Home Office

Guide to Perimeter Intrusion Detection Systems (PIDS)

Publication No. 05/12

In partnership with

CPNI
Centre for the Protection of National Infrastructure

Guide to Perimeter Intrusion Detection Systems (PIDS)

Publication No. 05/12

Guide to PIDS

Publication No. 05/12

FIRST PUBLISHED MARCH 2012

Home Office Centre for Applied Science and Technology
Langhurst House
Langhurstwood Road
Horsham
RH12 4WX
United Kingdom

Telephone: +44 (0)1403 213800
Fax: +44 (0)1403 213827
Email: cast@homeoffice.gsi.gov.uk
Website: www.homeoffice.gov.uk/science-research/cast

Or:
TDF/22
Central Support
PO Box 60628
London
SW1P 9HA

Foreword

Adherence to the guidance presented in this document does not in itself confer immunity from legal obligations.

Users of this guidance document should ensure that they possess the latest issue and all amendments. These are available from CPNI, or direct from CAST.

Acknowledgements

This document was produced following consultation with members of the CPNI Electronic and Imaging Systems Programme – Detection and Control Working Group.

CONTENTS

1 Introduction

This guide has been written by the Home Office Centre for Applied Science and Technology (CAST) in partnership with the Centre for the Protection of National Infrastructure (CPNI). It is intended to help security managers and practitioners working for the UK government and critical national infrastructure to effectively specify and manage Perimeter Intrusion Detection Systems (PIDS).

PIDS are systems used in an external environment to detect the presence of an intruder attempting to breach a perimeter.

This document provides guidance on the specification, selection, usage and maintenance of the four main categories of PIDS:

Barrier-Mounted

PIDS deployed on or in conjunction with a fence or other physical barrier (e.g. microphonic cable).

Ground-Based

PIDS deployed below ground (e.g. pressure sensitive cable). These do not require a physical barrier.

Free-Standing

PIDS deployed above ground that do not need to be installed on or in conjunction with a physical barrier (e.g. bistatic microwave link).

Rapidly Deployable

PIDS that are designed for temporary deployment; for example, to protect a mobile asset. Rapidly deployable PIDS are often battery powered and transmit their alarms wirelessly, and are available in each of the above application areas.

Guidance for Wide Area Detection Systems (WADS) will be incorporated in a revision of this document scheduled for 2013.

To aid the effective selection and application of PIDS, a common protocol for evaluating PIDS is required. To this end, the Home Office Centre for Applied Science and Technology (CAST) has produced a suite of performance evaluation standards for PIDS as part of its work with the Centre for the Protection of National Infrastructure (CPNI).

2 Further information

It is impractical to include everything of relevance in this guide and each individual site will have specific issues which will need to be addressed. Specialist advice and supporting guidance documents are available through the relevant CPNI sector adviser, or from the CPNI website:

www.cpni.gov.uk

For government users protective security policy which determines appropriate selection of PIDS is set out in:

- the *Security Policy Framework* (SPF), which includes the:
- *Security Assessment for Protectively Marked Assets* (SAPMA) questionnaire, for assessing the security of protectively marked material.

For Critical National Infrastructure (CNI) users, the selection of appropriate PIDS will be made following production of a detailed Operational Requirement (Level 1 and Level 2) and consultation with CPNI.

Security products approved for use are listed in:

- the CPNI *Catalogue of Security Equipment (CSE).*

3 Scope

This document has been prepared to provide users with guidance on the specification, installation, operation and maintenance of PIDS.

Before attempting to write a performance specification for a PIDS, it is important to ensure that a detailed operational requirement (OR) has been produced. Advice can be found in the CPNI publication *Guide to Producing Operational Requirements for Security Measures*.

Figure 1 shows the recommended stages for selecting and installing a PIDS. The shaded portions of the flow chart are covered within the scope of this document.

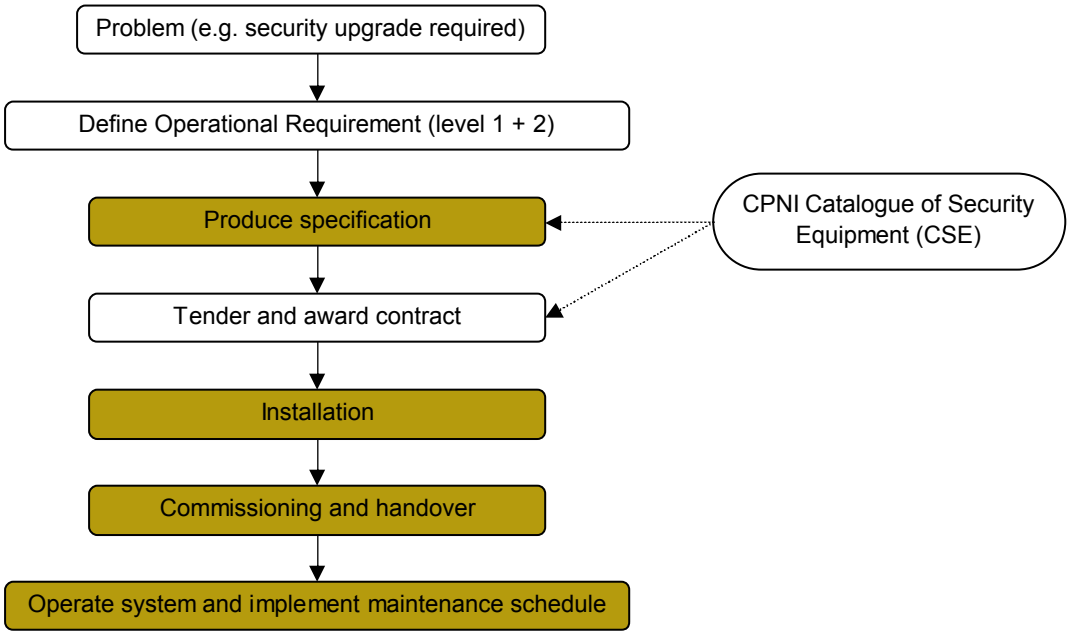


Figure 1: Stages in the selection and installation of PIDS

CPNI regularly carry out evaluations of PIDS to the suite of standards that have been prepared by CPNI and CAST. This programme of evaluations is guided by the government and CNI security community who specify which PIDS are of most interest. The procedure for evaluating PIDS is as follows:

- Security community register interest with CPNI in specific PIDS technologies or systems;
- SEAP panel agrees systems to test;
- Evaluation of commercially available PIDS to the appropriate CAST/CPNI PIDS evaluation standard; following this
- SEAP panel make decision based on evaluation results.

4 Specification

4.1 General specification

The specification and selection of any PIDS depends upon a number of factors relating to the operational requirement and local circumstances:

Landscape and topographical features;

Integration with other types of equipment or systems;

Climatic conditions;

Local regulations;

Local environment and current / planned infrastructure;

Whether or not there is a physical barrier and what it consists of;

Duration of required deployment (rapidly deployable PIDS);

Response force arrangements; and

Personnel on site.

Specific points to be addressed in a PIDS specification or other associated contract documentation include:

Specifying PIDS – It may be acceptable to indicate or exclude a particular PIDS technology; within tender documentation users should specify a list of products, from the CSE, which meet the minimum required CPNI Grading for the application. If a single system is specified then there can be problems in determining liability and responsibility if the system does not perform as required (assuming that it has been installed correctly).

Integration with existing systems – Specification of a PIDS should not be done in isolation. If the system is required to be integrated with other systems – for example cameras, lighting or existing control room software – then information on this should also be included. Who will be responsible for the integration?

Areas to be protected – Including length of the perimeter to be covered; details of any barriers already in place; and space (width) available over which detection can take place.

Duration of deployment – The planned period of time over which the PIDS will be deployed will affect system selection. Rapidly deployable PIDS are only to be utilised for 'temporary cover'. Additionally, the system will require re-commissioning after a maximum period of two weeks during a deployment. This allows the security risk to be re-assessed and checks of the integrity of the system's wireless communication link to be undertaken, to ensure that the system is functioning as required.

Consideration should also be given to the required lifetime of a permanent system – a system that will require replacement on a relatively short timescale is likely to be unsuitable for a permanent PIDS installation.

Physical requirements – See Section 4.2 'Physical requirements'.

Environmental conditions – Including weather conditions and wildlife (further information is provided in Section 4.3 'Environmental selection criteria').

Threat types – Types of attacks to be detected.

Acceptable performance levels – Further information is provided in Section 4.4 'Performance requirements'.

Operator interface – How should the alarms (intruder, tamper) be displayed and logged? Further information on operation and monitoring options is given in Section 4.5 'Control and indication'.

Alarm transmission for permanently installed PIDS – Wireless transmission is not recommended and should not be used for the SEAP HIGH or ENHANCED Protection Level or SEAP Class 2, 3 or 4 systems because of concerns over denial of service, substitution or replay attacks. If wireless alarm transmission is being considered at BASE Protection Level or Class 1, users must consider the response to a loss of communications - technical advice should be sought from CPNI.

In all instances a back-up/secondary communications link is required and should be tested during operational checks.

Alarm transmission for rapidly deployable PIDS – Where sites require ENHANCED or HIGH Protection Level, or Class 2, 3 and 4, rapidly deployable PIDS using wireless communications as their primary communications link must only be used for a maximum of two weeks.

Tamper detection – State the system aspects to be protected and the expected action. For example, an alarm should occur if:

Any system cabling is cut or shorted;

The sensor is rotated or repositioned; or

Any housing covers are removed.

Alarm verification – To help distinguish false alarms from true alarms which require a response, it is useful to have a method of verifying the alarm in the control room. Possibly the most common and straightforward method of verifying alarms involves obtaining CCTV imagery from immediately before, during and after the alarm. This imagery allows the most appropriate response to be made to the alarm. For this to work effectively, the camera and PIDS zones must match and images should be automatically presented to the operator on generation of an alarm.

Section 4.5 'Control and indication' contains further advice on specifying an alarm verification system.

Power requirements – Details of what power is available and where it can be accessed should be provided. If the system should include protection against voltage surges it should be stated. Which standards or regulations the

installation should comply with are to be stated. Details on the battery life and charging time should be sought for rapidly deployed systems.

