RISCAuthority

administered by FPA Fire Protection Association

S23 Guidance for specifiers of Video Surveillance Systems (VSS) in security applications

Version 2 Published 2022

Acknowledgements

The assistance of various partnering stakeholders in the preparation of this guide is gratefully acknowledged. Contains public sector information licensed under the Open Government Licence v2.0. Permission to reproduce extracts from British Standards is granted by BSI Standards Limited (BSI). No other use of this material is permitted. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop.

Contents

Summary of Key Points

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The table below summarises the key points of the document.

Need for clear rationale	• VSS is a highly effective, flexible security solution which is usually more cost effective than the equivalent level of security offered by on site security personnel but it is not a panacea and there must be a persuasive rationale for its selection in favour of other, more conventional, techniques.
Privacy dimension	• Unlike other solutions, privacy is an important issue demanding the close attention of the system owner.
System requirements must be clearly understood	• A decision to opt for VSS should not be taken until it is determined through a thorough risk assessment whether the system is to be monitored, if so by whom, the nature of the response and whether images are to be recorded.
Technological advancement	• VSS has made significant strides through digital technology with much improved picture quality and, in particular, the ability to employ sophisticated image analysis.
Complexity and customer satisfaction	• The technology has more complexity than traditional security measures and owners would be well advised to be fully involved at the design and commissioning stages to ensure that results, under all conditions, meet their expectations.
Detector-activated VSS has potential	• Detector-activated VSS systems monitored at a remote video response centre, which are predicted to grow in popularity, allow intrusion to be detected and observed without the need for continuous on site monitoring or expensive guarding.

Symbols used in this guide


Good practice


Bad practice


Discussion topic

Frequently asked question

1 Introduction

This guide describes video surveillance systems (VSS), also known as CCTV (closed-circuit television), technology and practice in security applications. Readers with limited technical knowledge of the subject will benefit through gaining a better understanding of the subject and the issues of relevance to customers and specifiers. In particular, specifiers should be better equipped to recommend and specify systems with a sufficient grasp of the subject to allow them to liaise and negotiate confidently with VSS providers.

2 Scope

The guide sets out to provide an appreciation of all the elements of the subject felt to be of most importance to a risk management advisor, an insurance surveyor or a reader with similar objectives and level of knowledge (as contrasted with a specifier such as a VSS consultant responsible for designing a system in the fullest technical detail).

Since such a reader is likely to have a particular interest in the reliable detection of, and intervention in, intrusion into a target area (a 'secure area') by persons intent on theft or causing damage or disruption, the guide provides an in-depth look at detector-activated VSS (abbreviated to DA VSS in this guide). However, the specifier of a DA VSS system needs to have an appreciation of the wide range of considerations applicable to all VSS systems and therefore, before DA VSS systems are specifically dealt with, the guide first explores some important basics of VSS systems – those that need to be taken into account when specifying and managing any/all types of VSS applications.

3 Basics of VSS systems

Understand and think about the basics before taking a decision to proceed

3.1 Overview

The main property that defines a VSS system is that it is 'closed' – meaning the system transmits signals to a pre-determined location rather than being 'open' and available to anyone with a receiver (as in broadcast TV).

Thus, at a fundamental level, closed-circuit television is a means of providing images from a television camera for viewing elsewhere via a dedicated transmission system.

In a security context an overt VSS system's basic purpose is to deter potential wrongdoers and, if that fails, to facilitate an intervention and/or apprehend and prosecute offenders, even if this is after the event. To achieve this there must be at least one camera, a transmission link, a viewing screen (monitor) and/or recording device.

3.2 Privacy issues

Video images of individuals captured on systems at places to which the public have access, eg in a public building or a street but also at such locations as a retailer or leisure facility, are deemed 'data' as far as the Data Protection Act (DPA) is concerned. Operators of VSS need to observe the legally enforceable data protection principles in the DPA and reference the Information Commissioner's VSS Code of Practice. These days they need also to be familiar with the Surveillance Camera Code of Practice, developed by the Surveillance Camera Commissioner as part of the Protection of Freedoms Act 2012. The codes are similar in the way they approach the key issues impacting privacy. Further information is provided in Appendix 1.

3.3 Potential roles and applications

Table 1 contains a few examples of how effective use is often made of VSS, monitored both on and off site. Certain of these applications (for example, where there is target property in the open) may also be effectively protected by DA VSS systems, described in detail in section 4, where additional examples are suggested.

VSS can be relatively expensive to install and maintain. It is technologically advanced and may be a challenge to manage and operate successfully. With that in mind, the questions that must always be asked are:

- is VSS necessarily the best or only way forward?;
- what is it I need to see?;
- why do I need to see it?;
- do I need to be sure to see it as it happens?;
- who will observe the images and where?;
- what response is required to events observed?;
- who will make that response?; and
- do the images need to be captured on a recording device?

In arriving at a decision as to whether to pursue a VSS solution, specifiers need to ensure they thoroughly understand the security hazards being addressed and whether the case for VSS over competing solutions is clear. The tendency to see VSS as being an 'easy way out' or 'the silver bullet' must always be open to challenge.

There may be a strategy providing better and/or more cost effective protection using tried and tested measures such as physical devices and barriers, premises intruder alarms, perimeter barrier security, lighting, threat removal/reduction etc. These conventional solutions often need to be considered in place of, or as adjuncts to, VSS.

Situation	Hazards	VSS system function
Open (eg unfenced) site	Trespass, theft, vandalism, arson	Monitor behaviours and actions
Closed (eg fenced) site	Vandalism, arson, sabotage	Detect unauthorised/suspicious persons, observe behaviours and actions
Premises interiors	Theft, dishonest staff, espionage, sabotage, vandalism, arson	
Entrances	Inadequate access control	Observe compliance with secure procedures, detect abuses such as 'tailgating' and wedging open, facilitate admittance of legitimate visitors, operate automatic number plate recognition
Sensitive secure operations	Hold up, personal attack, hostage taking, extortion, disruption, espionage	Monitor for suspicious behaviour and potential threats, display environment to subjects, monitor dynamically upon operation of alarm device
Vulnerable personnel	Hold up, personal attack, hostage taking, assault, stalking, interference, nuisance	
Vulnerable/target asset	Theft, disfigurement, destruction, sabotage	Monitor behaviours and actions threatening the asset(s), track attacker(s), monitor exits
Where automatic alarm systems are installed	Inadequate information to validate an alert as a confirmed alarm	Confirm activations with images

Table 1: Some typical uses of VSS

Carry out a thorough risk assessment

- What are the values at risk and/or consequences of loss or damage or exposure of intangibles or persons?
- Determine the history of security breaches, methods of attack etc.
- Identify the means of access/escape and ease of removal of property.
- What is the level of natural surveillance by occupiers?
- Are security guards present when the premises are otherwise unattended?
- What access do the public have and when?
- Assess the character and crime record of the location/immediate surroundings.
- What are the environmental conditions?
- What value is there in the existing security – eg strength of perimeter barriers?

3.4 Risk assessment

Again, the specifier must always have a credible rationale for the purpose of installing a system. The objective of the whole system and each camera must be clear. An holistic approach is needed, taking into account that all the elements of a system must be optimised and harmonised to the defined security requirement – lighting, security of interconnections, image handling and recording devices. VSS technology is an excellent example of how the results hang on the strength of the weakest link.

Before work on system design can start an analysis of the threats and hazards needs to be completed. These need to be identified and assessed in terms of likelihood and impact. This will allow a design to take shape tailored to the individual and unique requirements of the location. The logical steps in risk assessment for VSS will include those in the adjacent panel. The conclusions of the risk assessment will inform a high level 'Operational Requirement' (see section 3.6) and the final form of the system – subject also to the application of any standard or code of practice.

3.5 Standards and industry codes

The national (BSI) standards for VSS comprise a suite in the series BS IEC 62676. This is applicable to the use of VSS for all security purposes except, (in the UK), the detector-activated application, which has its own standard, BS 8418. The 62676 suite is incomplete as this guide is prepared. There are also two standards dealing with the responsible management and operation of VSS, chiefly in a privacy context, and one addressing recordings to be used in evidence. See appendix 3 for details of standards and guides.

For some years prior to the introduction of these standards specifiers could rely only on such codes of practice as were published by inspection bodies. Currently these are the National Security Inspectorate's (NSI's) NCP 104 Code of Practice for the Design, Installation and Maintenance of VSS Systems and the Security Systems and Alarm Inspection Board's (SSAIB's) SS 2003 Code of Practice for Closed Circuit Television Systems. Conformance with the contents of these codes can give the specifier and operator a degree of comfort that good practice is being followed, particularly where there are currently gaps in standards or uncertainty over their application.

Four "Grades" reflecting fours levels of risk are specified for VSS systems:

- Grade 1: low risk – there are no requirements for the level of protection and no restriction on access;
- Grade 2: low to medium risk – low level of protection level and low restriction of access;
- Grade 3: medium to high risk – high protection level and high restriction of access; and
- Grade 4: high risk – very high level of protection and very high restriction of access.

These grades govern the security, integrity and resilience of a VSS system in terms of, for example, resistance to unauthorised interference, functionality, utility and quality (of outputs). As a generalisation, specifiers will find that the requirements and recommendations at grades 3 or 4 are more appropriate to significant or onerous security risks whilst those at grades 1 and 2 are more appropriate to situations with a requirement merely for informing the operator of non threatening conditions or events at the location.

An important distinction between the BS/European VSS standards and the BS/European standards for intruder and hold-up alarm systems (I&HAS) is that, due to the need to tailor VSS to the widely variable circumstances of each location, the components, sub-systems and functions of a VSS system are permitted to have different security grades within the one system. This complicates the risk assessment exercise and the application of any process for the approval of systems, eg through a certification scheme.

For this reason, and because the whole field of VSS is in a state of flux in the UK and Europe, at present the certification schemes of the inspection bodies (NSI and SSAIB) do not call for their approved installers to observe to the letter Part 1 System Requirements of either series (although in their codes of practice they do 'call up' Part 7 (IEC 62676-4): **Application guidelines** which gives recommendations and requirements for the selection, planning, installation, commissioning, maintaining and testing of VSS systems in security applications).

3.6 The Operational Requirement

It is important that a high level Operational Requirement be developed at an early stage. For the sake of brevity, from this point and throughout the remainder of this guide, the term Operational Requirement is abbreviated to 'OR'.

The OR sets out an overview of the key objectives and operations of the proposed system. It is good practice for the OR to open with a concise statement of the security challenge(s) facing the site that the VSS system is intended to address. It should thereafter consist of a number of statements under headings that reflect the key issues governing the design of a potential system. It should be concise and succinct. BS EN 62676-4: **Video surveillance systems for use in security applications. Application guidelines** contains a comprehensive list of topics to be considered for inclusion in an OR.

No two cases will be the same and the exercise is a good discipline that crystallises the goals and possible snags. It also has the benefit throughout the design stage of bringing stakeholders back to the object of the exercise, as it is all too easy to be deflected.

With the aim of achieving consistency in the terminology used by the parties involved in the crime prevention and VSS sectors five categories of imaging objectives have been defined. Use of these terms helps the system designer to understand the attributes of the VSS image that will be required to meet the objective. These are as follows:

1. **Monitor and control**: At this level of detail an observer can monitor the number, direction and speed of movement of people across a wide area such as a car park.
2. **Detect**: The presence of a person in the field viewed is clear, eg in a space such as a yard expected to be unattended.
3. **Observe**: Some characteristic details of the individual, such as distinctive clothing, can be seen, eg to establish that smokers clustered at an exit appear to be staff rather than strangers.
4. **Recognise**: Viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before – as is necessary, for example, to control access to the premises.
5. **Identify**: Picture quality and detail are sufficient to enable the identity to be established beyond reasonable doubt as would be desirable for evidential purposes.

When these picture 'standards' were first introduced they used picture height benchmarks, ie the percentage of the screen occupied by the target figure (currently assumed to be 1.7m tall). Today, the percentages for each benchmark are deemed to be:

- monitor and control: 5%;
- detect: 10%;
- observe: 25%;
- recognise: 50%; and
- identify: 100%.

Observe | Recognise | Identify

Figure 1

Whilst this measure is less valid as an indicator today as a result of improved resolution in some imaging technologies, the quality definitions themselves continue to be understood and applied.

The use of these terms in the OR when setting objectives for the system is encouraged as they will be understood and applied reliably by any competent, reputable VSS company (see Appendix 3: Regulatory framework and guides). For each task that the specifier wishes the system to perform there should be a written objective, ideally employing these terms or embodying them in performance standards tailored by the specifier. For example:

- '**detect** individuals approaching the stores building';
- '**recognise** known individuals requesting admittance'.

In addition, and if anticipated at this stage, the OR needs to capture all the remaining factors with which the system supplier and operator will need to become completely familiar. The following are a few examples:

- period of observation – during what hours is the protection required?;
- site conditions – eg site lighting, special problems with weather etc;
- monitoring and image storage – where, and by whom, will the system be monitored and operated?;
- response/intervention – eg is a voice challenge via local loudspeaker required? Will personnel be dispatched?

