (where a monitor is fitted) by an example of "no picture" or "video loss" message.

NOTE 1 It is advisable to implement procedures and/or technologies to detect camera masking in high-security applications.

NOTE 2 In some applications a video content detection system is necessary to determine whether an expected level of information exists within the image. This protects against deliberate masking of the camera(s) field(s) of view, failure of the lens, or inappropriate or inadequate illumination.

4.6.6 Tamper security

4.6.6.1 Means should be provided to detect and indicate the tamper conditions specified in Table 1.

4.6.6.2 Tamper indications should be audible and/or visual. Local indication at the supervised premises should be indicated to the person setting the system.

4.6.6.3 The setting/unsetting device should be provided with tamper detection in accordance with Table 1. If the device is opened, it should not be possible to affect the correct functioning nor change the state of the CCTV system.

NOTE Examples of setting/unsetting devices include keypads and digital key readers.

Table 1 **Tamper detection and indication**

Tamper detection of interconnections, components, enclosures, equipment	**Indication**		
	Local	**RVRC (remote)**	
		System set	**System unset**
Interconnections to detectors	M [D]	M	Op
Detector enclosures – when opened by normal means, removal from mounting, orientation adjustment and where used, masking	M [D]	M	Op
Pluggable connectors [A]	M [D]	M	Op
Power supply housings – when opened by normal means	M [D]	M	Op
Camera housing(s) and associated power supply [B] – when opened by normal means, removal from mounting, orientation adjustment	M [D]	M	Op
Control equipment – when opened by normal means [A]	M [D]	M	Op
Setting/unsetting device(s) – when opened by normal means	M[C, D]	M	Op

NOTE Local indication means at the supervised premises and is, as a minimum, indicated to the person setting the system.

Key: M = mandatory, Op = Optional

A) Not mandatory if located within a secure area with restricted access (see 4.6.9.1).
B) It is accepted that some camera housings and associated power supplies might not include all forms of tamper detection might not be supplied.
C) Not mandatory for portable set/unset devices.
D) Local indication is not mandatory if indication is given at the RVRC in the Unset state.

4.6.7 Fault detection

4.6.7.1 Means should be provided to recognize and indicate the fault conditions specified in Table 2.

4.6.7.2 Fault indications can be audible and/or visual.

4.6.7.3 Except where setting and unsetting is carried out by the RVRC, means of local fault indication at the supervised premises should be indicated to the person setting and unsetting the system.

Table 2 **Fault recognition and indication**

Fault to be recognized	Clause	Indication		
		Local	RVRC (remote)	
			System set	System unset
Camera video loss – in excess of 30 s	**4.6.5**	Op[F]	M	Op
Low battery – wireless detectors	**4.6.14.5.3**	M[A]	M[B]	Op
Loss of communication and low battery – Wireless digital key reader or wireless keypad	**7.1.2**	M[D]	M[E]	Op
Loss of communication – Wireless and semi-wired detectors	**4.6.8**a) and b)	M[A]	M[B]	Op
Control equipment	**4.6.9.6** & **4.6.13.2**	M [C]	M	Op
Transmission path(s)	**4.6.11.3** & **4.6.12**	Op	M	M
Uninterruptable power supply (UPS)	**4.6.14.4.6**	M [C]	M	Op
Control and transmission equipment power supplies	**4.6.14.3.4** & **4.6.14.6.4**	M [C]	M	Op
Detector power supplies	**4.6.14.3.4** & **4.6.14.4.5**	M	M	Op

NOTE Local indication means at the supervised premises.

Key: M = Mandatory, Op = Optional

A) Individual detector indication is required.
B) Individual detector indication is not required.
C) Local indication is not mandatory if indication is given at the RVRC in the Unset state.
D) Individual keypad indication is required
E) Individual keypad indication at the RVRC is not required
F) Mandatory if monitor is fitted.

4.6.8 Wireless and semi-wired detectors

Where wireless or semi-wired detectors are used, the following functions should be provided.

a) Faults at the detector should be reported in accordance with Table 2.

b) The loss of communication between the control equipment and any detector should be notified within a period not exceeding 20 min, in accordance with Table 2.

c) Every detector should be uniquely identified to the CCTV system.

4.6.9 Control equipment integrity

4.6.9.1 The control equipment should be located within the supervised premises such that access to the control equipment is restricted.

NOTE Such an area could be a security office or a store room where the area is only accessible by designated staff and/or users of the system. Equally it could be the supervised premises, which only employees have access to in working hours.

4.6.9.2 Where there is unrestricted access to the control equipment in the set condition, tamper detection should be provided in accordance with Table 1.

4.6.9.3 The control equipment should be protected using a secure validation process, e.g. a unique password, or electronic key, to prevent unauthorized access to the CCTV system.

4.6.9.4 The CCTV system should be configured so that its status (set or unset) can be determined at the RVRC.

4.6.9.5 The CCTV system should be configured so that authorized RVRC operators can remotely program the CCTV system parameters.

NOTE 1 It is essential that RVRC operators do not have access to reprogram a remote CCTV system unless they have been authorized to do so.

NOTE 2 It is desirable that the CCTV system is capable of remote diagnostics and remote correction.

4.6.9.6 If the control equipment fails, a fault signal should be indicated in accordance with Table 2.

4.6.9.7 The CCTV system should monitor the media used for communication between receiver(s) and control equipment, at least every 100 s to verify its continued availability to convey signals.

NOTE For example, this would be used to detect jamming.

4.6.10 Event log at the supervised premises

Event log(s) at the control equipment should be maintained at the supervised premises in a dated and timed retrievable format. The total capacity of the event log(s) should be at least 2 000 events. The log(s) should be protected against the accidental or deliberate deletion or alteration of the contents.

The event log should, as a minimum, include the following:

a) operation of detectors resulting in an incident or an alert, or initiating an entry sequence;

b) changes in CCTV system status, e.g. set, unset, part-set;

c) unsuccessful attempts to communicate with the RVRC;

d) successful communication with the RVRC and confirmation that an alarm condition has been reported;

e) CCTV system faults and warnings, for example restarts after mains power supply failure and video loss;

f) overriding of prevention of setting;

g) detector isolation not carried out by the RVRC; and

h) detector omission not carried out by the RVRC.

NOTE The events shown in the bulleted list above can be included in one or more logs at the supervised premises.

4.6.11 Data transmission to the RVRC

4.6.11.1 A minimum of one data transmission path should be provided as the method of communication between the CCTV system and the RVRC.

NOTE 1 Dependent on the risk of security breach to the supervised premises, an additional transmission path might be necessary.

NOTE 2 Standards covering data transmission include BS EN 62676-1-2, BS EN 62676-2-1, BS EN 62676-2-2 and BS EN 62676-2-3.

4.6.11.2 The transmission path should have the capability to transmit data to the RVRC.

4.6.11.3 Failure of the transmission path should be reported to or detected by the RVRC within three minutes and in accordance with Table 2.

NOTE It is advisable to use a transmission path dedicated to the CCTV system for added security and reliability of transmission.

4.6.12 Retry procedure

A retry procedure should be put in place in case the CCTV system fails to establish a connection with the RVRC. The CCTV system should attempt to connect to the RVRC a minimum of six times within ten minutes. If after ten minutes there is still no connection, an indication should be made in accordance with Table 2.

NOTE Communications receivers at an RVRC might be identified by the telephone number which routes to them or by an IP address, for example. This is dependent on the technology in use.

4.6.13 Authorization procedure

4.6.13.1 Prior to the transmission of data relating to the event , an authorization procedure should be performed after a connection is established between the CCTV system and the RVRC. The authorization procedure should confirm the identities at each end of the connection.

4.6.13.2 If the authorization procedure cannot be completed, the CCTV system should be configured to retry the authorization procedure. The authorization and retry procedure should take no more than ten minutes to complete. If after ten minutes there is still no authorization, a fault indication should be made in accordance with Table 2.