Standby power supplies – What should happen if there is a power failure or power fluctuations? What back-up power is required? How long would it need to last? It is essential that any back-up power facility is provided to ensure that the PIDS will continue to operate and will be capable of signalling an alarm to an operator in the event of a power failure. Would CCTV be available in the event of power failure? Further details are provided in Section 4.5.4 'System resilience'.

Radio interference/radiation – The PIDS should not interfere with any other electronic equipment in use; and operation of the PIDS should not be affected by the use of other electronic equipment. Devices should comply with electromagnetic compatibility (EMC) regulations and should be 'CE' marked. EMC requirements for security equipment are specified in BS EN 50130-4:1996 'Alarm systems. Electromagnetic compatibility. Product family standard: Immunity requirements for components of fire, intruder and social alarm systems'. This is a particularly important consideration if wireless alarm transmission is proposed.

Special environments – There may be environmental constraints to be considered. For example, in areas where there is a risk of explosive atmosphere (e.g. oil rigs, refineries), the PIDS and any enclosures must be intrinsically safe and comply with relevant safety regulations.

Access constraints – Give details of any restrictions on access to the site (particularly for heavy plant equipment), requirement for an escort, or time constraints limiting when an installation may be conducted.

Visibility – If the installation needs to be covert, this should be detailed.

Contractual requirements – Warranty period and conditions, retention of payments and other terms and conditions need to be considered. The specification should state that commissioning tests will be performed prior to acceptance of the system; this should also be reflected in the contract documents.

To help ensure that performance requirements are met, and to provide a baseline performance log against which degradation of the system can be monitored, the site should ensure that commissioning tests are performed prior to acceptance of the system. This requirement should be included in the contract documentation and the results of the commissioning tests need to be handed over in order to form this baseline. Tests comparable with those performed during the initial commissioning should be performed at the following frequencies:

12-monthly intervals for BASE Protection Level systems;

6-monthly intervals for ENHANCED and HIGH Protection Level, and Class 1, 2 and 3 systems; and

3-monthly intervals for Class 4 systems.

Consideration should be given to the period over which FAR is assessed against the performance requirements. See Section 5.2 'Commissioning' for further information.

The performance of a PIDS over an extended period - and under various environmental conditions - cannot be determined during an initial, relatively short, commissioning period. Therefore it is important that the installation contractor remains liable for any inability of the system to meet the required performance criteria that may be revealed during the warranty period. The results of evaluations carried out to the CAST/CPNI PIDS evaluation standards can be used to gain an understanding of the performance capabilities of PIDS. Such results are held by CPNI and CAST and may be made available upon enquiry via CPNI sector advisors. Appendix I of the CAST/CPNI PIDS evaluation standards contain advice on using the results from different evaluations performed to the standards, to make comparisons between systems.

Information to be considered when specifying performance requirements is provided in Section 4.4 'Performance requirements'.

4.2 Physical requirements

It is important not to over-specify the system by including too many physical constraints which might unwittingly compromise performance. However, the following factors can have a substantial impact on the suitability of a PIDS solution and should be included in the specification where relevant:

Ground surface/mounting position/burial medium – Will a free-standing system operate over gravel, concrete, tarmac, grass, sand, bodies of water or a combination of different media along its length? Will a ground-based system be buried in sand or clay-based soil? The performance of a PIDS can vary considerably, depending on how well suited the particular technology is to the operating environment. The full specification (build) and condition of any fence in the case of barrier-mounted systems is important to note. Tables 1, 2 and Section 7 contain more information on the effect of environmental factors on different PIDS types.

Local topography – Are there any undulations in the ground surface? Undulations occurring over the distance of a metre - up to several tens of metres - can shield the presence of an intruder from some detection technologies, particularly in the case of microwave systems, or active or passive infrared. Are there any surface objects (roads, fences, lighting columns etc.) to be negotiated?

Conducting bodies – Microwave and other active electromagnetic systems can be affected by metal or other conducting bodies close to their detection zones both above and below ground. This includes metallic fences, vehicle access and also flowing water. The presence of such bodies in proximity to the planned route of the PIDS must be declared in the specification.

Zone lengths – Long zone lengths can make it difficult for operators to identify the cause of an alarm and/or locate an intrusion. Some PIDS provide positional information on intrusion location. PIDS zones should be matched with the field of view of one or two CCTV cameras where video verification of alarms is required. It is, however, important to perform tests at all zone ends to ensure that camera footprints overlap sufficiently and detection capability is not compromised.

Mounting of sensors, processors, junction boxes – These system elements should be mounted such that detection is expected before any components of

the system are reached by an intruder. For example, mounting the processor box for a barrier-mounted PIDS on the fence fabric is not recommended.

Future site expansion – Provision may need to be made for any forthcoming expansion plans at the site, such as additional capacity within cable ducting and electrical enclosures. Consideration at an early stage is likely to save costs.

4.3 Environmental selection criteria

As perimeter intrusion detection systems are typically used in outdoor scenarios, they are subject to changes in environmental and other local conditions.

It is important therefore to consider and specify the environmental conditions within which the PIDS would be expected to operate.

Detailed site drawings showing entrances, exits, roads, paths, fences, power, ducting etc. should be included with the specification to help potential suppliers identify and assess the situation as a whole.

PIDS are likely to experience changes in their operating environment during the course of a day (for example different day/night variations in wildlife and on-site personnel activity) and also throughout the year (for example seasonal weather variations). These factors can have different effects on PIDS' performance. Some circumstances could cause an increase in the number of false alarms; others could reduce the detection performance.

Table 1 provides information on some of the main weather conditions that should be considered.

Table 1: Weather conditions and their impact on PIDS

		Impact		
Condition	**Example value / range**	**Barrier-Mounted**	**Ground-Based**	**Free-Standing**
Temperature	-20 °C to +55 °C	Ice formation at extremely low temperatures can increase the loading of a fence and cause false alarms. Not likely to be a significant problem in UK.	Frozen ground and thermal expansion and contraction of the ground can cause false alarms. Not likely to be a significant problem in UK.	Rapid changes in ground surface temperature can cause alarms for some systems (e.g. PIR).
Humidity	0 - 95% non-condensing	High humidity may affect electronics by causing corrosion. This can be minimised by ensuring all housings have the correct IP rating for the environment in which they will be used.		

Condition	Example value / range	Barrier-Mounted	Ground-Based	Free-Standing
Exposure to sunlight		UV radiation can cause plastic components, particularly cable ties, to become brittle and eventually fail.	No appreciable effect.	Solar radiation can affect the performance of some technologies, rapid changes (e.g. caused by clouds moving across the sun) causes false alarms with PIR systems. Consideration should be made for the positioning of PIDS with respect to the rising and setting sun, particularly PIR and video based detection systems.
Wind speed	up to 65 km/hour	Fence and topping vibrations caused by high winds are a significant cause of false alarms for barrier-mounted PIDS.	Ground heave caused by the roots of trees moving in the wind can cause alarms. Debris blown through the field of an active system may cause alarms.	The alignment of free-standing systems may be affected. Blowing grass can significantly change thermal patterns for PIR sensors. Debris may also be blown through the detection zone by high winds.
Rainfall or rain rate	up to 25 mm/hour	Heavy rainfall can induce fence and topping vibrations.	Sodden ground does not transfer pressure well and pooled water is highly RF absorbent, causing particular problems for active systems.	Very heavy rainfall may cause false alarms; reduce detection performance; or reduce the effective range of detection zones.
Fog		No effect. CCTV views may be obscured restricting alarm verification.		Little effect on systems other than active IR and laser scanners where fog disperses the beam. Thick fog can cause continuous false alarms for these system types. CCTV views may be obscured restricting alarm verification and the effectiveness of video based detection systems

Condition	Example value / range	Barrier-Mounted	Ground-Based	Free-Standing
Snowfall	up to 30 cm/hour	Snow settling against host fences can increase the loading on the fence and affect fence dynamics.	Deep snow can disperse the pressure of an attacker. It can also act as settled water, reducing the detection ability of EM radiating systems.	Falling snow can trigger false alarms in beam break type systems. Conversely, the uniform ground temperature afforded by snow cover reduces the likelihood of false alarms for PIR systems.
Freezing conditions (ground frost, ice)		Significant ice formation can increase the loading of a fence and cause false alarms. Relay switches can freeze into position at very low temperatures – causing continuous alarms. Not likely to be a significant problem in UK.	Relay switches can freeze into position at very low temperatures – causing continuous alarms. Not likely to be a significant problem in UK.	Freezing conditions can cause ice to build up on the surface of the sensors, reducing their detection performance or increasing their false alarm rate. Relay switches can freeze into position at very low temperatures – causing continuous alarms. Not likely to be a significant problem in UK.
Lightning strikes	inside a radius of 1 km	Lightning strikes can damage system electronics. Mitigate by suitable earthing or other measures.		

Table 2 contains general environmental (non-weather) conditions which need to be considered.

Table 2: Environmental conditions and their impact on PIDS

Condition	Impact
Pedestrians adjacent to perimeter	Where people have access to the perimeter (e.g. a public footpath alongside the perimeter fence), microwave or other radiating field systems may detect them. Pedestrians may also stray into the detection zones where there is no physical barrier in place. In addition, pedestrian activity alongside a barrier could cause alarms from PIDS mounted on the barrier.
Legitimate pedestrian or vehicular access	May require certain zones to be switched off at particular times of day, for instance.
Vehicular traffic routes adjacent to perimeter	Heavy vehicular traffic can cause vibrations which can cause false alarms if in close proximity to a ground-based or barrier-mounted PIDS installation. Extreme vibrations may cause free-standing PIDS sensors to move out of alignment and cause false alarms. Passive

Condition	Impact
	infrared systems are sensitive to distant hot objects, e.g. vehicles. If they are not angled correctly, they could be triggered by the hot exhaust of vehicles passing by.
Machinery	Heavy machinery in the vicinity may cause vibrations and generate false alarms in PIDS as above.
Rivers and streams	Microwave systems are particularly sensitive to bodies of moving water. Consideration should be made as to whether flooding is likely as very few PIDS are designed for water immersion.
Coastal	Electrified fence systems are particularly sensitive to high salinity environments, where salt deposits can form causing short circuits. Strong winds, sea-fog and birds are other factors to consider for all PIDS types.
Trees and vegetation	Trees and vegetation encroaching into a detection field of a free-standing PIDS or very close to / touching fences (barrier-mounted PIDS) could cause false alarms when blown by winds. Trees may also produce fruit or other organic debris which can interact with the detection zone. The roots of trees that are moving in the wind can cause particular problems for ground-based PIDS as the movement is seen as changing pressure in the ground. Grass, if left unmaintained, may cause false alarms in free-standing PIDS when blown by the wind.
Underground and overhead power cables or supplies	Power cables, transformers etc. can result in electrical interference which may affect some PIDS. The presence of any power cables or supplies in or around the detection zone should be declared in the specification. Electrical shielding may be required to prevent this giving rise to false alarms.
Wildlife	Common animals such as rabbits, foxes, dogs or birds often cause false alarms. Systems which are immune to false alarms from a few animals may still false alarm in the presence of large numbers of animals.
Drainage problems	Flooding or water saturation in any part of the detection zone may have significant impact on the performance of some systems. For example, moving bodies of water can cause microwave systems to false alarm. Moving or static bodies of water can cause either false alarms or reduced performance in some ground-based PIDS, particularly RF radiating field systems. Adequate drainage should always be installed and well maintained.