The influence on system design of these and other additional factors that might emerge will become clearer, and can be refined, following the VSS site survey.

Stretching a system beyond its capabilities drastically impairs results – use recognised terminology to establish system performance to match the Operational Requirement

3.7 The site survey

Assuming VSS has been identified as a solution, or potential solution, the location may need to be surveyed by the specifier (for a second time if necessary) specifically for VSS protection. The conventional security survey that preceded the VSS survey will have provided an overview of the physical risk, sources of threat and all relevant circumstances. The location can then be re-examined to start to formulate a strategy for a VSS scheme of protection.

It is not essential to arrive at a final design at the survey stage but the specifier should at least aim to be familiar with all the options for camera views, the selection of equipment and its operation. Having reliable notes and a marked up plan will greatly assist evaluation of proposals received subsequently from installers/consultants.

Ideally, sufficient information is recorded at this stage for the system provider to be able to select suitable cameras, and camera positions, to capture the scene in the required level of detail. The high level OR can be refined/fleshed out or revised during these activities as necessary. For example, will it be necessary to monitor the entire site or just pinch points or sensitive locations?

What function do you require the system to perform? There can be more than one requirement for a given space and each may require description as the technical requirements to meet each need may differ.

If the threats at the location could take different forms consider each scenario in turn. Will targets be persons who may be stationary, walking, running or in a vehicle? What speeds could be involved? Relate all the factors recognised during the survey to how a response would be made.

Take account of	
Environmental issues	topography, undulations in terrain, vegetation, growth of foliage over the year, position of the sun season to season, particularly east/west at sunrise/sunset
	reflection from laying water
	wildlife, animal runs
	local weather record, eg high wind, mist on moors, at coast, snow
Layout	configuration of structures, lines of sight, blind spots
	property in open – where? does it move?
	vehicles parked on site

Table 2

3.8 Specifying systems – technical issues

The overall quality of images obtained will depend upon the quality of the poorest element, be it the camera, transmission system, viewing or storage (recording) system.

A VSS system will normally include at least each of these:

1. camera (or cameras);
2. means of transmitting images between the camera(s) and designated location(s); and
3. viewing facilities at designated location(s).

Except for the most basic systems, control and/or recording equipment will also be necessary to meet the OR.

There is a large body of 'legacy systems' in service, ie those using the original, analogue VSS technology – images represented by continuous variation in the amplitude (or some other measure) of the electromagnetic wave energy generated inside the camera. Mainly in the last 10 years however, analogue technology has been largely superseded by digital technology and during this transition period a portion of the 'legacy' estate of VSS installations has formed into a third, hybrid, body of systems – originally analogue but now with compatible digital elements, to ensure that analogue data can be converted into digital data for better storage and recovery.

The development of corporate IT networks over local and wide area networks (LANs and WANs) has provided a new infrastructure for the conveyance of VSS to remote observers. Network video systems may be connected to existing network infrastructure or an independent parallel network dedicated to the VSS system. However, it should be borne in mind that video is greedy of bandwidth. The skills of the provider, eg in selection of products and compression technology (see section 3.8.4), and the owner's network experts will be required if the data load and security issues are to be managed to the satisfaction of the customer.

FAQ

Key terminology

- **What is 'focal length'?**

This has to do with the geometry of the lens and camera sensor which dictates whether the field of view captured by the camera is 'normal', (equating to the human eye), 'telephoto', rendering higher magnification and a narrower field of view or 'wide angle' rendering a lower magnification and a wider field of view. A lens with a variable field of view is a 'zoom lens'.

- **What is 'depth of field'?**

This is the distance over which a target remains in focus when moving towards or away from the camera. As an object starts to move outside the depth of field, either when moving towards, or away from, the camera, its image will become progressively more blurred.

- **What is 'resolution'?**

The performance of a camera in relation to the amount of detail it resolves. This dictates the ultimate quality and utility of the image available to the monitor and recorder, all other factors being equal. In the VSS business, language such as, 'high resolution' and 'high definition' is freely bandied about but in fact there are no VSS standards for what these manufacturers' claims translate to in terms of actual technical performance. See HD cameras.

- **What is 'sensitivity'?**

Denotes the performance of a camera according to the amount of light reflected from the scene. As the light falls past the level at which the camera produces an acceptable picture, the image becomes progressively more grainy and 'snowy' until no meaningful information is available. However, there is no consensus in the VSS business as to how these conditions should be measured.

3.8.1 Camera technology

The device at the heart of a standard VSS camera that captures the images presented by the lens is a CCD (charge coupled device) or CMOS (complementary metal oxide semiconductor) sensor. These convert the visible, infrared or thermal image into an electrical signal. The electronics in the camera produce an output video signal for transmission or viewing/recording in either analogue or, increasingly, digital form.

Analogue cameras

Analogue cameras generally provide a composite video signal, which is a scanned electrical representation of the image with timing and brightness information encoded into the signal. The timing is recovered at the monitor to synchronise the camera image with the monitor display and so enable a steady image to be viewed or the entire signal is recorded on to a video cassette recorder for later playback. Analogue cameras give acceptable results and are cost effective but digital technology allows camera designers to build in features that analogue technology cannot provide.

Digital cameras

In simple terms each picture cell (pixel) on the camera's sensor is assigned a number, in binary digit form, translating to the brightness (and colour, if applicable) levels of an image. The pixel information representing the image is scanned and processed to remove unnecessary information (to reduce network loading and storage requirements) and is then transmitted over the network as a series of frames to the display and recording elements of the system.

This management of the video output allows the image to be 'engineered', enabling additional information (metadata) to be added by the camera itself – for example, video motion detection (see section 3.8.9.1) and target tracking (see section 3.8.9.2). Furthermore, in very low light conditions, images can be enhanced inside the camera, affording better identification and recognition performance. Advantage can also be taken of the ability to record footage inside the camera (a fixed and/or removable memory card), known as edge recording, which thus, when connected to a computer, arguably becomes a complete VSS system in itself.

IP camera/network camera

An Internet Protocol camera, (IP camera or network camera), is a digital output camera specifically designed to work over a network – often the internet. It achieves this through having an on-board video server with its own IP address, capable of streaming the video. Being a digital device it shares all the versatility of any digital camera with the additional benefit of the ability to be set up and adjusted from a remote location and having remote 'maintenance'.

Furthermore, wired IP network cameras can be supplied with power over the LAN ethernet (PoE), a technology that enables power to be provided to a network camera using the same cable as that used for the network connection, thus eliminating the need for a mains power supply at each camera location.

Another advantage of IP video surveillance carried over a larger user's network is that the IT department already has the necessary expertise for implementing and maintaining much of the system. Since the cameras have IP addresses just like any other network device, IP networking in principle adds value to the existing infrastructure of servers, switches and cabling.

Monochrome and colour cameras

Both types are capable of broadly similar results and the benefits of colour pictures for image recognition and analysis are obvious – the presence of colour information adds huge value to the viewer's knowledge and understanding of what is displayed. That said, the colour camera is unavoidably less sensitive than the monochrome equivalent, giving mostly unacceptable night time results unless good lighting is available. Unfortunately, unlike the monochrome camera, the colour camera sensor is not sensitive to infrared (IR) light (see section 3.8.2). However, switchable colour/mono cameras are available where only IR illumination is acceptable at night, or necessary for covert surveillance.

Figure 2: Dome camera

Figure 3: Traditional PTZ camera with on-board IR lighting

Figure 4: If the OR is only adequately met by having constantly available fixed views, static cameras must be the choice

HD (high definition) cameras

Whilst there may be no actual industry standard in the VSS business defining 'high definition' as such, megapixel cameras of various, but increasing, resolution may be sourced making very high quality images available where essential – for identification for example. A state-of-the-art HD camera will be marketed as '1080p Full HD', a device that is, in fact just over 2 megapixels.

In addition to the higher resolution, these cameras allow wider angle images and the ability to digitally zoom without an unacceptable loss of quality. The picture quality allows suppliers to claim that a single camera with this resolution should be capable of viewing a wide area where previously several standard cameras would have been needed. However HD cameras are intrinsically less sensitive than standard cameras in that they require additional lighting to achieve high quality images in marginal lighting and at night. It is particularly important in this area to make every effort to verify manufacturers' claims of performance.

Pan/tilt/zoom (PTZ) cameras

PTZ cameras, also referred to as 'functional cameras' or 'fully functional cameras', can be directed remotely by an operator. The camera may be moved in the horizontal (panning or azimuth) and/or vertical (tilting or elevation) planes and, in addition, be adjusted for focal length (zoom – ie to make the target view appear closer or further away with the consequence, respectively, of narrowing or widening the angle of view). Most, but not all, functional cameras perform all three functions (panning, tilting and zooming). Only one or two of the three functions need be provided or operational if that would meet the requirement.

Traditional PTZ assemblies are still to be seen in operation but are being overtaken by the dome type format. Slow panning speed (sometimes a few degrees per second) was a severe limitation of early PTZ cameras. Depending on the age of the PTZ, quick and effective movement of the camera was aggravated by the size and weight of the assembly, further weighed down by the directional infrared (IR) lighting that older tube type cameras often had to carry to cope with low light conditions.

The introduction of the chip (CCD sensor) into cameras significantly reduced their size and weight. This allowed the speed and accuracy of PTZ cameras to be greatly increased. Nowadays, fast dome PTZs pan at up to 500 degrees/second and are capable of continuous rotation. At the same time, they can, if necessary, be 'inched' at extremely low speed without vibration.

An important feature of the present day dome PTZ is the ability to programme the camera to move to (or return to) pre-set views. In this way, the camera can pan, zoom in (or out) and automatically refocus on locations identified as critical in the risk assessment and OR. This can be under the command of the operator or when directed automatically through operation of an intrusion alarm detector.

Alternatively, so called 'auto tracking' cameras are capable of monitoring the change of pixels generated by the video chip. Pixel change due to movement within the field of view causes the camera to capture the point of variation and move the camera so that the source is always kept centred on the video chip. Electronics then optimise the size of pixel fluctuation as a percentage of the view.

A PTZ camera with pre-sets may have a 'home' location as defined in the OR. The camera may be programmed to automatically return to this 'parked' position pending a further incident requiring repositioning.

A PTZ camera can also be made to cycle through the pre-sets – holding at each position for a programmed period of time. It may be argued that one programmed PTZ can be allowed to take the place of a number of static cameras but, in practice, the results are invariably a compromise because a PTZ can only look one way at a time.

For obvious reasons, unless measures are taken to mask or limit access to views that are not legitimate for security monitoring, there is a greater risk of a privacy breach with a PTZ camera than with a static camera.

Figure 5: The observer might 'recognise' the individual but, for practical purposes, thermal images are unlikely to meet an acceptable standard for 'identification'

3.8.1.1 Specialised cameras

Low light cameras

Available light level will have a major influence on the choice of camera. In fact, most regular cameras can operate at quite low levels, eg below lux levels generally considered as the minimum for security observation. However if artificial light is limited, the camera and lens will need to be selected for the worse case light environment, as it is the lens and the sensor element in combination that determine the camera's low light performance.

In this context, artificial light does not necessarily include infrared sources, for which a different camera selection needs to be made to match the infrared response of the sensor to the lighting type. Enhanced sensitivity camera/lens combinations for low light (sub 1 lux) can be expensive and it is normally more cost effective to provide lighting sufficient for use of regular cameras. See also section 3.8.2.

Thermal cameras

Conventional cameras are unable to capture images in complete darkness. In common with the ubiquitous PIR intruder alarm detector, thermal cameras exploit the fact that thermal radiation is emitted from every object with a temperature above absolute zero. As with the humble PIR device, the greater the temperature variation in the field of view, the better the results, as the video image from the thermal camera will be clearer due to the greater contrast between the subject and the background. Thermal cameras are compatible with video analytics (see section 3.8.9.2), being insensitive to shadows, changing light conditions etc.

Thermal cameras also perform better in difficult environments such as smoke or fog, or where a target could be largely concealed, eg screened by vegetation or hiding in shadows. The camera's ability to detect thermal radiation makes it difficult for an intruder to escape detection in a scene that may be too large for the observer of a conventional image to resolve a target.

However the technology is not generally considered capable of performing 'identification' as such, so its application lies mostly in that of 'smart' incursion detection.

Miniaturised cameras

The quality of images from these tiny colour cameras, measuring just a few millimetres across, has made great strides in recent years and they find a wide variety of applications, some of the better known being their use in endoscopes, covert surveillance and to capture the image of an ATM user. Tiny cameras are also increasingly built into body worn cameras (especially of interest to the police and fire authorities) and incorporated into spectacle frames with the added benefit that the images match the actual scene being viewed by the wearer.

The miniaturised cameras, optics and high-power batteries developed for smartphones have given impetus to this rapidly growing sector of video technology. Some versions allow remote access to live video and GPS location information with obvious application for those working in risky roles or where groups of individuals need to be coordinated.

