CCTV Site Security
Buyer's Guide

A BUYER'S GUIDE TO CCTV

helping you to make rational,
informed, responsible decisions

Construction Site Security – A Buyer's Guide to CCTV

Construction site security has changed. Up and down the country, guards are being replaced with monitored CCTV systems, driven by better crime prevention results and massive cost savings. The transition is creating headaches for the quantity surveyors, site managers and purchasing professionals, unfamiliar with CCTV products and services, tasked with obtaining an effective security system at a sensible price.

This guide's for you. It cuts through all the technical jargon and marketing hype to focus on the questions you need to ask and the answers you should expect from professional suppliers, allowing you to make rational, informed, responsible decisions.

10 questions

you need to ask to help you make rational, informed, responsible decisions.

Introduction

In theory, all monitored CCTV systems work the same way:

- Intruders break into a site;
- CCTV images are transmitted to a control room where they are reviewed by an operator;
- An alarm is confirmed and a response initiated, directly issuing a warning to the intruders over a public address system and/or contacting the Police or other security service team;

When these three actions are completed in quick succession, evidence shows that most intruders move on before any serious damage or theft occurs.

Sounds simple, doesn't it? However, the specification of the security system installed has a profound impact on how effectively these actions can be performed. This guide highlights 10 essential questions to be considered when purchasing CCTV products and services for a construction site. They are the perfect starting point for talking to suppliers or drawing up tender specifications.

1. Which areas do you need to protect?

It stands to reason that the larger the area to be protected, the more CCTV equipment will be required. So it's good practice first to consider what plant and equipment is most at risk and what control you have over where it will be left when it's not being used. For example, perhaps you could enforce a policy where everything of value is returned to a secure compound every evening.

In reality, what needs to be protected will change over the duration of a project. During early ground-works, the focus will probably be a small number of heavy machines and perhaps some fuel. Later it may become necessary to protect cabins, raw materials, a wider range of equipment and perhaps the building itself and its contents, at which point it is often most efficient to secure the perimeter of the entire site. It's therefore useful to identify security systems and suppliers that can grow with your requirements, tailoring their services and costs to the stage of the development.

Perhaps in later stages you will need to layer additional security detection such as intruder, or fire, smoke and heat detection when high-value goods arrive or fire risk increases, as the building progresses.

BEST PRACTICE: Your supplier should conduct a security risk analysis based on your input, including an assessment of how your needs will likely change over time.

2. How will my system be triggered?

Let's start by understanding what happens in a commercial CCTV monitoring station, known as a Remote Video Response Centre (RVRC). Your CCTV images are not continually reviewed by a dedicated person; not only would this not be cost-effective, research shows that operators working in this mode suffer "monitor blindness", where their concentration quickly dips and incidents are missed. Instead, operators within a commercial RVRC respond to alarms, meaning that other than for maintenance purposes, your images will only be seen at the RVRC if the on-site system determines that an *incident* has occurred.

So what constitutes an "incident"? The presence of an intruder is most usually defined by the activation of a Passive Infra-Red (PIR) detector that senses body heat and movement. PIR detectors are installed across the site and create triggers whenever anyone passes by. When the system is armed, these triggers are treated as alarms and are sent through to the RVRC.

The range of PIR detectors available is vast, from small internal burglar alarm units that cost just a couple of pounds each to very sophisticated wireless devices that can detect movement up to 100m away and cost much more than a CCTV camera. The specification of the correct type of PIR detectors is critical if the monitored CCTV system is to be effective. Put simply:

NO DETECTION = NO ALARM = NO RESPONSE

BEST PRACTICE: All proposals should include a plan of the site showing the location and fields-of-view of all the detectors as well as the cameras. Check the ranges of the PIR detectors specified to ensure that they provide sufficient coverage, with no gaps in perimeter protection, for example. Ensure your supplier conducts a "walk test" during commissioning to check the detectors are operating correctly.

Video Motion Detection

Most modern CCTV systems offer some form of Video Motion Detection (VMD), a technique in which successive images of a video stream are automatically compared and an alarm generated when major changes occur. Some suppliers present VMD as an alternative to the use of PIR detectors and offer a significant cost saving as a result. However, whilst VMD can be effective in sterile internal environments, (e.g. a corridor or an office), there are invariably too many natural fluctuations for such systems to operate reliably outdoors (e.g. foliage blowing in the wind, cloud shadows, moving headlights, etc.). Furthermore, one of the biggest problems facing RVRCs is repeated false alarms which cause operators to become complacent and not take alarms as seriously as they should. Systems triggered purely by VMD will certainly generate many false alarms.