4.4 Performance requirements

4.4.1 Detection

Using the CPNI Catalogue of Security Equipment (CSE) to short-list potential PIDS, users can be assured that they have been tested and proved capable of providing adequate detection and false alarm rates.

It is, however, still necessary to specify detection and false alarm rates when procuring any PIDS in order to ensure that the system is installed and functioning correctly before it goes into operation.

The types of attack styles which PIDS are required to detect should be defined in the specification. Typically, PIDS would be expected to produce alarms in the event of the detection zone being breached by a human using any reasonable means such as walking, running, crawling or cycling for ground-based and free-standing PIDS; and cutting through or climbing over a fence by various means for barrier-mounted PIDS. Although a 100% overall detection rate is desirable a minimum 95% detection rate should be expected[1], which translates to one in twenty attacks being successful (a detection rate of 90% would increase the likelihood of a successful attack to one in ten).

When writing a specification, it is advisable to refer to the relevant CAST/CPNI PIDS evaluation standards, where all standard attack styles are listed.

It is important to state that the PIDS is required to demonstrate at least minimum detection performance across the entire length of the detection zone at all times and that commissioning tests will be conducted at random positions along the detection zone to ensure this requirement is met. If it is acceptable for detection performance to change under certain environmental conditions, this should be stated.

Tests should be identified and implemented during the commissioning of the system to ensure that the PIDS is functioning correctly (NB. see Section 5.2 'Commissioning').

System components may have vulnerability to defeat. Appropriate selection of sensor type together with system design can provide mitigation. If the system is being installed to counter a specific threat, this needs to be defined at the specification stage. If the threat is considered particularly unique or high profile, further advice should be sought from CPNI.

4.4.2 False alarms

False alarms are typically caused by the weather or wildlife (Figure 2). The reason for some of these alarms is that, to the detection system, the event 'looks' like a real attack. For example, a large animal running across a detection zone could cause a drop in the received signal of a bistatic microwave system which would be similar to the drop in signal caused by a human breaching the perimeter. However, there may on occasion be no obvious cause.

[1] Note that PIDS selected from the CPNI Catalogue of Security Equipment will have reached a similar level of performance during evaluation.

Figure 2: Pre-alarm video still of a false alarm cause (fox), captured with thermal imager

Naturally, it is important for any PIDS to produce a minimal number of false alarms. If there are large numbers of false alarms then extra work will be created in assessing the alarms and responding accordingly. This can rapidly lead to loss of operator confidence in the PIDS and consequently, a true alarm may be missed or ignored.

The number of false alarms exhibited by a system may be controlled by adjusting the sensitivity or other system parameters. Typically the sensitivity would be decreased to reduce the number of false alarms; however, in doing so the detection performance is often reduced as well. A compromise must be reached between the number of acceptable false alarms and the detection performance required.

The required false alarm rate (FAR) should be specified in a way which is most meaningful to the application. Examples include:

x alarms per day per kilometre;

x alarms per 30 days per 100 metres; or

x alarms per shift.

The following can be used as a guide as to what can be expected in terms of FAR (stated as alarms per day per linear kilometre – ADK):

0-10 good;

50 mediocre (in bad weather);

50 poor (in good weather);

100+ very poor (and will be ignored).

These values should only be used as a guide. It is important that users or response forces make appropriate considerations specific to their site and circumstances when specifying an acceptable false alarm rate.

4.4.3 Availability/reliability

The specification should stipulate an expected level of reliability from the system in terms of a maximum acceptable proportion of ‘downtime’. For example ‘The system must reliably operate for at least 99% of the time each

month'. At a level of 99% reliability, the system may not operate reliably for approximately four days in any year. Additionally, a mean-time-to-repair may be specified.

If no downtime can be tolerated then the specification must require the provision of secondary systems or procedures to bridge any periods of downtime.

4.5 Control and indication

The control and indication equipment to be used in conjunction with the PIDS must be determined before a system has been procured. Failing this, the situation may arise where a system is theoretically very good, but is so complicated and difficult to operate that it does not get used properly. At the specification stage it is important therefore to determine how the operators will interact with, and respond to, the PIDS as this will affect the specification of the system.

Aspects which need to be considered are given below.

4.5.1 Staffing and facilities

It is essential that monitoring of alarms is coordinated with an adequate response capability comprised of properly trained staff.

There should be sufficient staff to effectively monitor the PIDS; and their other duties should be reasonable to allow for flexibility should additional staff time be required to respond to changing monitoring requirements.

There should be a hierarchy of access permissions to the system with no 'privilege inflation', i.e. staff should only have the access permission level they require to carry out their duties and no more. Regular reviews of permission levels and associated passwords, log-in information, etc. should be made, particularly if/when staff members leave or if new guarding contracts are placed. Such reviews should be incorporated in any general security procedures that are in place, such as reissuing automatic access control (AACS) passes and changing lock combinations.

Examples of permission levels are:

Administrator/Engineer – full access with the ability to change settings (engineers should not be allowed access without supervision);

Supervisors – ability to view alarm records, edit and create reports; and

Users/Guards – ability to view, classify and reset alarms only.

There should be procedures in place when the external investigation of alarms and/or detention of intruders is required. This should be specified in conjunction with any guarding patrol schedules if appropriate and an additional, remote, means of notifying alarms may be required, e.g. pager.

If a dedicated control room is to be used, consideration should be given to its design to ensure it is fit for purpose. Advice can be found in the CAST publication 14/98 *CCTV: Making it Work – CCTV Control Room Ergonomics*.

When considering how the PIDS should be operated and what monitoring is required, it is important to consider if and how the PIDS is required to interface with any other elements which comprise the overall site security system. It is important to consider this prior to procuring the PIDS as any integration requirements should be included in the specification.

If the PIDS is to be integrated with other components (for example cameras, video recorders) then, should the common interface fail, it is important that there is a back-up method of control. This will allow part of the system to remain operational in these circumstances.

Integrating the different components of the security system can make it much easier for operators to use and can prevent duplication of work. Further guidance on this can be found in the CPNI/SSG publication *Achieving Successful Integrated Electronic Security Measures*.

4.5.2 Operation

Consideration needs to be given to a number of factors relating to PIDS operation in order to allow the efficient running of a security system and to cut down on false activations and the loss of system confidence that can result.

Depending on the site, its environment and level of activity, different operating modes may be required for day time, night time, summer, winter or poor weather conditions. These operating modes can take the form of pre-set states that can be readily switched between by an operator with the appropriate permission level. If this approach is to be taken, it is important that each mode of operation is tested to meet the required performance level.

In designing the system, a number of questions need to be addressed:

Are alarms required following a single activation; multiple activations within a set time period; or activation in combination with another system?

A PIDS can be set to alarm following a single event or when two or more events occur within a set time. The latter can reduce false alarms but may also introduce additional vulnerabilities. PIDS should be selected from the CSE and the system configuration, used during CPNI testing, should be applied; site-specific testing can be used to modify these settings as required.

In certain circumstances it is possible for two separate detection systems to be combined by AND'ing their alarm outputs. This requires detection to occur on system 1 AND system 2 - within a defined period of time - before an alarm is signalled to the operator. The benefit is a reduction in false alarms, which will be maximised if differing detection technologies are used. However, there is a consequence to AND'ing alarms: if an intruder is only detected by one of the systems, then the operator will not be alerted. Alternatively, a layered alarm management approach can be used on the individual alarm outputs, with some alarm management systems facilitating different levels of operator alert dependent on individual PIDS, or combinations of PIDS alarms.

Multiple sequential true alarms from one system or from multiple systems enable the progress of an attacker to be tracked and also reduces the probability of the alarm going unnoticed.

How quickly, following alarm activation on a PIDS, should the alarm be displayed to the operator?

A PIDS alarm should be displayed to the operator as soon as possible. If CCTV footage is to be automatically displayed in conjunction with an alarm, there should be minimal delay and it should be displayed on the specific monitor(s) where the operator will expect it to appear.

Long delays in signalling an alarm and then displaying the CCTV footage (if required) can make it more difficult to verify the cause and will delay any response.

Following an alarm, how quickly should the PIDS be able to signal another alarm (reset time)?

Long reset times following alarm (for example, 60 seconds) will reduce the number of false alarms from poorly performing PIDS, but true alarms may be missed during this period. Short reset times (for example, 10 seconds) on the other hand are likely to increase the number of times that a single alarm cause is reported.

Is accurate positional information on the intruder required, or just the alarm zone?

A correctly configured PIDS system will report the zone information with an alarm, accompanying CCTV footage can provide a degree of positional information. It is recommended that each alarm zone is no longer than 100 m in length.

Some PIDS are available that have the ability to determine accurate intruder location within alarm zones. Such features should be rigorously tested at the commissioning and acceptance testing stages and should not be relied upon as the principle means of location verification.

Is an audit trail of actions taken by all users required?

Audit logs can help in analysing system performance.

An audit log should contain date and time of event; identification of event (provided by system if applicable or entered by operator); perceived cause of event (as established by operator); operator response to event; and date and time when the event is reset. This can help in monitoring the quantity, type and cause of alarms experienced, along with whether the appropriate response was taken.

Audit logs can also record details of any changes that are made to the PIDS. This will make it possible to identify when changes have been made and by whom.

4.5.3 Alarm handling

How will the alarms be enunciated? e.g.

Audio alarm enunciation;

Visual alarm enunciation; or

Audio and visual alarm enunciation.