4.6.14 Power supplies

4.6.14.1 General

4.6.14.1.1 The power supply should be placed in the housing of one or more CCTV components or in a separate housing.

4.6.14.1.2 Power supplies should be monitored for prime power source, alternative power source, charger and output faults and identifiable to each power supply or through one common fault output identifiable to each power supply.

4.6.14.1.3 Power supply faults should be indicated locally at the supervised premises and/or at the RVRC in accordance with Table 2.

4.6.14.1.4 Wireless components (such as wireless detectors and keypads) should be supported by a prime power source (e.g. battery) that should be capable of operating continuously under all anticipated conditions of operation up to and including the next routine maintenance.

4.6.14.1.5 Power sources for wireless components should be replaced periodically, for example at routine maintenance visits.

4.6.14.1.6 Low battery voltage should be recognized and indicated in accordance with Table 2.

4.6.14.1.7 Where the need for a UPS is identified in the Operational Requirement, fault indications should be indicated in accordance with Table 2.

4.6.14.2 Alternative power source

4.6.14.2.1 There should be an alternative power source (or sources) for equipment listed in **4.6.14.2.4** and **4.6.14.2.5** in case the prime power source fails.

NOTE It is advisable to consider supporting equipment such as cameras and illumination with an alternative power source.

4.6.14.2.2 A change-over between the prime power source and the alternative power source and back again should not create an alarm condition or otherwise influence the status of the CCTV system.

NOTE An example of an alternative power source is a battery.

4.6.14.2.3 If a battery is used as the alternative power source, the date of installation should be recorded.

4.6.14.2.4 The alternative power source should have a capacity to support the CCTV control equipment and the devices used to transmit data to the RVRC for a minimum period of 30 min following failure of the prime power source.

4.6.14.2.5 Power supplies to detectors and semi-wired detectors should be fitted with an alternative power source capable of supplying power for a minimum of 4 h.

NOTE This excludes wireless components (such as wireless detectors and keypads) which have their own prime power source.

5 Installation

5.1 Wiring, cabling and connections

NOTE Attention is drawn to BS 7671 for the installation of wiring and connections and to BS 4737-3.30 for insulated and sheathed cables for interconnecting wiring.

5.1.1 Extra-low voltage cables and signalling cables should not be installed in ducting and/or trunking that is carrying low voltage mains cables, or parallel to low voltage mains cables, unless screened, insulated and/or segregated.

5.1.2 Wherever practicable, extra-low voltage cables should not be brought into CCTV equipment through the same entry point as low voltage mains cables.

5.1.3 Cables should be of a type and size appropriate to their application, taking into account equipment manufacturers' specifications, transmission rate, electrical interference and voltage drop.

5.1.4 Cables should be clearly labelled at termination points, interconnections and junction boxes to facilitate future maintenance and servicing.

NOTE Labelling may be tabulated in a cable schedule or included on a schematic diagram.

5.1.5 Fixed interconnection cables should be mechanically supported.

5.1.6 Interconnection cables likely to be subject to accidental damage and/or deliberate interference should be mechanically protected.

5.1.7 Fixtures for components of the CCTV system should be installed in accordance with the manufacturer's recommendations.

NOTE Examples of CCTV system components are control equipment, cameras, mountings, detectors and artificial illumination.

5.1.8 Components of the CCTV system should be able to withstand the conditions of the environment in which they operate (see **B.4** and **B.5**) and checked to fulfil their function within the CCTV system.

5.2 Detectors

Detectors should be installed and configured in accordance with the manufacturer's recommendations and in accordance with **4.3**.

NOTE If a detector is located in a position where it is likely to be subject to accidental damage, it might be appropriate to provide mechanical protection.

5.3 Camera equipment

The installation of camera equipment should be carried out in accordance with BS IEC 62676-4:2014, **4.7** and **15**.

6 Commissioning

6.1 Supervised premises documentation prior to commissioning of a CCTV system

The CCTV company should provide the following information to the RVRC at least 24 h before the CCTV system is commissioned:

a) supervised premises address;

b) CCTV company details;

c) supervised premises plan (see **9.1.2**);

d) operational schedule (set/unset times, etc.);

e) response plan (see **8.3**);

f) user contact details/ESP details;

g) associated intruder alarm system information [third party alarm receiving centre (ARC), supervised premises details, etc.];

h) inventory of CCTV equipment installed; and

i) fault reporting procedure (see **6.7**).

6.2 Checklist

A checklist including the criteria given in the checklist in Annex E should be undertaken and the results recorded. Aspects of the CCTV system that do not to conform to the checklist when checked should be modified accordingly and re-checked.

NOTE Though it is important to check the criteria given in Annex E, they can be presented in a different format to the example table.

6.3 Engineer walk test

6.3.1 This functional test should be undertaken at the supervised premises by the CCTV company in association with the RVRC and customer.

6.3.2 Basic tests should demonstrate the following with the CCTV system in the "set" condition.

a) The conformity of detection areas and fields of view of associated cameras to **4.3** and **4.4**.

b) The configuration of detectors conforms to **4.3.4**.

c) The image quality generated via available transmission paths is in accordance with **4.4.1.2** and **10.5**.

d) The accuracy of recorded data, notably labels used to describe the CCTV system (see **4.4.1.8** and **11.3**).

6.4 Reference images

6.4.1 Day and night reference images of the detection areas should be reviewed by the CCTV company to ensure that they meet the system design proposal.

6.4.2 For functional cameras, reference images relating to each of the preset positions should be reviewed by the CCTV company to ensure that they meet the system design proposal.

6.5 Night remote check

6.5.1 The CCTV system should be accessed remotely at night by an RVRC operator to check that the artificial illumination present allows clear images to be obtained of each intended view (see **4.4.2**).

6.5.2 The CCTV company and/or customer should be able to obtain these night images from the RVRC when necessary.

6.6 Environmental soak test

Following the engineer walk test (see **6.3**); the performance of the system should be evaluated by the RVRC and CCTV company for a period of not less than seven days to identify the trends in the protected environment, e.g. animal runs, shortcuts by pedestrians.

The cameras should be checked on configuration to ensure that they are correctly focused both during the day and at night.

At the end of the soak test period any performance issues should be recorded and resolved to the satisfaction of the customer, the CCTV company and the RVRC.

6.7 Faults

6.7.1 The RVRC should notify their contracted party of any CCTV system configuration faults.

6.7.2 The contracted party should arrange for configuration faults to be corrected.

6.7.3 Corrective actions should be carried out before the CCTV system is made live.

NOTE The contracted party might be the customer, CCTV company and/or another third party.

6.8 CCTV system acceptance certificate

On completion of commissioning, the RVRC should issue a CCTV system acceptance certificate to the contracted party for whom the RVRC is providing monitoring.

NOTE Prior to issuing the acceptance certificate, the RVRC might require the CCTV company to demonstrate aspects of the system's functionality or performance.

The certificate should confirm the date and time the CCTV system was accepted by the RVRC to their contracted party or their nominated representative.

6.9 Liaising with the customer upon completion of the installation and leaving the supervised premises

6.9.1 Operating instructions for the CCTV system and user access keys/codes should be given to the customer/user. A customer signature acknowledging receipt of these should be obtained.

6.9.2 The customer/user should be shown the extent of the detection areas. The customer/user should also be shown how to operate the CCTV system, including operating detectors and given other training necessary to operate the CCTV system.

6.9.3 As-fitted documentation should be completed and any documentation for the customer left at the supervised premises.

6.9.4 Methods and procedures for communication between the RVRC and the customer/user should be discussed and agreed.

6.9.5 Surplus materials from the CCTV system installation should be removed from the supervised premises. The supervised premises should be left in a tidy condition.

