ADPRO® PRO E™

Passive-Infrared Perimeter Intrusion Detection Systems (PIR PIDS)

Introduction to PIR Technology Manual

September 2014

Document: 27385_01

ADPRO®
by xtralis®

Disclaimer

The contents of this document is provided on an “as is” basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:

i. in the case of services, the cost of having the services supplied again; or
ii. in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect.

Document Conventions

The following typographic conventions are used in this document:

Convention	Description
Bold	**Used to denote:** emphasis Used for names of menus, menu options, toolbar buttons
Italics	**Used to denote:** references to other parts of this document or other documents. Used for the result of an action.

The following icons are used in this document:

Convention	Description
	**Caution:** This icon is used to indicate that there is a danger to equipment. The danger could be loss of data, physical damage, or permanent corruption of configuration details.
	**Note!** This icon is used to highlight useful advice and recommendations as well as information for an efficient and trouble-free operation.

Contact Us

UK and Europe	+44 1442 242 330
D-A-CH	+49 431 23284 1
The Americas	+1 781 740 2223
Middle East	+962 6 588 5622
Asia	+86 21 5240 0077
Australia and New Zealand	+61 3 9936 7000
www.xtralis.com	

Table of Contents

This page is intentionally left blank.

1 General Notes

1.1 Information about this manual

Use of the manual	This manual is intended to be used as a planning aid in order to specify an effective combination of ADPRO by Xtralis products that satisfies your individual requirements without losing sight of costs.
Illustrations in this manual	The illustrations in this manual are purely for your guidance and understanding and may differ from your device depending on the actual device version.
Loss of manual	In the event of loss of this manual, a replacement can be ordered from Xtralis.

1.2 Purpose of this manual and target group

This non-binding introduction to security technology and PIR technology is intended to provide basic information for insurance companies, consultants, engineers, professional installers, integrators and obviously end-users on how a carefully designed perimeter intrusion detection system can preventively reduce the risk of a possible threat as part of an integrated total building security concept.

1.3 Applicable documents

1.3.1 Manuals

- 27387_01_ADPRO_PRO E_PIR_System Design and Planning Manual
- 27386_01_ADPRO_PRO E_PIR_Installation Manual
- 26571_01_ADPRO_PRO E_PIR_System Setup Manual

1.3.2 Guidelines and standards

- VdS guideline on system components for monitoring open areas VdS3456
- VdS Security Manual Perimeter VdS 3143
- prEN50606 External Perimeter Security Systems (in development)

1.3.3 Xtralis Websites

www.xtralis.com

Xtralis Security Solutions Support Site

www.xtralissecurity.com

Data sheets and commercial information are available in the public section. Upon registration (free of charge), our partners can find more advanced and detailed information such as manuals, Xtralis white papers, presentations, images, videos, certificates and software and drives. This information is provided free of charge.

Landing page ADPRO PRO E Passive-Infrared Detectors

www.xtralis.com/adpro_pro_e_detectors

Xtralis Product Videos

www.xtralis.com/video.cfm

This page is intentionally left blank.

2 Definitions

2.1 Perimeter

2.1.1 Historically

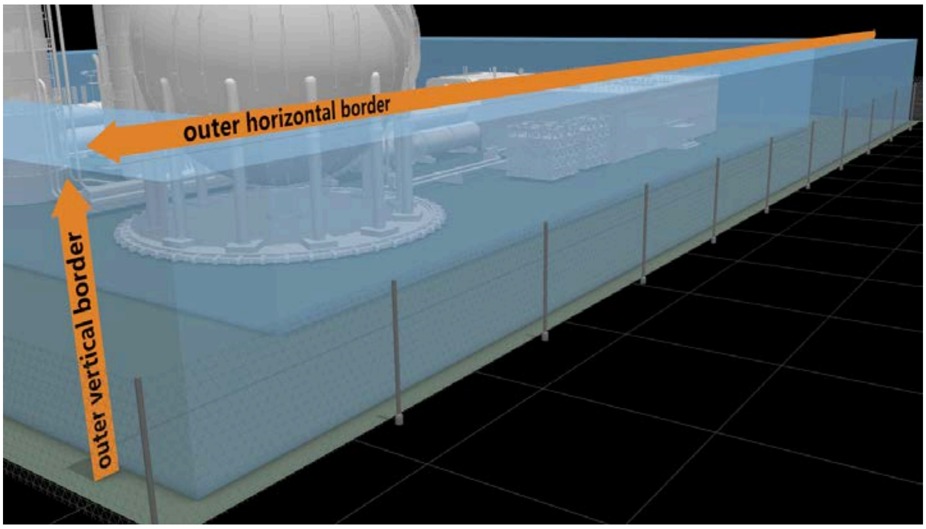
Perimeter (from the Greek peri meaning "around") protection has been used for thousands of years. Stakes, palisades, walls or (water-filled) ditches have been used to provide effective protection as mechanical security systems.