What form will the display take?

Alarms can be displayed as a simple text-based list of alarms. Mimic panels can be used although these have been largely superseded by more sophisticated graphical user interfaces (GUIs). Mimic panels can however be an effective fall-back in the event of a system failure. GUIs typically contain maps or images of the site with alarm locations overlaid to help operators rapidly identify where the alarm originated. Alternatively the PIDS alarms can be integrated into a single GUI with other components of the security system, for example access control system (AACS). Where screens are used to display information, it is important that they are uncluttered and easy to view with the information presented in a clear and concise manner. The size of screen required to achieve this, relative to the viewing distance should also be considered.

Is verification of alarms required?

This can take the form of audio (especially for remote sites) or visual verification (this could be provided by CCTV systems which, on alarm, are triggered to store footage from just before, during and after the alarm).

Where CCTV has been identified as a solution, the following principles should be followed: the CCTV should provide an imaged intruder size that is a minimum of 10% of screen height using fixed cameras. Pan-Tilt-Zoom (PTZ) cameras can be used to supplement the fixed cameras. A loop of imagery should be presented including activity both before and after the alarm to enable a human operator to determine the cause of the alarm and route taken by any intruder(s). Each alarm zone should be linked to one or more camera views. It may be necessary to use multiple camera views to maintain 10% screen height on long or wide alarm zones. If the PIDS is to be supplied with a digital video recording system for the purpose of confirming alarms, the length of footage recorded pre- and post-alarm should be specified as well as any requirement for redundant data storage (e.g. a redundant array of independent disks, known as RAID technology) to reduce the likelihood of video data loss in the event of a hard drive failure.

How will the alarms be managed and what will the operator be required to do?

Alarm logs can be created automatically or manually by the operator. If logs are created manually this can provide the operator with a lot of extra work and could lead to some alarms being missed by mistake. Logs created automatically on a computer system can be saved electronically or printed out to provide a permanent record of events.

Actions which operators might be expected to perform are to ‘accept’ the alarm event (silence any audible signal); ‘verify’ the cause of the alarm event; deploy the required ‘response’; add supplementary information to the alarm log such as observed cause; and then to reset the alarm.

Some alarm management systems do not allow alarms to be reset until an alarm cause is inputted to the log. This compels the operator to verify all alarms.

Operators should be provided with clear instructions on how to determine the cause of alarms and what response is required for different types of alarm.

Weather data may be used to help decide the likely cause of an alarm; however it should not be used as the sole means of determining the cause of alarm.

How will multiple alarms be processed?

While multiple alarms from PIDS could be caused, for example by heavy rain, the operators should be warned that multiple alarms may also be a deliberate diversion caused by a potential intruder. Consideration should be given to how multiple alarms will be stacked or queued by the entire system, or for an individual zone, and whether alarms from particular zones should be given higher priority.

All tamper alarms should be investigated promptly as they could indicate deliberate sabotage or a fault within the sensor. It is recommended that separate alarm signals are used for tamper/fault conditions and for intrusion events so that a tamper alarm can be given a high priority and cannot be simply reset without investigation of the cause.

It is important to ensure that control room operator(s) are not overloaded and that their workload is realistic.

Further guidance on the use of CCTV systems can be found in the CAST publication 28/09 *CCTV Operational Requirements Manual.*

4.5.4 System resilience

It is recommended that a dedicated uninterruptible power supply (UPS) is used to provide resilience should the power to any system components fail. Depending on the site, it may be acceptable to shut down some non-essential services to conserve power.

A procedure should detail to control room staff what happens in the event of power failure or malfunction/breakdown and how such events are to be recorded and handled. Such a procedure should contain details of the UPS capacity/lifetime and what to do if the system power fails completely, contact details for maintenance/support team, additional guarding arrangements etc.

It is desirable to have a comprehensive maintenance contract which specifies expected response times for repairing the PIDS should there be a fault, as well as the acceptable limits on downtime as described in Section 4.4.3 ‘Availability’. Further information on maintenance is provided in Section 6 ‘System management and maintenance’.

4.6 Documentation

Manufacturers of the proposed PIDS should provide the documentation listed below to ensure properly informed decisions can be made regarding the PIDS’ suitability and the reliability of the information provided in the tender documentation:

Topographical requirements and climate conditions the systems are designed to operate in, including formal performance measurements where available;

Details of any radiation emitted by the system (e.g. frequency, polarisation) and devices which may be affected by it, or which may themselves have an effect on the PIDS;

Details of any certification or formal testing from approved bodies (including CE Certification);

Independent test certification as evidence of system and component compliance with European electromagnetic compatibility (EMC) directives;

Quality control standards or guidelines of the company and those of any subcontractors used for the installation or maintenance of the system;

A list of approved suppliers, installers and maintainers;

Procedures, manuals and drawings for installation, commissioning and maintenance;

Parts list – availability, cost, lead times, ease of replacement;

Details of health and safety issues associated with the installation, running or maintenance of the system, including information on toxic or dangerous materials in the product or which may be released during an attack or over the lifetime of the product;

Range of available physical sensor configurations, such as recommended mounting heights and ranges;

Maintenance burden – including reliability (request that the contractor provides a figure for the mean time between failure for their system in their tender), maintainability (request figures for likely maintenance burden and any increase associated with service life, e.g. certain system components may require regular checking) and service life (PIDS are likely to require major overhaul within 7-10 years). It is important to consider the length of service life expected and this should be included in the specification; and

Training requirements – including who should be trained (for example operators, supervisors). Personnel with different system access permission levels should receive only the training pertinent to their permission level. Where and when is training to be provided? For example, training might be provided on site, through an initial course during commissioning and refresher courses later on.

4.7 Selecting a system

Once a system specification has been published and tenders received from competing system installers, the user should assess the bids for technical compliance with the specification before deciding which to procure.

As the tender documents are of a technical nature, assessing them is often delegated to a technical consultancy.

5 Installation

5.1 General

PIDS should provide effective detection performance, a minimal false alarm rate and facilitate effective alarm verification (through adequate zoning).

Following installation and prior to acceptance of the PIDS, it should be subjected to a range of commissioning tests (discussed further in Section 5.2 'Commissioning'). This gives the user confidence that the PIDS is working to, or exceeding, the level determined by the performance specification. It gives the user the chance to reject the installation if it does not fulfil the stated requirements. The contract must state that commissioning tests will be performed prior to acceptance of the system.

The contractor should be instructed to install the PIDS according to the manufacturer's installation procedures. If these are not followed then problems of responsibility could arise if the PIDS fails to perform as expected.

Some types of free-standing PIDS have dead zones near to the sensors, where detection of certain types of attack such as crawling or rolling is not possible. It is important to have these dead zones covered, either by overlapping the detection zones of the adjacent sensors or using another technology to protect this region (see Figure 3).

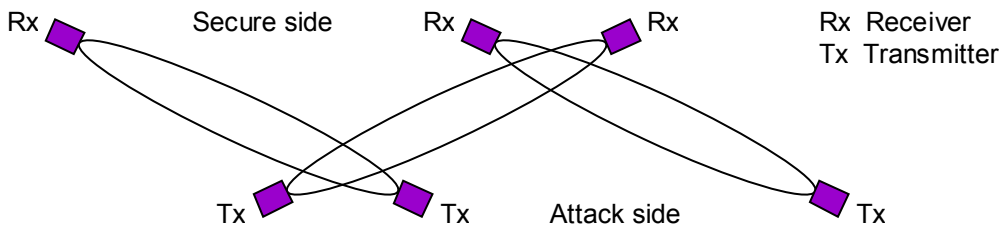


Figure 3: Example overlapping of bistatic microwave PIDS to protect dead zones

Where PIDS consist of separate transmitter and receiver units, similar units should be located together to minimise the risk of interference (as in Figure 3). Wherever possible, the receivers should also be located on the secure (defended) side of a perimeter to minimise the risk of an intruder tampering with the alarm signalling mechanism.

It may be necessary to angle PIR sensors down slightly in order to limit the field of view to a certain range. For instance, the hot exhaust of distant vehicles may be well outside the perceived detection zone but visible to the PIR sensor which would cause it to false alarm. Also, due to the effects of direct sunlight (see Table 1), it may be wise to position the sensors so they are not facing directly east or west.

Only the sensor cable of a barrier-mounted system should be mounted on the fence. As far as possible, all other cabling should be located at a stand-off position on the secure side of the fence.

Processor boxes and allied equipment should be positioned as far from the perimeter as possible and preferably indoors.

Where tamper protection is required, tamper switches should be fitted to all removable lids, inspection covers and openings to cables and components which will signal an alarm in the control room when they are opened. It is good practice to have a tamper circuit which is separate to the alarm circuit.

Please refer to CPNI's *CNI Security Systems Implementation Guidance* for further advice on the application of cabling protection such as anti-tamper protection and cable containment systems.

Outdoor equipment should be mounted in suitable IP-rated enclosures and fixings should be chosen to suit the environment.

Labelling cables and keeping a record of all cable/core identities ensures that any changes that may be required at a later date can be made more easily. A standard colour code and labelling method should be used throughout the installation; this should be recorded in the handover documentation.

Installation contractors must comply with all site health and safety requirements.

5.2 Commissioning

Commissioning tests assess the functionality and performance of a PIDS to ensure that the system has been installed to, and performs in accordance with, the required specification. All those concerned with commissioning will need to be familiar with the contents of the specification.

Commissioning tests also provide performance data from which any future deterioration can be measured and hence remedial action justified. In the event that any adjustments are made to the PIDS - either as a result of initial commissioning tests or for any other reason - the tests would need to be repeated. This is because any change in system set-up could influence performance.

The installation contractor should conduct a site acceptance test (SAT) following system installation. This should include a structured demonstration of (all) the system functions to show that it is performing to specification. Although helpful, this should not preclude the end user from conducting independent commissioning of the new system to satisfy themselves with regard to its performance.

A commissioning test plan should be devised to assess the performance of the system in relation to different attack methods and to ensure the PIDS is providing uniform detection along the length of each detection zone. The amount of time required for commissioning will vary depending on the size and complexity of the system and can range from a few hours to several days. An example of a checklist of some general commissioning points of good practice is provided in Appendix C.

The commissioning attacks should be comprised of a variety of attack styles. For example, it is recommended that a free-standing PIDS is assessed against a range of target profile sizes and speeds by using a variety of attack styles such as crawling, running and cycling across the detection zone.