7 Setting/unsetting procedures of the CCTV system on the supervised premises

7.1 General

7.1.1 The CCTV system should be configured not to cause activations during the setting or unsetting procedures (see **7.2** to **7.5**) unless otherwise agreed in writing (for example, where the monitoring of people/traffic is a requirement of observation during an agreed operational practice). The CCTV system state (set/unset) should be clearly indicated and visible from the last place the CCTV system is set or from the entry point to the supervised premises.

7.1.2 The integrity of communication links between the control equipment and any wireless and/or semi-wired devices used for setting and/or unsetting should be notified within a period not exceeding 20 min. When communication cannot be verified a fault signal should be generated in accordance with Table 2.

7.1.3 If a building within the secure area might be occupied when the system is set then a set/unset indicator should be visible from inside the building.

NOTE It is advisable to consider providing an audible indication that the system is setting/unsetting to alert people at the supervised premises.

7.1.4 Setting of the CCTV system should be prevented when a fault condition exists. A user should be able to override the prevention of setting provided this is included in the event log at the supervised premises (see **4.6.10**).

7.1.5 If a detector is in an active state at the time of setting, an indication should be given at the place of setting and if applicable at the RVRC.

7.1.6 Setting and unsetting devices should have the following number of differs: logical (electronic) 10 000 and mechanical (key switch) 3 000.

7.2 Setting and unsetting outside secure areas at the supervised premises

The CCTV system setting and unsetting process, as completed from outside the secure area(s), should be in accordance with the following.

a) The place of setting and unsetting the CCTV system should be permanently within the field of view of a camera.

b) When a digital key is used to set the CCTV system, it should only be able to function from within the field of view of a camera.

c) The setting/unsetting range of the digital key should be a maximum of 10 m from the point of entry to the supervised premises.

7.3 Setting and unsetting inside secure areas

7.3.1 Unsetting

The CCTV system unsetting process from inside a secure area should be in accordance with the following.

a) The unsetting device (e.g. a keypad or digital key reader) should be situated inside a secure area.

b) During the unsetting procedure, the detectors covering the defined entry route (see **8.4**) should be configured to prevent activations from events occurring within the entry route unless otherwise agreed in writing. During the unsetting procedure, detection of events occurring outside the entry route (see **8.4**) should become activations.

c) The unsetting procedure should be carried out within an agreed period of time. If this is exceeded, the CCTV system should be configured to initiate an activation.

NOTE It is also advisable to define a particular time of day or night to carry out the unsetting procedure.

7.3.2 Setting

The CCTV system setting process from inside a secure area should be in accordance with the following.

a) The setting device (e.g. a keypad or digital key reader) should be situated inside a secure area.

b) During the setting procedure, the detectors covering the defined exit route (see **8.4**) should be configured to prevent an activation from being initiated for events occurring within it unless otherwise agreed in writing.

c) The setting procedure should be carried out within an agreed period of time and a timer should be implemented to monitor this.

d) The setting procedure should be completed either:

1) manually, by the user; or

2) automatically, as a result of the timer expiring.

NOTE It is important to complete setting manually, wherever practicable.

e) The CCTV company and/or customer should produce written procedures to be followed detailing the actions to be taken if the setting procedure is attempted when a detector is in an active state.

NOTE See Annex F for further guidance on the CCTV system setting procedure in the active state.

7.4 Automatically timed setting and unsetting

When the setting or unsetting of a CCTV system occurs automatically, these scheduled times should be for after staff leave the supervised premises and before staff are scheduled to arrive, respectively. This procedure should be clearly documented and agreed between the customer and the CCTV company and shared with the RVRC.

NOTE This inevitably means that the supervised premises are left unsecure for periods of time each day. It is advisable to modify the automatic settings for holiday periods such as bank holidays when staff might not be scheduled to be at the supervised premises.

7.5 RVRC initiated setting/unsetting

An RVRC should only set or unset the CCTV system or part of the CCTV system as the result of an authenticated request to the RVRC. RVRC initiated setting/unsetting should be logged.

8 Responsibilities and considerations

8.1 General

The CCTV company should create a documented agreement in consultation with the customer and the RVRC detailing responsibilities.

As a minimum this agreement should include:

a) maintaining the artificial illumination (**4.4.2.4**) and checking the correct operation of artificial illumination (**4.4.2.5**);

b) fault reporting (**8.3**);

c) adjustment of clocks in accordance with the BST time change where they are used to control artificial illumination (**4.4.2.8**);

d) responsibility for informing authorized persons at the supervised premises of the need to conduct themselves so that activations as a result of their presence are minimized and methods through which this can be achieved (**8.4**);

e) responsibility for investigating and eliminating the causes of a high number of unwanted activations, which have resulted in a detector being omitted or isolated, before it is re-enabled;

f) procedures for detector isolation (**4.6.4**) and detector omission (**4.6.3**);

g) expected response on notification of failure of the control equipment;

h) expected responses at the RVRC regarding detector status information (**4.3.1**);

i) maintenance of the CCTV system in accordance with the manufacturer's recommendations throughout the monitoring service (Clause **14**); and

f) the frequency with which the RVRC operator should compare stored reference images with current images (**14.1.2.6**).

8.2 Information regarding the supervised premises

8.2.1 The CCTV company should ensure that all the information required by **6.1** is provided to the RVRC before the CCTV system is commissioned.

8.2.2 The CCTV company should ensure that if the customer proposes changes after commissioning to the layout of the supervised premises, the location of materials or parked vehicles, or changes to site operational procedures, they should be discussed with the CCTV company and the RVRC.

8.2.3 Agreed changes to the CCTV system should be implemented and the affected parts of the system re-commissioned in accordance with Clause **6**.

8.3 Response plan

8.3.1 There should be a documented agreement in the form of a response plan, agreed between the RVRC, the CCTV company and the customer, detailing the action to be taken by the RVRC upon receipt of an activation, fault or a reported failure. The CCTV company should ensure that the customer receives a copy of the response plan. This response plan should form part of the supervised premises documentation (see **6.1**).

8.3.2 The response plan should include procedures for the RVRC operator to follow to determine whether an incident has occurred in cases where there is no identifiable cause for an activation. This part of the response plan should detail the areas to be viewed. It should also include whether images prior to the activation should be viewed from some or all of the zones.

NOTE 1 The actions are likely to depend upon whether the supervised premises are an open site or a closed site, and whether the activation occurs during the day or at night.

NOTE 2 The normal mode of operation for these CCTV systems is not to display images at an RVRC unless there has been an event at the secure area. However, if stated in the contractual terms and conditions between the customer, CCTV company and the RVRC, the RVRC operator might be permitted to view the secure area at other times. The customer might also be able to view the secure area remotely.

8.3.3 The response plan should include details of the actions in response to individual CCTV failures of the CCTV system such as failure of the artificial illumination, video loss, detector failure, control equipment restart failure, tamper indication and transmission path failure (see **8.1**).

NOTE This agreement might involve additional criteria, such as whether the customer or a user should be informed. Some failures of the CCTV system might require the RVRC operator to review images from the supervised premises. Where the customer has other contractual obligations, e.g. insurers, third-party occupiers, it is recommended that the customer makes these parties fully aware of the agreement.

8.4 Staff access

The CCTV company should ensure that:

a) the customer documents and implements a process to inform staff of ways to minimize unwanted activations when accessing the secure area [see **8.1**d)];

b) the customer specifies defined entry and exit routes into and out of the supervised premises. These should be communicated to staff and the RVRC;

c) staff are informed that when they plan to enter or exit the supervised premises by non-designated routes, the RVRC should be notified in advance.

9 RVRC operator procedures

9.1 General

9.1.1 The RVRC should ensure the supervised premises documentation (see **6.1**) provides a clear understanding of the layout of the supervised premises and the areas to be viewed when a detector initiates an activation.

9.1.2 RVRC operators should be able to describe accurately the nature of incidents as they occur. In order to achieve this, the supervised premises plan [see **6.1**c)] should show detailed information to include the detection and camera fields of view.

