

a basic guide to  
**BS 8418 systems**  
for installers



December 2010

---

For other information please contact:

British Security Industry Association

**t: 0845 389 3889**

f: 0845 389 0761

e: [info@bsia.co.uk](mailto:info@bsia.co.uk)

[www.bsia.co.uk](http://www.bsia.co.uk)

## Introduction

BS8418 is the code of practice for the installation and remote monitoring of detector activated CCTV systems. BS8418 has undergone a review and the 2003 version is now being replaced by the 2010 version. Significantly, there is a “dual running” period of one year, which expires on 31st July 2011. This allows Installers to use either version of the Code of practice and is subject to availability of compliant manufactured equipment.

The purpose of this installer guide is to provide a summary checklist of the main elements of British Standard BS 8418:2010. This guide does not replace the requirements in the standard. Where applicable the relevant clauses in BS 8418:2010 are indicated by the square brackets e.g. [4.1.a].

## 1. Safety, security & legislative considerations

- Observe all aspects of Health and Safety when designing the system, e.g. emergency exits, future maintenance requirements and fire regulations.
- Consider the requirements for Security screening of employees in accordance with BS7858
- Consider the effects of light / noise pollution on the local environment; The Clean Neighborhoods and Environment Act 2005.
- The requirements of the Private Security Industry Act 2001 for example, monitoring, recording and use of CCTV in private & public places under contract.
- Attention to the requirements of the Data Protection Act 1998, e.g. customer records, retention of recorded images etc.
- Information Commissioners code of practice:2008 for the use of CCTV in relation to identifying individuals.

## 2. CCTV system design considerations

Design of the system should address the perceived risks as decided by the owner and take into account the needs and operation of the system. This assessment is often known as an “Operational requirement”, which can be a document in its own right or form part of the system design proposal.

### 2.1 System design proposal (SDP) [4.1]

- A SDP needs to be created and should include the following key items;
  - a. Drawing(s) and written detail showing the positions of cameras and detectors providing their location and fields of view; to include type(s) and a brief technical description.
  - b. Drawing(s) should show the extent of the secure area (area where unauthorized access is intended to be detected) and location of vehicles / other moveable objects that could compromise the effectiveness of the system.
  - c. Drawing(s) should either be to scale or show the dimensions of the secure area, buildings, etc.
  - d. Identify both fixed / functional camera identity associated with detectors, including presets association.
  - e. Type and location of audio devices.
  - f. Location and brief technical description of control equipment, power supplies, storage devices and other peripheral equipment to be used in the system.
  - g. Details of lighting provision and who is responsible for its provision.
  - h. Transmission paths used by the system and who is responsible for its provision.
  - i. Services for which the owner may be responsible, such as mains power, telephone connectivity etc.

## **2.2 Detector positioning, selection and configuration [4.2]**

- In general, the detection area should fall within the field of view of the camera(s) they are associated with. Annex A.1, A.3 and A.4 of BS8418 provides example diagrams of correct / Incorrect alignment [4.2.1].
- Ensure detectors do not overspill outside the site boundaries e.g. onto public paths or roadways. BS8418 Annex A.2 provides example diagrams for correct / incorrect positioning of detectors [4.2.2.2].
- Ensure PIRs facing east or west are not affected by the sun or from reflection and shadows [4.2.2.3].
- BS8418 Annex B provides on site related factors to consider for the correct location and operation of detectors. These include;
  - a. Preferred use of multiple short range detectors over long range detection.
  - b. Consideration of expected movement on site.
  - c. Consider the layout and topography of the secure area.
  - d. Environmental factors such as sunlight, insects, vegetation, vibration etc.
  - e. Geographic conditions i.e. weather, mist, humidity.
  - f. Sources of heat.
  - g. Open sites as opposed to closed secure sites.
- It is important to select detection that meets the operational requirement as specified by the owner. BS8418 Annex C provides guidance on types of technology used in detection equipment. Some of the key points being;
  - a. Use of detectors (such as PIRs) that are suitable for use in external environments.
  - b. The use of multiple sensors / technologies to add resilience to the system and limit unwanted alarms.
  - c. Following the manufacturers guidance on Installing and configuring detectors is often critical for correct operation.
- Ensure detectors are uniquely identifiable to the system. Note: Multiple detectors should not be identified as a single entity but each individual detector must have its own ID [4.2.3.6].
- Where wireless and semi-wired detectors are used, they should provide indication of low battery voltage and loss of wireless signal to the control equipment. These need to be reported to the RVRC when the system is set.

## **2.3 Camera positioning and configuration [4.3]**

- Ensure the cameras' fields of view cover all areas of the associated detectors [4.3.1.2].
- To 'verify' an event, set the field of view so that a 1.6m high human target fills at least 10% of picture height. To 'recognise' an intruder the target should fill a minimum of 50% of picture height [4.3.1.3].
- The entry / exit route to the secure area should either be viewed with a fixed camera or a functional camera with its parked position viewing the entry / exit route [4.3.1.4].
- If functional cameras are used as the sole means of viewing the detection area, use should be made of defined presets and where necessary discrete adjacent zones corresponding to each preset. Each position should be defined and documented in the SDP [4.3.1.5].
- Where functional cameras using presets associated with detectors are used, access to change the presets should be restricted to the Installer / RVRC [4.3.1.6].
- As a general rule, cameras should not overlook public areas [4.3.1.7].
- Cameras should be uniquely identified, which should be displayed at the RVRC and should correspond with the SDP [4.3.1.9].
- Camera positioning and configuration of the CCTV system should conform to BS EN50132-7 [4.3.1.1].

