A basic guide to BS 8418:2015 CCTV Systems for Installers

April 2017

For other information please contact:

British Security Industry Association
t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

1. Introduction

The purpose of this installer guide is to provide a checklist of the main elements of British Standard BS 8418:2015. Where applicable the relevant clauses in BS 8418 are indicated by square brackets e.g. [4.1.a].

This guide is designed to be an aide-memoire and does not replace the requirements in the standard.

BS 8418 is the code of practice for the installation and remote monitoring of detector-activated CCTV systems and has undergone a substantial revision which was published on 31st January 2015. There was a short "dual running" period, which expired on 31st July 2015. It is also likely that there are existing older systems compliant with previous versions of the standard.

Note: The references to BS IEC 62676 series of standards in BS 8418:2015 are referred to as BS EN 62676 series of standards in this document, as they have since been adopted by CENELEC (European electrotechnical standards body) and published as such in the UK.

2. Safety, security & legislative considerations

- Observe all aspects of health and safety when designing the system layout, e.g. installation and maintenance of equipment mounted at height, emergency exits and fire regulations.
- Consider the requirements for security screening of employees in accordance with BS 7858.
- Consider the effects of light / noise pollution on the local environment; The Clean Neighbourhoods and Environment Act 2005.
- The requirements of the Private Security Industry Act 2001, e.g. 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.
- The Information Commissioner's Office (ICO) CCTV code of practice for surveillance cameras and personal information.
- Surveillance Camera Commissioner's (SCC) Surveillance camera code of practice.

3. CCTV system planning and design considerations [4.1]

- A threat assessment and risk analysis should be completed prior to design.
- An operational requirement document, addressing the customer's needs and the threat assessment and risk analysis. It should describe the needs, justification and purpose of CCTV system.
- The CCTV system operational requirement should conform to BS EN 62676-4:2015 [5.3].

4. CCTV system design proposal and specification [4.2]

- A documented CCTV system design proposal and specification that meets the operational requirement should be created to address:
  – the customer's needs
  – the safety, security & legislative elements in section 2 above
  – the threat assessment and risk analysis
  – is designed in such a way as to reduce the risk of unwanted activations
- All components of the CCTV system should comply with relevant national standards and be suitable for the environment in which they will be installed.

Note 1: the operational requirement could be defined within the system design proposal and specification.
Note 2: the system design proposal and specification could include detailed drawings.

5. Detector selection, positioning and configuration [4.3]

- Detectors should be installed and configured in accordance with manufacturer's recommendations/ instructions and meet the operational requirement.
- The detectors area of activation should cover (and not overspill) the field of view of the corresponding camera.
- Ensure detectors are not mounted so that they are adversely affected by environmental conditions such as the rising and setting of the sun and heat sources etc. [4.3.3.3].
- Each detector should be uniquely identifiable at the RVRC. [4.3.4.2].
- The system should be capable of detecting a tamper at all detection devices and associated cabling when the system is set. [Table 1].

Note: The use of multiple sensors/technologies may add resilience to the detection system and therefore limit unwanted activations. Multiple detectors should not be identified as a single entity, each individual detector should be uniquely identifiable at the RVRC.

6. Camera positioning and configuration [4.4]

- Ensure that cameras are positioned so that the associated detectors area of coverage can be viewed [4.4.1.1].
- In setting the field of view (please refer to BS EN 62676-4:2015, 6.7), the size of an object (the target) that will be displayed on the display screen, should be related to the operator task that is required to be undertaken. The targets below are for PAL and NTSC, in terms of percentage of resolution of screen height [4.4.1.2]:
  - For inspection – not be less than 400%,
  - For identification – not be less than 100% for PAL & 120% for NTSC,
  - For recognition – not be less than 50% for PAL & 60% for NTSC,
  - For observation – not be less than 25% for PAL & 30% for NTSC,
  - For detection – not be less than 10% for PAL & NTSC, or;
  - For monitoring – not be less than 5% for PAL and NTSC.
- To view entry/exit routes, fixed cameras or a functional camera in its parked position should be used [4.4.1.3].
- Where functional cameras are used in isolation, use should be made of presets so that an RVRC operator will observe each incident as though it were viewed by a static camera [4.4.1.4].
- Cameras should not overlook public areas [4.4.1.6].
- Cameras should not be mounted so that they are adversely affected by environmental conditions e.g. the rising and setting of the sun, bright light sources, reflections etc. [4.4.1.9].
- Fields of view should be illuminated (either naturally or artificially) to ensure that the CCTV images meet the CCTV system design proposal and specification [4.4.2.1].

7. Audio challenge (where installed) [4.5]

- Care should be taken to avoid noise pollution beyond the site boundaries.
- The audio challenge should be clearly audible (without distortion) in all areas of detection.

Note: Audio challenge may be a requirement of obtaining a URN for a Police response.