3. How will my system perform at night?

Most CCTV demonstrations are conducted in the daytime (and look very good as a result) but it is at night when the systems have to earn their keep. Nothing is more frustrating for a RVRC operator than to be responding to an alarm, believing that a serious incident is in progress but be unable to see clearly what is happening because it's too dark.

All CCTV cameras require some illumination to operate correctly at night. The options are:

1. White flood lights
2. Flood infra-red (IR)
3. Cameras with integrated IR

White flood lights are effective but can be problematic in residential areas. All local authorities have individual legislation covering night-time white light pollution, which must be checked and taken into account.

Both flood solutions (white light and IR) require the whole site to be lit continually and incur installation and operating costs. Further, any hardwired illuminators reduce the flexibility to adapt to changing requirements as a site develops and "black-spots" are often created by the rise of the building.

Some cameras have integrated IR, meaning that wherever the camera is pointing, a beam of IR points in the same direction. This negates the need to illuminate the whole site and with everything self-contained in one unit, no additional wiring is required. However, it is important to check that the range of the IR is sufficient for the deployment.

For example, a camera with integrated IR may be able to see half a mile in daylight but only 50 metres at night.

BEST PRACTICE: Your supplier should clearly indicate how all protected areas are to be illuminated, either with white light or infra-red. Ask to see some night time images from each camera to check visibility prior to signing off the commissioning of the system.

4. How will my system be protected against sabotage?

Elements of your CCTV system will invariably be positioned at the extremities of a site, protecting a fence line for example, making them susceptible to discrete attack by determined criminals.

One of the most obvious approaches is to cut the power assuming that this will disable the CCTV system. You can protect against this by specifying the use of an uninterruptible power supply (UPS), a device consisting of a large bank of back-up batteries and some clever electronics to manage their automatic deployment if power is removed. For the system to remain fully operational during an attack, the UPS must itself be secure and able to support the continued operation of all elements including cameras, illumination, recording and communications.

Confusing Terminology

Some CCTV cameras are defined as ''Day/Night Cameras'', a term that is open to misunderstanding. In particular, it does not mean that these cameras can see in the dark; every CCTV camera needs illumination to work properly. ''Day/Night'' is a term used in the security trade to identify cameras that operate in colour during the day but automatically switch to a black and white ''night mode'' in low light conditions. Most CCTV cameras designed for outside use include this feature.

Beware also of two very distinct uses of ''infra-red'' or ''IR'' in security applications. Passive infra-red (PIR) detectors sense very low level infra-red radiation emitted by passing bodies and are used to alert the system to a possible intruder. IR illuminators emit powerful infra-red radiation (i.e. heat) that is reflected by objects in the field-of-view. It is these IR reflections that CCTV cameras use to create night time views.

WITHOUT INFRA-RED

WITH INFRA-RED

The UPS should also generate an alarm as soon as the power is cut, allowing the RVRC to investigate immediately the cause of the disconnection. Finally, the UPS should be of sufficient capacity to maintain the system on full load (including illumination) for a period long enough to carry out this investigation and for a response/maintenance team to arrive on site (typically a minimum of 4 hours).

Another approach to sabotage is to try to disable the communications between the site and the RVRC such that alarms and video cannot be transmitted. The solution is to specify a system with multiple means of communication, perhaps wired broadband plus 3G wireless back-up, or dual 3G services from different service providers. The system should be capable of auto-rollover from one communication service to another and any service disruption should be reported to the RVRC as an alarm for investigation. The most secure systems also include some form of automatic and regular polling from the RVRC to the on site system asking it to confirm that it is operating correctly. Should the system go off-line, an alarm will be raised at the RVRC.

All the elements of the CCTV system should also be protected from physical attack. Camera locations should incorporate anti-climb mechanisms and all equipment should be located in robust cabinets or vandal resistant housings. Wherever possible, exposed cables to cameras, PIR detectors and illuminators should be avoided. Some devices (e.g. PIR detectors) incorporate tamper alarms. The best systems will indicate that a detector has been moved to leave a blind spot even if it is still functioning.

The system should be configured such that these tamper activations are routed to the RVRC even if the overall system is unset, preventing sabotage in working hours going undetected. An accredited RVRC should maintain at least two reference images of each camera (one in the day, one at night) and have a process in place for regularly comparing live views to the stored images to ensure that none of the cameras have been misdirected.

BEST PRACTICE: Ask your supplier to explain their anti-sabotage strategy. Specify the use of a UPS and back-up communication channels. Look for any areas of particular weakness and question single points of failure.