These generally very effective perimeter security facilities were intended to prevent possible attackers from approaching essential mechanical barriers such as drawbridges or castle walls (without detection), or at the very least, make that task very difficult. As a result, action could be taken at a very early stage and defensive forces deployed.

2.1.2 Today

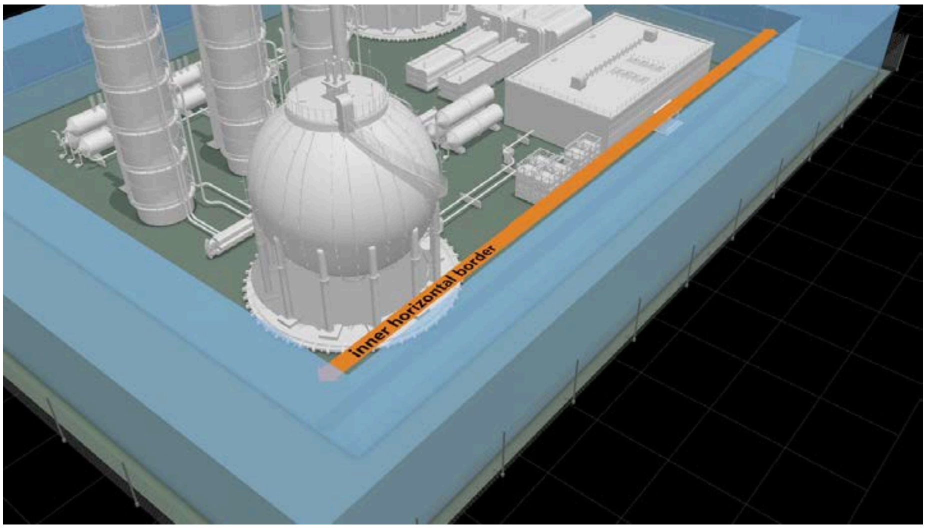
Today's modern perimeter security facilities only differ from a historic castle moat in terms of the materials and devices used (fences and detectors). The basic security concept however is the same.

In addition to mechanical security technology, a wide variety of electronic detection and verification systems (video surveillance) is available to us today. In combination with well-planned organizational measures, it is also possible to contribute effectively to providing protection against unauthorized access, theft, hold-up and theft by intruders, or sabotage such as arson.



The perimeter, as referred to in Xtralis documentation, is the area surrounding a building or a technical plant. Today, these are often oil pumping stations and the associated pipelines, water reservoirs, photovoltaic systems or transmitter masts, logistics centers, etc.

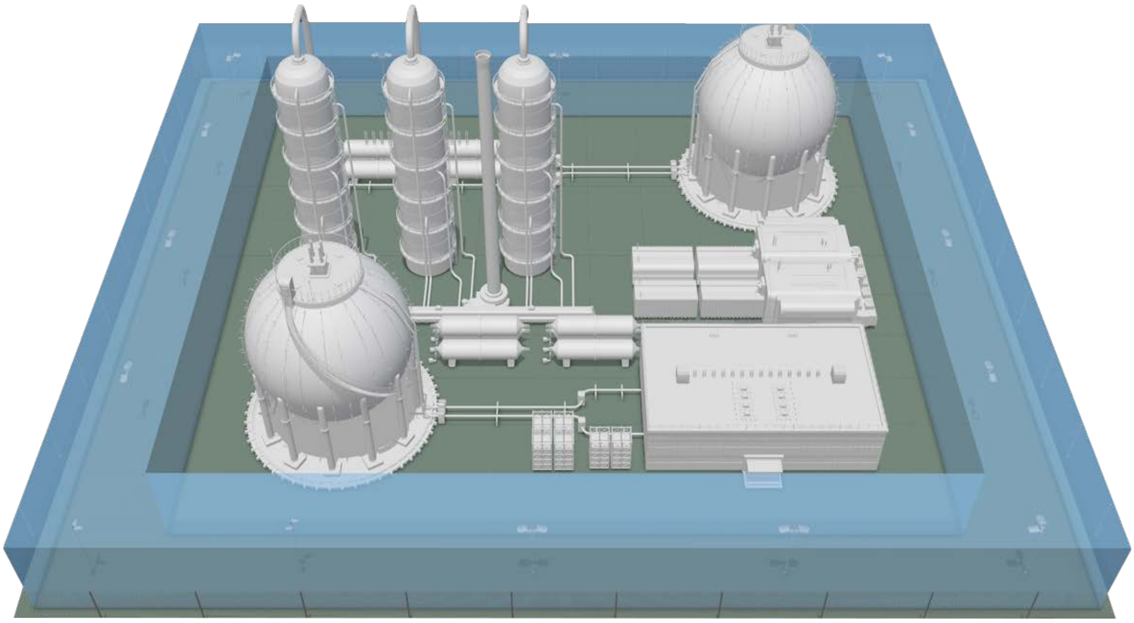
In the horizontal plane, the legal boundaries of the site demarcate the external limits of the perimeter.



