

BS 8418:2015+A1:2017



BSI Standards Publication

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



Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2017

Published by BSI Standards Limited 2017

ISBN 978 0 580 98849 3

ICS 13.310 | 33.160.40

The following BSI references relate to the work on this document:

Committee reference GW/1/10

Drafts for comment 14/30293253 DC; 17/30361938 DC

Amendments/corrigenda issued since publication

Date	Text affected
October 2017	A1: see foreword

Contents

	Page
Foreword	ii
Introduction	1
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviations	2
4 CCTV system planning and design	5
<i>Table 1 — Tamper detection and indication</i>	11
<i>Table 2 — Fault recognition and indication</i>	11
5 Installation	15
6 Commissioning	16
7 Setting/unsetting procedures of the remotely monitored CCTV system	18
8 Responsibilities and considerations	21
9 RVRC operator procedures	22
10 Management and operation of the RVRC	23
11 RVRC procedures and documentation	24
12 Activation management	26
13 Service levels	26
14 General maintenance and personnel screening	26
Annex A (informative) Diagrams for positioning detectors	28
<i>Figure A.1 — Alignment of long range and wide angle detectors</i>	28
<i>Figure A.2 — Correctly positioned detectors near a supervised premises boundary</i>	29
<i>Figure A.3 — An incorrectly adjusted detector facing an entrance gate, where the detection exceeds the secure area</i>	30
<i>Figure A.4 — An incorrectly positioned detector providing a detection area outside the field of view of the camera</i>	31
<i>Figure A.5 — Example of multiple cameras positioned to view the total detection area</i>	31
Annex B (informative) Factors affecting the design requirements for a detector-activated CCTV system	31
Annex C (informative) Types of technology used in detection equipment	33
Annex D (informative) Illumination of the field of view of the camera	35
<i>Figure D.1 — Correct artificial illumination of the field of view of a camera</i>	35
Annex E (normative) Checklist criteria for the commissioning of a detector-activated CCTV system	35
<i>Table E.1 — Template for the commissioning of a CCTV system</i>	35
Annex F (informative) Setting procedure with a detector in the active state	37
Bibliography	38

Summary of pages

This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 38, 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 these committees can be obtained on request to their secretary.

Supersession

This British Standard superseded BS 8418:2010, which was withdrawn on 31 July 2015.

BS 8418:2015+A1:2017 supersedes BS 8418:2015, which is withdrawn.

Information about this document

Text introduced or altered by Amendment No. 1 is indicated in the text by tags A1 A1. Minor editorial changes are not tagged.

BS 8418:2015 was a full revision of the standard, and introduced 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.

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, *Closed-circuit television (CCTV) — Management and operation — Code of practice*¹

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*

¹ At the time of the publication of BS 8418:2015, BS 7958:2009 was under review.

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

[SOURCE: 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 1 Formerly known as Portable ACE or ACE.

NOTE 2  A remote device is not considered as a digital key. 

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".*

[SOURCE: 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 device**

remote non-CCTV system interface which enables a user to control and monitor the CCTV system

NOTE 1 The remote device might be a bespoke system component or an application running on a PC, tablet, phone or other computing device.

NOTE 2 External network connections might be made through a direct IP or dialled connection or through a Cloud or proxy server service. 

3.1.31 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

3.1.32 RVRC operator

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

3.1.33 secure area

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

3.1.34 semi-wired detector

wireless detector with a wired power supply

3.1.35 set

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

3.1.36 supervised premises

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

3.1.37 tamper

deliberate interference with a CCTV system or part thereof

3.1.38 uninterruptable power supply

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

3.1.39 unset

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

3.1.40 unwanted activation

avoidable alert

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

3.1.41 user

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

3.1.42 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 [8.1h](#)].

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 [4.2.2c](#)].

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 [6.1c](#)) 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 [4.2.2h](#)) 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](#)).