9.2 Activation delay procedures

9.2.1 The CCTV company and/or RVRC should agree activation delay procedures with the customer. The procedures should be documented, and the activation delays recorded.

NOTE A delayed activation procedure is where there is a delay between an event being detected and an activation occurring.

9.2.2 Where an activation occurs, the RVRC operator should have direct access to a minimum of one image from the initiation of the first event.

NOTE 1 Images in an on-going sequence are preferable.

NOTE 2 This refers to images of the initial entry and not only from the point at which the event was elevated to an activation.

NOTE 3 An example of the necessity for an RVRC operator to have access to images of initial entry is where there is a timed entry procedure. A period of time might elapse between a person passing through the area and the point at which the event escalates from an entry procedure to an activation, so the RVRC operator would need to view the actual entry.

9.3 Equipment faults

9.3.1 When CCTV system faults are discovered, these should be notified to the contracted party.

9.3.2 Failure of the artificial illumination or other illumination problems should be reported in accordance with the documented agreement in **8.1** by the RVRC operator within 24 h of their discovery.

9.4 Omitting detectors

The RVRC operator should authorize omissions (see **4.6.3.2**). Where the RVRC authorizes the omission of a detector, it should be carried out by the RVRC operator. The RVRC should inform the CCTV company of all omissions.

NOTE 1 By agreement, some customers might wish to be informed of omissions.

NOTE 2 Where omission has been carried out by the user, it is accepted the RVRC may not be aware of the omission and therefore will not be in a position to notify the CCTV company of its occurrence.

9.5 Construction and facilities

As a minimum, the construction and facilities of the RVRC should conform to BS 5979:2007, Category II or BS 8591:2014, Category II.

10 Management and operation of the RVRC

10.1 General

The RVRC should be managed and operated in accordance with BS 7958:2009, Annex A.

10.2 Lost monitoring

When monitoring is lost at the RVRC, CCTV systems should be monitored at another RVRC and/or at the supervised premises within 15 h.

10.3 Logging and recording

The RVRC should log or record the following:

a) date and time of activations;

b) transmitted images (see **10.5**);

c) transmitted audio;

d) inbound and outbound telephone calls regarding incidents and customer/user requests, with indexing to any telephone recordings, particularly in relation to customer and user;

NOTE Attention is drawn to the Data Protection Act [1].

e) reports of incidents and RVRC operator actions in response (see **11.1** and **11.5**);

f) detector omission (see **4.6.3.3** and **9.4**); and

g) detector isolation (see **4.6.4.3**).

10.4 RVRC support

RVRC support should include the following:

a) a sufficient number of RVRC operator terminals to meet the expected peak activation levels at any time, as assessed and judged by the RVRC;

b) a minimum of two operators in an RVRC at all times. These operators should be capable of carrying out all operational procedures. At least one operator should be present at their workstation at any time;

c) items of control equipment involved in the receipt, display or onward transmission of video or audio, including power supplies;

d) a standby facility or procedure that can be brought into use either automatically or manually by an RVRC operator within 1 h from the moment they become aware of a fault;

e) adequate replacement equipment for receiving, processing and displaying images that is common to more than one connected system;

f) arrangements for a trained engineer to attend an RVRC, when required, within 4 h of a fault being detected;

g) facilities to queue and prioritize activations when all operators are occupied; and

h) a sufficient number of incoming communication channels/paths and enough receiving equipment to cope with the maximum demand anticipated.

NOTE This is to prevent inadequate communication channel capacity at the RVRC so that it can receive activations from all supervised premises with at least one free channel/path at all times, even when the anticipated maximum numbers of activations are being queued. It is important for the RVRC to make a judgement regarding what is sufficient by assessing previous records and using expert RVRC knowledge.

10.5 Picture quality

The picture quality of transmitted images should be at least sufficient to enable an RVRC operator, with normal or corrected vision, to determine the nature and detail of a viewed event in accordance with **4.4.1.2**.

11 RVRC procedures and documentation

11.1 Non-image records and event logs at the RVRC

NOTE Attention is drawn to the Data Protection Act [1].

Non-image records and event logs at the RVRC should be maintained for a minimum of six months and should include the following:

a) the time of transmission from a supervised premises;

b) the time and date that an RVRC operator logs onto a workstation and the identity of the RVRC operator;

c) the RVRC operator actions that result from an incident reported from the supervised premises;

d) the time at which the RVRC operator closes down the session, in addition to any cause code recorded;

e) CCTV system faults received from remote sites;

f) CCTV system faults within the RVRC receiving equipment and workstations;

g) important customer instructions, the time and date they are received by the RVRC and the time(s) and date(s) that they are actioned by the RVRC;

h) the times at which an RVRC operator initiates and closes a routine patrol of the supervised premises.

11.2 Storage of images received

11.2.1 Images received at the RVRC should be stored electronically on a medium such as a hard drive. Reference images (**6.4.1**) should be stored electronically within the RVRC and should be accessible to the RVRC operator during live event handling for comparison purposes. For functional cameras, reference images relating to each of the preset positions (**6.4.2**) should be stored.

11.2.2 Documented procedures should be established for indexing and accessing images stored from a particular incident.

11.2.3 The retention period for the images should be agreed with the customer.

NOTE Attention is drawn to the Data Protection Act [1].

11.3 Images for evidential purposes

Where data and/or images are stored digitally and might be required as evidence for a crime, then this should be in accordance with BS IEC 62676-4:2014, Clause **11**.

NOTE See BS 10008 for evidential weight and legal admissibility of electronic information.

11.4 Confidentiality

Procedures should be established to authenticate the exchange of confidential information between the RVRC and the customer. Details should be agreed with the CCTV company and the customer.

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

NOTE 2 Examples of confidential information include changes to setting/unsetting times, requests to the RVRC to set or unset, the cancelling of activations, and names and addresses of users.

11.5 RVRC operator actions

RVRC operators should follow documented procedures (see Clause **9**) when handling activations. They should be trained in procedures for producing evidential images, should they be required to do so. When recording information from an activation, the RVRC operator should take into consideration and document any information that they judge to be potentially useful for investigative and evidential purposes.

11.6 Image quality check

When, during the handling of an activation, the quality of an image is identified as too poor to allow the RVRC operator to determine the nature and detail of a viewed event in accordance with **10.5**, a formal notice should be issued by the RVRC to the CCTV company and/or customer (as appropriate) advising of the nature of the problem and requesting that remedial action be taken.

11.7 Critical data omissions

When, during the handling of an activation, critical data required to complete the response plan are unavailable or inaccurate (e.g. there is a user who is no longer valid on the system), a formal notice should be issued by the RVRC to the to the CCTV company and/or customer (as appropriate) requesting the supply of the missing data.

12 Activation management

12.1 Classification of activations

The RVRC should classify activations. As a minimum, the classification system used should distinguish between alerts and incidents. The activity for each detector/camera combination should be recorded and classified according to the cause of the activation so that the CCTV system can be managed effectively with regard to the CCTV system faults or deficiencies.

12.2 Multiple unwanted activations

When multiple activations occur, the response plan should be carried out in accordance with **8.3**. Where necessary, detectors should be omitted in accordance with **4.6.3** or isolated in accordance with **4.6.4**.

13 Service levels

13.1 General

The RVRC should conform to BS 5979 or BS 8591.

13.2 Activation response time

The evaluation of images received at the RVRC as a result of each initial activation should commence within 90 s of their arrival for 80% of initial activations and 180 s of their arrival for 98.5% of initial activations.

13.3 CCTV system fault reporting

The RVRC should notify the customer of faults found within the CCTV system within 60 min unless a different time limit is agreed between the RVRC, the CCTV company and the customer in writing.

13.4 Incident reporting

Incidents occurring during the period in which the CCTV system is set should be reported in writing to the customer's nominated address within 24 h.

NOTE The nominated address may be a fax number or an e-mail address.

