UBS 8418 - Detection-activated VSS

a basic guide for installers

Contents

1. Introduction

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

The guidelines for designing, installing, commissioning, maintaining, and operating detection-activated Visual Surveillance Systems (VSS), whether they are permanent or temporary/portable. It is aimed at VSS companies and their installation and maintenance engineers.

The standard is relevant regardless of how long the VSS is installed or whether its equipment can be reused at different sites. It outlines recommendations for two types of systems: Type A and Type A+. The choice between these depends on a threat assessment and risk analysis, considering the potential threats and consequences of incidents. Type A sets the basic standard for all systems covered by this scope. In contrast, Type A+ includes all the Type A recommendations and additional security features to enhance protection against system compromise.

Note: The references to the BS IEC 62676 series of standards in BS 8418 are referred to as the 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 health and safety aspects 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 following BS 7858.

Consider the effects of light/noise pollution on the local environment; The Clean Neighbourhoods and Environment Act.

The requirements of the Private Security Industry Act, e.g. monitoring, recording and use of VSS in private & public places under contract.

Pay attention to the Data Protection Act requirements, e.g., customer records, retention of recorded images, etc.

The Information Commissioner's Office (ICO) VSS Video Surveillance code of practice for surveillance cameras and personal information.

Surveillance Camera Commissioner's (SCC) Surveillance camera code of practice.

3. VSS system planning and design considerations [4.1]

- A threat assessment and risk analysis should be completed before design.
- An Operational Requirement document addressing the customer's needs, threat assessment, and risk analysis. It should describe the needs, justification, and purpose of the VSS system. [4.1 & 4.2]
- The VSS system operational requirement should conform to BS EN 62676-4.- *Clause 5 - "Operational Requirements specification".*

4. VSS system design proposal and specification [4.2]

- A documented VSS system design proposal and specification that meets the operational requirement should be created to address the following:
    - 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 VSS 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. [5.12 & 4.2]

5. System design – [5]

- Detection devices should be installed and configured following the manufacturer's recommendations/instructions and meet the operational requirements. [5.1]
- The detection device activation area should cover (and not overspill) the field of view of the corresponding camera. [5.1]
- Unless it is unsuitable, the detection areas should be positioned within the camera(s) field of view, allowing the Remote Video Response Centre (RVRC) to observe the reasons for activations. [5.1]
  - Situations in which it is deemed unsuitable for positioning a camera over a detection area include instances, where a motion detection device is placed inside public restrooms, with the corresponding camera(s) focused on potential entry/exit locations, or when a motion detection device is set up within a private residence, with any related camera(s) monitoring potential entry/exit points. [5.1]
- When a detection device is oriented towards a boundary, it must be situated in a manner that prevents the detection of movement outside the secured area. [5.1]
- Multiple detection devices should not be connected to one single input unless the RVRC can individually identify each detection device connected to it. [5.1]
- In scenarios where wireless or partially wired detection devices are utilised, any loss of communication between the control equipment and a device should be indicated to the individual setting the system. [5.1]

  NOTE 3 The integration and management of detection devices via an intruder alarm control panel typically offer several advantages: [5.1]
  - Activation and deactivation of the system using a PIN, a digital key (like a proximity fob), or an application;
  - Provision of both primary and secondary power sources for the detection devices;
  - Distinct recognition of each detection device's triggers;
  - Facilities for both engineer and user to conduct walk tests;
  - Option to exclude certain detection devices;
  - Conducting soak tests on detection devices;
  - Record and review a history of various events (system activation/deactivation, alarms, omission, etc.).

Note: This becomes especially pertinent in cases where a functional camera is set to switch between multiple preset positions based on the location of the detection device or the site of an occurring event. Under such conditions, the device must signal independently at the RVRC. Without this, it's impossible to ascertain if two incidents have happened in close sequence. [5.1]

6. Camera positioning and configuration [5.2]

- Cameras should be installed to allow visibility of the zones covered by detection devices. The representation of a person on the screen must adhere to the requirement cited in BS EN 62676-4, Section 6.7, depending on the specific purpose (identification, recognition, observation, or detection), with detection as the basic requirement. Cameras should, as much as possible, avoid capturing public spaces.