3.8.2 Lighting

3.8.2.1 Visible lighting

The qualities of the artificial lighting at the location govern the performance of the system during twilight and overnight use. As with the human eye, lighting is the key to good vision. As a basic principle, the more light, the better the results.

For a colour system, the lighting technology in use is as important as the quantity of light. This is because the colour rendition of different lighting types varies. Often, the system must be accommodated to existing lighting arrangements. It is vital that the specifier understands the effects of different technologies on colour VSS results, particularly where the types in use are mixed.

FAQ

Visible lighting technologies: how is VSS affected?

- tungsten and tungsten halogen lamps give excellent colour rendition and start up immediately on switch-on but are not economic for continuous use;
- most other types (gas discharge lamps) suitable for colour VSS have a start-up time of 1 to 12 minutes which prevents their use by operators as instantaneous sources;
- low pressure sodium lamps (yellow light) can be used only with monochrome systems;
- lamps suitable for colour systems include the metal halide lamp, some types of high pressure sodium lamp and the white light LED lamp (the state-of-the-art lighting technology);
- vandal resistant lamps and luminaires (light units) are available.

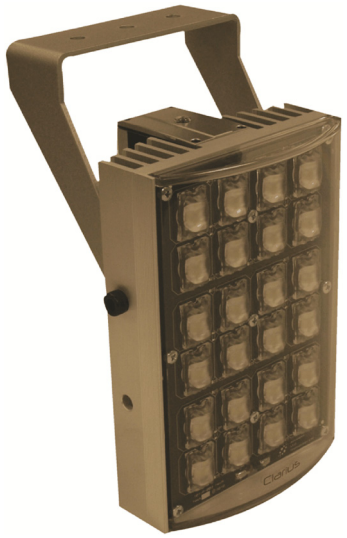


Figure 6: White LED illumination allows high quality images from colour cameras 24 hours a day (courtesy GJD Manufacturing)

Figure 7: White LED lighting switches on instantly (no start up delay)

Figure 8: Infrared illuminator (courtesy GJD Manufacturing)

Fortunately, this is not an issue for monochrome systems – they can live with all types of lighting in common use and can operate with much less light than colour systems. For this reason, so called 'day/night cameras' are frequently specified to meet the OR. These switch from colour to monochrome operation when the light falls to a level at which a monochrome camera, on balance, gives better results than a colour camera, albeit the absence of colour detracts from the ability to interpret certain content in images.

Street lighting levels, around 5 lux, are satisfactory. Most cameras can operate with much less. However, good lighting is a deterrent in its own right. Uneven lighting can actually assist an intruder by providing light to work with and shadows to hide in. Scenes and objects with low reflectance (dark walls, bitumen surfaces etc) will require more light than reflective surfaces.

As a general principle the scenes to be viewed and the facades of the buildings should be bathed in a good and even overall level of light. That way the intruder is ideally silhouetted against the sides of the buildings. That said, and subject to light pollution control, additional luminaires that face the expected direction of intrusion can have the effect of 'blinding' the approaching intruder.

However, the propagation of light, both visible and infrared, is subject to the inverse square law. This means that the intensity of the light is inversely proportional to the square of the distance from the source. Thus, for example, a target double the distance from the light fitting receives only a quarter of the light. Accordingly, wherever practicable, area lighting should be as evenly distributed as possible. Some types of lighting (especially LED) have precise beam patterns which cut off at the edges sharply. Care is therefore required with PTZ cameras that all potential views will be illuminated without unlit borders. For fixed cameras it is vital that the beam pattern matches the angle of the camera/lens set up.

Lighting can be switched on automatically by timer and/or photocell but the cheaper, domestic self-contained PIR-activated light fittings can have erratic performance and are often easily interfered with, so they should be avoided. Lighting must not be allowed to directly face a camera to avoid 'flaring' (a haze in the picture around the light source, or across the whole image, that degrades the information in the image).

For remote monitored systems linked to movement detectors, the lighting can be linked to the system so that it switches on just before the camera (to allow the iris to settle before images are transmitted) or the lighting can be operated from the monitoring point following activations.

3.8.2.2 Infrared (IR) lighting

IR lighting is a practical solution where visible lighting would be unacceptable or covert operation is required. Running costs are modest. IR lighting cannot be used in a colour system and monochrome cameras need to be selected for their IR response. As with visible light patterns the steep fall off in light intensity with distance from source can be countered with distributed free-standing IR lamps attached to the buildings to give even, general area lighting. Adverse weather effects can cause IR reflection and this should be taken into account at system design and commissioning stages.

There are many cameras on sale with IR LED elements surrounding the camera lens for a cost effective lighting solution. These cameras may suffer from the presence of insects which may obscure the image and expert advice should be obtained before they are considered.

3.8.3 Detection

In some circumstances the task(s) identified in the OR can be assisted if changes at the protected location are automatically brought to the attention of the observer(s) through automatic detection technology linked to the VSS system; the most obvious example of a change likely to require attention being the movement of objects or persons. It can be arranged that an event involving significant movement is brought up on a monitor screen hitherto dormant or showing a different view. It might also be made to register the change at any image recording device included in the system, eg uprating the quality of the recording for the duration of the event and 'bookmarking' the point on the recording at which the event occurred.

Detection technology of the type designed for intruder alarm systems (typically the PIR) may be used internally but, if used externally, it must be designed to withstand adverse weather conditions and function with as few false activations as possible from environmental factors. However there is a limit to how far the physics of the technology allows this and false triggering from events occurring in the monitored zone of an exterior detector are inevitable.

As an alternative to the versions of intruder alarm detectors modified for external applications the specifier may opt to explore the possibility of using Video Analytics and Video Motion Detection which may (or may not) offer better false trigger rates although the challenges of unwanted alerts are similar.

See Appendix 1 for a description of the detector types most frequently specified for external use with a VSS system.

(Note: the inclusion of event detection in a system does not, in itself, make it a detector-activated VSS (DA VSS) system in terms of BS 8418: ***Design, installation, commissioning and maintenance of detector-activated video surveillance systems (VSS). Code of practice****.*

3.8.4 Control, processing and image storage

At the heart of most systems will be a Digital Video Recorder (DVR) – probably one expressly designed for use with VSS. The amount of video a DVR can store is of course limited to a finite amount but capacities vary enormously between products and models. When the disc is full the oldest material will be overwritten with new. As a result, a key factor for the specifier to consider, taking account of the OR, is the capacity of the device. In addition, thought should be given to the possibility that sequences will at some point need to be replicated and taken off site, eg for use in a crime investigation and for this purpose inclusion of a DVD writer or equivalent provision may be desirable. Useful advice is to be found in 'UK Police Requirements for Digital VSS Systems', which is available on the internet for download.

A further factor to consider at the outset is the image retention time deemed necessary as this may have a bearing on the quality at which it is technically feasible to retain the images. A period between 14 and 31 days is normally suitable (see IEC 62676-7 for examples of how storage capacity can be calculated). See Appendix 2: Privacy Issues.

The specifier or user should understand the importance of challenging the system supplier as to the quality of the images that can be expected when viewing recordings as compared with the live images displayed on the monitor(s). If the supplier is relying excessively on a compression process (see below) when calculating necessary storage capacity, the user may find the recorded images unsatisfactory. It is important therefore to review the recorded picture quality and compare it with the live view before signing off a new VSS system.

Not only does such a DVR record the video from the cameras in a similar way to a home DVR, it also functions as the device where inputs and outputs are configured, processed and controlled. However the real time video signals from a number of cameras would soon fill the drive of even a high capacity DVR and, before this is addressed by the system designer, consideration needs to be given by both designer and customer as to the trade-offs that will probably be inevitable if images need to be held over realistic timescales.

In reality most security VSS systems do a perfectly effective job with some sacrifices made in image content compared with say studio or broadcast quality television. This is because the eye/brain combination does not detect, or disregards, subtle dislocations in scene changes or tolerates modest deficits in picture quality, provided what remains on screen is unambiguous. The following are the engineering options made available with VSS equipment to control the sheer volume of video data needed to display and record useable information:

Frame rate, sometimes referred to as 'update rate', is the rate at which each new complete image is built on the monitor screen. In the UK and Europe, the standard frame rate of real time broadcast television is 25 full frames per second (fps). The frame rate can be reduced by a surprisingly large factor before the eye discerns unacceptable jerkiness. For example, in most security applications, assuming a carefully placed camera and good quality equipment are in use, a frame rate of a minimum of six frames per second may be acceptable where a near-real time viewing rate is essential. If the target is likely to be fast moving, then a rate of, say, 12 fps may be necessary. Either way, the saving in captured/stored data is obvious.

A useful trick that will appeal in many insurance specified applications, where it is intrusion rather than behaviours that must be captured, is to make use, where provided, of a recording function that dynamically uprates an economical (low) frame rate to a high rate for a finite time following activation of an alarm sensor.

Frame rate is not to be confused with 'multiplexed/time lapse', available where many cameras are being recorded 'simultaneously' over very long recording periods. However, the relentless growth in affordable video storage capacity results in less use being made of this expedient but it may be an option provided the OR can still be met. The penalty is that when the time gap between each complete new frame is progressively increased, there is a point at which the information available quite clearly consists of separate still images and events will inevitably be lost.

Compression denotes a range of techniques designed to reduce (compress) the amount of data that need to be managed/retained for a given picture quality with the object of retaining as much of the original information as possible and minimising loss of information such as detail and colour. One method for example preserves information only when a change in the scene occurs, removing redundant or repetitive information and thus permitting the essence of what the camera is seeing to be captured for display, recording and/or transmission. There will come a point however where an excessive degree of compression will undermine the system's fitness for purpose.

3.8.5 Local interconnections

The connections between the control and processing equipment and the cameras are generally either a co-axial or twisted pair cable or short range radio or microwave link. Use of the correct cabling and care in setting up are crucial to performance. On very large sites, line amplifiers may be needed. Standard cameras need a local mains electricity supply. Alternatively, cameras are available that run on low voltage DC conveyed by the same multi-core cable that carries the video.

Unlike intruder alarm interconnections, unless special steps are taken, any failure of the video line may go unrecognised by the system (see section 3.8.8).

Operations running their own LAN (Local Area Network)/Intranet have the option of using their network for the VSS installation via, usually these days, Cat 5 or 6 wiring. These connections are capable of powering local devices such as IP cameras as can power over ethernet (PoE) systems which carry electrical power along with data on ethernet cabling, even over long distances.

3.8.6 Video transmission to a remote location

Subject to costs, medium distances might be bridged with radio, microwave, optical fibre or possibly other point-to-point methods.

Long range transmission requires the services of public networks, high speed broadband being the obvious solution. 3/4G cellular radio may need to be used in some applications and also finds use as a back-up (secondary) transmission path.

Distributed organisations with outlying sites interconnected, usually via VPN (Virtual Private network) IP connections through their own network, can allow local VSS installations around their branches to piggy-back on their network. The implications of network sharing, bandwidth usage and infiltration need to be addressed and difficulties/compromises are not uncommon.

3.8.7 Viewing images

The quality of the monitored image will be a limiting factor if it falls below the performance of the remainder of the system. Consequently selection of adequately specified monitors plus the form of display and the controls available are important. Ideally, the final selection of the monitor(s) on which images are to be viewed at the location should be made only after a representative selection of images has been displayed to site personnel for their assessment, including images in all prevailing light conditions and any multi-camera presentations or images subject to compression (see section 3.8.4) at the maximum rate that will be in use.

Figure 9: In practice, it is unrealistic to expect the continuous viewing of large banks of screens to be effective

Reference to the OR will influence the equipment selected. What purposes does the system serve? For instance:

- general surveillance;
- periodic, routine video patrolling;
- continuous observation of a critical location or object;
- observation in reaction to a specific event, eg access control, alarm condition;
- performance of other tasks when defined events are observed; and
- all, or a mixture, of these.

Monitoring an unchanging scene, or images requiring no action, for any length of time, is not a task that a viewer can perform with any reliability. Equally, monitoring more than a few (say five) screens, irrespective of what they show, is also stressful. The object is to sustain the attention of the operator and minimise the risk of the operator missing events that the system has been provided to report.

The size of the monitor should not be excessive, allowing for the display of multiple views where applicable. All things being equal, a modestly sized monitor will seem to provide a higher quality image than a large monitor. However, the size(s) of monitor(s) selected will hinge on the task, the anticipated contents of the picture and the comfortable viewing distance, which will be influenced by the ergonomics of the facility.

A ‘dark screen’ policy, whereby an image is displayed only when, for example, unexpected movement or an alarm condition has occurred, minimises operator fatigue and maximises the chance of the desired response. However, in some cases a scene is so important that it must be displayed continuously in which case it might be allowed its own dedicated monitor. Similarly, it is a benefit to have a screen available for separately tracking live events, allowing the other monitor(s) to continue to show their normal scenes.

Small, simple systems are frequently seen that use a video splitter or video switcher to display more than one camera view on a single screen. A quad video splitter simply splits a single screen into quarters allowing four cameras to be viewed/recorded simultaneously. Some splitters allow up to nine cameras to be displayed on a single screen. If event/alarm inputs are provided, a full screen image from the camera ‘in alarm’ can then be presented.