14 General maintenance and personnel screening

14.1 CCTV system maintenance

14.1.1 Maintenance agreement and routine visits

14.1.1.1 Maintenance should be carried out at agreed intervals, which should be not less than twice annually.

14.1.1.2 Documented criteria for the corrective and preventative maintenance of the CCTV system should be agreed between the customer and CCTV company.

*NOTE Examples of maintenance can be found in BS IEC 62676-4:2014, Clause **17**.*

14.1.1.3 Preventative maintenance should be scheduled to take place once during the sixth calendar month following the first month in which the CCTV system acceptance certificate is issued and at six monthly intervals thereafter. Preventative maintenance visits that occur during the month before or month after the scheduled month should not affect the preventative maintenance schedule.

14.1.2 CCTV company maintenance engineer actions

14.1.2.1 The maintenance engineer should inform the RVRC that maintenance/repair is due to take place.

14.1.2.2 At each visit to the supervised premises, the maintenance engineer should consider whether any of the environmental factors (see **B.4**) have changed to adversely affect the operation of the CCTV system. If this is discovered to be the case, remedial action should be documented and agreed with the customer.

14.1.2.3 As part of the preventative maintenance visit, the engineer should carry out a check of the night images (see **10.5**).

14.1.2.4 When changes to the CCTV system and configuration of transmission equipment are required, the RVRC should be informed of the changes that affect the monitoring response and, those parts affected, tested through to the RVRC in accordance with **14.1.3.1**.

14.1.2.5 Once a repair has been completed, the maintenance engineer should inform the RVRC.

14.1.2.6 The image of each detection area should be compared with the relevant stored reference images by the CCTV company in conjunction with the RVRC at each maintenance visit. If necessary new reference image(s) should be created and stored at the RVRC, e.g. in the event of a camera repair or replacement.

14.1.3 RVRC maintenance actions

14.1.3.1 Following **14.1.2.4**, the RVRC should check the parts of the CCTV system which have been repaired, in conjunction with the CCTV company, to confirm that they are fully operational and conform to **4.6**. The customer and/or CCTV company should be advised immediately if the CCTV system is not fully operational.

14.1.3.2 The RVRC should review CCTV system specification documentation and operational logs when the CCTV company carry out preventative maintenance visits to identify any fault or deterioration in the CCTV system operation. Once completed, the RVRC should check (see **14.1.3.1**) and approve any changes and modifications that have been made to the CCTV system.

14.2 Personnel screening

Person(s) with access to the RVRC or its records and personnel at the CCTV company should, as a minimum, be screened in accordance with BS 7858.

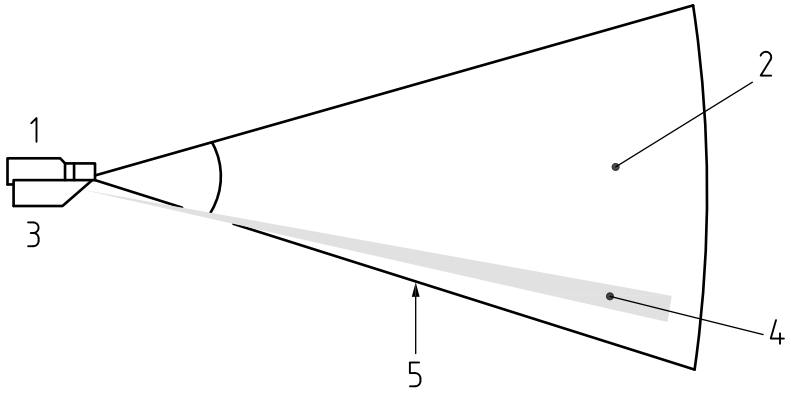
NOTE Attention is drawn to the requirements for SIA licensing under the Private Security Industry Act 2005 [8].

Annex A (informative) Diagrams for positioning detectors

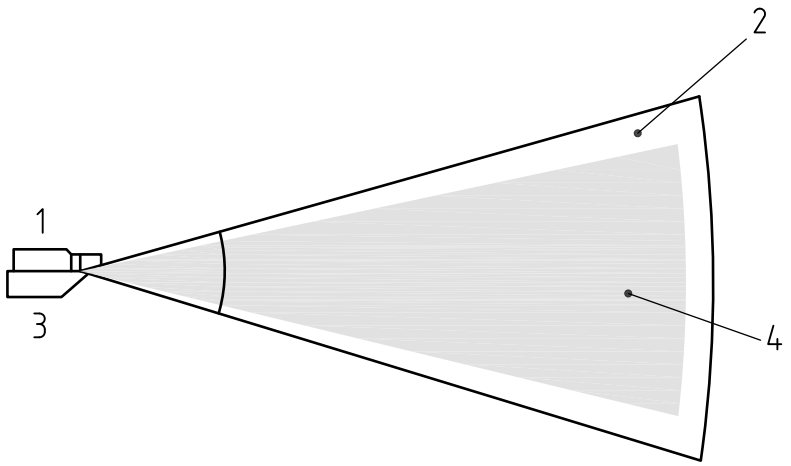
A.1 Alignment of long range and wide angle detectors

Figure A.1 shows examples of the alignment of long range and wide angle detectors in accordance with **4.3.1**.

Figure A.1 **Alignment of long range and wide angle detectors**



a) Example of the correct alignment of a long range detector



b) Example of the correct alignment of a wide angle detector

Key

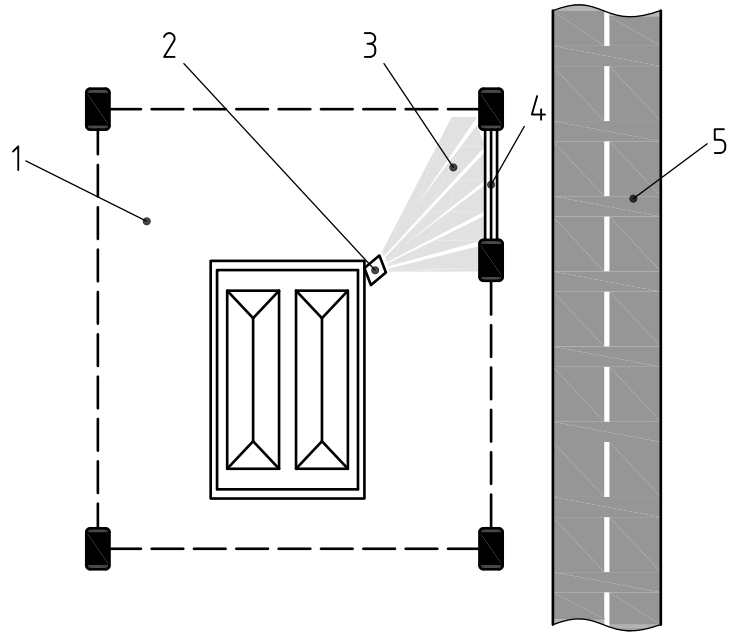
1 Camera
2 Camera field of view
3 Detector
4 Detection area
5 Anticipated direction of intrusion

A.2 Position of detectors near a supervised premises boundary

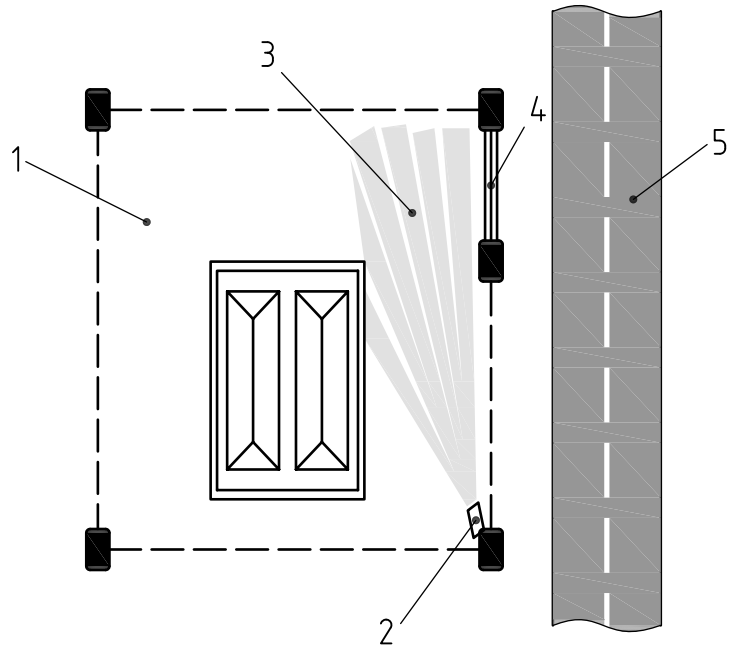
A.2.1 Correctly positioned detectors

Figure A.2 shows examples of correctly positioned detectors that are in accordance with **4.3.3.2**.

