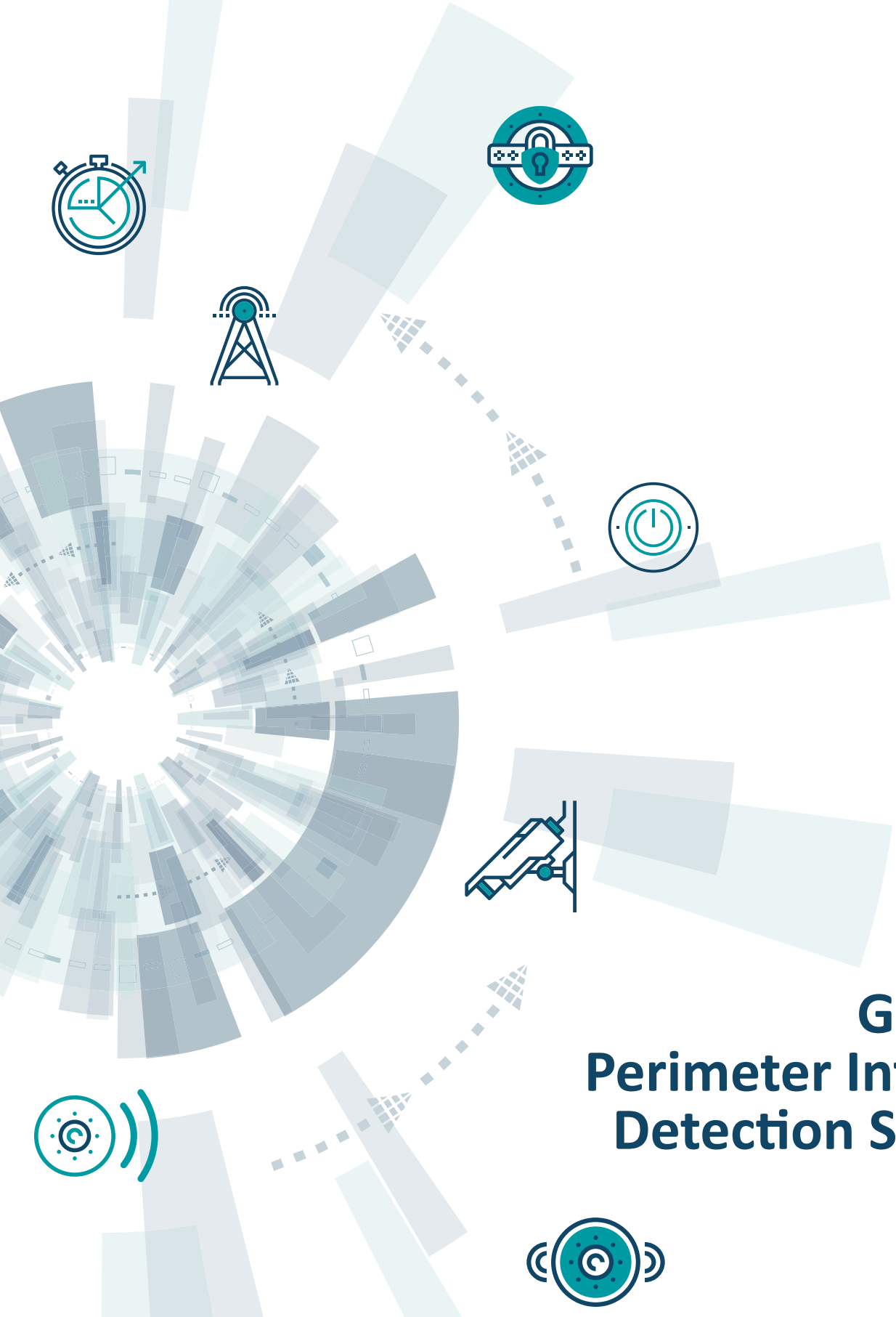
CPNI

Centre for the Protection of National Infrastructure



Guide to Perimeter Intrusion Detection Systems

Disclaimer

This guide has been prepared by CPNI and is intended as a guide to Perimeter Intrusion Detection Systems. This document is provided on an information basis only, and whilst CPNI has used all reasonable care in producing it, CPNI provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, CPNI accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, refraining from acting, relying upon or otherwise using the guidance. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