A video switcher can display each camera view for a fixed time in sequence before moving to the next view, or views may be selected manually. By this means an overview of multiple cameras can be maintained without each having to have its own monitor. The ‘dwell time’ (the time a given camera view remains on screen) can be determined by the operator. If required, alarm inputs can generally be added so that any scene in alarm will be presented and sequencing will be suspended. Failing that, events occurring at a time that the particular view is not on display are of course not observable. Sequencing can be maintained on a second monitor if one is connected. The operator should be able to exercise control whereby the display can be switched at will from one scene to another.

Systems are often purchased without the full implications of the demands made by the need for effective monitoring being recognised – what value does the system have if the monitoring arrangements cannot be relied on?

For the larger installation, in which more flexibility is required so that cameras outputs may be distributed in a wide range of permutations between various monitors and recording facilities (each with its own sequencing, dwell time settings, multi-image display etc) more sophisticated switching and video multiplexing is necessary. Many modern digital recording systems have a 'virtual matrix' built into them, thus reducing the physical system complexity.

There will be an unavoidable reduction in the quality of results presented for each camera view if many are displayed on a single screen but there might be case for doing this if eg the views are related spatially or in the sense of a given crime scenario, in which case, being able to observe fast moving developments, with minimum operator head/body movement, could be an advantage. However, splitting a screen into more than say four pictures requires careful assessment.

There are various ways the control equipment may interface with the operator; buttons, joysticks, PC mouse, touch-screen etc.

3.8.8 Tamper/sabotage protection

The owner or system specifier needs to consider the possibility and impact of sabotage. It might be suggested that, assuming the primary objective of the large investment in the system is to address a security vulnerability, the system itself is at risk unless anti sabotage measures are taken – mechanical protection and tamper detection. This should be integral to the risk assessment process.

The need for the following should be considered and specified if necessary. However, none of the following will necessarily be included by the system supplier, unless system grade 3 or 4 is specified *and* they are specifically called for in the OR itself:

- tamper detection circuits to be included and should be continuously monitored;
- indication of tamper to be provided at the location and notified to a responsible party beyond the location if transmission facilities have been provided or a connection can be made to another notification system (eg an intruder alarm system);
- vulnerable components such as pluggable connectors, control equipment and recorders should be located in a secure area or within tamper-monitored enclosure(s);
- if detectors are included (to alert the viewer to an incident) the housings containing their power supplies should be equipped with tamper detection to detect opening through their usual method of opening;
- tamper detection should be fitted to detect removal of cameras from their mountings and, wherever practicable, orientation adjustment; and
- housings containing fitted cameras should be equipped with tamper detection to detect opening through their usual method of opening.

In addition, BS EN 62676 Part 1 System Requirements requires the following:

- at grade 2 and above: report video loss;
- at grade 3 and above: report change in the specified field of view and deliberate camera masking; and
- at grade 4: report video substitution; significant reduction in contrast.

Equipment physically resistant to sabotage can be sourced if necessary to satisfy the risk assessment. Vandal, even ballistics, resistant camera housings and luminaires are available.

To an extent, if a totally vandal-hardened installation is required, reliance must be placed on the skill, ingenuity and motivation of the installer. For example BS EN 62676-4: **Video surveillance systems for use in security applications. Application guidelines**, calls for cameras to be installed in such a way that makes it 'difficult' for an intruder to change the field of view, eg through installing in a 'suitable' location/height, use of 'appropriate' physical mounting and by the use of security fixings. Interconnections (eg cabling, antennae) should not be accessible so they are easily 'torn off'. Clearly, if sabotage is a critical factor, the closest possible liaison between the specifier and installer is desirable for a satisfactory result.

Figure 10: Bosch MIC Series 440 explosion-protected PTZ camera (picture courtesy Bosch Security Systems UK)

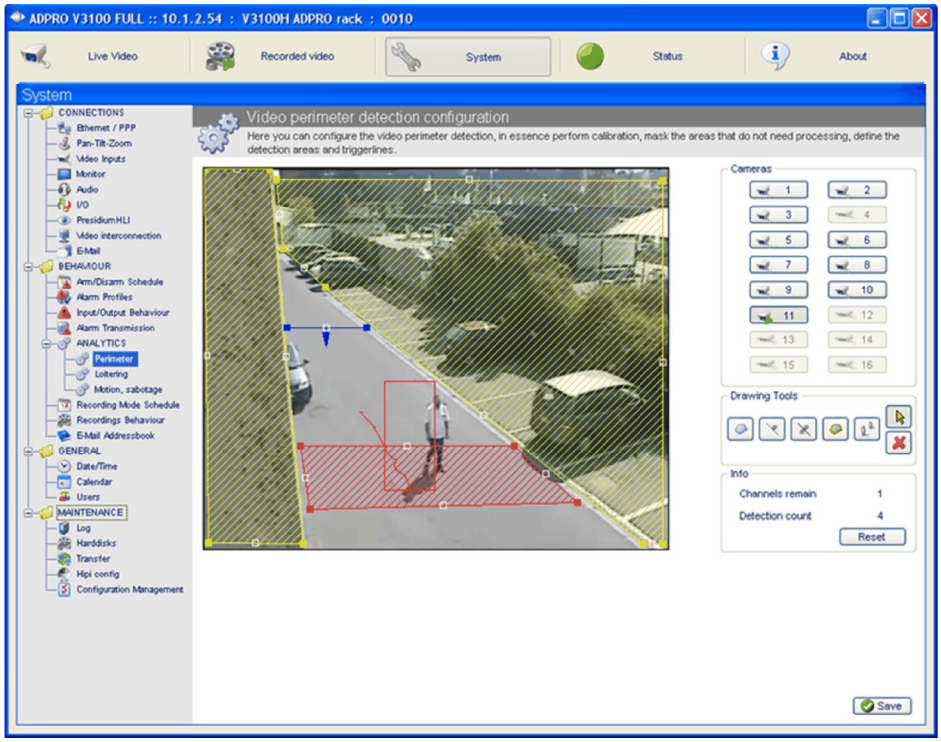


Figure 11: Intrusion detection: the operator delineates the zones in which detection is required

Figure 12: Here ADPRO LoiterTrace© software has alerted the operator to a loiterer

3.8.9 Video software applications

3.8.9.1 Video motion detection (VMD)

Video Motion Detection is an electronic method of detecting any changes in the field of view (or a selected part) of a camera by comparing each successive frame for differences in content. There are various proprietary methods of filtering to improve discrimination between objects/movement that need to be reported and sources of false alerts (eg division of the view into cells and analysis of successive changes in adjacent cells implying concerted movement across a scene) but the technology has moved on and evolved into what is referred to as Video Analytics (see following section).

3.8.9.2 Video analytics (VA)

This performs analysis on video information within selected zones in a more ‘intelligent’ way than simply registering movement (see previous section). It is capable for example of detecting loitering, eg persons, objects or vehicles remaining in an area for a suspicious time; removal detection: detects when an object has been removed; unexpected/unwanted behaviour, eg detects and tracks for the observer people or vehicles moving in the wrong direction, erratically, excessively fast. Software is available that ‘learns’ the normal patterns of human circulation in a street or park and thereby highlight and log behaviours of individuals who act or move in unusual ways.

A powerful attribute is the ability to calculate position allowing a target to be tracked over considerable distances via multiple cameras relative to a known layout. When employed with an on, or off, site monitoring service, a high degree of confidence can be had in the veracity of alerts. It is simple for this software to detect various camera tampering events including video loss. This, or similar, software can also be programmed to react to the ‘signature’ of flames/smoke.

This is a technology that is developing rapidly and caution should be exercised with regard to manufacturers’ claims. Systems tested and certified to ‘i-LIDS’ are preferable. ‘i-LIDS’ or the ‘i-LIDS library’ is the government benchmark for VA systems, prepared for the Home Office by the Centre for the Protection of National Infrastructure (CNPI).

3.8.9.3 Automatic number plate recognition (ANPR)

This application employs a form of optical character recognition (OCR) to capture the alpha-numeric information on a vehicle licence plate. The vehicle can be illuminated with IR light to allow operation in all light conditions. An image of the car and/or occupants may also be stored. The application allows the index number to be looked up on a database so that, for example, police can be alerted to vehicles of interest or a staff car park barrier can be programmed to automatically allow access to authorised vehicles.

3.9 Temporary systems

The Surveillance Camera Commissioner has made it known that, in locations to which the public has access, and where acute security threats arise that can be expected to abate if circumstances change, he would prefer to see such a 'hotspot' monitored by a system that can be readily dismantled (for deployment, as needed, elsewhere perhaps). Arguably, this makes more intelligent use of equipment and avoids having to install a 'permanent' system which may well remain in place long after the need for surveillance is no longer supported by the threat. This is likely to be built into a future revision of the Commissioner's Code of Practice if and when it is extended from public authority/police systems to systems in general.

More generally, temporary VSS designed for rapid deployment can be a suitable solution to meet the security needs of construction sites, unoccupied buildings and similar short term security challenges. A temporary VSS product may simply consist of a single camera mounted on a mast or attached to a surface or post. A more elaborate set-up can include a camera with fully functional PTZ capability, audio challenge and IR lighting, all in the one 'package' linked, if required, to PIR detectors dispersed around the site. Images may be sent for viewing and/or recording via an IP VSS system over a telephone or a roaming type 3/4G mobile phone connection.

Battery power can be included should no mains or locally generated electricity be available or to cater for interruptions of the mains supply. Some products can even draw a supply from wind and/or solar energy devices. An on board hard disc drive can also be included to store full motion video, even to evidential quality standard, over long periods.

Such systems may allow a remote authorised person with a PC/laptop or mobile device to take control of the camera and pan or zoom. This also allows a guarding service on site to monitor sectors that might not be immediately in view at the assignment base. In either case, they can be used to initiate the dispatch of a guard or commercial mobile security response to the location. However it is important to understand that temporary systems, as described here, do not conform to BS 8418 (detector-activated VSS for which see Section 5) and do not qualify for a police URN (unique reference number).

4 Detector-activated VSS systems

Bridging the boundary separating conventional intruder alarm and VSS systems, detector-activated VSS (DA VSS) systems offer an adaptable solution to security exposures that can be effectively addressed with automatic intrusion technology, yet demand the intervention of a remote observer, and the exercise of judgement, before an event can be notified with confidence as a 'confirmed incident' to the police (or other responding authority).

To be effective such systems need to be carefully designed, use suitable and reliable equipment and be properly maintained and monitored. To help provide the framework in which this can be achieved, such systems have their own specific UK Standard, BS 8418: **Installation and remote monitoring of detector-activated VSS systems. Code of practice** and separate, specific installer accreditation schemes run by NSI or SSAIB. It is therefore important to establish at the start of this description of DA VSS that, in the eyes of the police authorities, a VSS system only qualifies as a 'detector-activated VSS system' per se if it conforms to BS 8418. Consequently, for clarity, in this guide, references to DA VSS discuss systems that conform to that standard or, if not, deviate only on certain requirements currently being challenged as part of a review of the standard underway at the time this guide is in preparation (see section 4.5).

The following passages paraphrase the 'Introduction' in BS 8418 and, in a few words, provide a profile of the key the parameters of this variant of VSS:

- when a detection device (eg a movement detector) or camera function (eg VMD, see section 3.8.9.1) senses an event, images are transmitted to, and displayed at, a remote video response centre (RVRC) – an operation providing a service equivalent to that provided by an alarm receiving centre (ARC) for intruder alarm systems;
- prior to taking action, RVRC operators view these images for a period of time and take action in accordance with an agreed 'Response Plan'. An emergency police response is only requested by the RVRC if there is positive evidence in these images of unauthorised access to the secure area *and* of 'actual criminal or other untoward activity';
- the normal mode of operation for DA VSS systems is not to display images at the RVRC unless there has been an event in the secure area.

DA VSS is a highly effective, flexible security solution relative to conventional security measures, especially in situations where manned security would not be cost effective and/or conventional security is difficult to apply or adapt. A typical application is where property lies in the open, particularly where freely accessible, and thus exceptionally exposed to theft and damage. In very high risk situations the technology provides an effective additional form of protection in backing up traditional security solutions. The effectiveness of such systems is enhanced by their ability to respond (especially via an 'audio challenge') to trespassers detected and seen to be on site before they commit criminal acts.

A DA VSS system is intended to monitor a 'secure area', ie an area within which a change (such as movement) is detected using methods normally similar to those of an intruder alarm system. Notification of this event, along with associated VSS images, together amounting to 'an alert', are transmitted over a transmission network to the RVRC. If, in the judgement of the RVRC operator, a crime is underway, or seriously threatened, (elevating the 'alert' to an 'incident') the RVRC is entitled (for BS 8418 certificated systems protecting sites falling in the police areas where the force awards unique reference numbers (URN) to DA VSS systems) to make direct contact with the police control room. A voice warning, audible in the secure area, may also be played at the site ('audio challenge').