## **2.4 Illumination [4.3.2]**

- BS8418 Annex D provides a drawing of the correct illumination required of a camera and detectors fields of view [4.3.2.1 & 4.3.2.2].
- Illumination provided should allow an RVRC operator to verify the presence or absence of a human form upon display of an image during both day and night conditions [4.3.2.3].
- Artificial illumination should be maintained in accordance with manufacturers recommendations. This may be an owner and / or maintainer responsibility [4.3.2.4].
- IR illumination should not surround the camera lens on external cameras [4.3.2.9].
- Where possible, artificial illumination sources should not be positioned to directly face cameras as they may impede the clarity of CCTV images [4.3.2.8].

## **2.5 Audio challenge [4.4]**

- Where Audio challenge is installed it should be clearly audible (without distortion) within the area of coverage of the relevant detectors as indicated in the SDP. Challenges should be initiated by the RVRC and can consist of pre-recorded announcement or live voice operation [4.4].

**Note:** Attention is drawn to the ACPO / ACPOS policies for further requirements on BS8418 systems that require a Police response.

## **2.6 system performance and integrity [4.5]**

- Agreement should be in place between the system owner and RVRC as to the minimum frequency of activations from a detector before it is omitted. Omitted detectors should be restored when the CCTV system is returned to an unset state [4.5.3].
- Agreement should also be in place between the owner and RVRC when it is acceptable to isolate a detector. Such instances might be where detector omission has failed to resolve an excessive number of unwanted alarms or where a change to site operation (builders working on site) would mean the detector would send unwanted alarms to the RVRC [4.5.4].
- Camera signals should be monitored for video loss. Failure to restore the loss within 5 seconds should result in the RVRC being notified [4.5.5].
- Tamper detection should be provided to the following [4.5.6];
  - a. Cables supplying detectors.
  - b. Detector enclosure (through its usual method of opening) including removal from mounting, orientation adjustment and masking.
  - c. Housings containing power supplies to detectors should be equipped with tamper detection to detect opening through its usual method of opening.
  - d. Pluggable connectors should be located in the secure area or within an enclosure provided with tamper detection.
  - e. Control equipment should be located in the secure area (an area that will create an immediate alarm) or within an enclosure provided with tamper detection.
- When the CCTV is set, tamper signals should be reported to the RVRC. When the CCTV system is unset, tamper signals should be reported at the RVRC and / or at the protected premises using an audible indication [4.5.6].
- Control equipment should be protected using a secure validation process. The RVRC should be able to determine the status of the system and be able to remotely program the system where authorised to do so [4.5.7].

- There should be agreement between the RVRC and the owner as to the action to be taken in the event of a failure of the system to restart and where multiple restarts have occurred within a 24hr period.
- A 10,000 event log is required on site [4.5.8].
- Two transmission paths are required, both being capable of transmitting images to the RVRC.
- The system should have a full authorisation and retry protocol [4.5.10 / 4.5.11].
- A back-up UPS is required (where mains power is not supplemented by a stand by generator) to supply control and communications equipment for a minimum 4 hrs. Power supplies to detectors should also have 4hr battery back-up.

### 3. Installation [5]

- Installation should conform to good industry practice, e.g. wiring in accordance with BS7671. Cables of differing voltages should be segregated where required, marked as appropriate, selected based on their application, mechanically supported and protected from accidental damage. Equipment installed to manufacturers recommendations.

### 4. Commissioning & hand-over acceptance [6]

The following tests should be carried out by the installing engineer, in conjunction with the user and the RVRC [5.2]:

- Testing of detectors, cameras and their fields of view (day and night) [6.3 a/b].
- The accuracy of recorded data, notably labels used to describe the CCTV system [6.3d].
- Reference images to be taken to compare against live operation (day and night) [6.4/6.5].
- Soak test the installed system for a minimum 7 days and carry out any corrective action before live alarms are transmitted [6.6].
- Acceptance certificate to be issued by the RVRC at commencement of monitoring [6.8].
- The installer should demonstrate the operation of the system to the owner and obtain a signature confirming its hand-over. Written operating instructions should be provided to the owner and any necessary documentation, such as contact details for the RVRC, an "as fitted" specification, site drawings and appropriate manufacturers information etc. should be prepared and provided [6.9].

**Note:** An example commissioning checklist is provided in Annex E of BS8418

### 5. Setting/Unsetting procedures [7]

- Operation of the set / unset device during setting or unsetting should not create an activation [7.1].
- The setting / unsetting location (including the range of any device used to set / unset) should be in permanent field of view of a camera [7.2].
- Ensure that a monitoring action agreement exists with the owner as to the agreed course of action to an event that occurs during set / unset periods. This should include details on the entry / exit procedures [7.3 / 7.4 / 7.5].

## 6. Owner responsibilities [8]

- A documented agreement should exist between the owner and the RVRC detailing the owners responsibilities. Examples include, checking operation of illumination devices and reporting their failure to the RVRC, adjustment of clocks, investigating and eliminating causes of unwanted activations, following procedures for detector omission and isolation, agreed user maintenance of the system, changes to site layout etc [8].

## 7. Maintenance [14]

- A maintenance agreement should be in place that provides for both corrective and routine maintenance of the system. Routine maintenance should be twice annually as a minimum and can include one inspection remotely via the RVRC [14.1].
- Following a maintenance visit, the RVRC should be informed of the outcome of the visit to ensure operational integrity of the system is maintained [14.1.2 & 14.1.3].

## Further information

Form 196 - BS8418 – A user guide is available from [www.bsia.co.uk](http://www.bsia.co.uk)