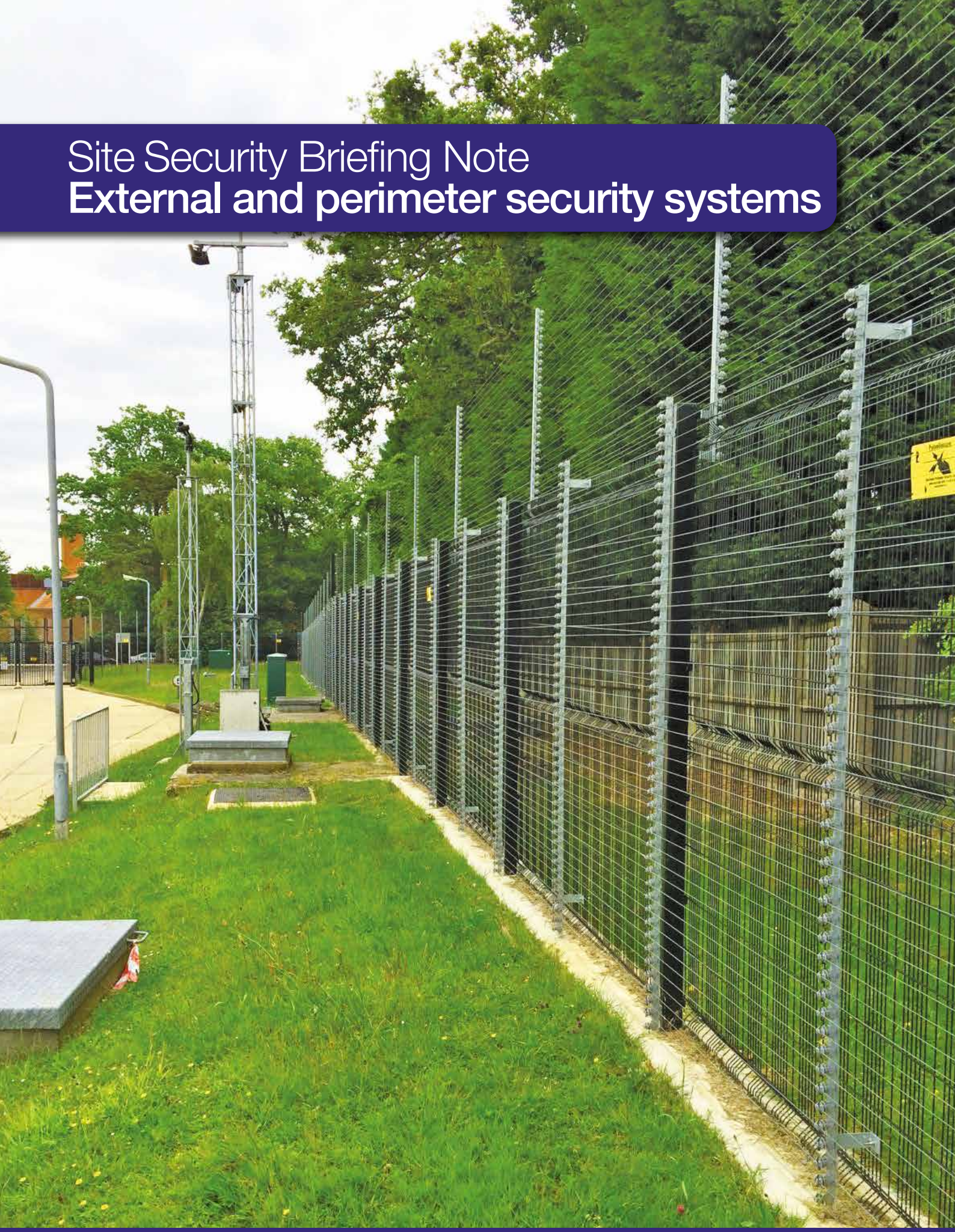
Site Security Briefing Note
External and perimeter security systems



RISCAuthority

administered by

FPA Fire Protection Association

INTRODUCTION

This document provides a description of external and perimeter security (EPS) systems, their practical application and an overview of the technologies currently employed. EPS systems are designed to detect intruders present in, entering or attempting to enter external areas outside enclosed buildings which may or may not themselves have the protection of an intruder and hold-up alarm system (I&HAS).