Note that monitoring centres at which non certificated DA VSS systems are terminated are not permitted to contact the police control room using the privileged number reserved for ARCs and RVRCs notifying activations from systems with URNs. Instead they are known, controversially, to make 999 calls relying on the emergency operator to connect them through the emergency service. This introduces delay and the risk that the call will be rejected as coming from a Type B security system (cf ACPO Security Systems Policy).

Making good use of the audio challenge facility nips crime in the bud and prevents waste of police time

Figure 13: Camera with audio challenge facility

In order to qualify for the police URN and level 1 (immediate) police response, a BS 8418 system must also conform to the ACPO policy. One aspect of this is that the police policy requires the system to at least have the capability of audio challenge, even if it is decided its use would be inappropriate. As with I&HAS the system must also be installed by a DA VSS installation company approved by a United Kingdom Accreditation Service (UKAS) listed inspection body, currently the NSI (National Security Inspectorate) and SSAIB (Security Systems and Alarm Inspection Board).

Quite separately, the RVRC must be accredited by one or both of these bodies, each of which maintains listings of approved companies that are available to customers. The customer will normally have separate contracts with the BS 8418 VSS installer and the BS 8418 RVRC (note that in principle a system using BS 8418, or similar, DA VSS technology and procedures may be monitored 'in-house' at a customer's own monitoring operation but it would not qualify as a BS 8418 system or be entitled to a police URN. To qualify it would have to meet BS 8418 in all respects including being monitored by a RVRC as defined in BS 8418, ie conforming to BS 5979, Category II). As this guide is being prepared a new standard, BS 8591, destined to replace BS 5979 in respect of security systems other than I&HAS (thus inclusive of VSS in all its forms) is nearing readiness. During the transition stage the police will provide URNs to systems terminating at RVRCs conforming either to BS 5979 or to BS 8591.

RVRCs are usually 'third party' businesses set up by independent operators or subsidiaries of electronic security firms. The RVRC operation, or a subsidiary, may also contract with the customer to install the DA VSS on site but this is the exception. Thus, in most cases, responsibility for the VSS security service is split between the installer/maintainer and the RVRC.

It makes sense to have the full benefit of the VSS system during business hours but save on monitoring costs at other times through Detector-Activated technology

The RVRC normally has no involvement with the site unless/until the system is fully 'set' and an event occurs – the triggering of an alarm device in the majority of cases. If agreed between the owner and the RVRC, the RVRC operator may also be requested to 'dial in' periodically to view the secure area. If required, the RVRC service can be extended to provide ancillary services such as observing opening and closing of the system/site, access control etc.

Putting aside the RVRC functions, a DA VSS system can usually also function as would any other type of VSS system, ie the system generally has monitor(s) and recording facilities installed on site which are available for the use of the owner/appointed site security personnel during times when the site is occupied. Increasingly, taking advantage of IP technology, users are also able to view images remotely, eg on their home/laptop computers or mobile devices.

For the most part, these systems are used outside buildings and the equipment (cameras and detectors) are manufactured to standards that tolerate the expected conditions. When a detector is activated (eg by movement) images from one or more cameras, overseeing the same part of the secure zone as the detection device, are sent over a link to the RVRC. For many years following the introduction of the technology this link invariably took the form of an ISDN telephone connection. However ISDN transmission technology has been overtaken by systems carried on private/public networks employing IP and/or 3/4G cellular radio (see section 4.4.2).

4.1 Some typical uses of DA VSS

Typical uses are illustrated in the following table which superficially has a certain amount in common with the table appearing earlier in this guide illustrating general applications. However, in the majority of the incidents visualised below a clear distinction exists in that observers are alerted and able to interpret what they see through the operation of automatic detection rather than routine viewing, this being the key feature and benefit of DA VSS.

Situation	Hazards	Function
Protection of moveable property within a closed site, eg a walled or fenced yard	Theft, vandalism, arson, sabotage	Capture images of trespasser(s) before they can reach the property; evaluate situation and warn-off or summon response
Site security/management within a open site, ie where there is free access (eg marina, school grounds, car sales forecourt)	Theft, damage, nuisance, assault	Evaluate images when, due to the hour or the behaviour/appearance of the 'target(s)', a security breach could occur – manage situation remotely or summon a response
Detection of unauthorised entry into a building	Theft, vandalism, arson, sabotage, espionage, assault, hold-up	Capture images of intruders attempting to enter, or already inside, a building and summon response
Protection of fixed property (eg roofing metal, cable)	Theft, damage	Detect the unauthorised approach to, or actual interference with, target property; summon response
Object protection (eg museum exhibit)	Theft, damage, defacement	Capture images of unwanted behaviour relative to the object, evaluate situation and warn-off or summon response
Visual confirmation of intruder alarm signal	All of above	Use images to establish whether person(s) have broken into the secure zone
Oversight or control of an event (eg access control)	Exposed keyholders	Use images to manage a process, eg validating and facilitating access whilst guarding against any lapse in security

Table 3: Typical uses of DA VSS

4.2 What happens in the RVRC?

When responding to an activation the RVRC must follow the actions set out in the 'Response Plan' (see section 5.2). The following is a summary of the sequence of events for a typical set-up. Some are requirements of BS 8418 but equipment and practice varies and these operations are not necessarily supported at non BS 8418 monitoring centres:

- an on-site detector triggers which causes the system to open a transmission path to the RVRC and send live pictures from the associated camera;
- activations are classified to distinguish between 'alerts' (no positive evidence in images of unauthorised access or criminal activity) and 'incidents' (activation where there is positive evidence in images of conditions requiring an emergency response and/or of actual criminal activity);
- there may be a delay between an event being detected and an activation occurring so that, for example, if the activation coincides with a keyholder entering, any timed entry procedure should be allowed to run its course;
- in addition to live pictures, the display shows, or allows ready access to, frozen images of the scene at the moment the detector triggered and at pre-determined points immediately following, or on a continuous 'rolling buffer' basis, allowing the operator to review footage immediately before, during and post incident;
- to assist the operator to decide how to classify the activation (alert or incident) images prior to the activation may be viewed from some or all of the zones;
- a 'reference image' will be available to the operator showing the scene in normal conditions by day or night; for functional cameras with pre-sets, reference images are stored for each of the pre-set positions;

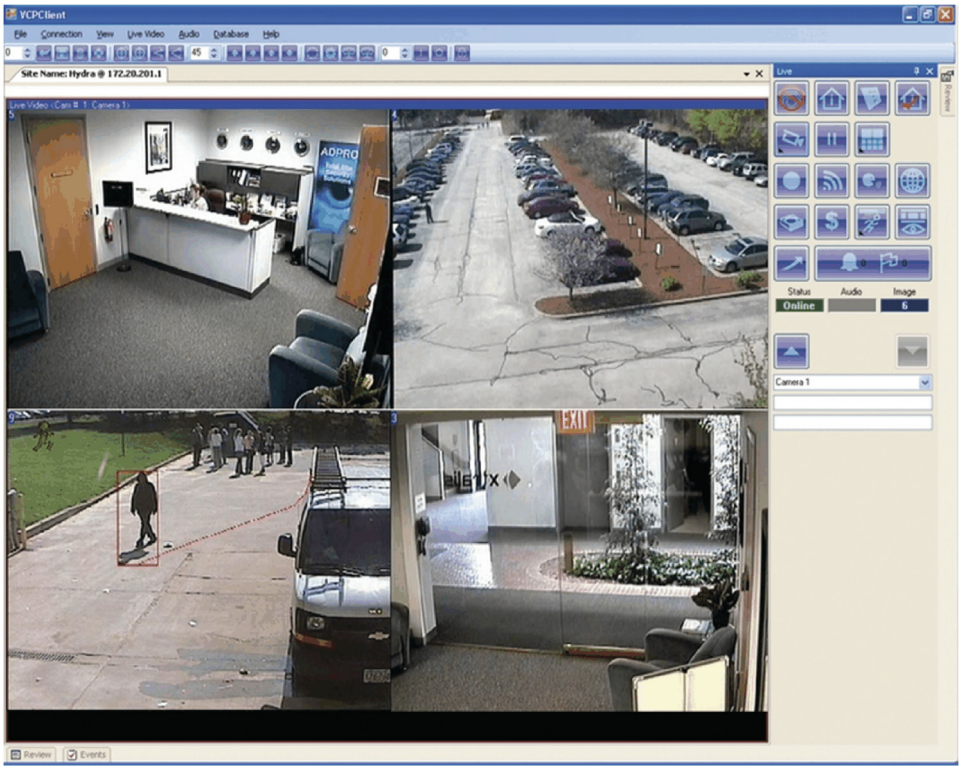


Figure 14: Example of an RVRC operator's screen: here the ADPRO VideoCentral Platinum© platform with VA in operation is both detecting and tracing the route of the target

- the operator may have to acknowledge the incident and may then move on to subsequent alerts generated by other detectors and cameras;
- if there is a graphical mimic presentation of the site, an icon indicating the location of previous alerts in the current monitoring session may be displayed;
- if the camera concerned has positioning functionality, the operator may change the field of view or move to pre-set positions;
- the operator is free to display images from other cameras and adjust their fields of view if applicable in order to track events;
- *some* RVRCs require or, through the software oblige, the operator to complete a tour of every camera and pre-set view before moving on to deal with other incoming alerts but the impact on the operator's performance is an issue (see 'Other activities' below);
- if the images indicate that the RVRC needs to take action, the keyholder and/or a response service and/or the police may be contacted (only a very small proportion of activations are referred to police);
- alternatively or additionally, the RVRC may attempt to take control of the event through an audio challenge facility – this allows the operator's voice (or a pre-recorded challenge) to be heard via a public address system at the site;
- the operator's function may be to escalate the response in an agreed sequence – eg switch on lights, instigate a low key warning, follow with a sterner warning, call keyholder and call police if necessary;
- if no suspicious activities are seen by the operator, the response plan may require that other cameras are checked before the connection is shut down;
- all received images are recorded (retention period agreed with the owner);
- all activations and key operator activities are logged; and
- during the night the VSS system is accessed by a RVRC operator to check that the artificial illumination allows clear images of each view.

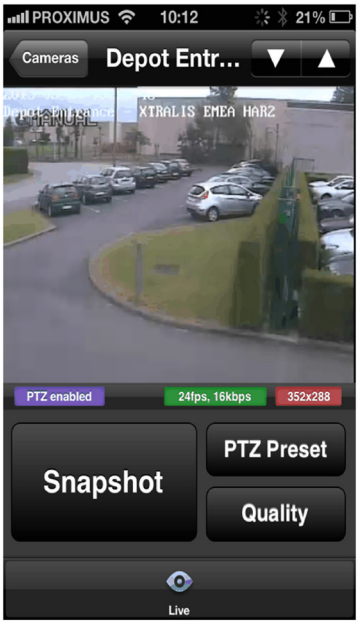


Figure 15: Presentation on the Smartphone of an owner, site guard etc

Other activities

There may be an agreement that at prescribed times or intervals, the RVRC carries out a routine 'video patrol' of the location.

The operator may have instructions to perform certain location management actions such as admitting persons or vehicles to site when arriving at an entrance, observing cleaners, monitoring plant etc.

However such services may not be offered by the RVRC due to the amount of time that the operator is tied up on the task and the consequences for adequate attention to incoming alerts.

Increasing use of Video Analytics in DA VSS systems holds huge potential but also challenges RVRC operators and owners to agree response plans that anticipate all eventualities

4.3 The site survey

For the most part, the issues that specifiers must pay regard to are common to those outlined in the site survey for a conventional system but with particular attention paid to the strength and control of the perimeter and conditions and activities occurring at or beyond the location over which the owner may or may not have control. An appreciation of all normal and abnormal operations and movements will need to be acquired.

Certain other site conditions hold slightly different implications for DA VSS:

- unstable structures: detectors as well as cameras need robust, vibration free mounts;
- sunlight is also a problem, not only when on the face of cameras but also PIR and IR detectors;
- wind induced surface movement and reflections on laying water cause false triggering and degraded images;
- wildlife, windblown waste etc are particular problems.

4.4 Specifying the DA VSS system

A tailored OR should be drafted as with any VSS system.