For barrier-mounted PIDS, destructive fence penetration attacks detailed in the evaluation standard[2] are clearly not appropriate for commissioning at an operational site. Table 3 describes a series of simulated attacks that can be used for commissioning purposes.

Table 3: Examples of simulated barrier-mounted PIDS attacks for commissioning

Test Description	Comments
Perform two impacts, within the preset 'double knock' period (if used), using an impact tester[3]. This test should be carried out at specified locations on any panel or zone that is protected by the system – for example 300 mm from the base of each panel and 300 mm in from the right-hand post of each panel from the defended side, which should produce an alarm in each case.	This is a standard test used to simulate bolt cropper cuts on the fence fabric which is often used to determine the uniformity of response of barrier-mounted systems. [If the system is set to alarm on a different number of impacts, then the test should be adjusted accordingly]
Use a 4 m lightweight extending pole with hook to agitate the barbed tape concertina topping at specified locations. The attack should be detected and displayed correctly.	This can be used to test how the system would respond to attacks where the barbed tape concertina is agitated for example climb-over attacks.
Using a hacksaw, cut through either strands of a dummy panel or 4mm diameter strands of wire, either of which has been attached to the barrier protected by the system. The attack should be detected and displayed correctly.	This can be used to simulate penetration attacks using a hacksaw.

For most single-fabric fences, it will be possible to conduct the simulated test from the defended side, if more practical. The locations at which commissioning attacks are performed should be selected so that they reflect the worst case locations based on the attack style being used. The locations need to be recorded so that subsequent tests can be performed at the same locations within each zone. This will enable comparisons of performance between zones, and of the whole system over time, to be made. It is important that each attack is repeated at least three times in each zone to ensure validity.

Other test methods may be derived from those recommended by the system manufacturer for maintenance purposes, but these should not be used as the sole commissioning attack styles. The suite of CAST/CPNI PIDS evaluation standards contain lists of attack methods used for evaluating PIDS; however an exhaustive commissioning trial, testing all attack styles at every position, is impractical.

For barrier-mounted and ground-based PIDS that utilise a single run of cable to form several zones, the detection zone boundaries should be thoroughly checked to ensure that they match what is expected; and that they correspond

[2] See CAST publication 07/12 *Barrier-Mounted PIDS Evaluation Standard v3.0.*
[3] Impact tester calibration should be approximately 75 N for 358 welded mesh fences and 90 N for Portcullis palisade or equivalent.

to the appropriate camera views. Zones for such systems are often defined in computer software as length intervals or GPS coordinates and errors in incorporating this information in the system design can be easily made.

The results of the commissioning attack trials should be recorded. An example results table is shown in Table 4.

Table 4: Example commissioning attack trial results table

			Attack detected?		
Test	**Zone**	**Position**	**1**	**2**	**3**
Walk	1	15 m	✓	×	✓
Bicycle	1	25 m	✓	✓	✓
Crawl	1	45 m	×	✓	×
Walk	2	15 m	✓	✓	✓
Bicycle	2	25 m	✓	✓	✓
Crawl	2	45 m	✓	✓	×

The performance of the PIDS over an extended period and under various environmental conditions cannot be determined during the commissioning period. The installation contractor should remain liable for any inability of the installation to meet the specified performance criteria, as a result of environmental conditions or deterioration, which may be revealed during the warranty period. Provision should be made for additional tests to be carried out, at the appropriate time(s), particularly on systems that have any form of environmental compensation built into them. It is not uncommon for 5% to 10% of the contract cost to be retained subject to the system meeting the false alarm requirements over the warranty period.

It is also important to assess the false alarm performance during commissioning. Whilst an extended period of alarm monitoring would be preferable, this is often not practical during commissioning or acceptance testing. A period of 30 days is deemed to be appropriate in most cases.

It is important that within the false alarm monitoring period the different operating scenarios are identified, such as day time (working hours), night time and weekends. This allows a range of potential alarm causes to be considered, for example: increased vehicular traffic and pedestrians during working hours; animal activity during night hours; and fog or sun glare at dawn. Any obvious trends in alarms on certain days; at certain times of day; or from certain alarm zones can then be assessed. This detailed information can be used to inform setting adjustments that might be required on specific zones or to take mitigation measures against sources of false alarms, such as tree pruning or animal control for example.

This alarm information should then be used to calculate a false alarm rate (FAR) which can be compared to that specified in the performance requirement. Section 4.4.2 ‘False alarms’ contains some indicative FAR figures.

Where PIDS are installed as part of an integrated security system (for example with an existing alarm management system or CCTV) the system

should be tested as a whole. This will ensure that the PIDS operates effectively as part of the integrated system.

Commissioning tests should not only test PIDS performance, but should also test any other required functionality. This could include a test to remove power to the system to ensure that the uninterruptible power supply (UPS) works as required; or that the PIDS fails safe (in alarm) depending on the requirement given in the specification.

When commissioning or performing any other form of test, it is essential to have good communication (for example, two-way radio) with the control room. This ensures that control room staff can confirm if an alarm has been received. It will also allow the control room staff to check whether the tester has generated any unexpected alarms.

The results of these commissioning tests should be used to determine whether the PIDS meets the specification and should therefore be accepted. As well as meeting the stipulated false alarm rate, the installed PIDS should be expected to produce the level of detection given in the specification (95% minimum recommended against those styles detailed in the appropriate evaluation standard) when subjected to a random subset of the attacks described in the specification document.

The results, along with the PIDS settings, should be retained and used to make comparisons with results of subsequent tests to check on the continued performance of the PIDS. It is important that the settings are read directly from the system rather than using figures recorded in the documentation which could be inaccurate, highlighting a possible unauthorised change.

5.2.1 Commissioning documentation

On acceptance and handover of a PIDS, drawings and manuals covering the installation, operation and maintenance must be provided to the person responsible for maintenance and operation of the system on the site. It is of particular importance that manuals covering system operation are written so that they can be understood by a non-technical user.

Either the commissioning documentation or other manuals associated with the PIDS should include the following information:

A description of the manner and limitations of operation, including duration and supply for the backup power systems;

Copies of any certificates of compliance with relevant standards or schemes;

Set-up/sensitivity parameters of the installed PIDS;

Comprehensive instructions for the switching on, operation, switching off and isolation of the system;

Comprehensive instructions for dealing with emergency conditions and any precautionary measures necessary;

Instructions for maintenance of the system to keep it in an effective and safe condition, including frequency of activities and the materials to be used; and

The names and contact details of all component suppliers, together with type and model references, serial numbers, duty rating, capacity and the order number and date.

System Drawings:

To assist with future system maintenance and to help prevent inadvertent damage to components due to other unassociated works on the site it is useful to have detailed drawings of all parts of the system.

Drawings should include diagrams and schedules to show all the information necessary so that the system can be safely operated, maintained, inspected and tested, as far as is reasonably practicable. The drawings should be fully cross-referenced and coordinated with the operation and maintenance manual. An overlay of PIDS zones onto a site plan is essential. Where the installation includes CCTV verification, this should also be overlaid.

The drawings should also include wiring diagrams for the various components and for the system as a whole. In addition to schematic diagrams, drawings should be included showing the physical arrangements (panel and rack layouts, cabling layouts etc.) to assist the location and identification of the components which make up the system. A schematic layout of the overall system and interconnection diagrams should also be provided.

6 System management and maintenance

Once a new PIDS has been procured, installed and commissioned, it is important to establish good working practices and a comprehensive maintenance schedule to ensure that it provides effective service on a long-term basis.

Good working practices include:

Ensuring all staff are well trained and their performance is monitored and appraised regularly;

The control room environment[4] should be kept at a comfortable temperature, with adequate lighting and ventilation;

Keeping procedural and system documentation readily available, including logs of commissioning and subsequent performance tests; and

Having clearly defined procedures for fault logging and resolution.

It is not only the PIDS which should be maintained but also the area around the PIDS including control boxes etc. This is covered further in sections 6.1 'Site maintenance' and 6.2 'PIDS maintenance'. The maintenance schedule should also have tasks to check that the OR is still applicable, check whether the installation still fulfils the OR and determine whether there has been any change in site layout etc.

During the life of a PIDS the initial operating parameters may change, for example:

Electronic components may deteriorate because of ageing;

Cable ties attaching barrier-mounted PIDS sensor cable to a fence may have loosened/degraded;

Sensors and enclosures may corrode or degrade;

Sustained high winds may have forced transmitters or receivers to drift out of alignment;

Existing vegetation in the detection zone will grow (i.e. grass length will vary) or unwanted vegetation may intrude into the detection zone; and

The local area may be physically altered in some way, for example new buildings or roadways may be constructed.

All of the changes listed above could affect the operation and performance of the PIDS and it is therefore important to check the integrity of the PIDS at regular intervals. Regular maintenance and testing of the system will give confidence that the PIDS is performing satisfactorily.

---

[4] CPNI/SSG publication *Guide to Security Lighting* and CAST publication *CCTV: Making it Work – Control Room Ergonomics*

What maintenance should be carried out; when it should be done; and who will undertake it all need to be considered. The contractor should be requested to provide the maintenance requirements of the proposed PIDS and the cost for a maintenance and support contract in the specification. When placing such a contract, it is important to state what response times are required to fix problems or resolve issues. If a maintenance contract exists, the operators should be aware who has the authority to call out the maintenance team if a problem arises and what the response time should be. It is imperative that the maintenance regime and any maintenance contractors are approved by the supplier. This will ensure that the supplier can be held accountable for any failure of the PIDS to maintain the required performance during the warranty period.

The PIDS should be supplied with a maintenance log to provide details of the type and frequency of maintenance and testing that the manufacturer recommends. This information should also be included in the maintenance schedule.

Following any maintenance, repairs, upgrades or adjustments, the PIDS should be retested to ensure that it continues to operate as required in the specification.

The maintenance log will include maintenance tasks carried out along with corresponding test results. The maintenance log should also contain a copy of the commissioning test results which can be used for comparison with any subsequent tests. Details of all breakdowns, repairs, replacements and system adjustments should also be recorded in the maintenance log book so that it forms a complete history of the PIDS. It is recommended that maintenance log books should be classified as Restricted or Commercial-in-Confidence as a minimum and stored appropriately. The information contained in the log book is sensitive by its nature and in the wrong hands it could be used to take advantage of any vulnerability identified during maintenance tasks. Log books should not be removed from the site.