NOTE: Privacy masking can be employed to avoid accidental surveillance of areas not meant to be monitored.

7. Illumination [5.3]

- The areas within camera view should be sufficiently lit to enable an RVRC operator to confirm whether or not a human figure is present during daylight hours and, if necessary, in dark conditions.

8. Audio challenge (where installed) [5.4]

- Actions should be taken to avoid noise pollution beyond the site boundaries.
- An audio challenge facility may be required to obtain a URN for police response (without distortion) in all detection areas.

9. Data transmission system [5.5, 5.5.1 & 5.5.2]

- The data transmission system needs to be capable of streaming live video continuously until the RVRC operator disconnects. [5.5.1]
- At least one pathway for data transmission must be established as a means of communication between the VSS and RVRC, as specified in the SDP, with a maximum delay of 24 hours for reporting path failure. [5.5.1]
- In the event that the data transmission cannot connect to the RVRC, the system should attempt to re-establish this connection. [5.5.1]
- The likelihood of physical or cyber threats to the transmission system should be evaluated. If necessary, enhanced resilience should be implemented, for example, by adding more transmission paths, setting a shorter time frame for reporting transmission path failures, and incorporating a VPN or encryption. [5.5.1]

  NOTE: Be aware of relevant data protection laws. [5.5.1]

- Should alterations to the VSS data transmission equipment be necessary, the RVRC must be notified about the changes affecting the monitoring response, and the impacted components should be tested in collaboration with the RVRC. [5.5.1]

- A malfunction in a Type A+ system data transmission system should be reported within a maximum timeframe of 10 minutes. If the threat assessment and risk analysis indicate a requirement for greater resilience against failure or compromise, consideration should be given to implementing a secondary transmission path. [5.5.2]

10. Fault recognition [5.6]

- The system should be able to monitor faults locally when the VSS system is unset, and by the RVRC when set [5.6 and Table 2].

11. Video integrity [5.7]

- The connection of camera signals from the camera to the control equipment should be supervised for any loss of video. In cases of video loss, it should be distinctly displayed on-site, for instance, on a monitor by showing a 'no picture' or 'video loss' message.

12. Control equipment integrity [5.8]

- Control equipment must be situated within the monitored premises or area. To prevent unauthorized access to the configuration or operation settings of the control equipment, a robust validation process should be employed, such as a unique password or an electronic key.

NOTE: Be mindful of the applicable data protection laws.

12.1. Type A+ systems [5.8.2]

- Type A+ system-based control equipment ought to be placed in a specific zone within the supervised premises, ensuring access is limited and available only to authorized personnel. [5.8.2]
- For a type A+ system configuration of the VSS should enable its status (whether set or unset) to be ascertainable by the RVRC. [5.8.2]
- In instances where the RVRC has the capability to modify the type A+ system configuration, the adjustable parameters should be defined in an agreement between the VSS company and the RVRC, and this information should be communicated to the customer [5.8.2]

13. Event log at the supervised premises [5.9]

- Event logs in the control equipment must be kept on the supervised premises, recorded in a format that allows for retrieval by date and time. At a minimum, the event log should contain:
  - activations of detection devices;
  - alterations in system status, such as set, unset, or part-set;
  - omissions of detection devices; and
  - any faults

14. Power supplies [5.10]

- An alternative power source, or multiple sources, should be in place for detection devices or semi-wired detection devices, ensuring they can operate for at least 30 minutes in the event of a primary power source failure. [5.10.1]