Unless embodied in the OR itself, some key features of the assignment should be added to assist the bidding firm who will be unfamiliar with the issues. These might include:

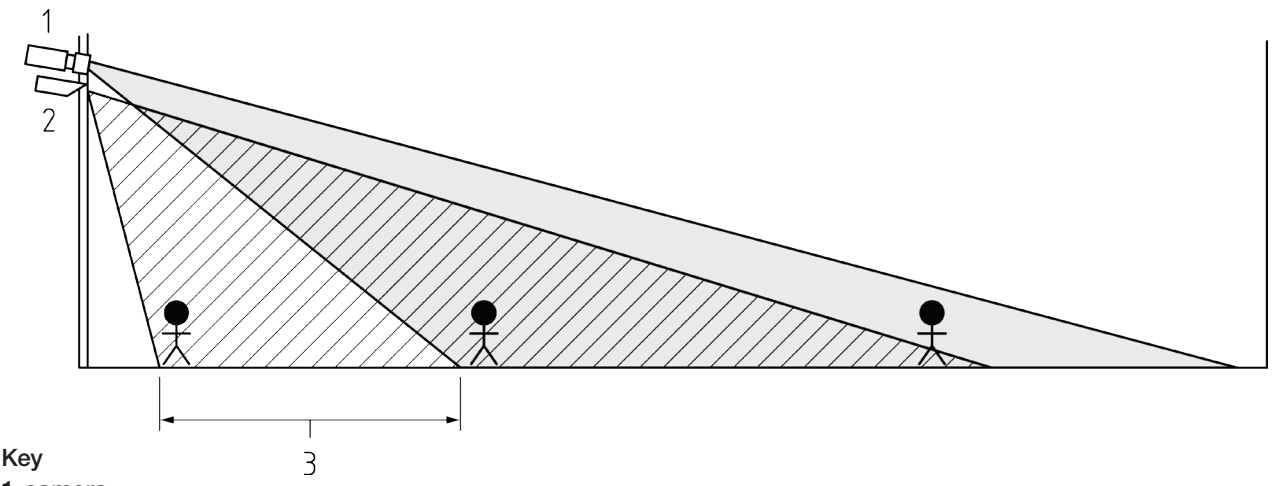
- period of observation: eg daily between 21.00 and 08.00 and all Sundays/public holidays;
- location features: eg the site lighting will be in 100% operation during the monitored period; there will be no vehicles in the customer parking area;
- locality issues: eg this site is exceptionally exposed to mists rolling in from the moor during autumn and winter which frequently prevents the compound from being seen clearly;
- response required: eg intruder(s) are to be warned off via the audio challenge facility (note, in some circumstances this may be subject to noise pollution legislation restrictions). Any vehicle seen in the customer parking area should be regarded as suspicious. The operator shall check the status of (at least) the yard gates and the performance car display apron (wheel clamps in place; bollards raised?) via the pre-set views of these two scenes before the connection is closed.

More knowledgeable and experienced specifiers will wish to submit an outline specification entering into some detail as to matters such as camera and detector positions, lighting and required responses. The specifier needs to remain flexible and open minded if viable, alternative DA VSS strategies are suggested.

4.4.1 Detectors for DA VSS

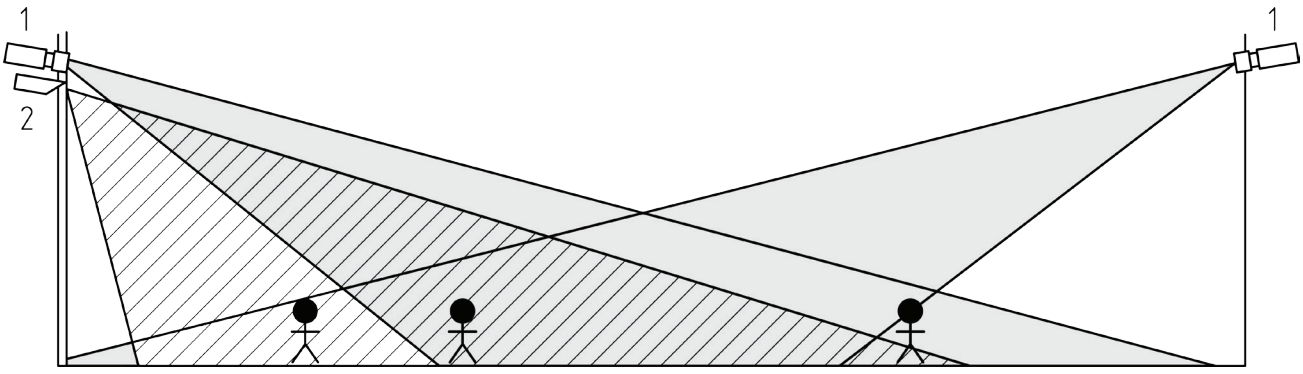
The great majority of detectors in use in the DA VSS application are purposed-designed exterior-use rated versions of I&HAS detectors familiar in internal applications – particularly the PIR which has proved the most cost effective and versatile. Software based detection, often built into the camera itself, consists of video motion detection (abbreviated to VMD), perhaps as a basic component of a much more sophisticated video analytics (VA) package (see section 3.8.9.2) but, up to the present time, these technologies have been unpopular with RVRCs (unless paired in parallel with conventional detectors) due to false triggering.

Figure 16: Incorrectly positioned detector with an extended area of coverage



Key
1. camera
2. detector
3. area of coverage not within the cameras field of view
Note: this can result either in unwanted activations, or in genuine activations that cannot be viewed by the respective camera

Figure 17: Multiple cameras correctly positioned to view the area of coverage of the detector



Key
1. camera
2. detector

In positioning a detector, the first, and most important, principle is that the detector's field of operation (sensitivity to movement) must not extend beyond the field of view of the associated VSS camera(s). It must be established that activity elsewhere, either within, or outside, the site will not be picked up by the device. If necessary, dual technology, and/or detectors configured for sequential operation, can be resorted to.

In Figure 16 (from BS 8418) the zone (3) below the camera can be the source of activations but cannot be viewed by the camera. In Figure 17 the RVRC operator has the ability to establish the cause of an activation by viewing camera 1 and/or camera 2.

Best results are obtained if detection zones in the secure area are of limited size and well within the range capability of the unit thus increasing the chance of detection and minimising false triggering. The position should be selected for optimum response (normally) across the plane of the detection field and the environmental factors mentioned above need to be considered before siting is finalised.

See Appendix 1 for a description of the detector types most frequently specified for external use with a VSS system.

4.4.2 DA VSS transmission

The transmission (remote signalling) technology in use for the most part at the present time, employs IP over a fixed broadband line to signal (send) information to the RVRC. Ideally a dual path transmission system should be provided, both paths of which should be capable of transmitting images to the RVRC, and because of their importance to the overall effectiveness of a DA VSS system, such transmission systems should include suitable self monitoring for failure/faults.

The reporting requirements are unclear at present but, as this guide is being prepared, BS 8418 is undergoing revision and the clause dealing with 'communication integrity' (currently 4.5.9) is sure to be clarified.

Leaving aside what BS 8418 may have to say on this matter, specifiers can have more confidence in the efficacy of the transmission link between the DA VSS system and the RVRC if it is known to incorporate one of the proprietary (intruder) alarm transmission systems (ATS) operating at ATS 5 (grade 4) performance level, ie one with 3 minute fault reporting.

For the higher security system at least, dual path signalling with fault reporting at 3 minutes on both paths would be consistent with the superior resilience demanded of the system itself. In any case, given the importance of this link in the resilience/security of the overall system, ATS that have third party certification to a relevant standard, eg LPS 1277 3.0, are likely to be preferable.

4.5 Current BS 8418 issues

BS 8418 is the only available British Standard or code for DA VSS. Neither inspectorate body maintains a code specifically dealing with this technology at present although the inspectorate bodies apply their VSS Codes of Practice to this sector (NSI: NCP 104 **Code of Practice for the Design, Installation and Maintenance of VSS Systems**; SSAIB: SS 2003 **Code of Practice for Closed Circuit Television Systems)**.

The security industry say they find some requirements in the current edition of BS 8418 so onerous and/or impracticable that they rarely quote for a BS 8418 conforming system and, as a result, very few certificated systems exist in the field. Not only does this have the consequence that specifiers cannot ask for a BS 8418 system with full confidence that the customer will be offered such a quotation, but those DA VSS systems that are being installed (and in reasonable volumes at this time) are, to a significant extent, being installed to no particular standards whatsoever, leaving any interested party with no assurance that the system is in any way fit for purpose.

That said, some NSI/SSAIB installers have achieved accreditation to the standard and can be identified from those inspectorate organisations' websites – as each maintains a separate listing of companies authorised to issue the appropriate BS 8418 certificates.

Putting aside the issue of transmission systems, the rump of the VSS industry difficulties with BS 8418 revolve around clauses dealing with tamper detection and power supplies. The table over the page contains reference to the clauses that appear to cause the most difficulty and commentary on the impact a relaxation may have on security. It also examines in each case the potential consequences of relaxation.

As this guide is being prepared, the responsible BSI committee is in the process of reviewing BS 8418 in a way that allows systems to be more cost effective whilst possibly allowing certain of the more onerous requirements to remain available for high security applications. The relaxations in the column headed 'Possible relaxation' are currently under discussion although it will not be known until the publication of the revised document whether these (or a different solution) are adopted. Meanwhile in the interests of benefiting from robust DA VSS technology it is of course open to specifiers to selectively entertain proposals for systems with these relaxations but which comply with BS 8418 in all other respects.

Clause	Practical issues	Possible relaxation	Potential impact of alternative
4.5.6. detector tamper detection: detection of masking	only available in the higher graded detection devices	make optional	detector(s) could be masked during an unset period
4.5.6.2 f) camera tamper detection: removal of camera	few dome cameras have this facility	make optional	camera(s) could be moved; view changed or lost
4.5.12 power supplies: UPS required	high cost of UPS	30 minutes battery standby for signalling only	system is disabled if power cannot be restored quickly

Table 4: Potential relaxations in requirements of BS 8418

Specifier's checklist for new DA VSS systems

The following will need to be addressed for all systems:

- Specify that the system conforms to BS 8418 (subject to any agreed dispensations – see section 4.5 and 'Potential relaxations in requirements of BS 8418' above) and, if the best possible police response is to be assured, that a URN is obtained.
- Check that the codes published by the Information Commissioner and Surveillance Camera Commissioner will be observed.
- Agree the operational requirement (OR); what is the purpose of the system, for example, the detection of intruders or the recognition of individuals (eg to manage access to the site)?
- Ensure that the installer and RVRC agree a tailored Response Plan with the owner/user: ie determine the action to be taken by the RVRC upon receipt of an activation with reference to the behaviour/actions of a human target, whether day/night, site open or closed, where there is no identifiable cause of activation and in the event of faults and failures including communication failures and problems with artificial lighting.
- Agree the activities/behaviours that are to be regarded as suspicious/innocuous, what form intervention should take and who is to be informed: police/guarding service/owner/user/keyholder/installer.
- Consider including an audio challenge facility (mandatory for systems with a police URN) and implement if necessary.
- Establish whether the RVRC should be briefed on the nature of any legitimate and authorised activity that takes place in the secure area when the system is set.
- Ensure a suitable contract for service and maintenance is agreed.

At least some, if not all, of the following will also need to be considered, failing which their treatment may default to minimum industry standards or the standard practice of the installer and/or RVRC:

- determine how the system is to be set and unset. That is, from outside the secure area (the process must be within the field of view of a camera); from inside the secure area (a 'safe' access route will be required that is as short as practicable to minimise the unavoidable security compromises); through use of an automatic timer (this inevitably means that the premises are left without protection for a time each day) or under the control of the RVRC;
- consider what camera views are required to meet the OR. Have site conditions and topography been taken into account? Consider whether it would be desirable to specify the actual camera and associated detector locations/positions;
- ensure that each camera and its associated detection device share the same field of view with detector 'leakage' minimised;
- do the type and performance of associated detection devices or software need to be specified (eg is linear as opposed to a volumetric detection preferred; should there be supplementary video analytics)?;
- consider whether the demands of the OR suggest that the use of high definition technology may be required;
- if applicable specify which views are to be made the pre-set positions of any functional (eg PTZ) camera(s);
- check that pre-activation recordings are to be viewed;
- establish whether the artificial illumination at the site requires change or improvement and whether use must be made of IR illumination in conjunction with IR sensitive camera technology;
- specify the degree of resilience required for the system power supply, eg should there be a UPS? Does some or all of the site lighting also need to be backed up?;
- explore whether the owner/user needs or wishes to have access to the system via their own computer or mobile device (if this feature is made available by the equipment/RVRC);
- on a larger or more complicated site, assess whether the RVRC operator should have the benefit of a graphical mimic presentation of site layout depicting activations as they occur;
- indicate whether the operator is to complete a 'camera tour', ie the inspection of all or selected camera views (including pre-set views?) before the RVRC shuts down an alert condition;
- consider what would constitute significant changes at the site as noted by the RVRC operator (eg presence of unexpected vehicle or object, whether or not impeding views) and what action should follow;
- agree the rate of false triggering before a detector may be 'omitted' (as defined in BS 8418) by the RVRC;
- specify the frequency of checks for picture degradation, eg through comparison of stored reference images with current images;
- state whether the site is to be checked periodically by the RVRC operator and if so with what frequency;
- indicate the required/preferred transmission system (network/signalling products, services and responsibilities;
- agree the retention period to be set for images stored at the RVRC; and
- ensure that as part of the handover, and prior to acceptance of the system, key stakeholders (eg specifier, owner, user, keyholder) will receive training in the use of the system and have demonstrated to them, both during the day and at night, each camera image, including pre-sets, the video quality of recorded images etc.

