

Code of Practice for the installation and remote monitoring of detector activated CCTV Systems

Integrated systems – combining CCTV, Access Control and Intruder Detection – are emerging as a key characteristic of the security industry. A new Code of Practice sets out to raise the standard of their installation and operation.

Introduction

Norbain SD's decision to enter the Intruder Detection sector earlier this year reflected the anticipated growth in integrated systems as well as growth in the intruder sector alone. Since that decision was implemented, Norbain appears to have been proved right. Intruder may be a maturing market but the demand for integrated systems is mushrooming. Sales of intruder detection products are very promising, supported by Norbain's enviable track record on customer service and logistics.

To some extent all three sectors are now engaged in a battle to see which sector will win the race to establish control of the overall system. Manufacturers have been quick to identify that integrated systems still require a lead technology to act as the pivotal control centre of the system. Different sectors have different claims on this pole position – intruder is competing with Access Control with their respective control 'know how', CCTV with its transmission strengths, even networking and IP specialists might come to the fore. It may take a major manufacturer or brand with an extensive cross sector product portfolio to establish their hold on the integration market.

Defining Moment

BS8418 – the new Code of Practice for the installation and remote monitoring of detector activated CCTV Systems – is set to both raise the standard of integrated systems and define the character of those systems too.

But above all, it will drive integrated systems as a commercial opportunity. According to a BSIA survey, only 14% of premises in the UK have security systems. This suggests a huge commercial opportunity exists for the industry. The attitudes of the police and insurance industry are key in driving that figure up. Because of the waste of police time in chasing false alarms (98% of activations are false), some end users have lost confidence in the value of investing in security. However, going forward, if a user wishes to be guaranteed a level 1 police response, adherence to BS8418 will be mandatory. And where the police go, the insurance industry is sure to follow. End users will find themselves motivated by financial (ie insurance) as well as security concerns to pursue the integrated solution route.

Standard Scope

BS8418 covers the design, positioning, configuration, performance, commissioning, operation and maintenance of remotely monitored and detector activated CCTV systems. This means that the standard only covers integrated systems. It also means that it is the system and not individual products or components that comply with the standard. For instance it is not possible to purchase products that comply with BS8418.

A key purpose of adhering to the standard is to qualify for a Unique Reference Number (URN) which is issued by the local police authority to guarantee a level 1 police response. Without a URN, this level of police response is not guaranteed. It is this purpose that has led to the standard being stringent for the elimination of false alarms is a key police objective.

BS8418 Summary

Here is a bird's eye view of some aspects of BS8418. For a comprehensive picture we recommend you obtain a copy of the standard from BSI at www.bsi-global.com.

Field of View

The standard is adamant that camera and detector fields of view should match one another and be confined to within the site's boundaries and not extend into public areas.

Light

PIRs facing east or west must not be affected by the sun or from reflection and shadows

Only high quality PIRs must be used to avoid false triggering

Cameras should not face directly into sun or light. However, there should be sufficient light (night and day) to illuminate the cameras' fields of view.

System integrity

Each individual detector must be uniquely identifiable to the system

All cabling and detection devices should incorporate tamper protection.

Event verification

To 'verify' an event, the field of view should be set so that a 1.6m high human target fills at least 10% of picture height

To 'recognise' an intruder the target should fill a minimum of 50%

Fixed cameras are the recommended option for vulnerable areas (e.g. the entry/exit route) or a PTZ camera with its park position viewing the vulnerable area

If PTZ cameras are used in isolation, use should be made of presets so that the operator will observe each incident as though it were viewed by a static camera.

Audio

An audio challenge facility is recommended and required to guarantee level 1 police response

The audio challenge should be audible in all areas of detection.

Business Continuity and Disaster Recovery

The installation of a back-up UPS system should be considered

The system should have the ability to monitor and indicate video loss to the RVRC

Ensure that the system has an alternative signaling path to indicate failure of the main signaling path to the RVRC

The system should have a full connection and retry protocol

Plan to ensure that the fully detailed event log-system history be retained and held at the protected site.

Unique Reference Number

To obtain a URN, installers of remotely monitored detector activated CCTV systems will need to comply with all of the following: -

ACPO Security Systems Policy

BS 8418 Installation and remote monitoring of detector activated CCTV systems – Code of Practice

BS EN 50132-7: CCTV Application guidelines

The system must have the capability of audio challenge.