Freedom of Information Act (FOIA)

This document is authorised and issued by CPNI

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Contents

1 Introduction 4

1.1 What is a Perimeter Intrusion Detection System? 4

1.2 Steps for Deployment 4

2 Selection 5

2.1 Factors 5

2.2 Types of PIDS 6

3 Specification 10

4 Installation 11

5 Commissioning 12

5.1 Considerations 12

5.2 Documentation 13

6 System Management and Maintenance 14

6.1 Site Maintenance 14

6.2 PIDS Maintenance 15

7 Summary 16

1 /vš Œ} µ Ÿ}v

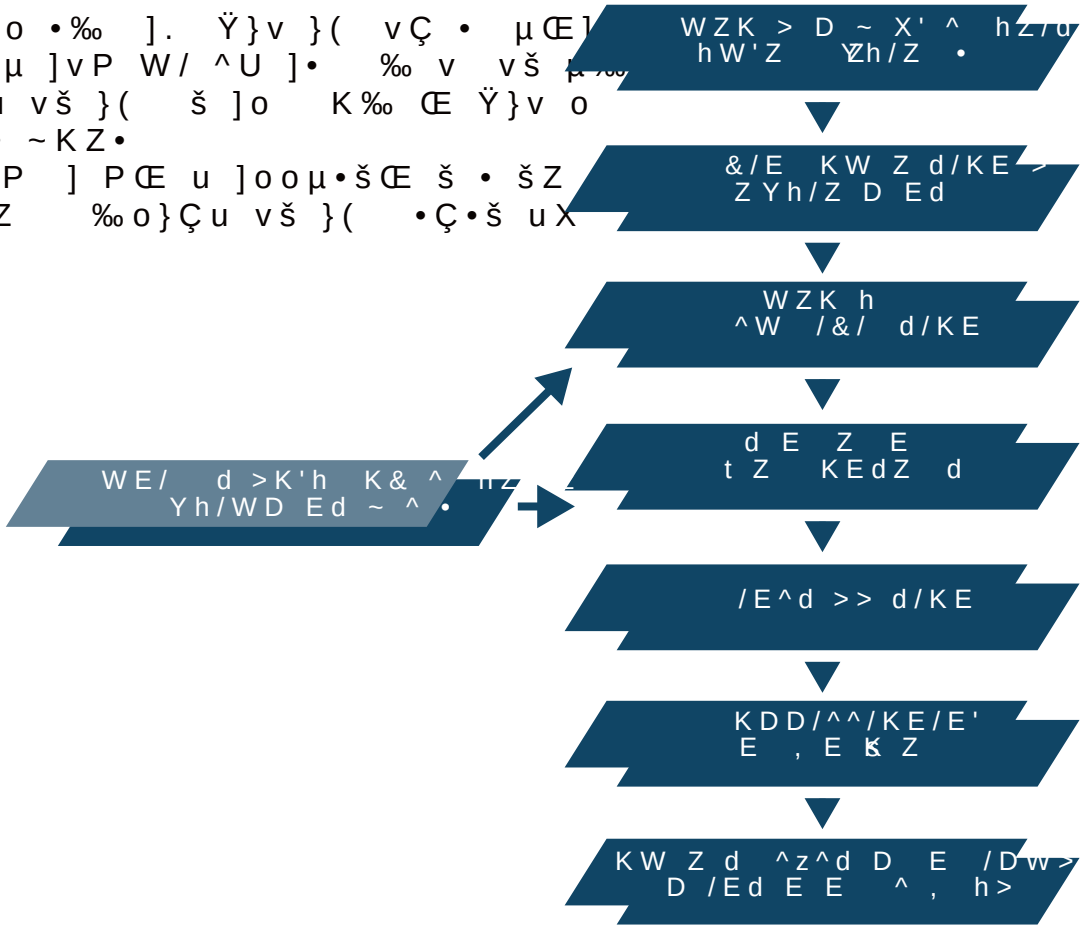
1.1 What is a Perimeter Intrusion š Ÿ}v ^Ç•š uM