There are a number of different reasons why an EPS system might be considered necessary, for example:

- the site has no significant physical perimeter security and none will be provided
- deterring attacks on the perimeter security
- substituting for human surveillance through transmission of signals to a monitoring centre out of operational hours, so that a response can be made
- the existing physical security of the site perimeter is considered inadequate and improvement is not cost effective and/or practical
- an EPS is seen as the most cost effective additional protection for property stored in the open
- there are safety hazards on site and the presence of trespassers must be notified with minimum possible delay
- the existing physical security of the site perimeter is considered adequate only provided attempts at its penetration will be reliably detected to allow an intervention to be made
- the assessed risk is of such severity that an intruder detection system is considered necessary, irrespective of the value of the sum total of all other security measures that are, or will be, in place (building security, perimeter security, manning levels, surveillance, intervention resources etc)

SPECIAL FEATURES OF AN EXTERNAL SYSTEM

Before looking at the specific technologies commonly employed by EPS systems, it is useful to consider the particular requirements of, and constraints on, such systems that differentiate them from other security system solutions. It would, for example, be an oversimplification to assume that an EPS system is simply an adapted version of a standard intruder system (i.e. an I&HAS) inside a building, albeit that under certain conditions an I&HAS might be extended in a limited way outside of the supervised building(s) (see below). The architecture and functioning of an EPS is basically different from an I&HAS.

For example:

- an I&HAS in buildings is generally of consistent and simple design whereas an EPS system is often bespoke, extensive and complex
- an external system may have to be designed to take account of the presence of personnel on site at times of day when an operational I&HAS is protecting an unoccupied building
- EPS systems generally allow the user to activate and deactivate protection zones according the needs of the site, in contrast with most I&HAS systems which are designed on the basis that the entire system will be activated when set
- the components of an external system are inevitably more exposed to the elements and criminal interference
- EPS system detectors often output detailed information on detected events, whilst the output of I&HAS detectors is usually binary i.e. ‘clear’ or ‘alarm’
- I&HAS detectors are designed to minimise false alarms whereas the inevitability of nuisance alarms is recognised in the design of EPS detectors
- an external system may receive some of its power from local wind or solar generation
- in the UK, the activations of an I&HAS system are usually channelled via an Alarm Receiving Centre (ARC) to the police and/or keyholder for a response but police will not accept signals from an EPS system and it follows that any external detection capability extending from an I&HAS system must not be allowed to cause a signal to be sent to police – consequently activations by either type of system have to be responded to by those already on site or keyholders.

A sophisticated external system will allow the user to influence processing in terms both of the sensitivity of detection (the amount of suppression of nuisance alarms at the expense of 'genuine' alarms) and the so-called 'protection level' (a value influenced by the user that governs the degree of certainty of a particular category of event generating an alarm condition).

Such a system will also allow the user to determine the 'alarm level', being an indicator of the weight the user wishes to attach to each level of alarm output generated by the system after the processing described above has operated on the input signal. The nature of the response to be assigned to each level is a matter for the user (e.g. low priority/slow response, higher priority/faster response). Furthermore the flexibility of a sophisticated system allows the user to 'promote' and 'demote' the various protected zones according to the circumstances (time of day, threat level etc).

As external systems are subject to the elements, which can significantly impact their performance (fog for example), processing, user indication and user control need to be more sophisticated than an I&HAS masking detection capability.

TYPICAL SYSTEMS

Ideally, the decision to include electronic security for the site is taken at the very outset of the security planning because the integration of electronic measures can have a bearing on the decisions taken for physical and manned guarding measures. For example, the value of electronic detection is amplified when designed in such a way that an alert is given in advance of a physical barrier being breached. Extending this principle, a layered approach becomes an attractive option whereby the electronic detection is effectively deployed in the 'dead' zone between two or more barriers (layers).

For optimum results, the physical circumstances of the assets to be protected, the expected style and method of attack and the performance required of the system should be taken into account in determining the type of solution to be selected. Each solution has its strengths and weaknesses according to the application. The available solutions can be seen as broadly fitting one or more of the following high level descriptions:

Detection of:

1. Breach of an alarmed physical barrier e.g. by climbing or penetration
2. Incursion into a protected area that does not have an alarm protected barrier
3. A person or persons present, or moving, in a protected area

A family of security solutions is available for each of these scenarios:

1. Breach of a physical barrier

1.1 Perimeter Intrusion Detection Systems ('PIDS')

Perimeter fence and wall mounted solutions are often referred to as 'PIDS'. This form of detection relies on linear or interlinked discrete sensors to pick up and analyse the mechanical disturbance of an existing or specially provided metal fence/gate or (less often) a wall. Generic types of detector commonly specified in this application are tabulated on page 8.