6.1 Site maintenance

Maintenance of the site, and in particular the area around the PIDS, should be completed on a regular basis to help prevent gradual reduction in PIDS performance over time. This can be monitored and/or performed by the PIDS operators or site maintenance team.

Site maintenance requirements should include the following areas:

The ground in and around the PIDS, barrier and/or detection zone should be kept clear of foliage and vegetation (Figure 4). Trees and bushes should be kept cut back to reduce the possibility of causing false alarms and long grass should be avoided;

The site should be kept clean and tidy, as any litter or debris can be blown around by wind or can attract wildlife, both of which can cause false alarms; and

Any means available to prevent such wildlife interacting with the barrier or detection zone should be considered.

Figure 4: Movement of vegetation such as this against the fence can cause false alarms for barrier-mounted PIDS

6.2 PIDS maintenance

Operational checks which include regular maintenance and testing of the PIDS is essential to prevent problems arising and to ensure that a fault, resulting in loss of detection, can only exist undiscovered for a period that is considered acceptable. The frequency of operational checks, including performance testing, will be influenced by factors such as personnel availability; the nature of assets being protected; and the level of confidence required in the PIDS. The frequency of operational checks required for each CPNI Grading is specified within CPNI's *CNI Security Systems Implementation Guidance*. The table specifying operational check intervals for systems designed to meet the CPNI security levels is reproduced in Table 5.

Table 5: Recommended frequency of operational checks

CPNI Protection Level	Visual Inspection	Functional Check	Remote System Checks	CPNI Class	Visual Inspection	Functional Check	Remote System Checks
HIGH	A	B	X	4	A	B	X
				3	B	C	X
ENHANCED	B	C	X	2	C	D	X
				1	D	E	E
BASE	C	D	E				

Key :

A	Daily	B	Weekly
C	Monthly	D	Quarterly
E	Six Monthly	X	Not Permitted

The PIDS maintenance schedule should include, but not be limited to, the following checks:

The condition of the surface of the detection area;

The condition of fence/barrier;

Integrity of cable ties for a barrier-mounted system;

The physical condition of the equipment including

Screws and hinges are not corroded or degraded;

No tamper-resistant fixings/seals have been compromised;

The UPS/stand-by power supplies are operating correctly; and

Test and check the performance of the PIDS.

Operators may wish to perform a simple confidence check (one per zone) to ensure that a PIDS is still functioning. For barrier-mounted systems, this could take the form of a simplified version of the impact test described in Table 3 of Section 5.2 'Commissioning'; or a simple 'walk' across the detection zone in the case of buried or free-standing systems. If, during testing, a zone fails to alarm, a further test at the same position and another test a short distance away, but still within the same zone, should be carried out. If these also fail, the zone should be considered defective and a report produced so that remedial action can be taken.

However, as part of a preventative maintenance programme, it is important to check that the uniformity of detection around the perimeter remains comparable with that achieved during the initial commissioning tests. To do this, a sensitivity profile test should be performed which involves carrying out a series of tests/attacks as conducted during the initial commissioning (see Section 5.2 'Commissioning'), at repeatable locations in each zone of the perimeter. In areas that give concern, a more thorough sensitivity profile – for example at 10 m intervals – for the zone should be carried out.

Over time this provides a more rigorous test of the whole PIDS against a range of attack styles. This should be conducted on a regular basis to help swiftly identify any problems and can be compared with the commissioning results to identify any gradual deterioration or changes in performance.

Typically, PIDS will cover a number of zones and it is important that sensitivity profiling is conducted on all zones at the required frequency. A methodical test regime should be implemented with a different part of each zone tested on each occasion to ensure uniformity of detection around the entire perimeter.

Any testing of the PIDS should be carried out in conjunction with the operators in the control room to ensure that an alarm is received. Particular care should be taken if inhibiting any part of the system for such tests. The use of a time-out facility is recommended whereby the zone returns to operation after a defined time.

When testing the performance of PIDS, the use of inbuilt "self-test" functions is not recommended as these may test only the communications link and not the PIDS itself.

Assessing the number of false alarms that occur; making comparisons between zones; and looking for trends can indicate whether a particular zone warrants further investigation. These differences could indicate a problem in a particular area.

It is recommended that some simple electrical tests are also periodically carried out. This should include using any diagnostic tools supplied by the manufacturer, continuity testing and the testing of all earth connections in the system. Such tests can be specified in a routine maintenance contract with the PIDS manufacturer or supplier.

Following any maintenance or testing, repairs or adjustments should be made that are necessary to ensure that the performance is maintained as required in the specification and as demonstrated during the commissioning period. The operators must be informed of any element of the system which is not operating to the required standard. Every effort should be made to provide temporary cover for any part of a perimeter that would otherwise be unprotected due to unserviceable equipment. It is essential that a procedure is in place to ensure that prompt and adequate follow-up action is taken. It is advisable that critical spares are kept on site to enable common issues to be remedied. Depending on the type of PIDS, critical spares may include fuses, rubber seals or lenses.

7 PIDS application types

The different application types of PIDS each have their generic strengths and weaknesses which should be carefully considered when producing a perimeter security specification.

The relative effectiveness of these different categories of PIDS cannot easily be assessed due to their use of different technologies and widely varying deployment requirements. What follows is a relative analysis of the strengths and weaknesses of each of the four categories and the technologies within them.

7.1 Barrier-mounted PIDS

One of the main advantages of using any form of barrier-mounted PIDS is the presence of a barrier which provides a physical delay to the intruder's progress. By introducing a delay this can assist in the verification and response processes which are initiated following an alarm.

There are different advantages and disadvantages between the two generic categories of barrier-mounted PIDS - fabric-mounted PIDS and post-mounted PIDS. Within these two sub-categories there are differences between systems using different technologies. Some examples are provided below.

7.1.1 Fabric-mounted PIDS

These are PIDS that are attached directly to the fabric of the fence. The performance of these systems can vary depending on the type of fence fabric and its condition. Some fence fabric types are more suited to hosting fabric-mounted PIDS than others. For example, rigid welded mesh designs such as '358' are generally better suited for PIDS than looser designs such as chain link where vibrations cannot travel efficiently through the fabric. Systems listed in the CSE will be annotated with the host fence upon which they were tested.

Some fabric-mounted PIDS offer the ability to protect an entire perimeter with one continuous length of cable and one processing unit - optical fibre based systems are an example. Such a system will clearly have cost benefits in terms of infrastructure, as the individual zones along the perimeter do not require separate power and signal cable feeds. However, such systems are sometimes only cost effective on long perimeters due to the high unit cost of the single processing unit. The zones in such a system are defined in software by either GPS co-ordinates or in terms of measured length along the fence. If this is not done carefully, it can lead to inaccurately defined zones that do not match with the correct CCTV camera views; particularly careful commissioning and maintenance is required. A whole PIDS system relying on one processor unit and one power supply may present resilience issues in the case of system failure when the entire perimeter can be unprotected as opposed to a single zone for some traditional systems.

To maximise detection of climbing attacks, barriers hosting PIDS must include an appropriate topping/barbed tape topping.

7.1.2 Post-mounted PIDS

Electrified fence systems use high voltage, low current, short duration pulses to deter an attacker. Such systems provide detection as well as deterrence but can require additional maintenance commitment. The wire strands, held in place with plastic insulating clips, require regular inspection – particularly following sub-freezing conditions – in order to maintain functionality of the detection capability. Additionally, in some environments a build-up of conductive material on the insulators can cause false alarms, for example a build-up of salt in coastal locations. Where this is likely to occur an appropriate cleaning regime will be necessary. Note that electrified fences can be configured to alarm upon a single missed voltage pulse or after several missed pulses. The voltage below which an alarm is generated can also be selected. Appendix A provides further information on some regulatory aspects of electrified fence deployment.

Electric field/capacitance type systems can be affected by the amount of humidity in the air – water vapour increases the capacitance between the wires which can lead to lower performance levels.

Taut wire systems tend to have very low false alarm rates. Older, switch-based taut wire systems can require a high level of maintenance and fault finding can be problematic. Newer analogue taut wire systems tend to require less maintenance.

7.2 Ground-based PIDS

The main advantage of ground-based PIDS is covertness, such that even a knowledgeable attacker should have no awareness of the presence of the system. This feature can make ground-based PIDS a good early warning system at the far perimeter of a site, giving security personnel additional time in which to apprehend any intruders. Systems listed in the CSE will be annotated with the burial substrate within which tests were conducted.

Once installed, the systems also do not compromise the aesthetics of a site. Such systems are also less affected by weather conditions than above-ground PIDS.

Disadvantages of ground-based PIDS include high cost due to the ground works which must be undertaken to install most systems. Installation can cause considerable disruption, and together with the ground-settling and commissioning periods it may take quite some time to get a system fully up and running. Ground-based PIDS provide no delay or deterrence as there is no physical barrier.

There are several different types of ground-based PIDS, each with its own strengths and weaknesses.

7.2.1 Radio frequency (RF) radiating field systems

Sometimes called ported coaxial cable or ‘leaky feeder’ systems, these systems can produce good overall performance. These systems have good discrimination between animal target sizes, but are still susceptible to some false alarm causes, notably due to accumulated water following heavy rainfall. However, the RF radiation emitted by these systems can be detected. Where surface water is present, detection is less effective.

7.2.2 Microphonic cable systems

These PIDS offer reasonable performance at a modest price. Installation cost and disruption can be minimised for some systems by installing the cables directly into a small slot cut into the ground rather than requiring a wide trench. They can suffer false alarms from wildlife. As with all systems that directly detect ground vibrations, microphonic cable PIDS can be vulnerable to heavy traffic in the vicinity and the pressure transmitted by roots of trees and other vegetation that are moving in heavy wind.

7.2.3 Optical-Fibre cable systems

The sensor cable of an Optical-Fibre (Fibre-Optic) system (but not necessarily the electronics) is immune to RF interference. As optical-fibre systems generally use one cable run for a whole perimeter, an installation can often require just one processing unit and power supply. However, the processing unit of such systems can be high cost, meaning that it can be an expensive solution for short perimeters. For longer perimeters, their price per linear metre can drop to an affordable level.