W Œ]u š Œ /vš Œ µ•]}v š Ÿ}v ^Ç•š u• ~W/ ^•
v}š À Œ] šÇ }(š Zv}o}P] • •]Pv
Á]šZ šZ • u ‰µŒ‰}• U š} š š v]vš Œ µ Œ
© u‰Ÿv P š} Œ Z ‰ Œ]u š Œ•(v‰ }Œ Ÿ}v
}µv ŒÇX dZ • š Zv}o}P] • v o ••].]v
(}µŒ]•Ÿv š š P}Œ] •U v u oÇ ŒŒ} Œ ru}Ÿ µ vš U
(Œ r•š v]vPU PŒ}µv r • v Œ ‰] oÇ
‰o}Ç o •Ç•š u•X
dZ]• } µu vš ‰Œ}À] • v }À ŒÁ] Á }(šZ
À]o o š Zv}o}P] • • Á oo • Z]PZro À o
Pµ] v }vW

1. ^o Ÿ}v
2. (v‰ }Œ Ÿ}v
3. /v š oo Ÿ}v
4. }u u]••]}v]vP
5. D v P u vš v
u]vš v v

1.2 ^š ‰• (}Œ ‰o}Çu vš

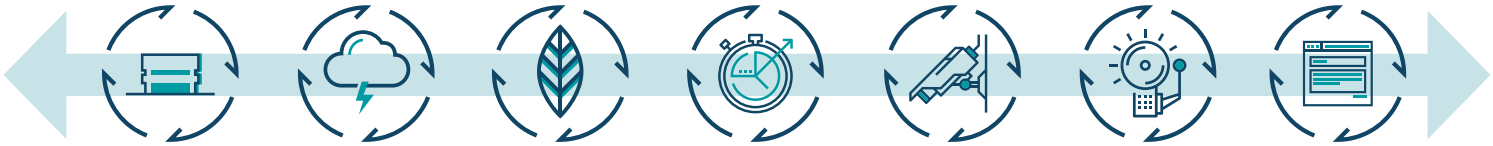
dZ •µ ••(µo •‰]. Ÿ}v }(vÇ • µŒ]
•Ç•š uU]v oµ]vP W/ ^U]• ‰ v vš µ‰
šZ À o}‰u vš }(š]o K‰ Œ Ÿ}v o
Z ‹µ]Œ u vš• ~KZ•
dZ (}oo}Á]vP] PŒ u]ooµ•šŒ š • šZ
‰Œ]}Œ š} šZ ‰o}Çu vš }(•Ç•š uX



2 Selection

2.1 Factors

Several factors play a role in determining the suitability of a PIDS to be deployed in a site. They relate to the operational requirements as well as the local circumstances in which the system will operate. The below is a non-exhaustive list of questions that may be explored prior to selecting a PIDS.



Environment

Consider the local environment in which the PIDS will operate

Is there a physical barrier around the perimeter?

Is there existing infrastructure to mount the system on?

Is legitimate access required at particular times of the day?

Is there a public footway in the vicinity which may trigger an alarm?

Are there underground services which may prevent the installation of ground based PIDS?

Climate

Consider the climatic conditions of the area

Will the PIDS be deployed on a site subject to strong winds?

Is fog common in the area which may obscured video surveillance views or cause false alarms?

Is heavy rainfall common?