Figure A.2 **Correctly positioned detectors near a supervised premises boundary**



a) Example of a detector facing an entrance gate, adjusted to avoid overspill.



b) Example of a correctly positioned inward-facing detector where the detection area runs alongside a supervised premises boundary

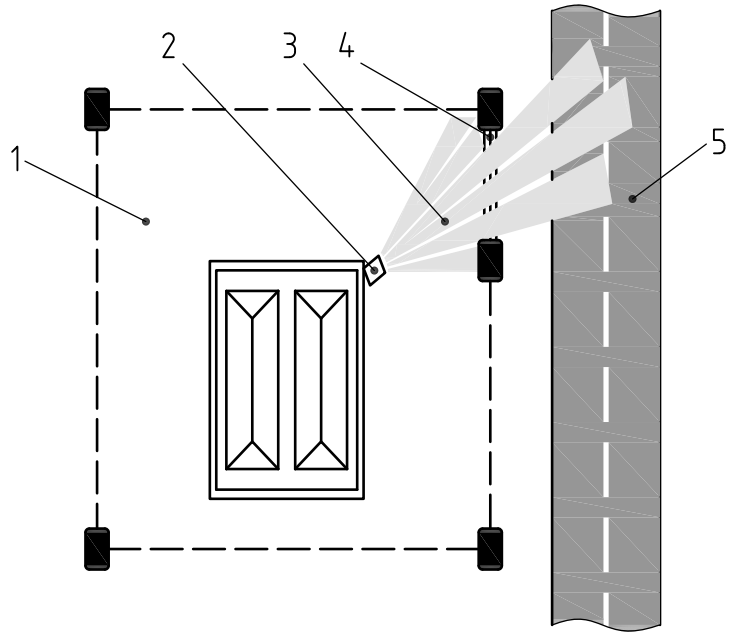
Key

1 Secure area
2 Detector
3 Detection area
4 Entrance gate
5 Public road

A.2.2 Incorrectly adjusted detector near a supervised premises boundary

Figure A.3 shows an example of an incorrectly adjusted detector not in accordance with **4.3.3.2**

Figure A.3 **An incorrectly adjusted detector facing an entrance gate, where the detection exceeds the secure area**



Key

1 Secure area
2 Detector
3 Detection area
4 Entrance gate
5 Public road

NOTE An incorrectly adjusted detector can increase unwanted activations.

A.3 Incorrectly positioned detector with an extended area of coverage

Figure A.4 shows an example of an incorrectly positioned detector not in accordance with **4.3.1** where the area of coverage extends outside the camera's field of view.

A.4 Multiple cameras correctly positioned to view the area of coverage of the detector

Figure A.5 shows multiple cameras positioned to create a field of view that covers the entire area of coverage of the detector, in accordance with **4.3.3**.

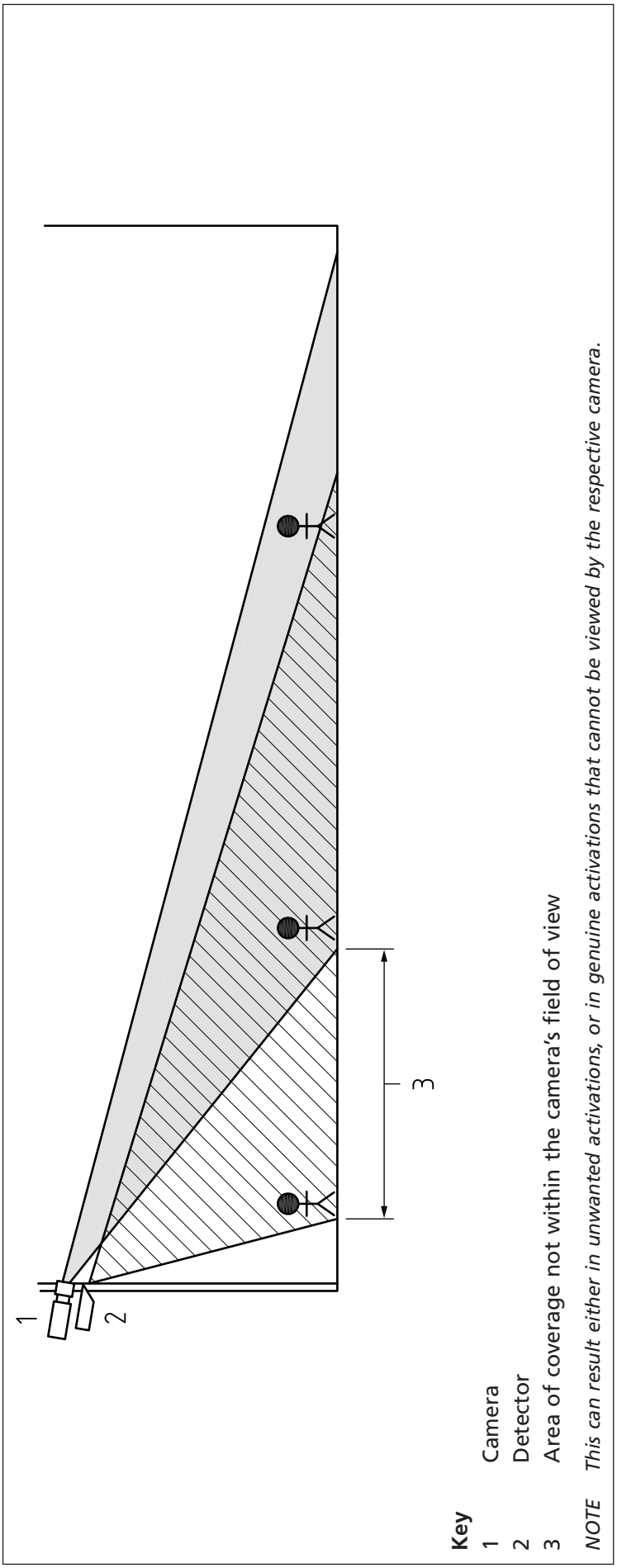


Figure A.4 **An incorrectly positioned detector providing a detection area outside the field of view of the camera**

Key

1 Camera
2 Detector
3 Area of coverage not within the camera's field of view

NOTE This can result either in unwanted activations, or in genuine activations that cannot be viewed by the respective camera.