7.2.4 Balanced Fluid-filled tube systems

These systems can produce good detection and false alarm performance although covertness may be compromised by the requirement for access pits used to pressurise the tubes. Such access pits are often similar in appearance to drain rodding points. These systems have a higher maintenance overhead as it is recommended that pressure checks are carried out at least annually.

7.3 Free standing PIDS

The main advantages of a free-standing PIDS system are reduced installation cost due to no requirement for a physical barrier and a lower level of groundworks is required. They do not hinder legitimate activity, such as the movement of vehicles, and if required, installations can be designed to be discreet/covert.

The main disadvantage however relates to the lack of a physical barrier offering delay to an intruder, meaning that a prompt response to alarms is required as an attacker can be well within the site within seconds. This can also make alarm verification difficult.

Systems listed in the CSE will be annotated with the surface material over which they were tested.

There are several different types of free-standing PIDS, with their own strengths and weaknesses.

7.3.1 Active infrared systems

These systems have no dead zones near to the transmitter/receiver units but can be particularly susceptible to the effects of fog causing false alarms. These systems are only to be installed over flat ground as undulations can create dead zones. The alignment of transmitters and receivers over long ranges can be difficult. Features are available for these systems which can reduce false alarms from small or fast-moving wildlife (such as requiring more than one beam to be broken, or beams to be broken for longer than a

defined period of time). These systems also typically require a hard-wired synchronisation cable between each pair of transmitters and receivers, preferably in underground ducting.

7.3.2 Passive infrared (PIR) systems

These systems are not recommended for use as the primary detection solution for outdoor environments as their poor immunity to changing temperatures results in either a very poor detection rate or a very high false alarm rate. PIR systems generally use two types of optics to gather the infrared energy from the scene: Fresnel lenses; or more expensive mirror optics which are more accurate for long range (~100 m) applications. A variety of coverage patterns exist, from short and wide detection zones to long and narrow zones. Careful positioning is required due to dead zones and sources of false alarms such as sunlight or other distant, hot objects.

7.3.3 Bistatic microwave systems

Dead zones exist near both the receiver and transmitter units, which are normally protected by overlapping adjacent zones, or by careful positioning of units. These systems have good immunity to the effects of weather though this requires a well-maintained detection area and care should be taken in proximity to metallic objects and moving bodies of water as reflections and absorption of the microwave field can occur, leading to reduced performance.

7.3.4 Doppler microwave systems

These systems use one transmitter/receiver (transceiver) unit and a maximum range can be defined, beyond which targets can move undetected. Such PIDS can be used to cover the dead zones of other free-standing PIDS or where activity beyond the required detection zone might cause false alarms, as is the case with other technologies (such as PIR). As these are microwave systems, they possess many of the same disadvantages as bistatic microwave systems (see Section 7.3.3), such as a dead zone near to the transceiver and susceptibility to metallic objects and moving bodies of water.

7.3.5 Dual-technology systems

In order to reduce false alarms, these are typically AND-gated, requiring both technologies to detect before signalling an alarm. This can make these PIDS more vulnerable to defeat than single-technology systems. The sensitivity of each sensor is therefore often increased beyond what would be appropriate if used individually. Alternatively, OR-gating is available, where either technology will report an alarm separately. This would improve the detection rate performance but also increase the number of false alarms. Doppler microwave and PIR is a common technology combination for dual technology systems.

7.3.6 Laser scanner systems

As with active infrared systems, laser scanner systems can be susceptible to the effects of rain and fog. These PIDS can often have the ability to define parameters such as minimum target size or beam break time in a software environment.

7.3.7 Video-based detection systems

Video based detection systems (VBDS) are systems that analyse the video from CCTV systems and are designed to be able to automatically detect unusual activity within an imaged scene. For more information, please see Appendix B.

7.4 Rapidly deployable PIDS

Rapidly deployable PIDS have specific advantages and disadvantages compared with permanently installed free-standing, barrier-mounted or ground-based systems. These systems use the same detection technologies as permanently deployed PIDS but are generally battery powered, deployed on tripods or clipped to fences and transmit their alarms wirelessly.

The main advantages include portability enabling use at different locations; and no requirement for permanent infrastructure in their use.

Some disadvantages are that these PIDS are only designed for use on a temporary basis, ideally for periods of no longer than two weeks. Periods longer than this will require the re-commissioning of the system every two weeks. Battery power sources are utilised, which present potential issues regarding frequent re-charging or replacement and loss of the system's detection function during this down time. Battery life can often vary from manufacturers claims depending on deployment scenario. The wireless communication schemes generally used by rapidly deployable PIDS are a less secure method of transmitting alarm information compared to hard-wired connections. The risk of compromise of this communication link is one of the reasons that rapidly deployable systems are only recommended for a maximum deployment of 2 weeks. As a rapidly deployable PIDS is often deployed on a tripod, it can be susceptible to theft or vandalism when deployed.

Commissioning and set-up time is significantly reduced due to the rapid nature of deployment; which means that the careful alignment of sensors and camera views, which is required when setting up PIDS, can be compromised potentially leading to lower performance than for permanently deployed systems.

Appendix A: Electrified fences

The primary function of an electrified fence is as a detection system. Because of its nature of operation and physical appearance some regard it as a physical barrier. However, as a barrier, it is a good deterrent but offers little delay. As a detection system it can offer low false alarm rate and good detection performance against climbing and penetration attacks.

A.1 Health and safety

HSE guidance states that electrified fences "should not pose an unacceptable electrical risk, providing that the energy is limited to 5 joules (BSEN 60335-2-76:2005) and that each fence is designed and installed so as to avoid the creation of man-traps". BS1722 part 17 (2006)[5] specifies that an electrified fence fitted on the protected side of a fence that is accessible to the public, must be at least 100 mm inside the fence and no greater than 200 mm; when installed close to an existing fence (but not fixed to that fence) it must be further than 1 m from the fence to avoid entrapment; barbed tape or barbed wire must be at least 1 m away from an electrified fence; and stipulates that warning signage must be installed at 10 m intervals to comply with Occupiers Liability Act requirements.

A.2 Layout

The installation of electrified fences should follow guidelines set out in BS1722 part 17. Various configurations are possible:

A.2.1 As a topping to an existing fence

Electrified toppings are a good deterrent against climb-over attacks and being installed at height present less risk of accidental contact to the general public, although where in close proximity to a public footpath or bridleway, the requirements of the 1980 Highways Act must be considered. This form of topping may be more aesthetically acceptable than barbed tape coil.

A.2.2 Fixed to a host fence on the secure side

This configuration can be used on a single line of fencing if access to the inside of the fence is limited. The main disadvantage of this configuration is that detection will only be made after the host fence has been penetrated.

A.2.3 Fixed to a host fence on the attack side (in a sterile zone)

This configuration offers good deterrence and the host fence provides a post-detection delay. In this configuration, the fence must be in a sterile zone to limit accidental contact with the electrified fence by members of the public.

---

[5] This British Standard is based on PAS 47:2003 (an interim code of practice for electrified security fences).

Appendix B:Video based detection systems

Video Based Detection Systems (VBDS) analyse imagery from CCTV cameras and highlight events of interest. The systems are designed to provide assistance to human operators in identifying events of interest that occur in areas covered by their CCTV systems. This leads to three common uses of this technology:

Triggering recording;

Cueing events for a human operator to interpret; and

Live event monitoring (or post-event analysis) of events and alarm generation.

In all three cases, a good detection rate (typically greater than 95%) is required. A higher false alarm rate can under some circumstances be tolerated in the first application, whereas a low false alarm rate is necessary in the remaining applications, which is generally concerned with the deployment of a response force. Operator confidence may be undermined in any situation where a high false alarm rate persists.

At the most basic level, VBDS detect changes in areas of the picture over time. Systems apply varying amounts of processing before comparing events against a rule base or running an algorithm to evaluate whether an alarm condition has occurred. Higher level capabilities, such as tracking or object classification, require larger amounts of processing and larger and more flexible rule bases and/or complex algorithms.

It is worth noting that a VBDS will only detect reliably when good quality imagery is available. A site must have cameras covering the areas where detection is required and, if event detection is required at night, suitable lighting must be provided. Environmental conditions can have an adverse effect on detection rates. Heavy rain and fog will affect visibility and can reduce the detection range.

B.1 Components of a video-based detection system

A VBDS can be divided into four sub-systems:

Video feeds;

Analysis hardware and software;

The user interface; and

Alarm outputs and integration with other systems.

B.1.1 Video feeds

VBDS require high quality video feeds to achieve good detection rates and low false alarm rates. Cameras must be securely mounted as camera shake can have an adverse effect on VBDS performance.

If a VBDS is to be used with a legacy CCTV system, it is important that it is fully audited and, if necessary, overhauled.

Particular attention must be paid to the location and angle of cameras with respect to the sun. Very small amounts of direct light glare and even indirect glare (low angle sun reflected from a tarmac surface for example) at particular times of day can be a major source of false alarms for VBDS fed from poorly angled CCTV cameras. This is a good example of how a camera scene that may be quite suitable for human viewing could cause significant problems for a VBDS.

It should be remembered that the angle of the sun in the sky changes throughout the year, so some camera adjustment may be necessary when the seasons change. If done correctly, this will only need to be done for one seasonal cycle. If it is likely that there may be a problem with this (i.e. cameras directed due east or west), then such realignment along with any corresponding adjustments to the VBDS should be captured in any installation or maintenance contract.

Further guidance on the technical aspects of good quality CCTV installations that are suitable for use with VBDS can be found in the CPNI guidance note *CCTV for CNI Perimeter Security* and CAST Publication 28/09 *CCTV Operational Requirements Manual*.

B.1.2 Analysis hardware and software

VBDS use a combination of hardware and software to analyse the imagery provided by the video feeds. For PIDS applications i-LIDS approved systems should be used.

Many manufacturers are enhancing the functionality of their systems with the addition of other functions such as enhanced user interfaces and Digital Video Recorder (DVR) capabilities. This additional functionality is not covered by the i-LIDS assurance process.

Some more modern VBDS use ‘learning’ type algorithms to assess a scene. Such systems are able to ‘learn’ the scene they are imaging and can identify patterns, such as the appearance of wildlife at regular times of day, and exclude such events as alarm causes – reducing false alarms. These systems can be straightforward to set-up and commission.

Other VBDS use a rule base, i.e. they are manually configured to alarm for targets of particular size, speed, direction, etc. and ignore others. Such systems can require very careful set-up and commissioning to achieve their optimum performance.