Will the system be exposed to direct sunlight?

Landscape

Consider the landscape, flora, fauna and topographical features of the area

Will local wildlife set off the PIDS?

Are there bodies of water which may reduce performance?

Are there ground undulation or surface objects which may prevent the system from detecting an intruder?

Does the ground become saturated which may affect the PIDS performance?

Duration, Deployment & Maintenance

Consider the requirements for the PIDS system

Will the PIDS be deployed permanently or temporarily?

Does the system need to be covert/discreet?

What are the maintenance requirements and approximate service life of the PIDS?

Integration

Consider whether the PIDS will work in conjuction with other components such as lighting, video surveillance or sound systems

What other types of equipment and systems are planned or in use?

Who will be responsible for the integration?

How will the system integrate with the overall security strategy?

Response

Consider how and where a response will be initiated from

Will the system be monitored from an onsite control room or remotely?

Is there a permanent presence of security personnel who can respond to an alarm?

Regulations

Consider any regulations the PIDS will have to adhere to

Electromagnetic compatibility (EMC)

Safety regulations

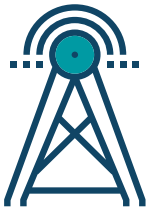
2.2 Types of PIDS

Different PIDS technologies have their generic strengths and weaknesses which should be carefully considered. The following section covers a relative analysis of the strengths and weaknesses of each category and the technologies within.

BARRIER - MOUNTED

GROUND - BASED

FREE - STANDING



RAPIDLY / DEPLOYABLE

Barrier - Mounted

PIDS deployed on or in conjunction with a fence or other physical barrier.

SYSTEM	STRENGTHS	WEAKNESSES	CONSIDERATIONS
Barrier - Mounted	◆ The presence of a barrier provides a physical delay which aids in the alarm verification and response processes ◆ Some barrier mounted PIDS offer the ability to protect an entire perimeter with one continuous length of cable and one processing unit. This has associated cost benefits in terms of infrastructure	◆ Resilience may be compromised if the system relies solely on one processor unit and one power supply ◆ Fence and topping vibrations caused by high winds are a significant source of false alarms	◆ Performance is subject to type of barrier ◆ The processing unit can be high cost; therefore, it can be an expensive solution for short perimeters ◆ Care must be taken when defining zones to ensure they match the correct camera views
Electrified Fences	◆ High deterrence factor ◆ Electrified fences tend to have low false alarm rates	◆ Wire strands require regular inspection ◆ False alarms may be caused by a build-up of conductive material on the insulators e.g salt in coastal locations ◆ Electric field/capacitance type systems can be affected by the amount of humidity in the air leading to reduced performance	◆ 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 be selected ◆ Electrified fences should be ideally mounted behind the secured side of the host fence

Ground - Based

PIDS which are deployed below ground. They do not require a physical barrier.

SYSTEM	STRENGTHS	WEAKNESSES	CONSIDERATIONS
All	• They can be covert, making it a good early warning system • Site aesthetics are not compromised once installed • Less affected by weather conditions than above ground PIDS	• Generally high installation cost due to the ground works • Installation causes considerable disruption • Performance is subject to ground (water) saturation	• Provide no delay or deterrence when not deployed in conjunction with a physical barrier. Prompt response to alarms is required in these cases
Radio Frequency (RF) radiating field	• Good overall performance • Good discrimination between animal target sizes	• False alarms caused by accumulated water following heavy rainfall • Where surface water is present, detection is less effective • RF radiation emitted by these systems can be detected and be interfered with	
Microphonic cable	• Reasonable performance at a modest price • Installation cost can be minimised by installing the cables into a small slot cut rather than a trench	• False alarms from wildlife • Can be vulnerable to heavy traffic in the vicinity as well as to pressure transmitted by roots of trees and vegetation moving in heavy wind	
Optical-Fibre cable	• The sensor cable is immune to RF interference • Generally, one cable run is used for a whole perimeter, and the installation often requires just one processing unit and power supply	• Resilience may be compromised if the PIDS system relies solely on one processor unit and one power supply	• The processing unit of such systems can be high cost; therefore, it can be an expensive solution for short perimeters
Balanced Fluid-filled tube	• Good detection and false alarm performance	• Higher maintenance overhead as pressure checks should be carried out at least annually	• Covertness may be compromised by the requirement for access pits used to pressurise the tubes