Image: Jacksons Fencing

A vibration sensor

Implementation issues:

Clearly, such detection needs to be supplemented in the case of a gate by sensors that detect its opening by normal means. It is vital that fences bearing intrusion detection devices of this kind are rigid, robust and well maintained. Chain-link fencing for example

would be a poor choice. The rigidity of fencing such as 'Securi Mesh 358' welded mesh panels is ideal (see RISCAuthority guide: Site security: fences, walls and gates).

The results from installation on a wall are likely to be variable depending on the type and condition of the wall and expert evaluation is called for before a commitment is made to the selected solution. Special measures will probably be necessary to ensure that sensitivity across the surface is adequate and uniform. In the case of both a fence and a wall the barrier should be suitably extended at the top, e.g. with barbed tape with adequate system sensitivity to scaling and climbing clearly demonstrated.

If the detection solution is not of the type capable of pinpointing the location of attempted intrusion the protection must be divided into independently indicating zones of such length as to allow rapid, unambiguous location of intrusion on the part of a local observer. The PIDS and any CCTV system need to be linked in such a way that the penetrated zone is displayed automatically to the operator upon a detection event (see RISCAuthority document S23 Guidance for specifiers of CCTV in security applications).

1.2 Electric fence

A form of 'PIDS' in that a linear detection function is combined with an active element designed to deter and repel an intruder. Unlike a conventional 'PIDS' however these solutions are mechanically complex and have potentially onerous safety and security considerations associated with them.

The product usually employs a 'taught wire' system whereby not only do the wire strands administer a disabling, brief, high voltage shock to an attacker but also register cutting or displacement of the wire to generate an alarm.

Implementation issues:

The electric fence can be installed against and parallel with a new or existing fence, either on the attack or defended side of the perimeter, or as a stand-alone implementation as a topping to a wall to deter climbers. Aside from its detection and deterrent capability the product functions, as does any other fence, to exclude intruders and trespassers, although it is not designed in itself to delay physical intrusion as effectively as conventional high security fencing and, being a semi-mechanical device, there may be a greater need for periodic inspection and maintenance.

Provided the product conforms to HSE guidelines, the administered shock should not cause permanent harm but, nonetheless, it should not be installed where adventurous children or those going about their normal business could come into contact with it. Warning notices must be posted in accordance with HSE guidelines. The product

Full height electric fence

Electric fence topping to mesh fencing

The ubiquitous external PIR

Infrared beam units

Laser scan detector

and installation should conform to *BS 1722-17 Fences. Specification for electric security fences. Design, installation and maintenance.* This standard covers matters such as spacing of posts, wires, min/max voltages (and shock duration), links to alarm and CCTV systems and power back up. Other parts of BS 1722 contain guidance for manufacturers and installers of other types of conventional fencing such as chain link, timber, palisade and steel mesh. Members of two trade bodies, the Fencing Contractors Association (FCA) and the European Fencing Industry Association (EFIA), are required to maintain best industry practice.

2. Incursion where there is no barrier

As there is no physical barrier on which to mount detection devices, the generic detector types suitable for this application include movement detectors, especially narrow beam or 'curtain' external versions of the passive infrared detector (PIR), point-to-point beam interruption type devices and the recently developed laser scan device. These are included in the table on page 8 which also includes the more exotic buried sensor solution, which is only rarely used but can have an application in selected situations.

Implementation issues:

The dominant device for this application is the PIR detector, which is designed to be sensitive to movement across the field of view rather than toward/away the unit.

Each of these devices has particular potential false alarm issues which must be taken into account before implementation. The false alarm exposure is, needless to say, exacerbated by the absence of a physical barrier between the detection and outside human and environmental disturbances. However, conversely, where they can be used in support of physical barriers, they lend themselves to a layered strategy whereby the protection is deployed between two physical barriers, which serves both to screen the devices from false alarm sources and, at the same time, delay the attacker within the zone of high detection sensitivity, thus giving the electronics the best possible chance of generating a genuine, credible activation.

3. Detection of human presence and/or movement

Once again in this application the favoured device is the passive infrared detector which, in this case, is more effective with a wide angle field of sensitivity. In addition, a laser scan detector can also be specified for this purpose.