B.1.3 User interface

User interfaces vary in usability and complexity. Generally a VBDS should have different levels of access for guard force, administrators and technicians. These access levels should be password controlled. Some user communities consider the ergonomics of the user interface to be more important than the performance of the system. The viability of a VBDS in an operational environment depends heavily on the users’ ability to operate the system as well as the technical performance of the system.

B.1.4 Alarm outputs and system integration

Most VBDS systems provide, as a minimum, alarm outputs that can be integrated with alarm management systems. Some systems provide advanced integration facilities such as alarm management, DVR capability and Pan-Tilt-Zoom (PTZ) control. If the VBDS includes a recording facility or integrates with a DVR, it should be possible to store imagery for use in a criminal investigation. These systems should comply with the Digital Imagery Procedures and CAST UK Police Requirements for Digital CCTV Systems to ensure an audit trail for the Criminal Justice System.

B.2 Advantages and disadvantages

VBDS can generally be configured to a give a good (greater than 95%) detection rate. To maintain performance levels throughout the year, VBDS often require re-configuration to deal with seasonal variations.

VBDS require a high quality video feed. Legacy CCTV systems were generally not designed with VBDS in mind. Existing hardware may require upgrading and additional cameras and lighting may be required to ensure full coverage of the site. In some cases, the cost of upgrading systems has been a barrier for implementation of VBDS.

B.3 Management and maintenance

VBDS are often computer based rather than the more traditional hardware based detection systems. Operators and administrators need to be IT literate, as the operation of these systems requires the navigation of computer based systems. Technicians that maintain the system will need a skill set similar to that of an IT administrator.

The flexibility that VBDS provide creates a huge range of possibilities regarding the configuration options available to the user and administrator. Whilst a well designed VBDS will present this information in a clear and concise manner, training is required to ensure that the operator understands the information presented to them and that the administrator understands the consequences of modifying any of the detection parameters,

The infrastructure that the VBDS is connected to must be maintained to ensure the reliability of the systems. Often the level of maintenance required to achieve an acceptable level of performance for a human operator is below that required for a VBDS. This increased maintenance should be factored into the running cost of a VBDS.

B.4 Performance standards

A key aspect of the successful deployment of a VBDS is an understanding of the Operational Requirement (OR) for the different components of the system. The most important of these is whether the detection and false alarm performance of the system, as actually installed, meets the OR. As with other types of PIDS, a system with too low a detection rate will be ineffective against genuine incursions into a site. A system with too high a false alarm rate will not instil confidence in the human operators who will quickly learn to attach no significance to the alarms that the system produces.

B.4.1 Performance-based procurement and commissioning

The procurement of any VBDS should always be made against a baseline performance-based Operational Requirement. The OR should clearly state the level of performance that must be demonstrated before the system will be accepted by the site owners. The performance aspects of the OR will need to be negotiated with the suppliers at the outset of the procurement, along with the methods that will be used to demonstrate compliance with the performance measures.

In common with other types of PIDS, performance is primarily measured in terms of Detection Rate (DR) and False Alarm Rate (FAR). It is recommended that in terms of commissioning or site acceptance testing (SAT), a VBDS is treated as a standard PIDS and subjected to the same procedures as discussed in Section 5.2 of the main Guide to PIDS document.

Detection rate can be typically measured using free-standing PIDS type detection rate assessment attacks, i.e. walking, running, crawling, etc. across the monitored scene. An estimate can be made of false alarm performance by monitoring over a sample number of days, although it may be difficult to get a truly representative measure depending on the environmental conditions that prevail at the time of monitoring. As a minimum it is recommended that alarms are monitored over a variety of times of day to be able to determine whether there are likely to be any sun-glare related alarms – this can be a primary cause of false alarms for VBDS connected to incorrectly angled cameras.

It is typical to configure a VBDS for a specified level of detection performance first, and then measure the associated false alarm rate over a period of time.

B.4.2 The i-Lids performance standard

The i-LIDS video library is a Government initiative which provides a benchmark to facilitate the development and selection of Video Analytics (VA) and VBDS systems which meet Government requirements. i-LIDS is produced by the Home Office Centre for Applied Science and Technology (CAST) in partnership with the Centre for the Protection of National Infrastructure (CPNI) and consists of CCTV video, based initially on five different scenarios:

Event Detection:

Abandoned baggage detection: with alarm events consisting of unattended bags on the platform of an underground station;

Parked vehicle detection: with alarm events consisting of suspiciously parked vehicles in an urban setting;

Doorway surveillance: with alarm events consisting of people entering and exiting monitored doorways; and

Sterile zone monitoring; with alarm events consisting of the presence of people in a sterile zone between two security fences

New technologies detection: alarm events consisting of people and vehicles captured with three imaging modalities; near IR, medium wavelength thermal imaging and long wavelength thermal imaging

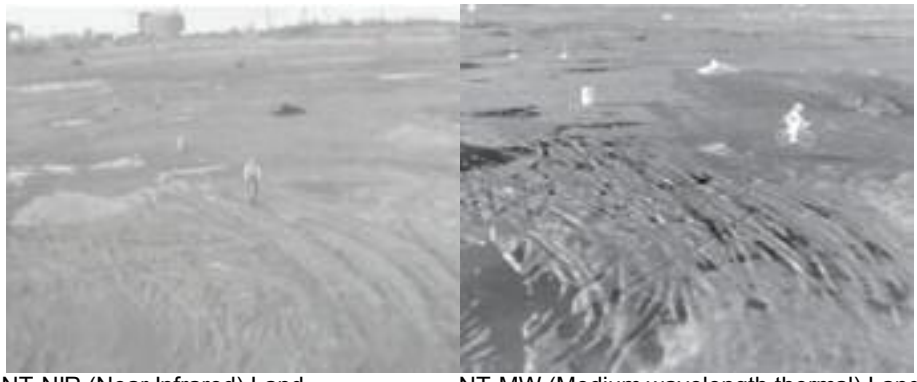
across three different scenes; over land, over water and over a river jetty structure.

Object Tracking:

Multiple-camera tracking: with Target events consisting of people ('Targets') travelling through a network of overlapping and non-overlapping CCTV cameras.

Example images from the sterile zone and new technologies detection (NT) scenarios are shown below:

Sterile Zone Stage 1 Sterile Zone Stage 2



NT NIR (Near Infrared) Land NT MW (Medium wavelength thermal) Land

Figure 5: Example images from the sterile zone and new technologies i-LIDS scenarios

Further details are available from the i-LIDS website, www.ilids.co.uk.

Within each Event Detection scenario, certain 'alarm events' are defined – for example, the presence of an intruder in a sterile zone. VBDS are required to report an alarm when any of these events occur in the footage, with minimal false alarm reports.

VBDS that are tested against the i-LIDS performance standard and appear in the CPNI Catalogue of Security Equipment (CSE) have been tested to the same level of assurance as the PIDS which appear within it. Systems in the CSE have been categorised into one of the following two performance bands:

Operational alert (Primary): suitable for use as the sole form of detection for that application; and

Operational alert (Secondary): suitable for use in conjunction with another detection system for that application.

Those achieving classification in either performance band can use the i-LIDS logo in Figure 6, which is scenario, company, system and version specific.

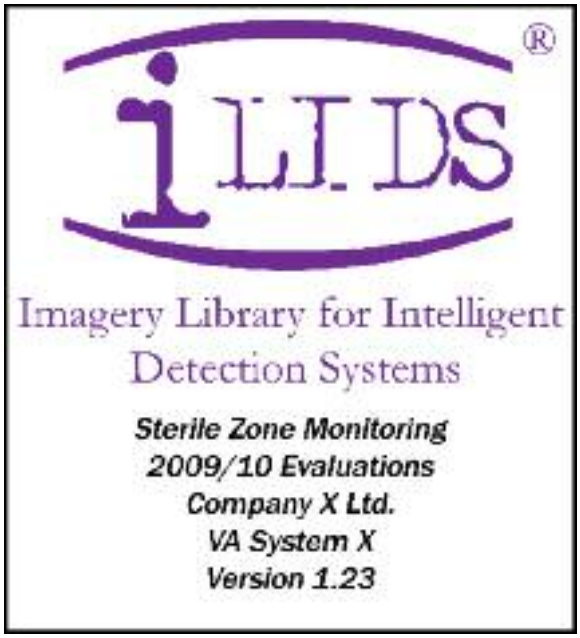


Figure 6: The i-LIDS logo

Appendix C: Example commissioning checklist

This is an example checklist including questions which will inform the amount of time and resources needed when performing commissioning or acceptance testing of a PIDS. It is strongly recommended that such a structured approach is followed which can also be repeated when any other performance testing is carried out during the lifetime of the PIDS.

Note that this list is not exhaustive and does not preclude further testing if deemed necessary.

	Yes	No	N/A
Detection Performance Tests			
Sensitivity settings recorded directly from system.			
Structure of trials – i.e. what detection rate tests are to be carried out?			
Test locations recorded to ensure future repeatability.			
Sufficient tests planned to allow for a minimum detection rate to be calculated (minimum 5 to 10 repeats of each style recommended).			
Record weather conditions on day of tests.			
Are detection tests possible in different environmental conditions?			
Functionality Tests			
Date and time synchronised For PIDS logs; CCTV and GUI.			
Can operator determine alarm cause and successfully reset / accept alarms?			
Multiple alarm stacking / zone prioritisation.			
Does the PIDS alarm in correct zone?			
Tamper alarm testing.			
Remove power – does UPS take over?			
If power removed completely (including UPS), does PIDS fail safe (constant alarm)?			
Are the correct CCTV camera views displayed for alarm verification?			

	Yes	No	N/A
False Alarm Rate Assessment			
Data being analysed begins after latest system change or zone maintenance.			
Data can be exported from system or daily alarm summaries per zone can be viewed on screen.			
Alarm video is available for duration of false alarm assessment period.			
Operator procedure involves selection of a likely cause of alarm? (reducing time needed to verify all alarms).			

Home Office Centre for Applied Science and Technology
Langhurst House
Langhurstwood Road
Horsham
RH12 4WX
United Kingdom

Telephone: +44 (0)1403 213800
Fax: +44 (0)1403 213827
E-mail: cast@homeoffice.gsi.gov.uk
Website: www.homeoffice.gov.uk/science-research/cast