8. CCTV system performance and integrity [4.6]

- The system should have the ability to monitor faults locally when the CCTV system is unset, and by the RVRC when set [4.6.5 and Table 2].
- Check that tamper indications operate locally when the CCTV system is unset, and to the RVRC when set [4.6.6 and Table 1].
- Event log/system history is retained and held at the supervised premises [4.6.10].
- The system should have at least one data transmission path. Additional data transmission paths may be required, dependent upon the threat assessment and risk analysis [4.6.11.1].
- Data transmission path failure should be detected by or reported to the RVRC within 3 minutes (at all times whether the system is set or unset) [4.6.11.3].
- Where a remotely monitored CCTV system utilises the same transmission path as an intruder alarm system, the supervision of the transmission path is likely to be covered by the BS EN 50136 standard for Alarm Transmission Systems.
- The system should have a full communications connection and retry protocol [4.6.12].
- Control equipment and devices used to transmit data should have the ability to operate for 30 minutes should a power failure occur [4.6.14.2.4].
- Power supplies to detection devices should be capable of powering them for 4 hours following a mains power failure [4.6.14.2.5].
- Agreement should be in place between the customer, the CCTV company and the RVRC as to the response required to system faults and when omission/ isolation by the RVRC would be acceptable.
- Tamper detection and indication should be in accordance with Table 1 [4.6.6].
- Fault recognition and indication should be in accordance with table 2 [4.6.7].

9. Installation [5]

Installation should conform to good industry practice, e.g. wiring in accordance with BS 7671. Cables of differing voltages should be segregated where required, marked as appropriate, selected based on their application (including the environmental conditions), mechanically supported and protected from accidental damage. Equipment should be installed to manufacturer's recommendations.

10. Commissioning & hand-over acceptance [6]

- The following tests should be carried out by the installing (or commissioning) engineer, at the supervised premises, with the system in the 'set' condition, in conjunction with the customer (or customers representative) and the RVRC [6.3.1]:
  - Appropriate testing of detectors and fields of view of cameras (camera configuration both day and night) [6.3.2 a/b, 6.6].
  - The accuracy of recorded data, notably labels used to describe the CCTV system [6.3.2 d].
  - Reference images to be taken, then reviewed to ensure that they meet the system design proposal and specification (both day and night) [6.4/6.5].
  - Soak test the installed system for at least 7 days, then record and resolve any corrective action before live alarms are passed to the Police [6.6/6.7].
- A CCTV acceptance certificate is to be issued by the RVRC following successful completion of commissioning [6.7/6.8].
- Provide sufficient training and documentation to enable the customer to use the CCTV system effectively, in accordance with the operational requirements [6.9.2].
- The installer should provide the customer with detailed 'as fitted' documentation incorporating an equipment inventory [6.9.3].

Note: An example commissioning checklist is provided in Annex E of BS 8418.

11. CCTV system setting/ unsetting procedures [7]

- The setting or unsetting of the system should not cause any activations, unless agreed in writing [7.1.1].
- Setting should be prevented when a fault is present (this may be overridden by a customer authorised user, as long as it records this event in the log) [7.1.4].
- There should be an agreement between the CCTV company, customer and RVRC that details the responsibilities for the correct operation of the system, the CCTV company, customer and RVRC should understand their respective responsibilities within this agreement [8.1].
- There should be a documented response plan, detailing the action to be taken by the RVRC following activation, fault or a reported failure [8.3.1].

12. Responsibilities [8]

The CCTV company is responsible for liaising with the customer and the RVRC to make a documented agreement detailing all responsibilities. Examples include, checking illumination and reporting failures, fault reporting, adjustment of clocks, investigating and eliminating causes of unwanted activations, the procedures for detector omission and isolation, maintenance of the CCTV system, frequency of checking against reference images, changes to site layout etc. [8]

13. Maintenance [14]

- Agreed and documented criteria for preventive and corrective maintenance of the CCTV system, between the CCTV company and the customer, should be in place [14.1.1.2].
- Maintenance visits should be carried out in conjunction with the RVRC to enable the CCTV system to be confirmed as fully operational.

Note: Preventive maintenance should be undertaken at least twice annually, in accordance with BS 8418:2015, Clause 14 and BS EN 62676-4:2015, Clause 17.

14. 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:
  - NPCC Police Requirements & Response to Security Systems Policy or Police Scotland policy.
  - BS 8418 Installation and remote monitoring of detector-activated CCTV systems – Code of practice.
  - BS EN 62676-4:2015 Video surveillance systems for use in security applications. Application guidelines.
  - Surveillance Camera Code of Practice.
- In order for the Police to allocate a URN to the system, the system must have the capability of audio challenge.

Note: CCTV systems without a URN will not be given level 1 Police response.

15. Further information

Form 196 - 'BS 8418 – A user guide' is available from **www.bsia.co.uk**

This document was created by the CCTV Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

CCTV has had a profound impact on crime prevention and detection. The UK leads the way in the application of CCTV and its use is wide-ranging, encompassing facial-recognition technology, remote video monitoring, video smoke detection, mobile systems and Automatic Number Plate Recognition (ANPR) as well as many other functions.

In order to provide guidance and simplification in the complex area of CCTV, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The CCTV section encourages debate on new developments and concerns, such as digital video evidence and facilitating communication protocols between different manufacturers' products. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, customers, the police, inspectorates and insurers. The section also works with government and the Surveillance Camera Commissioner on these issues.

CCTV must be operated responsibly in order to respect citizens' rights and maintain public confidence. Laws such as the Data Protection Act have an important role to play in achieving this. BSIA CCTV companies drive best practice in this area and can provide advice on how CCTV owners/operators can adhere to the relevant legislation.

As a security company, BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, customers, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Kirkham House
John Comyn Drive
Worcester
WR3 7NS

t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

@thebsia

bsia
british security industry association