However, irrespective of whether there is a physical perimeter or defined boundary, some applications require economic detection of a very large acreage – for example where assets are scattered as on an airfield – and/or it is imperative to have the earliest possible notice of incursions. Cost effective protection in this situation is possible borrowing from technology that has been in military use for some time, usually consisting of wide area ground radar systems which generate a signal when the radar field is penetrated. The field of detection is volumetric (a 'cloud' of sensitivity) rather than linear (point-to-point). Systems available for security applications

are optimised for credibility and false alarm management through technology capable of limiting detection to delineated sensitive zones, determination of target speed, range and direction of travel and target tracking in conjunction with CCTV.

Radar transceivers

Implementation issues:

As before, if the protected space has no, or only a questionable physical perimeter, the inevitable additional sources of false alarms must be taken into account. Terrain is important, particularly when deploying technology such as powerful long-range or wide area radars, for which terrain undulations and solid objects create shadows of insensitivity. For this reason, deployment of multiple low power units rather than a single long-range type is likely to give better results.

In reality, most of the above product types are versatile enough to be used in more than one of the above three applications as defined. For example, buried sensors and a latticework of active beams would serve perfectly well for detecting movement on an area basis, whilst a line of buried sensors or a series of curtain PIRs could do the job of supplementing a physical perimeter.

Improved reliability is achieved if discrete detectors using different technologies are linked in the logic of the system processor to produce alerts on coincidental triggering within a timeframe. Alternatively detectors are available that combine technologies in a single product, sometimes referred to as a 'dualtech'.

Inclusion of an uninterruptible power supply (UPS) is recommended for resilience on high security sites. Where cabling presents a problem detectors are available working on a wireless basis (discouraged unless unavoidable).

CCTV

Many end users and specifiers seeking a technical solution to the security of a bounded or unbounded area will simply opt for video surveillance (CCTV), assuming this to be the obvious choice. However there is a very significant manpower penalty with this option. Unless the CCTV system incorporates some form of image analysis, such as Video Motion Detection (VMD) or Video Content Analysis (VCA), the CCTV monitors must be continuously attended and observed in case a security event is missed.

Since standard CCTV technology, (including thermal imaging systems which operate in darkness), and the associated sophisticated analysis technologies are by nature so far removed from the security products coming within the EPS market, they are not considered in this guide, deserving their own guide (RISCAuthority guidance document *S23 Guidance for specifiers of CCTV in security applications*).

That said, a hybrid security solution developed in the UK known as Detector Activated CCTV (DA CCTV) exists that combines video with conventional EPS devices. In a DA CCTV system each camera is married to one or more EPS detectors in such a way that when an event is detected, associated 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.

Elements of a Detector Activated CCTV system (camera, PIRs, loudspeakers)

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'.

However, even where criminal activity is not seen, the system does have the potential to interrupt the incursion and drive the trespassers from site by operating local loudspeakers to broadcast an 'audio challenge' – a verbal message to the effect that the trespassers are in view and the police will be summoned if they fail to leave.

DA CCTV has three benefits in particular. The first is the minimisation of false triggering, through the ability to view an image of the location of the event before confirming the event as an alarm. The second is that systems conforming to the applicable standard (*BS 8418 Installation and remote monitoring of detector-activated CCTV systems – Code of practice*) are entitled to a police Unique Reference Number (URN). This means that when operating reliably they will receive the same level of police response to an alarm activation as does an I&HAS system with a URN. Thirdly, in combining the qualities of EPS devices engineered for the external environment and the benefits of video surveillance, security staff on site can usually be dispensed with.

Thus although a hybrid system, not qualifying as an EPS system as such, DA CCTV has been included in the table of EPS types on page 8.

TEMPORARY (AKA RAPIDLY DEPLOYABLE) SYSTEMS

Temporary external systems 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. At their simplest, these consist of a movement detector in a transportable housing, capable of networking with a number of others deployed strategically around assets and signalling to a security post or monitoring centre via a radio system such as one of the cellular/ mobile networks.

image: VPS (UK) Ltd

Temporary/mobile alarm/CCTV unit

Activation could summon a member of security staff or a guarding service to the location to establish the cause. A more elaborate set-up might consist of at least one fully functional camera on an elevating mast linked to on-board and/or deployed movement detectors, an audio challenge facility and hard disc recording, all in a single mobile package. Battery power, maintained by wind/solar charging, can be included should no mains or locally generated electricity be available or to cater for interruptions of the mains supply. An industry code of practice exists in this field namely 'SS 2004' published by the Security Systems and Alarm Inspection Board (SSAIB).