Free-Standing

PIDS deployed above ground that do not need to be installed on or in conjunction with a physical barrier. Ideally, free-standing PIDS are deployed inside a sterile zone if barrier mounted PIDS are not suitable.

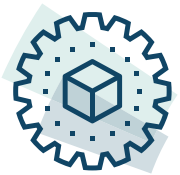
SYSTEM	STRENGTHS	WEAKNESSES	CONSIDERATIONS
All	◆ Reduced installation cost ◆ Do not hinder legitimate activity such as the movement of vehicles		◆ Provide no delay or deterrence when not deployed in conjunction with a physical barrier. Prompt response to alarms is required in these cases
Active infrared	◆ No dead zones near to the transmitter/ receiver units ◆ Features are available which can reduce false alarms from small or fast-moving wildlife	◆ Susceptible to the effects of fog causing false alarms ◆ 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	◆ Typically require a hard-wired synchronisation cable between each pair of transmitters and receivers, preferably in underground ducting
Passive infrared (PIR)	◆ A variety of coverage patterns exist, from short and wide detection zones to long and narrow zones	◆ Poor immunity to changing temperatures means they are less suited for outdoor environments ◆ Careful positioning is required due to dead zones and sources of false alarms such as sunlight	
Bistatic Microwave	◆ Good immunity to the effects of weather	◆ Dead zones exist near both the receiver and transmitter units, normally protected by overlapping adjacent zones ◆ Require a well-maintained detection area ◆ Performance is susceptible to metallic objects and moving bodies of water	
Doppler Microwave		◆ Dead zones exist near to the transceiver unit ◆ Performance is susceptible to metallic objects and moving bodies of water	◆ These systems use one transmitter/receiver (transceiver) unit ◆ A maximum range can be defined, beyond which targets can move undetected ◆ 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
Laser Scanner	◆ It is an affordable solution for sites with notable cost constraints where no other technology would otherwise be deployed	◆ Can be susceptible to the effects of rain and fog	◆ Often can define parameters such as minimum target size or beam break time in a software environment
Video Analytics	◆ Generally configured to give a good (greater than 95%) detection rate	◆ Video surveillance views may be obscured by fog, restricting alarm verification and the effectiveness of video analytics	◆ They analyse video feed to automatically detect unusual activity within an imaged scene ◆ Require re-configuration to deal with seasonal variations ◆ Require a high-quality video feed ◆ Existing hardware may require upgrading and additional cameras and lighting may be required

Rapidly Deployable

PIDS that are designed for temporary deployment. 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.

SYSTEM	STRENGTHS	WEAKNESSES	CONSIDERATIONS
Rapidly Deployable	• Portability enables use at different locations • Do not require permanent infrastructure • Commissioning and set-up times are significantly reduced	• Battery power sources are utilised, which may present issues regarding frequent re-charging or replacement, and loss of detection function during this downtime • The wireless communication schemes generally used are a less secure method of transmitting alarm information compared to hard-wired connections	• Designed for use on a temporary basis • For perimeter security applications, they should be used in conjunction with a barrier • Careful alignment of sensors and camera views is required. This could be compromised due to rapid deployment, potentially leading to lower performance than permanent systems

3 Specification



Before attempting to write a performance specification, it is imperative to ensure that a detailed operational requirement (OR) has been produced.
Set out below is a non-exhaustive list of items to be addressed in a PIDS specification or other associated contract documentation. These are subject to the site, deployment and system.