  NOTE: It is recommended to also provide an alternative power source for supporting equipment like control equipment, cameras, and lighting. If a battery is employed as the backup power source, the installation date should be noted. [5.10.1]
- When an Uninterruptible Power Supply (UPS) is required as per the Operational Requirement (OR), it must be capable of sustaining the VSS control equipment and the data transmission devices to the RVRC for a minimum of 30 minutes after the main power source fails. UPSs or standby batteries, as specified in the or, must have adequate capacity to operate the necessary equipment. [5.10.1]

  The following, if installed, should be backed up by a UPS or standby battery: [5.10.1]
  - NVR/DVR;
  - Analytic servers;
  - Alarm control panel and data gathering peripherals;
  - Network switches and routers; and e) Alarm and VSS transmission equipment. Power supply issues should be reported as outlined in Table 2."

14.1. Type A+ systems [5.10.2]

- Monitoring of power supplies should include checks for faults in the primary power source, backup power source, charger, and outputs. These faults should either be identifiable for each individual power supply or through a single common fault indicator specific to each power supply. [5.10.2]

- Wireless components, like wireless detection devices and keypads, ought to have a primary power source (such as a battery) that is capable of continuous operation under all expected operating conditions, lasting at least until the next scheduled maintenance. [5.10.2]

15. Setting and un-setting [5.11]

- The design of the system should avoid triggering alarms during the process of arming or disarming, except in cases where it's specifically agreed in writing (for instance, if monitoring people or traffic is necessary for observation during certain operational procedures).
- There should be a clear indication for the individual arming or disarming the system to confirm its successful activation or deactivation.
- The system should not allow arming if there are any faults or if any detection device is in an alarm state. However, a user can override this block, but this action must be recorded in the event log at the monitored location.
- In scenarios where the system is set or unset automatically, these actions should be scheduled for times after the premises have been vacated and before staff are due to arrive, respectively. This process must be clearly outlined, agreed upon by both the customer and the company, and then communicated to the RVRC.

NOTE: This implies that the premises may be left unsecured during certain times each day. It's recommended to adjust the automatic settings during holiday periods like bank holidays when staff might not be present at the premises.

16. Installation [6]

- Refer to BS 7671 for guidance on wiring and connection of electrical installations. As an example, within BS 7671, clause 521.10.202, it is required that all cables are adequately supported to prevent early collapse in case of a fire, applicable throughout the entire installation. [6.1]
- Extra-low voltage and signalling cables should not be run in ducts or trunking containing low voltage mains cables, or alongside them, unless they are screened, insulated, or separated. [6.1]
- Where feasible, extra-low voltage cables should avoid entering equipment enclosures through the same entry as low voltage mains cables. [6.1]
- The type and size of cables used should be appropriate for their intended use, considering factors such as the equipment manufacturers' recommendations, transmission rate, electrical interference, and voltage drop. [6.1]
- For ease of future maintenance and servicing, cables should be clearly marked at termination points, interconnections, and junction boxes. [6.1]
- Cables that are used for fixed interconnections should be mechanically supported and, in areas where they might be accidentally damaged or intentionally tampered with, should be given mechanical protection. [6.1]

NOTE: This labelling can be organized in a cable schedule or shown on a schematic diagram. Tamper detection/security [6.2]

17. Tamper detection/security [6.2]

- Methods for detecting and signalling tamper conditions, as outlined in Table 3, should be implemented. These tamper alerts should be either audible, visual, or both. Additionally, local tamper indications at the supervised premises should be made apparent to the individual responsible for arming the system. [6.2.1]
- Opening the device used for arming or disarming should not interfere with the proper operation or alter the status of the VSS system. NOTE: Devices used for setting or unsettling the system can range from keypads and digital key readers to biometric and remote devices.

18. Detection [6.3]

- Installation and configuration of detection equipment must follow the guidelines provided by the manufacturer.

  In terms of placement, the detection equipment should:

  - be mounted stably;
  - provide coverage for the area outlined in the SDP;
  - avoid extending beyond the limits of the premises, the area intended for protection, or the camera's field of view; and
  - fulfil the functional needs specified in the OR."