5. Who should I use and why?

The most important accreditation to look out for in this space is BS8418:2010, published by the British Standards Institute. Note that:

- The Association of Chief Police Officers (ACPO) demand that BS8418:2010 recommendations are followed before a site is allocated a unique reference number (URN), which is required for Police response;
- Many insurance companies use compliance to BS8418:2010 as an important factor in determining risk and calculating premiums.

Strictly speaking, BS8418:2010 is not a standard but a code of practice that covers every aspect of the "Installation and Remote Monitoring of Detector-activated CCTV Systems", from the specification and installation of the on-site equipment to the construction and operation of the RVRC. Check that your chosen contractor has a current certificate of inspection from either NSI (National Security Inspectorate) or the SSAIB (Security Systems and Alarm Inspection Board) for the relevant services.

Unlike many standards documents, BS8418:2010 is very practical in its recommendations. Indeed, many of the "BEST PRACTICE" comments in this guide are derived from the BS8418:2010 code of practice.

Equally, it is a legal requirement that all businesses and staff engaged in any kind of security work should be licensed by the industry regulator, the SIA – Security Industry Authority.

Security Industry Authority

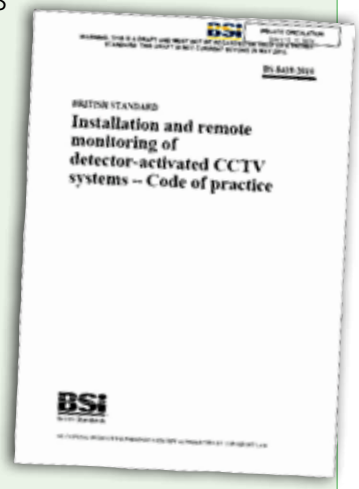
Under normal circumstances a security company providing a CCTV monitoring service must ensure that their operatives are licensed by the SIA for viewing CCTV in public spaces. Failure to do so could result in criminal prosecution and fines, not only for the security company but also for the contractor which is using their services. However, there are occasional exceptions, and each case must be looked at individually. The safest option is always to use a company whose operators are SIA licensed for CCTV monitoring.

Look for certification from specialist bodies such as the SSAIB to ensure that this requirement has been met.

BEST PRACTICE: Insist that all your suppliers (CCTV installation company, monitoring company and maintenance company) meet the requirements of BS8418:2010 and all their operators carry an SIA licence.

Revision Notes

When asking your suppliers about BS8418 conformance, be specific about version numbers. The latest revision, BS8418:2010 supersedes the much quoted BS8418:2003 (often simply referred to as "BS8418") and provides a much more comprehensive framework of recommendations than the previous revision.



6. Is everything included in the price? Are there extra benefits?

Sometimes an attractive headline price for the CCTV equipment can mask the total cost of the monitored service. Keep an eye out for hidden charges associated with:

- Delivery and removal of the equipment
- Installation, including any civil works required
- Re-siting of cameras, PIR detectors and other equipment required as the site develops

- Lighting and illumination
- Communication with the RVRC (some companies charge separately for transmission of alarms over a 3G network or perhaps you are being asked to deploy a dedicated broadband service solely for security purposes)
- Alarm handling (particularly where the installation company and the RVRC are separate commercial entities. Please note that some RVRCs charge on a ''per alarm'' basis.)
- Manned response (Police response is at no charge but is (strictly speaking) only available to BS8418:2010-accredited systems allocated a unique reference number (URN). Manned response arranged through a private security company will incur additional charges.)
- Finance charges associated with the purchase or lease of equipment

Construction Site Crime = Serious Crime

£400 million a year, that's the cost to the UK construction industry from theft, vandalism and arson

(source: Plant & Equipment Theft: A Practical Guide, D Edwards, 2007)

- Insurance – don't forget to account for any discounted premiums available from the deployment of a BS8418:2010 accredited solution

BEST PRACTICE: As with any contractual relationship, your supplier should clearly set out what is included and what extra costs are likely to be incurred.

7. How is "suitability" assured?

In most technology categories there are examples of good and poor quality products and CCTV is no exception. The problem for newcomers is knowing what to look for and distinguishing which is which.

As previously discussed, the most important factor relating to PIR detectors is their range (which should be obvious from the datasheet). Camera performance can easily be determined by looking at the images (remember to check at night).

Much more difficult to assess is the heart of any CCTV system, the digital video recorder (DVR). This vital component, usually hidden away in a cabinet, not only incorporates a sensitive high-capacity computer hard disk drive (HDD) to store all the video, it also interfaces to all the other sub-systems (PIR detection, pan-tilt-zoom camera control, communications with the RVRC, etc.) and is responsible for the intelligence in the system.