AREAS TO BE PROTECTED

- Length of perimeter
- Details of any barriers
- Area to be covered
- Threat types / Attack styles

PHYSICAL CONSTRAINTS

- Ground surface, mounting positions or burial medium
- Local topography
- Conducting bodies
- Mounting of sensors, processors, junctions

ENVIRONMENTAL CONDITIONS

- Weather: temperature, sunlight, wind speed, rainfall, fog, snow, lighting
- Non-Weather: public routes in the surroundings, access points, rivers, vegetation, wildlife

DEPLOYMENT

- Planned time
- Visibility: covert vs discreet
- Tamper detection
- Integration with other systems

PERFORMANCE

- Detection rate
- False alarm rate
- Extraordinary circumstances
- Acceptable downtime

OPERATOR INTERFACE

- Alarm display and logs
- Alarm transmission and verification
- Control and indication equipment
- Alarm response and procedures

POWER REQUIREMENTS

- Available power
- Details of battery
- Compliance
- Back-up supply
- Actions in the event of a power failure

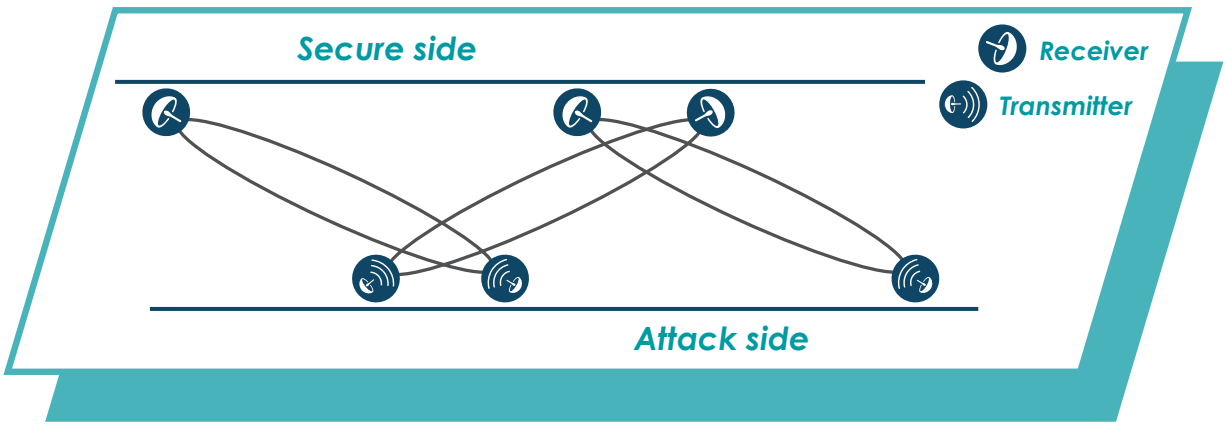
CONTRACTUAL REQUIREMENTS

- Warranty period and conditions
- Commissioning tests

4 Installation

The PIDS should be installed according to the manufacturer's installation procedures. If these are not followed, difficulties in determining liability could arise should the PIDS fail to perform. The following are some considerations for the installation of certain types of PIDS.

- PIDS with dead zones near to the sensors, such as some types of free-standing PIDS, are vulnerable to attack styles such as crawling or rolling. It is important to provide coverage to dead zones, either by overlapping the detection zones of adjacent sensors or using an additional technology.
- PIDS consisting of separate transmitter and receiver units should be installed in a way that similar units are located together to minimise the risk of interference. Wherever possible, both receiver and transmitter 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. These three principles are illustrated as follows:



- Cabling should be located at a stand-off position on the secure side of the barrier, except for the sensor cable of a barrier-mounted system which should be mounted on the fence.
- Processor boxes and associated equipment should be positioned as far from the perimeter as possible and preferably indoors.
- Tamper protection should be included where required. For instance, tamper switches should be fitted to all removable lids, inspection covers and openings to cables and components which will signal an alarm when they are opened.
- Outdoor equipment should be mounted in suitable IP-rated enclosures. Fixings should be chosen to suit the environment.