TABLE OF DETECTOR TYPES

Primarily to detect:	Description	Strengths	Limitations
Defeat of a physical barrier	Audio/vibration detection cable	Cost-effective; low complexity; reliable, tried and tested; good range of sensitivity adjustment	Exposed to false alarms from wild life, weather etc
	Linear capacitive detector	Capable of very high sensitivity to human contact/proximity	'Exotic' technology requiring expert set-up; only suitable in selected applications; excessive potential for false alarms
	Fibre-optic cable	Cost-effective; good range of sensitivity adjustment; immune from some common false alarm sources	None of significance
	Shock/vibration sensors	Discrete sensors with independent sensitivity adjustment for tailored protection in selected applications	Might be uncompetitive with linear detectors
	Detector activated CCTV	Systems conforming to BS 8418 enjoy Level I police response per the NPCC policy; exceptional false alarm control as images coincident with activation are subject to discrimination by an operator	High initial and ongoing cost; easily neutralised unless effective measures to control sabotage are taken; especially costly if immunity from mains failure is required
Incursion where no barrier exists	External grade passive infrared detectors (PIR)	Cost-effective; flexible detection patterns; intelligent processing	Undermined by hostile weather over time; false alarms from environmental factors such as wildlife, solar radiation etc
	External grade active infrared beams	Cost-effective; low complexity; 'certain'; high security; point-to-point protection that is difficult to evade when configured as a 'fence' of beams	Beam alignment critical; uneven terrain can allow 'crawl-under'; false alarms from environmental factors such as wildlife, precipitation, fog

	Microwave 'fence' detectors	Three-dimensional 'cigar' of 'certain'; high security; point-to-point protection that is difficult to evade	Uneven terrain can allow 'crawl-under'; possibility of unprotected space next to the transmitter and receiver above and below the 'cigar' as it fans out
	Laser scan detector	Sophisticated processing facilitated by detection of target size, speed and distance away, potentially allowing reliable detection and well-controlled false alarms	Higher cost than some competitive technologies
	Buried seismic/pressure sensors	Sophisticated; complex; capable of excellent sensitivity; totally covert (e.g. an attractive option if natural appearance must be preserved); useful if entrapment is the strategy	Poor cost effectiveness; requires expert survey and set-up as nature of ground, drainage etc is critical; highly exposed to false alarms from environmental vibration etc if sensitivity setting is excessive
	Detector activated CCTV	As above	As above
Presence/movement within an area	External grade passive infrared detectors (PIR)	As above	As above
	Laser scan detector	As above	As above
	Radar	Cost-effective if protection of a very extensive open area is required; field of sensitivity is adjustable and false triggering is controlled by sophisticated target behaviour analysis	Electronic processing might not completely neutralise the effects of weather conditions such as rain and snow and, unless the site is flat and open, long-range units are especially impacted by undulations and obstacles
	Detector activated CCTV	As above	As above

For more information see RISCAuthority guides:

BDM10 Code of practice for the protection of empty buildings - Fire safety and security

S10 Guidance for the protection of premises against attacks using vehicles (ram raids)

S20 Essential principles for the protection of property

S21 Measures for the control of metal theft

S23 Guidance for specifiers of CCTV in security applications

S29 Guide to electronic access control systems

S30 Terrorism - sources of guidance and support

S31 Unauthorised occupation of non-residential premises – guide to managing the risk

Site Security Briefing Note: security lighting

Site Security Briefing Note: site layout

Site Security Briefing Note: fences, walls and gates

Site Security Briefing Note: manned guarding

Other sources of information

The European electro-technical standards body CENELEC has a committee developing a type of standard known as a 'Technical Specification' on this subject: *TS 50661-1 Alarm systems - External perimeter security systems - Part 1: System requirements*. The UK is represented on the committee but it is not yet known whether UK will adopt the document on publication.

On its website the Centre for the Protection of National Infrastructure (CPNI) publishes an excellent guidance document: 'Guide to Perimeter Intrusion Detection Systems (PIDS)'. The document goes into considerable depth across the subject including system types, system design, the causes of false alarms and how they are combated, installation and commissioning, alarm handling and operation.

The assistance of Optex (Europe) Limited with document review and images is much appreciated.

Notes

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