Most DVRs are designed to be installed in air-conditioned computer rooms or benign office environments, not the middle of dirty, dusty construction sites, subject to multiple shocks, vibrations and extremes of temperature. If you want your system to work reliably, specify a DVR that is specially designed for harsh environments, perhaps a product used in the transport or aerospace sectors.

Whilst these devices are typically a little more expensive, they are more rugged in construction, have their hard disk drives mounted on vibration dampers and operate in sealed units that need no fans.

Another key element of quality is the operation of the RVRC. In these days of ubiquitous broadband it is important to ensure that your RVRC is a dedicated, professional facility and not simply a laptop in someone's bedroom! Your RVRC should comply with BS5979, *Remote centres receiving signals from fire and security systems – Code of practice*, which itself is a requirement of BS8418:2010. The RVRC should issue a "CCTV system acceptance certificate" for every site that it monitors confirming that the on-site system is fit for purpose and is operating correctly. There should also be an agreed and documented policy that defines what should happen for each type of incident from a site.

If you are planning to have a RVRC look after a number of your sites, it's a good idea to visit the facility and form your own impressions but remember, staffing and activity levels will be much lower in the daytime than at night. For particularly sensitive or valuable sites, you might also request that a RVRC representative visits your site such that RVRC personnel are able to put the images on their screen in context.

BEST PRACTICE: Check PIR ranges and example CCTV daytime and night-time images. Specify a DVR suitable for harsh environments. Investigate critical RVRC procedures (ideally visit). Demand BS8418:2010 compliance and take up customer references.

8. What happens if something goes wrong?

Construction site CCTV systems will, on occasion, fail. There are lots of moving parts (e.g. pan-tilt-zoom cameras, delicate computer hard drives) and it's a tough environment for any electronic equipment. Added to this, some people will be deliberately trying to put the system out of action.

So it's important to consider how your supplier responds to the following questions:

1. "How will you know that the equipment has failed or been tampered with? Will you rely on us to tell you? Or does your system and your RVRC regularly check that everything is as it should be?"

2. "How quickly will you commit to get an engineer to site in the event of a failure? How does this vary by geography?"

3. "If the system cannot be immediately rectified, how will you protect my site in the meantime? Regular manual review from the RVRC? Arrange for a guard to be present?"

4. "If your system is defeated and we suffer a loss, how will we be compensated? How much insurance cover do you offer? "

BEST PRACTICE: As with any contractual relationship, your supplier should clearly set out (the limit of) their responsibilities and highlight any exclusions.

9. Can you share costs across multiple departments?

Quality always has a price and if you follow each of the **BEST PRACTICE** recommendations in this guide, it is unlikely that you will end up choosing the lowest cost proposal. One way to stretch the security budget further is to use the CCTV installation to provide additional services to other parts of the organisation and have them contribute to the cost. Here are a couple of examples:

- *Health & Safety (H&S)* – many security companies are able to provide clients with remote access to on-site cameras, meaning that Health & Safety personnel are able to login and view a site from their office PC, taking control of the pan-tilt-zoom cameras and reviewing video recorded up to a month previously. Such a facility helps improve compliance (spot checks on protective equipment and working practices, for example) and allows the first stage of an accident investigation to be conducted discretely without leaving the office.

  Some systems also offer more sophisticated H&S features such as site-wide fire alarm and evacuation systems, carbon monoxide and gas detection, traffic monitoring and automatic number plate recognition (ANPR).

- *Project Management* – client remote access can also be used to track construction progress, monitor weather conditions and check subcontractor arrival/departure times, making it easier for project managers to control and report on multiple projects simultaneously. You can even offer regular progress images to your clients for inclusion in their promotional websites, marketing materials, etc.

BEST PRACTICE: Ensure remote access cannot be abused, making it available only to authorised personnel through a secure login.

10. Are there flexible finance options?

As with most types of construction equipment, there is a range of options available to you, from outright purchase to leasing to hire, with several subtle variations in between. For monitored CCTV systems, it is important to remember that you are purchasing not only the equipment but several ancillary services including monitoring (provided by the RVRC), installation, commissioning, decommissioning and maintenance. Furthermore, BS8418:2010 demands that the system design, the equipment installation and the monitoring service must each comply to achieve the standard.

BEST PRACTICE: If you are planning to purchase the equipment, ensure that you have contractual support for the other elements of the service, such as monitoring, service and maintenance.