19. Camera [6.4]

- Installation and configuration of cameras must to be inline with to the manufacturer's instructions.

  Regarding the placement of cameras:

  They should be securely mounted.

  NOTE 1: This is crucial to prevent false activations, especially when using video motion detection or analytics.

  - Cameras should be situated away from potential sources of false alarms or anything that might block their view, like insects, cobwebs, or precipitation.
  - Placement should align with the SDP.
  - Cameras must be positioned to ensure their field of view encompasses the related detection area.
  - Cameras should be situated where feasible to avoid overseeing neighbouring properties or public spaces.
  - Privacy masking should be implemented as needed.
  - The camera placement should satisfy the functional needs outlined in the OR.

  NOTE 2: BS EN 62676-4, Section 15.2 provides additional guidance on camera installation.

20. Control Equipment [6.5]

- Except for devices used for arming or disarming, all control equipment should be situated within the monitored premises or area, following the guidelines stated in section 5.8. Furthermore, this equipment should be installed and set up as per the manufacturer's instructions.

21. Response plan [7]

- A formal agreement, known as a response plan, should be established, and agreed upon by the VSS company, the customer, and the RVRC.

  At the very least, this response plan should cover:

  - the procedures the RVRC will follow in response to an activation and/or fault (refer to Annex F);
  - any routine remote patrols conducted by the RVRC using the VSS;

- circumstances under which the RVRC would exclude certain detection devices or cameras;

NOTE 1: The RVRC may have policies for temporarily excluding problematic detection devices.

- any reports that the RVRC is expected to provide.

NOTE 2: These reports might encompass activations, faults, and exclusions of detection devices.

- The VSS company is responsible for providing the customer with a copy of this response plan

22. Inspection, functional testing, and commissioning [8]

- Commissioning must encompass both visual and functional checks to ensure that: [8.1]
  - the system has been installed precisely as per the agreed operational requirement (OR) and/or the system design proposal; and [8.1]
  - it adheres to the commissioning guidelines specified in this British Standard. [8.1]

A detailed plan for system testing should be agreed upon, and selected tests should demonstrate at handover that the VSS complies with, an agreed System Design Proposal (SDP), including aspects outlined in the OR. [8.1]

Commissioning should be carried by following the procedures set out in 8.1 and Annex G.

NOTE: Testing methods described in BS EN 62676-4:2015, Annex B and Annex C, are useful for objective assessments to confirm system performance. Their application is subject to agreement between the customer and installer and is not mandatory for every installation. Alternative testing methods are also acceptable. [8.1]

- Upon the completion of commissioning, the VSS company must provide written confirmation to the RVRC that the system is fully operational, and the RVRC is prepared to commence monitoring of the premises. [8.1]
- A checklist incorporating the criteria outlined in Annex G should be completed, and its outcomes documented. Any components of the VSS that fail to meet the checklist standards upon inspection should be appropriately adjusted and subjected to a subsequent review. [8.2]

  NOTE: While it's essential to review the criteria specified in Annex G, the format of this evaluation can differ from the sample template provided in Table G.1. [8.2]
- A comprehensive demonstration of the VSS is required, showcasing how detection operates, the camera's field of view and the image quality under both daylight and dark conditions. [8.3]
- Additionally, there should be an explanation of the VSS's functionalities, including, if applicable, communication protocols with the RVRC. [8.3]
- Users should be provided with clear and straightforward operating instructions, covering both general operation and specific details on arming, and disarming the VSS. [8.3]
- Based on the VSS's complexity, user training on its operation might be necessary. This training should focus on preventing false alarms, for instance, by emphasizing regular maintenance of the monitored area, such as keeping it free of loose debris, managing overgrowth, and ensuring proper lighting. [8.3]
- Documentation, initially based on the System Design Proposal (SDP), should be revised to incorporate any VSS design changes identified as necessary during installation. The 'as-fitted' document needs to accurately reflect the final installation of the VSS, including detailed information on the equipment installed and its placement. This documentation should also include specifics about the types of cables used and their routing for more complex or larger VSS installations. [8.4]
- To ensure compliance with the Operational Requirement (OR) document or SDP, the VSS company should provide day and night reference images of the detection areas. These images should be kept on-site, regularly updated as needed, and compared with those stored at the RVRC during maintenance visits. [8.4]