Shortlisting a reputable installer with good experience of DA VSS systems should ensure that specifiers and owners receive skilled guidance

5 All systems

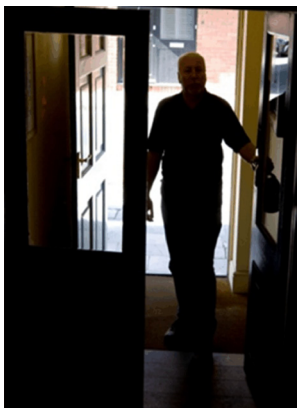


Figure 18: Unacceptable: the subject is strongly backlit and the camera needs to be repositioned

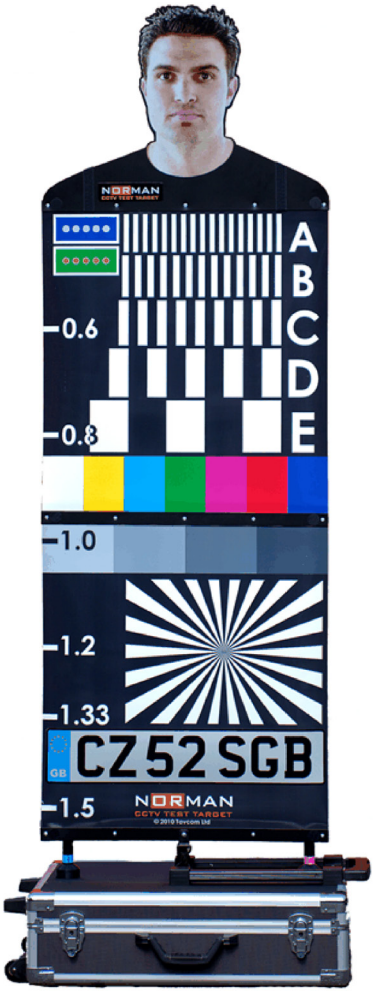


Figure 19: A test target (courtesy of Tavcom Training)

5.1 Completion/commissioning

On completion, the system is commissioned by the installer and then demonstrated and handed over to the customer. If the system is to operate at night the quality of the pictures must be assessed in night time as well as daytime conditions. The installer should ensure that the picture from each camera is acceptable to the customer, and meets the OR, through use of an industry test target such as those provided by the Centre for Applied Science and Technology (CAST). At this point a reference recording should be taken of each scene and retained by the customer. Each element of the system should be tested and the customer trained in its use.

For a DA VSS system the process will of course extend to a full walk test plus a check on the conformity of detection areas and fields of view of associated cameras plus a test that the image quality generated via available transmission paths is acceptable.

5.2 Documentation

At handover, in accordance with BS EN 62676-4: **Video surveillance systems for use in security applications. Application guidelines**, specified documents, including the following, will be supplied:

- the original risk assessment, OR and design specification;
- site plan marked up with the fields covered by the detectors (if any) and cameras;
- system drawings, test results;
- maintenance contract/schedule;
- remote surveillance service contract (if applicable);
- operating instructions, manuals and logbook;
- commission certificate and reference images.

The customer may also be able to purchase from the installer a suitable Data Protection documentation kit containing model forms, leaflets, logs and a compliance manual.

A similar and expanded set of documentation must be prepared in order to comply with NSI Code of Practice NCP 104 or SSAIB SS 2003 **Code of Practice for Closed Circuit Television Systems** if, respectively, the installer is a VSS company approved as a NACOSS Gold or Systems Silver installer or a SSAIB approved VSS installer.

For a DA VSS system the documents will include the agreed response plan which should be checked for acceptable procedures for dealing with detector omission and detector isolation as well as routine RVRC operator procedures.

5.3 System management

The owner should regularly check the performance of the system between service calls, reviewing each camera view in turn. Deterioration in performance is inevitable unless routine checks are made and failings rectified. A written record of faults must be maintained in the logbook or a dedicated fault reporting log. In particular the quality and the field of view of each camera should be checked to confirm that the OR is still being met, that changes in the scene such as foliage growth, parked vehicles, new structures etc are not interfering with results and that lighting is being maintained at the correct level.

5.4 Service/maintenance

Responsibly operated VSS systems, and those required to be in operation as a condition of insurance, will normally be required to have the benefit of a contract for preventative/corrective maintenance. The standards and codes of practice in operation in the UK do not currently contain recommendations or mandatory requirements for the time allowed for a corrective maintenance engineer to attend, or for the interval between preventive maintenance visits, as the actual location, size and complexity of the installation will influence the terms of these services negotiated with the VSS company. The components of systems in the open and the equipment supporting them such as detectors and lighting are significantly exposed to deterioration unless frequently checked and maintained. (As a rule of thumb there might be a reasonable expectation that a complex, high security system, vital to the location's security strategy, should have maintenance services at least on a par with the standard required for remote signalling intruder alarm systems, ie 6 monthly preventative maintenance and 4-hour call out).

NSI NACOSS Gold and Systems Silver approved companies must comply with the NSI Code of Practice NCP 104 and BS EN 62676-4 **Application guidelines** or, for DA VSS systems, BS 8418 or NCP 104 and BS EN 62676-4. SSAIB approved companies must comply with SS 2003 **Code of practice for closed circuit television systems** and BS EN 62676-4 for all types of VSS system.

The inspectorates are actively examining whether they should publish Codes of Practice specifically for DA VSS systems, particularly as there is an expectation that a revised BS 8418 will encourage the take up of such systems, and if they proceed, more specific/exacting guidance on DA VSS maintenance can be expected.

6 RISCAuthority guides containing additional guidance

The following documents, chiefly dealing with Intruder and hold-up alarm systems (I&HAS), contain additional information of relevance to specifiers of VSS:

S2: **Alarm signalling using the Internet Protocol Part 1 – An overview**;

S4: **The selection and use of electronic security systems in empty buildings**;

S6: **Electronic security systems: guidance on keyholder selection and duties**;

S9: **Intrusion and hold-up alarm systems (I&HAS): considerations for installers and other stakeholders**;

S12: **Police response intruder alarm systems**: **ten-step guide for purchasers**;

S14: **Police response intruder alarm systems**: **summary of insurers' typical requirements**;

S15: **Guidance on evaluating the performance of alarm transmission systems for use with intrusion and hold-up alarm systems**;

S17: **Intrusion and hold-up alarm systems**: **guidance on event processing and handling**;

S20: **Essential principles for the protection of property**.

These documents may be downloaded free of charge from the website: www.riscauthority.co.uk

Available to RISCAuthority members:

RI9: **Report to insurers: Intrusion alarm signalling using the internet protocol** (note: this document accompanies, and is a development of, document S2 above).

7 Glossary

3G (third generation mobile phone mobile communication standard): successor to 2G GSM/GPRS (the *de facto* global standards for digital mobile/packet-switched communications), fast mobile (cellphone) communication allowing higher rates of video transmission than 2G and currently available in most UK urban locations.

4G (fourth generation of mobile phone mobile communication technology standards): successor to 3G, very fast mobile (cellphone) communication allowing much higher rates of video transmission than 3G but not yet widely available in UK.

ACPO: Association of Chief Police Officers of England, Wales & Northern Ireland.

Analogue (signal): a method or representing (in this context) video information using continuously varying (eg) voltage (as distinct from a digital signal which is represented by a finite number of distinct values).

Bandwidth: the range of frequencies over which a circuit or electronic system functions with defined signal loss; the equivalent measure for a digital circuit would be expressed in bits per second.

Cat (category) 5 cable: a 'twisted pair' cable, usually used in buildings, carrying computer network (eg ethernet) signals.

CCD: charge coupled device; the sensor (or imaging) device in a modern camera that converts electrical charge into a digital value.

CMOS: complementary metal oxide semiconductor; camera sensor.

Depth of field: the distance, measured from the camera, over which the image is in focus.

DA VSS: detector-activated VSS system/technology.

Digital (signal): discontinuous representations of (in this context) video information through employment of discrete numbers (as opposed to the continuously variable signal of an analogue signal).

Dome camera: a camera mounted inside a transparent dome through which the camera can be seen or may be concealed; the camera may be of the fixed or PTZ type.

DVD: digital versatile disc; an optical medium that stores digital information by the reflection or scattering of laser light.

DVR: digital video recorder; a device that processes, encodes and records video signals in a digital format to a disk drive, flash drive, memory card, DVD or other mass storage device (replaced the VCR (video cassette recorder), as the popular method of storing video); see also NVR.

Field of view (also, angle of view): the extent of the scene captured by the camera within the horizontal and vertical limits of usable video information (the angle of view defines the scene in the horizontal plane alone).

Frame: a composition of lines that make one TV frame (a standard TV picture requires display of 25 frames/second).

Focal length: a measure of the distance between the lens and image sensor that denotes the angle of view.

Functional camera: (see PTZ camera).

IEC: International Electrotechnical Commission.

I&HAS: intruder and hold-up alarm system(s).

IR light: infrared light, invisible to the human eye.

ISDN: integrated services digital network; a digital data service over a public network (no longer available) which (latterly) featured two channels each of 64 kilobits per second (kbps; ie thousand bits per second), giving a total of 128kbps.

ISP: internet service provider; an organisation offering access to the internet.

LAN: local area network; a short distance data communications network (typically within a building or campus) used to link together computers and peripheral devices.

Lens: an optical device for focussing a desired scene onto the imaging device in a VSS camera.

Lux: unit of light for measuring illumination (the illumination of a surface when luminous flux of 1 lumen falls on an area of $1m^2$).

Matrix: a mathematical array; a logical network configured in a rectangular array of intersections of input/output channels.

Microwave: a form of higher frequency electromagnetic radiation which, for the purpose of this guide, is most often associated with microwave beams used as detection devices (usually externally) or point-to-point (line of sight) communication links.

Modem: (MOdulator/DEModulator); connects a device (eg a processor in alarm control equipment) via an audio channel communications link to another device with a modem, converting digital signals to audio tones.

Monitor: the device (a screen) that displays video images.

Monochrome: black-and-white video; a video signal that represents the brightness values in the picture, but not the colour values.

NVR: network video recorder; unlike a DVR, the video recorded on a NVR has been processed at each camera then streamed to the NVR for storage or remote viewing.

Optical character recognition (OCR): conversion into machine-encoded text of scanned images of (in context of number plate recognition) alpha/numeric characters.

Optical fibre: a technology designed to transmit signals in the form of light.

PIR: passive infrared (detector).

Pixel: (picture element); the smallest element of a video image.

PSTN: public switched telephone network, ie the public telephone service – capable of carrying digital information only at the relatively slow rate of a modem.

PTZ camera (pan/tilt/zoom camera): a camera carrying a motorised zoom lens which allows remote control of the focal length, mounted on a motorised assembly which allows the camera to be moved in both horizontal and vertical planes. These cameras can usually be programmed to move on command to pre-set positions selected as part of a viewing strategy in the event of an alert.

Quad video splitter: equipment that simultaneously displays four images from four separate sources on a single monitor, each occupying a quadrant of the screen.

Remote video response centre (RVRC): a continuously manned operation receiving multiple, concurrent VSS images from remote locations for the purpose of interacting with sites to provide security and related services (BS 8418).

Refresh rate: this term is usually used to refer to the rate at which the image is updated when image compression is in operation or in systems working other than in real time, eg time lapse mode.

Resolution: resolution is the term used in television to describe the performance of a camera in terms of the amount of detailed it resolves (ie reveals).

Sensitivity: a term used to denote the performance of a camera according to the amount of light reflected from the scene.

Secure area: area within the protected premises in which unauthorised access or attempted unauthorised access is intended to be detected (BS 8418).

Telephoto lens: a lens that makes distant objects appear magnified (through having a focal length longer than the physical length of the lens), not to be confused with a zoom lens.

UPS: uninterruptible power aupply; power supplies used (usually high security systems) to back-up the system when the mains power fails.

Video motion detection (VMD): a method of detecting a change in the video image, or a given part of it, for the purpose of detecting movement.

Zoom lens: a lens that can vary the focal length while keeping the object in focus, giving an impression of coming closer to, or receding from, an object (if the focus changes with magnification, it is more correctly a ‘varifocal’ lens).

Appendix 1

Figure 20: A wireless external PIR (courtesy GJD)

Detectors designed for external use that may be used with VSS

The following are the types of detector most often selected to support a VSS system or to form the detection element of a DA VSS system. Each has its own qualities and strengths as briefly described:

Passive infrared (PIR)

Essentially similar in design and operation to the familiar internal PIR unit but suitably 'ruggedised' with case and electronic components selected for their ability to withstand the harsher conditions experienced in the open. As with internal versions, they are available with wide or narrow angles of detection, or a combination of both, and optimum performance requires movement across the sensitive zone rather than towards/away from the unit. The PIR is by far the most common detector being versatile and cost effective.

Active infrared beam

Equivalent in design and operation to the internal IR beam device used in I&HAS. That is, detection only operates when the target crosses, and thereby breaks, the invisible light path between the transmitter and receiver units. However, in common with the internal version, there can be a high level of confidence that the detection will operate as required at the instant that the invisible barrier is breached. Beam and electronic configurations can be tailored to filter out unwanted alerts, eg by requiring simultaneous breach of parallel beams. Elaborate beam patterns are available whereby a 'fence' or 'net' of beams creates a virtual wall of electronic penetration detection with in-built logic to minimise false alerts from small animals, blowing paper etc.