5 Commissioning

Following installation, a range of commissioning tests should be performed. Commissioning tests assess the functionality and performance of a PIDS to ensure it has been installed to, and performs in accordance with, the required specification.
If the PIDS does not fulfil the stated performance, the installation can be rejected.

5.1 Considerations

- Commissioning tests provide performance data from which any future deterioration can be measured, and hence remedial action justified. If 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.
- The installation contractor should conduct a site acceptance test (SAT) following system installation. This should not preclude the end user from conducting independent commissioning of the new system to ascertain the system's performance.
- A commissioning test plan should be devised to assess the performance of the system. 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. A variety of commissioning attacks styles should be performed at varied locations and repeated multiple times to ensure validity.
- Where PIDS are installed as part of an integrated security system, it should be tested as a whole. If the installation covers video surveillance verification, this should also be overlaid. Testing should ensure alarms are received and displayed to the operator in the control room as per the specification.
- Tests should include removing power to the system to certify that the uninterruptible power supply works as required; or that the PIDS fails safe depending on the requirement given in the specification.
- Results of the commissioning tests should be used to determine whether the PIDS meets the specification and should therefore be accepted. The results should meet the false alarm rate and the level of detection given in the specification.

5.2 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 maintaining and operating the system. Commissioning documentation should include but not be limited to the following information.

- A DESCRIPTION OF THE MANNER AND LIMITATIONS OF OPERATION
- PROOF OF COMPLIANCE WITH RELEVANT STANDARDS OR SCHEMES
- SET-UP/ SENSITIVITY PARAMETERS
- INSTRUCTIONS FOR THE SWITCHING ON, OPERATION, SWITCHING OFF AND ISOLATION OF THE SYSTEM
- INSTRUCTIONS FOR DEALING WITH EMERGENCY CONDITIONS
- INSTRUCTIONS FOR SYSTEM MAINTENANCE
- THE NAMES AND CONTACT DETAILS OF ALL COMPONENT SUPPLIERS, AND ASSOCIATED INFORMATION
- DRAWINGS INCLUDING DIAGRAMS AND SCHEDULES SO THAT THE SYSTEM CAN BE SAFELY OPERATED, MAINTAINED, INSPECTED AND TESTED
- DRAWINGS SHOWING THE PHYSICAL ARRANGEMENTS TO ASSIST THE LOCATION AND IDENTIFICATION OF ALL COMPONENTS

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 the system effectiveness in the long-term. Good working practices include

- STAFF TRAINING AND PERFORMANCE MONITORING
- ADEQUATE CONTROL ROOM ENVIRONMENT
- KEEPING PROCEDURAL AND SYSTEM DOCUMENTATION READILY AVAILABLE
- HAVING CLEARLY DEFINED PROCEDURES FOR FAULT LOGGING AND RESOLUTION

The contractor must provide the maintenance requirements of the proposed PIDS. It is imperative that the maintenance regime and any maintenance contractors are approved by the supplier to ensure the supplier can be held accountable for any failure of the PIDS to maintain the required performance. Operators should be aware of who has the authority to call out the maintenance team if a problem arises and what the response time should be.

The maintenance schedule should include selected tasks to check that the operational requirement is still applicable and determine whether there have been any changes during the life of the PIDS that may have affected its operation and performance.