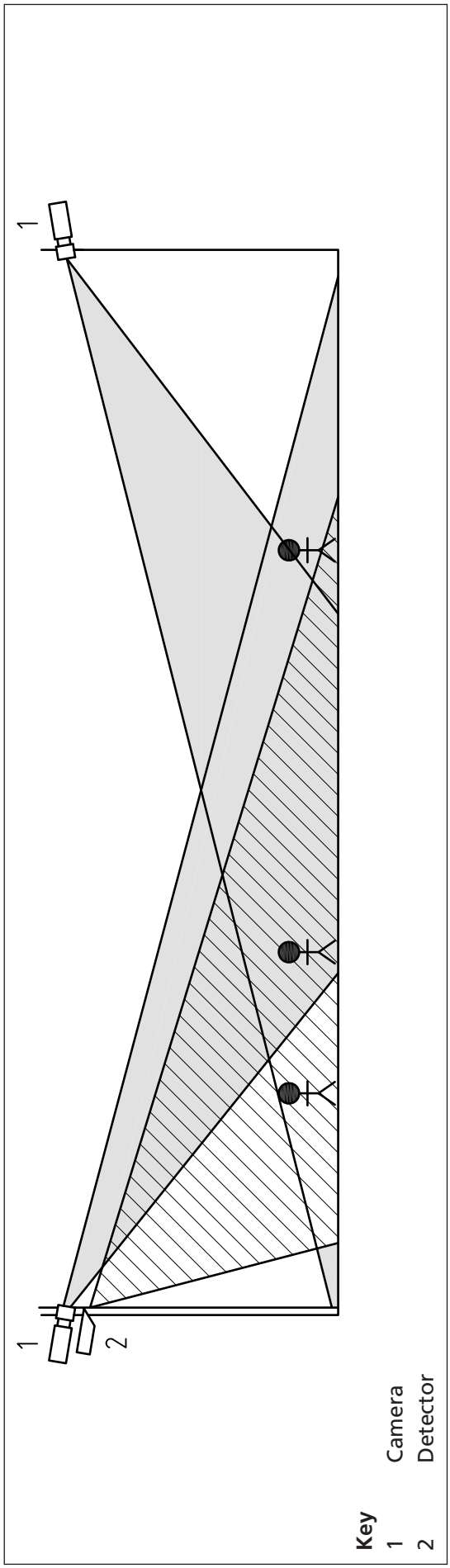


Figure A.5 **Example of multiple cameras positioned to view the total detection area**

Annex B (informative) Factors affecting the design requirements for a detector-activated CCTV system

B.1 Detector configuration

In respect of the need to verify an event (see **4.4.1.2**), it is advisable to consider installing multiple short-range detectors in preference to long-range detection methods.

B.2 Expected movement within a secure area

The customer may authorize specific activity within the secure area, or parts of it, when the CCTV system is set. Careful selection and design of the CCTV system, to prevent activations being generated from such authorised activity, while still generating activations from unauthorised activity is, in such cases, highly important.

B.3 Conditions of the secure area

The layout and topography of the secure areas can affect the functionality of a detector-activated CCTV system. Elevated ground and physical obstacles can limit the functionality of the detectors and/or prevent clear images of events.

B.4 Environmental factors

The following environmental factors can affect the functionality of CCTV cameras and detectors.

a) *Direct sunlight.* The position of the rising and setting sun in different seasons can create glare and blind the CCTV camera.

b) *Reflected light*. Light reflected from both natural and man-made substances (e.g. lakes, sheet metal) can create glare and blind the CCTV camera.

c) *Direct artificial light*. Flood lights or other artificial lighting shining directly onto camera's can create glare and blind the CCTV camera. (This might not be consistent, as in vehicle headlights from a neighbouring uphill road regularly shining on the camera.)

d) *Animals/insects*. These can enter the field of vision of the camera and cause unwanted activations.

e) *Vegetation.* Growth cycles and the movement of flora can obstruct the visibility of an event to a camera.

f) *Vibration and noise.* High levels of traffic and heavy machinery can cause inadvertent movement of the camera and prevent the capture of steady images.

B.5 Geographic location

The secure area might be subjected to certain weather conditions due to its geographic location. Weather conditions such as the following can adversely affect the functionality of a CCTV system.

a) *Mist*. Common over moorlands, coastal areas and low-lying plains, this can radically impair visibility in the field of vision of the camera and therefore have a negative impact on the clarity of images transmitted to the RVRC.

b) *Humidity.* Common in coastal areas, this can cause CCTV system components to corrode and malfunction.

c) *High winds*. Common in coastal areas, on high-ground or on exposed locations; these can cause the inadvertent movement of CCTV cameras and equipment or cause unwanted activations.

d) *Salt* (and other pollutants) can accumulate on lenses/covers and obscure the view. Cameras located near the sea, or in areas with high pollution levels, need to be cleaned regularly. This might require built-in wipers/washers or easy access to the camera (hinged mounting poles, etc.).

B.6 Sources of heat

It is important to keep detectors that are sensitive to infrared radiation away from heat sources including boilers, exhaust vents, air conditioning units, steam pipes and open fires.

B.7 Open sites

The lack of a secure surrounding barrier on an open site means that it is more vulnerable to unauthorized intrusions. Selection of the type, positioning and method of detection to meet the specific needs of an open site are therefore particularly important. It is also important to consider and agree the RVRC responses in accordance with the needs of an open site.

Annex C (informative) Types of technology used in detection equipment

C.1 General

Applications of detection technology vary considerably. Selecting the correct type or combination of technologies is important to meet the operational needs of the detector-activated CCTV system.

The following types of technology listed in **C.2** to **C.10** are some of the more common types of detection technology available.

C.2 PIR detector

A PIR detector is a common form of external detection device designed to provide either a wide or narrow angle of detection, or a combination of both, to provide optimum area coverage. Such devices offer resilience to unwanted activations and are able to withstand external environmental conditions. A PIR detector is sensitive to the movement of heat (e.g. a moving body) within or across the detection area.

NOTE Resilience can be achieved by using multiple sensors (i.e. of the same technology) within one detection device.

A detector is usually more sensitive to intrusion when movement crosses the field of view at right angles to the detection plane.

C.3 Active IR detector

An active IR detector consists of a transmitter and a receiver that detects an object which breaks the infrared path between these, such as a person or a vehicle.

C.4 Microwave

A microwave detector with a separate transmitter and receiver (these can sometimes be located in the same housing) is the most common type used. It is imperative that careful consideration is given to the terrain and animal life within the secure area (see Annex B) to prevent unwanted alarms and facilitate reliable detection.

Intruder detection is usually more sensitive where movement is towards or away from the detection area with relation to the detection plane.

C.5 Laser

Laser technology has the ability to rapidly detect movement, direction and object size. It is often used as a safety interlock to monitor vehicles and/or pedestrians driving or walking towards closing roller doors. It can also be used for perimeter protection. Mounting heights and orientation are often critical.

C.6 Video content analysis (VCA)

Video content analytics are used to analyse video for specific data, behaviour, or objects. This method of detection can be combined with another type of detection to provide improved reliability and reduce unwanted alarms.

*NOTE The use of video analytics can help with the problems caused by environmental hazards (see **B.4**).*

C.7 Video motion detection (VMD)

VMD is a technology which defines activity in a scene by analysing image data and the differences in a series of images. This method of detection can be combined with another type of detection to provide improved reliability and reduce unwanted alarms.

NOTE Video motion detection is generally built-in to the camera or digital video recorder/network video recorder (DVR/NVR) and can create unwanted alarms caused by shadows or light variations, and could be unreliable if not used with other detection technology.

C.8 Perimeter fence detection

A wide range of products fall into this category. It includes the most common forms of perimeter fence protection which use optical or acoustic cable based technologies. Other forms of perimeter detection include, but are not limited to, electrical sensor wire, mechanical trip wire and electromagnetic sensors.

C.9 Buried sensor technology

Perimeter detection that is via buried sensors or cable can use pressure, acoustic or electromagnetic technologies.