Laser intruder detector

This is an active device using pulsed infrared laser radiation capable of accurately detecting and locating targets within a secure area and discriminating on the basis of position, size, shape and direction of the object entering the monitored zone. Potentially, subject to careful orientation, superior false alarm immunity can be expected and the technology lends itself to pinpoint control of PTZ cameras.

Active microwave beam

These are equivalent in basic concept to the IR beam in that detection occurs with the break of a line-of-site path of energy between transmitter and receiver units. The beam has greater depth and breadth than an IR 'fence' resembling a three dimensional 'cigar shape' and is arguably more difficult to evade than an IR beam, provided any blind spots at either end of the beam are compensated for with physical obstacles. One further benefit is that challenging optical conditions such as thick fog that can affect an IR beam do not prevent these devices, employing radio magnetic energy, from operating normally. However, in common with IR beams, if crossing uneven/undulating terrain there may be unprotected zones or pools between the surface and beam that require physical security or civil works.

Video motion detection and video analytics

These may be used as detection or in conjunction with other simpler methods. See sections 3.8.9.1 and 3.8.9.2 for details.

Perimeter fence protection

Using a variety of technologies, this form of detection relies on linear detectors to pick up and analyse mechanical disturbance of an existing or purpose designed metal fence. As well as detecting interference some purpose designed 'electric' fences can administer a disabling (but not harmful) high voltage electrical shock. Robust, well maintained fences and a favourable environment can produce satisfying results but there are numerous potential problems. At a cost, high levels of security and reliability are achieved with twin fences enclosing a 'sterile zone' monitored by cameras.

Buried sensors

When expertly specified and installed, high quality seismic and equivalent sensors are both discreet and highly effective. They are at the more ‘exotic’ end of the spectrum of state-of-the-art technologies but there is no doubt that they have their place.

Wireless detectors

These may need to be resorted to where cabling presents problems but the environment and limitations of the technology can introduce problems of their own. Expert surveying, specification and installation are essential. These devices, unless of the semi-wired type, in which case they have a local wired power supply, rely on dry batteries. Depending on the standard applicable to the system type, interference with the power supply, low battery voltage and loss of wireless signal may be detected but there are other ways in which these devices might fail to which normally connected devices are not exposed.

Combined technology detectors

Detectors are available that combine technologies in a single product along the lines of the familiar internal dual technology movement detector (sometimes referred to as a ‘dualtech’). Alternatively, improved reliably is attained if discrete detectors using different technologies are linked in the logic of the system processor to produce alerts on coincidental triggering within a timeframe.

Appendix 2

Figure 21: Camera viewing an area with public access (courtesy BSIA)

Privacy issues

The VSS Code of Practice, published by the Information Commissioner's Office, contains measures designed to help support the operator's compliance with The Data Protection Act 1998. These actions are rigorous and demand preparation and resources. For example:

- a person or organisation is to be identified as legally responsible;
- the system is to be notified to the Information Commissioner;
- warning signs should be provided;
- the quality and integrity of the equipment should be maintained;
- images should not be retained for longer than necessary;
- data subjects should be allowed access to their images in certain circumstances;
- procedures and practices should be documented.

The onus for complying with the code rests with the VSS user or operator, whether as owner or occupier of the premises. The code applies to all systems that capture pictures of individuals, (other than systems installed in a home by the owner) which will include shopping centres, shops, banks, offices etc. There is a simplified checklist for operators of limited VSS systems monitoring small retail and business premises.

Specifiers must not overlook that operators may wish a system, fundamentally designed for security, to be employed in one or more other applications. If this is the case it is especially important that the operator's attention is drawn to the Code of Practice to avoid falling foul of the legislation.

Key terms and concepts

Personal data

Personal data is information relating to an identifiable natural person, ie a person who can be identified, eg through reference to his physical identity.

Processing

This means obtaining, processing, recording, holding or carrying out any operation on the personal data and images are deemed to be included.

Data controller

This is the person in the organisation who determines the purpose for which, and the manner in which, personal data are processed.

Data processor

If someone outside the operator's organisation provides processing services, (eg editing images showing members of the public) then that entity is a data processor working on behalf of the data controller. There has to be a written contract in place with clearly defined responsibilities and guarantees as to the security of the data, properly trained staff etc. An RVRC probably constitutes a data processor as far as the legislation is concerned.

Data subject

The data subject is the individual captured by the VSS system and subject to the processing as defined.

Subject rights

Data subjects have the right to view or be given a recording of the video sequence in which they are captured. This is termed subject access. They are also entitled to require that the data controller ceases video processing which might cause unwarranted damage or distress. Furthermore, if an automatic decision taking facility is in use (eg number plate or facial recognition system), data subjects are entitled to notification and have a right of appeal against a decision that has a significant effect on them.

Specifiers need to remember to alert prospective owners to the key requirements and recommendations concerned with privacy legislation so that they fully understand the implications of maintaining video surveillance on their premises

Figure 22

Key requirements of the Act

Mandatory requirements:

- notification of the existence of the system must be submitted to the Information Commissioner's Office (ICO);
- the owner must identify a person to take responsibility for the system and establish its purpose and rationale;
- cameras should not be allowed to view places not covered by the purpose but if there is a possibility that they could capture scenes of neighbouring domestic premises, the operator must consult those neighbours;
- the VSS operator(s) must be instructed to apply the system only in line with the stated purpose (eg no specific monitoring of employees' non criminal behaviour) and, if necessary, be adequately trained in privacy policy;
- signs, in a prescribed form, warning the public that they are entering a zone covered by VSS must be erected;
- there are stringent conditions covering the use of covert cameras (ie cameras used without signage) which must not be used unless there is specific criminal activity to be detected and then only for as long as necessary to capture the relevant evidence;
- the equipment must:
  - work accurately and be checked out for correct operation;
  - be properly maintained and protected from vandalism;
  - be repaired promptly when defective;
  - operate in suitable conditions (eg adequate lighting);
- assuming the system is a crime prevention measure and identification of individuals is an objective, recorded image quality should be sufficient for the purposes of law enforcement agencies; recordings must produce good clear pictures without unacceptable loss of detail during the recording process (see section 3.8.4); it should be straightforward to take copies of sequences when requested by police and the form of recording must be suitable for their use (BS 8495: **Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence** contains technical recommendations for image quality, authenticity, audit trail etc);
- elements that can make automated decisions such as facial recognition systems must not operate without human intervention;
- unnecessary recording should be avoided and recordings should be disposed of/wiped after a sensible time (typically 31 days but subject to system application);
- retained recordings and VSS monitoring must be subject to access control and appropriately secured against unauthorised disclosure;
- proper records must be kept of any recordings that are viewed or disclosed;
- only designated, properly trained staff should operate the system and view images.

Considerations for specifiers:

- fixed cameras should not be allowed to capture private property; if necessary, elements of the captured image can be 'blanked off' using digital masking; it may be possible to restrict the travel of moveable cameras;
- covert surveillance may be conducted only by law enforcement agencies who are subject to different legislation concerned with the investigation or prevention of crime; in exceptional circumstances, the covert monitoring of workers may be used as part of a specific investigation; the code supplies illustrations of where this may be acceptable; covert monitoring is not acceptable in any other circumstances.

Specifiers should draw operator's attention to the contents of the code. For example:

- avoiding recording that is not absolutely necessary and disposing of recordings when no longer required;
- except for monitors displaying a scene which is in plain sight from the monitor location (eg customers queuing in a bank), ensuring that screens can not be viewed by unauthorised people;
- viewing recorded images only within a restricted area and keeping recordings and recording equipment under lock and key;
- if the system covers a public space, awareness that the operators of the system face possible licensing requirements imposed by the Security Industry Authority.

Protection of Freedoms Act 2012

This legislation contains provisions relating to the regulation of surveillance and ANPR camera systems in public places operated by 'relevant authorities' – public institutions such as local authorities and the police in England and Wales. The aim is that surveillance camera systems continue to be an important tool available to tackle crime and prevent terrorism whilst balancing public safety objectives with the individual's right to privacy. Systems will be required to be appropriate, proportionate, transparent and effective in meeting their stated purpose.

The Act requires government to put in place a regulatory framework comprising a code of practice and a Surveillance Camera Commissioner. The Commissioner's **Surveillance camera code of practice** was published by the Home Office. It can be found at: https://www.gov.uk/government/publications/circular-0112013. The code articulates 12 guiding principles that must be adopted by system operators when implementing a VSS system and, although the code does not initially extend to non institutional operations such as businesses, 'other system operators will be encouraged to adopt it on a voluntary basis'. Significantly, the guide adds that the government may consider extending the application of the guide beyond public bodies with the implication that systems protecting private property could be drawn in later on as experience is gained.

Private Security Industry Act 2001

If the VSS system covers a public space, then any organisation providing monitoring services (such as a RVRC) will need to ensure it is in compliance with the Private Security Industry Act 2001 and the requirements of the Security Industry Authority (SIA). This also extends to circumstances in which the SIA takes the view that operators at the monitoring centre are carrying out remote security guarding of the premises.

Appendix 3

Standards and guidelines

The following are the principal documents governing or guiding the design and use of VSS systems.

BSI publications: BS EN 62676-1-2: **Video surveillance systems for use in security applications. System requirements. Performance requirements for video transmission.**

BSI publications: BS EN 62676-1-1: **Video surveillance systems for use in security applications. System requirements. General.**

BSI publications: BS EN 62676-2-1: **Video surveillance systems for use in security applications. Video transmission protocols. General requirements.**

BSI publications: BS EN 62676-2-2: **Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on HTTP and REST services.**

BSI publications: BS EN 62676-2-3: **Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on Web services.**

BSI publications: BS EN 62676-2-3: **Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on Web services.**

BSI publications: BS IEC 62676-5-1: **Video surveillance systems (VSS) for use in security applications. Part 5-1. Environmental test methods for image quality performance.**

BSI publications: BS EN IEC 62676-2-31: **Video surveillance systems for use in security applications. Live streaming and control based on web services.**

BSI publications: BS EN IEC 62676-2-32: **Video surveillance systems for use in security applications. Recording control and replay based on web services.**

BSI publications: BS EN 62676-3: **Video surveillance systems for use in security applications. Analog and digital video interfaces.**

BSI publications: BS EN 62676-4: **Video surveillance systems for use in security applications. Application guidelines.**

BSI publications: BS EN IEC 62676-5: **Video surveillance systems for use in security applications. Data specifications and image quality performance for camera devices.**

BSI publications: BS IEC 62676-5: **Video surveillance systems for use in security applications. Part 5. Data specifications and image quality performance for camera devices.**

BSI publications: BS EN IEC 62676-6: **Video surveillance systems for use in security applications. Part 6. Video content analytics. Performance testing and grading.**

BSI publications: BS 8418: **Design, installation, commissioning and maintenance of detector-activated video surveillance systems (VSS). Code of practice**.

BSI publications: BS 7958: **CCTV. Management and Operation. Code of Practice**.

BSI publications: BS 8495: **Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence**.

BSI publications: ISO 22311: **Societal security. Video-surveillance. Export interoperability.**

National Security Inspectorate (NSI): NCP 104 **Code of Practice for the Design, Installation and Maintenance of CCTV Systems**.

Security Systems and Alarm Inspection Board (SSAIB): SS 2003 **Code of Practice for Closed Circuit Television Systems**.

Information Commissioner's Office: CCTV code of practice.

Home Office: Code of Practice for Surveillance Camera Systems (Surveillance Camera Commissioner).

Association of Chief Police Officers of England, Wales & Northern Ireland (ACPO): Police Response to Security Systems (commonly referred to as 'The ACPO Policy').

Police Service of Scotland: Security Systems Policy.

Home Office and the Association of Police Officers (ACPO): UK Police Requirements for Digital VSS Systems.

Association of Chief Police Officers (ACPO): ACPO Good Practice Guide for Digital Evidence.

Home Office Centre for Applied Science and Technology (CAST): CCTV Operational Requirements Manual Publication 28/09.

Home Office Centre for Applied Science and Technology (CAST): CCTV supporting small businesses.

Centre for the Protection of National Infrastructure (CNPI): Imagery Library for Intelligent Detection Systems (commonly referred to as the i-Lids library).

CCTV Users' Group: Procedure manual for the operation of CCTV.

British Security Industry Association (BSIA) documents:

- **Form 109 Planning, installation & maintenance of CCTV systems. Code of Practice**;
- **Form 120 A guide to the maintenance and servicing of CCTV surveillance systems**;
- **Form 172 A basic guide to BS 8418 systems for installers**;
- **Form 196 A user guide to a BS 8418 detector-activated remotely monitored CCTV system**.

RISCAuthority

administered by FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
Tel: +44 (0)1608 812500
Email: info@riscauthority.co.uk
Website: www.riscauthority.co.uk