23. Document and records [9]

- The client or user should be supplied with the following documents:
    - The Operational Requirement (OR) document or System Design Proposal (SDP), as referenced in section 4.2;
    - The response plan agreed upon as per Clause 7;
    - The system test plan, detailed in section 8.1;
    - User acceptance documents and/or completion certificate, as mentioned in section 8.3; and
    - The as-fitted document is outlined in section 8.4.
- Additionally, the installer is responsible for providing the RVRC with a copy of the response plan and the reference images.

24. Maintenance [10]

- Maintenance Agreement and Routine Visits for the VSS - Scheduled preventative maintenance ought to be performed on-site at intervals agreed upon, which should occur no less frequently than twice a year. The initial maintenance visit is to be arranged within the first six months following the commissioning date. [10.1]
- There should be a documented agreement between the customer and the VSS company outlining the criteria for both preventative and corrective maintenance (responding to faults) of the VSS. This agreement should also specify the response times for service calls. [10.1]
- Actions of the VSS Company Maintenance Engineer - Upon arrival at the site, the maintenance engineer must notify the RVRC that maintenance or repair work is about to commence. [10.2]
- During each visit to the monitored premises, the maintenance engineer needs to assess the following: [10.2]
    - Any alterations in the building or site layout that might impact the system's functioning and [10.2]
    - Any environmental factors that could compromise the system's reliability. [10.2]
- All necessary corrective measures should be documented and agreed upon with the customer.
- The engineer must compare the image from each camera and detection area with the stored reference images and system specifications in coordination with the RVRC. If needed, new reference images should be created, stored locally and also at the RVRC.
- The cameras should be cleaned, and their brackets inspected and secured as necessary.
- The engineer is responsible for checking for updates to control equipment, which could be product-specific or related to software, including any antivirus software.
- Image recordings should be verified under daytime and nighttime conditions to ensure they match the specifications regarding duration.
- A comprehensive check of the transmission from all devices is essential to confirm the accurate reception of alarm notifications at the RVRC and on the local control equipment. This includes checking audio transmission, whether directional or bi-directional.
- If changes to the VSS or the configuration of the transmission equipment are necessary, the RVRC must be informed about the changes that impact the monitoring response. The affected components should be tested up to the RVRC, with all alterations documented and the as-fitted document updated.
- Upon completing the maintenance, the engineer should inform the RVRC and have all documentation signed off by an authorised person from the supervised premises.

25. Additional documentation

- NPCC Police Requirements & Response to Security Systems Policy or Police Scotland policy.
- User guide to a BS 8418 Detection activated remotely monitored VSS system. - https://www.bsia.co.uk/publications/video-surveillance/
- BS EN 62676-4 Video surveillance systems for use in security applications. Application guidelines.
- Form 219 - 'BS 8418 – Publication 219 - A Basic Guide to BS 8418 VSS Systems for Installers' is available from https://www.bsia.co.uk/publications/video-surveillance/
- Clean Neighbourhoods and Environment Act 2005 - https://www.legislation.gov.uk/ukpga/2005/16/contents
- Information Commissioners Office - https://ico.org.uk/
- Surveillance camera code of practice - https://www.gov.uk/government/organisations/surveillance-camera-commissioner/

This document was created by the VSS 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.

VSS has had a profound impact on crime prevention and detection. The UK leads the way in the application of VSS 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 VSS, 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 VSS 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.

VSS 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 VSS companies drive best practice in this area and can provide advice on how VSS 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.

About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.