

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



October 2004

---

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.

The purpose of this guide is to provide a check list of the main elements of British Standard BS 8418:2003. This guide does not replace the requirements in the standard. Where applicable the relevant clauses in BS 8418:2003 are indicated by the square brackets e.g. [4.1.a].

Only systems that are installed to BS 8418 can qualify for a Unique Reference Number (URN) which is issued by the local police authority to guarantee police response.

This guide is only an aide-memoire and does not replace any of the requirements of the standard.

## 1. Safety features

- Observe all aspects of Health and Safety when designing the system layout, e.g. emergency exits and fire regulations.

## 2. CCTV system design considerations

- Design the system specification to address the perceived risks, understand overall customers' needs.
- Select products to meet the system features that the customer has requested.
- Ensure that all components of the system comply with the relevant national standards.

## 3. Detector positioning and configuration [4.1]

- Detectors, should be installed to BS 7992, BS 4737 or BS EN 50131-1, and should only trigger on areas within the field of view of a camera and the area of activation should be confined to within the view of the specified camera [4.1a/b].
- Video motion detection should be installed to manufacturer's installation instructions [4.1a].
- Ensure detectors do not overspill outside the site boundaries e.g. onto public paths or roadways [4.1c].
- Ensure PIRs facing east or west are not affected by the sun or from reflection and shadows [4.1d].
- 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 [4.1e].
- Don't use low quality PIRs that can easily be subject to false triggering e.g. lighting control PIRs [4.1f].
- All cabling and detection devices should incorporate tamper protection [4.4.5].

## 4. Camera positioning and configuration [4.2]

- Ensure the cameras' fields of view cover all areas of the associated detectors [4.2.1b].
- To 'verify' an event, set the field of view so that a 1.6m high human target fills at least 10% of picture height [4.2.1c].
- To 'recognise' an intruder the target should fill a minimum of 50% of picture height [4.2.1d].
- Fixed cameras are the recommended option for vulnerable areas (e.g. the entry/exit route) or a PTZ camera with its park position viewing the vulnerable area [4.2.1e].

- Cameras should not face directly into sun or light. However, there should be sufficient light (night and day) to illuminate the cameras' fields of view [4.2.2a].
- If PTZ cameras are used in isolation, use should be made of presets so that the operator will observe each incident as though it were viewed by a static camera [4.2.1f].
- As a general rule, cameras should not overlook public areas [4.2.1g].

## 5. Audio challenge [4.3]

- An audio challenge facility is recommended. Care should be taken to avoid noise pollution beyond the site boundary [4.3].
- Where sites are so equipped, the audio challenge should be audible in all areas of detection [4.3].

## 6. CCTV system performance and integrity [4.4]

- Provide sufficient training to enable the customer to use the CCTV system effectively in order to achieve the desired level of security.
- Ensure the customer is provided with well defined written system management procedures.
- Inform the customer of the probable need for compliance with the Data Protection Act (1998).
- Power supplies are a major consideration. Give further consideration to the installation of a back-up UPS [4.4.11].
- The system should have the ability to monitor and indicate video loss to the RVRC [4.4.4].
- Check that tamper indications operate locally or to the RVRC depending on the unset / set state of the system [4.4.5a].
- Ensure that the system has an alternative signalling path to indicate failure of the main signalling path to the RVRC [4.4.8].
- The system should have a full connection and retry protocol [4.4.10/4.4.9].
- Plan to ensure that the fully detailed event log-system history is retained and held at the protected site [4.4.7].

## 7. Commissioning [5]

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

- Appropriate testing of detectors, cameras and fields of view (day and night) [5.2 a/b].
- The accuracy of recorded data, notably labels used to describe the CCTV system [5.2d].
- Reference images to be taken to compare against live operation (day and night) [5.3/5.4].
- Soak test the installed system for 7 days and carry out any corrective action before live alarms are transmitted [5.5].
- Acceptance certificate to be issued by the RVRC at commencement of monitoring [5.7].
- The installer should have provided the owner with a detailed system specification incorporating equipment inventory [10.1 b/c/gh].

## 8. Setting/Unsetting procedures [6]

- The setting/unsetting device should be installed. Operation of the device during setting or unsetting should not create an incident [6.1].
- Ensure that the owner's attention is drawn to their responsibilities [7].
- Ensure that a monitoring action agreement exists with the owner as to the agreed course of action to an activation [7.2].

## 9. Maintenance

- Inform the user of any inspection and servicing routines essential to maintain the serviceability of the CCTV system and assist the customer to formulate a satisfactory maintenance agreement [13.1].

## 10. Unique Reference Numbers [URNs]

- To obtain a URN, Installers of remotely monitored detector activated CCTV systems will need to comply with all of the following:
  - ACPO Security Systems Policy
  - BS 8418 Installation and remote monitoring of detector activated CCTV systems – Code of Practice.
  - BS EN 50132-7: CCTV Application guidelines.
- In order for the Police to allocate a URN to the system, the system must have the capability of audio challenge. Note that systems without a URN will not be given level 1 Police response.

## Further information

The Standard is available from BSI, 389 Chiswick High Road, London W4 4AL or visit [www.bsi-global.com](http://www.bsi-global.com)

For more information on the BSIA, call 0845 389 3889 or visit [www.bsia.co.uk](http://www.bsia.co.uk)