6.1 Site Maintenance

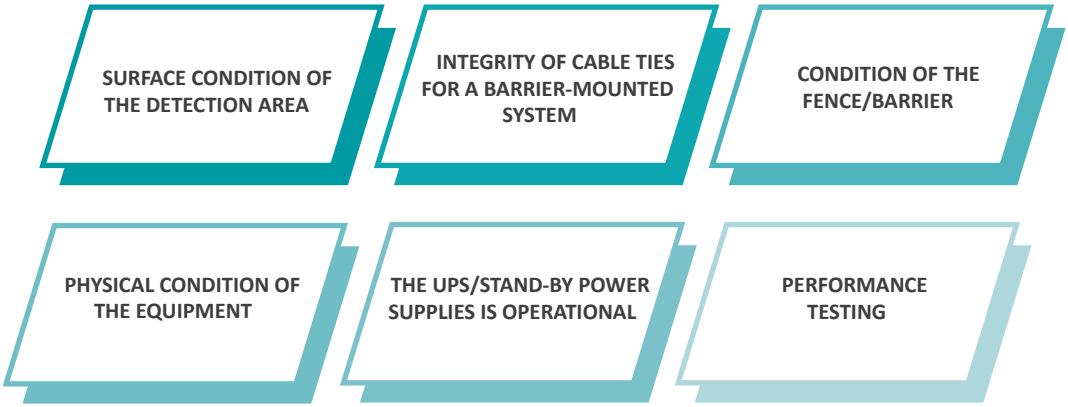
Maintenance of the site and the area around the PIDS should be completed on a regular basis to help prevent gradual reduction in PIDS performance. Maintenance regimes should be performed by the PIDS operators or site maintenance team to minimise false alarms. Requirements should include, but not be limited to:

- THE GROUND IN AND AROUND THE PIDS, BARRIER AND/OR DETECTION ZONE SHOULD BE KEPT CLEAR OF FOLIAGE AND VEGETATION
- THE SITE SHOULD BE KEPT CLEAN AND TIDY
- WILDLIFE SHOULD BE PREVENTED FROM INTERACTING WITH THE BARRIER OR DETECTION ZONE
- VEGETATION SHOULD BE KEPT CUT BACK TO REDUCE THE POSSIBILITY OF CAUSING FALSE ALARMS AND LONG GRASS SHOULD BE AVOIDED

6.2 PIDS Maintenance

The frequency of operational checks will be influenced by factors such as the nature of assets being protected, and the level of confidence required in the PIDS.

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



Operators may wish to perform a simple confidence check to ensure that a PIDS is still functioning. 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.

Assessing the number of false alarms that occur; making comparisons between zones; and looking for trends can indicate whether a zone warrants further investigation.

Some simple electrical tests should also be periodically carried out. Such tests can be specified in a routine maintenance contract with the PIDS manufacturer or supplier.

Following any maintenance or testing, repairs, upgrades or adjustments the PIDS should be retested to ensure it continuous to operate as required in the specification. Every effort should be made to provide temporary cover for any part of a perimeter that would otherwise be unprotected due to unserviceable equipment.

7 Summary

This guidance document has provided an overview of Perimeter Intrusion Detection Systems. The content can be summarised as follows:

Key Points

1. Operational requirements should guide the selection and specification of a PIDS
2. A thorough understanding of the site and local environment, landscape and climatic conditions is required prior to selecting a specific technology
3. There are four main types of PIDS with its associated strengths and weaknesses
4. False alarms should be anticipated for all types of PIDS, however they should be minimised by selecting the most appropriate technology to the site specifics
5. A specification should comprise detailed information about the required PIDS, including details of other systems to be used with the PIDS
6. PIDS should be installed following the manufacturer's installation procedures
7. Commissioning tests should be conducted upon installation and prior to acceptance
8. Maintenance of the PIDS and surrounding area should be completed regularly to help prevent gradual reduction in PIDS performance

Further Information

Specialist advice and supporting guidance documents are available through the relevant CPNI sector adviser, or from the CPNI website *www.cpni.gov.uk*

- Guide to producing operational requirements for security measures
- PIDS evaluation standards, which contain lists of attack methods used for evaluating PIDS
- The CPNI Catalogue of Security Equipment (CSE) list CPNI assured PIDS products