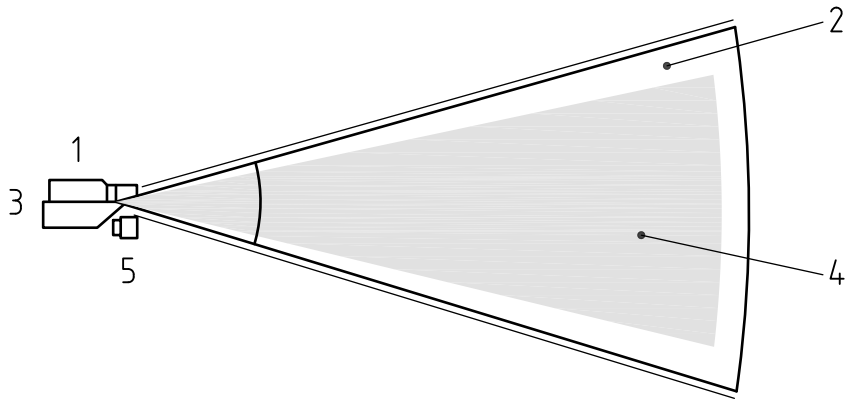
C.10 Combined technology

Using a combination of detection technologies can increase both detection capability and reliability. Combinations can exist within a single enclosure or by using two or more distinctly separate detection methods. Examples include a CCTV system using video analytics in conjunction with PIR detectors; a combined PIR/Microwave detector using electronic AND logic; and discrete detectors using separate technology such as PIR and ultrasonic. In operation, each technology type needs to activate within a programmable time window before an alarm is given. This approach is usually highly effective in reducing unwanted activations.

Annex D (informative) Illumination of the field of view of the camera

Figure D.1 shows an example of correct artificial illumination of the field of view of a camera that conforms to **4.4.2.1**.

Figure D.1 **Correct artificial illumination of the field of view of a camera**



Key

1 Camera
2 Camera field of view and illumination
3 Detector
4 Area of detection
5 Illuminator

Annex E (normative) Checklist criteria for the commissioning of a detector-activated CCTV system

The commissioning of a detector-activated CCTV system should be checked in accordance with the criteria given in Table E.1.

NOTE Table E.1 is a suggested template for use. Other methods of recording the information may be used as long as the same criteria are checked.

Table E.1 **Template for the commissioning of a CCTV system**

No.	Commissioning checks	Yes/no	Remarks
	Installation and configuration		
1	Has the CCTV system been installed and configured in accordance with the CCTV system design proposal (and any deviations agreed in writing with the customer)? (see **4.2.2**)		
2	Does the CCTV system conform to BS IEC 62676-4? (see **5.3**)		
3	Are cables clearly labelled at interconnections? (see **5.1.4**)		
4	Has the resistance of detection interconnections been recorded or the continuity of bus-wired interconnections been checked?		
5	Has a unique password been assigned to protect the CCTV system from unauthorized remote access? (see **4.6.9.3**)		
6	Has the transmission path(s) been tested for the correct transmission of signals to the RVRC? Has it been checked that the RVRC are receiving these signals? (see **4.6.11**, **4.6.12**, **4.6.13**)		
7	Have cameras been checked for correct focus both at night and during the day? (see **6.6**)		
8	Have day/night cameras been checked to ensure that they switch to mono in line with the manufacturer's specification?		
9	Have functional camera presets and detector outputs been recorded?		
	Detectors		
10	Has every detector and output device through to the control equipment been checked and found to function correctly? (see **4.3**)		
11	Have all detection areas been checked to fall within the fields of view of the associated cameras? (see **4.3.1**)		
12	Has the position of the detectors been checked so that they are not adversely affected by the strength and position of the sun (e.g. at sunrise/sunset)? (see **4.3.3.3**)		
13	Has each detector been checked to connect to a single input? (see **4.3.4.5**)		
14	Has the operation of tamper devices been checked? (see **4.6.6**)		
15	Has the area or volume of coverage of movement/vibration detectors including alignment of active beam detectors and anti-masking or range reduction facilities (as appropriate) been checked?		

Table E.1 **Template for the commissioning of a CCTV system**

16	Have the CCTV cameras and detectors on entry/exit routes been checked for correct operation and the entry/exit timer recorded?		
17	Have the detection devices of the set CCTV system been operated to check that the resulting alarm conditions are notified correctly?		
	Illumination		
18	Have camera field of views been checked to be correctly illuminated during both day and night conditions? (see **4.4.2**)		
	Audio		
19	Have the audible devices been checked (including audio challenge) for correct operation and audibility? (see **4.5**)		
	Power supply		
20	Has a record been made of the date of battery installation? (see **4.6.14.4.3**)		
21	Has the current required by all power supplies used in the CCTV system, in both set (but inactive) and alarm states, been logged?		
22	Has the mains supply been removed and the battery voltage used by the equipment verified to conform to **4.6.14**?		
23	Is the CCTV system able to function to its expected level of operation without the prime power source (see **4.6.14.2**)? (see **4.6.14.1.7** where a UPS is specified)		
24	Is there adequate standby battery capacity to conform to **4.6.14.2**?		
25	Are the mains supply fuses of the correct rating?		
	Customer considerations		
26	Has a customer signature been obtained to acknowledge receipt of and instructions for operating keys/codes to the CCTV system? (see **6.9.1**)		
27	Has the customer been shown the extent of the detection area and how to operate the CCTV system, including operating detectors? (see **6.9.2**)		
28	Has all documentation been completed and customer documentation left at the supervised premises? (see **4.1.2**; **4.2**; **6.9.1**; **6.9.3**; **8.1**; **8.3**).		
29	Have communication procedures been discussed and agreed with the RVRC and explained to the customer? (see **6.9.4**)		
30	Has the customer and/or user been given training on the use of the CCTV system(s)? (see **6.9.2**)		
31	Have surplus materials from the CCTV system installation been removed from the supervised premises and has it been left in a tidy condition? (see **6.9.5**)		

Annex F (informative) Setting procedure with a detector in the active state

In the event of the setting procedure being completed when a detector is in an active state, it is possible to configure the CCTV system to carry out one of more of the following actions:

a) prevent completion of the setting procedure until the detector problem is solved;

b) automatically omit the detector until the CCTV system is unset; or

NOTE 1 This is logged and reported to the RVRC as an exception.

c) immediately generate an activation associated with the detector following completion of the setting procedure.

NOTE 2 This condition would then be processed in accordance with the stated procedure and the customer notified.

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 10008, *Evidential weight and legal admissibility of electronic information – Specification*

BS EN 50130-5, *Alarm systems – Part 5: Environmental test methods*

BS EN 62676-1-2, Video surveillance systems for use in security applications – System requirements – Part 1-2: Performance requirements for video transmission

BS EN 62676-2-1, Video surveillance systems for use in security applications – Video transmission protocols – Part 2-1: General requirements

BS EN 62676-2-2, Video surveillance systems for use in security applications – Video transmission protocols – Part 2-2: IP interoperability implementation based on HTTP and REST services

BS EN 62676-2-3, Video surveillance systems for use in security applications – Video transmission protocols – Part 2-3: IP interoperability implementation based on Web services

Other publications

[1] GREAT BRITAIN. Data Protection Act 1998. London: The Stationery Office. [2)]

[2] GREAT BRITAIN. Human Rights Act 1998. London: The Stationery Office[2)]

[3] GREAT BRITAIN. Protection of Freedoms Act 2012. London: The Stationery Office

[4] Surveillance Camera Code of Practice 2013[2)].

[5] GREAT BRITAIN. Clean Neighbourhoods and Environment Act 2005. London: The Stationery Office.[2)]

[6] ASSOCIATION OF CHIEF POLICE OFFICERS (ACPO) OF ENGLAND, WALES AND NORTHERN IRELAND. *ACPO Policy on Police Response to Security Systems*. London: ACPO, April 2009.

[7] ACPOS. *ACPOS Security Systems Policy*. Scotland: Association of Chief Police Officers in Scotland. [3)]

[8] GREAT BRITAIN. Private Security Industry Act 2001. London: The Stationery Office. [2)]

[2)] This can be obtained from The Stationery Office, 51 Nine Elms Lane, London SW8 5DR, UK, or from their website: http://www.tso.co.uk.

[3)] The ACPOS Security systems policy is currently under review with Police Scotland who are expected to release a new 'Police Scotland – Security systems – Guidance document' (name might be subject to change).

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.™