An internal limit, which is not necessarily present, may be demarcated by a building; in this case an industrial plant. The outer walls of buildings inside the plot of land can therefore mark the inner limit of the perimeter.

The perimeter is also subject to legal limits in the vertical plane. Depending on the level of risk, perimeter surveillance should also be provided in the vertical plane (extending upwards/downwards).

2.2 Perimeter surveillance



Fundamentally, a perimeter surveillance system consists of one or more detectors and an evaluation unit, e.g. a controller. The system can be intelligently linked to other monitoring systems depending on requirements and the local circumstances.

Mechanical barriers which prevent encroachment for a certain time and resist intrusion attempts for a specific time (mechanical resistance) are complemented by ADPRO PRO E-detectors, which register intrusion at a very early stage, or make it possible to analyze what is happening, e.g. via video technology, or immediately trigger an alarm.

The ADPRO PRO E-detectors, which are based on the passive-infrared principle, are characterized by an extensive detection range, both in terms of distance and volume, coupled with low power consumption and low purchase and maintenance costs.

They are also inherently highly secure as they can detect attempts to sabotage the detector.

2.3 Applications outside the scope of this manual

This manual describes ways of protecting against outside perpetrators in relation to land-based commercial and industrial buildings or infrastructure, depending on a defined risk situation.

This excludes objects where there is a very high security risk such as nuclear power stations, military facilities or prisons.

Furthermore, no information is provided about marine and submarine security systems (port and harbor security).

Moreover, in the context of this guideline,no information is provided on the protection of individual persons.

We would be glad to advise you personally in this respect.

2.4 Perpetrator profiles

Different perpetrator profiles can be assumed in respect of the potential threats:

- Opportunistic perpetrator
  who takes advantage of a favorable opportunity to steal money or valuable objects (to fund a drugs habit) or commits acts of vandalism (e.g. graffiti, arson, sabotage).
- Professionals
  as individual criminals or criminal gangs, who are characterized by a specific modus operandi; e.g. targeted theft of special (automobile) parts, targeted theft of materials, sabotage or espionage.

2.5 Security Grading

The perpetrator "rating" or degree of effort required to circumvent a security system in accordance with EN50131-1 *) is defined as follows:

- **Grade 1: Low risk**
  An intruder or robber is expected to have little knowledge of security systems and is restricted to a limited range of easily available tools.
- **Grade 2: Low to medium risk**
  An intruder or robber is expected to have a limited knowledge of security systems and have the use of a general range of tools and portable instruments (e.g. a multimeter.)
- **Grade 3: Medium to high risk**
  An intruder or robber is expected to be familiar with security systems and have the use of an extensive range of tools and portable electronic instruments.
- **Grade 4: High risk**
  This grade applies when security takes precedence above all other factors. An intruder or robber is expected to have the ability or resource to plan an intrusion or robbery in detail and have a full range of equipment including means of substitution of components in a security system.

*) These definitions will need to be modified for use in the context of perimeter security during the development process for prEN50606.

2.5.1 Types of attack on a perimeter security system

- **Walking or running in an upright position**
  An intruder attempts to cross the perimeter while walking or running. This method generally applies to systems where no physical barrier (fencing) is present..
- **Climbing**
  An intruder attempts to penetrate the system by climbing. This only relates to systems where a physical barrier is present. It is not possible to climb over the monitored zone in these systems without equipment. A downstream detection system "suspects“ that the intruder has gained entry by climbing. However, the intruder may also have gained entry by cutting a hole.
- **Cutting a hole**
  As in the case of climbing, this type of entry is only possible when a mechanical barrier is present and the event is similar to that for "climbing". From a technological point of view, PIR detectors are inherently unable to detect the act of cutting holes. Even so, the system can be designed to ensure detection of

movement of the fence and above all subsequent entry after cutting a hole. The right choice of detectors is particularly important here.

- **Ladders**
  The term ladder refers to all equipment/resources used to climb over a barrier (e.g. also high trucks parked next to the barrier). Overcoming a mechanical barrier using a ladder can be categorized in various ways:
  - contact-based use of ladders (leaning against the barrier)
  - non-contact use of ladders (stepladders)

  From a technological point of view, PIR detectors are inherently unable to detect the act of stepping across a barrier. Even so, the system, or choice of the detectors, can be specified in a way that ensures reliable detection of this type of attack and subsequent entry. Here too, careful design of the system has a significant effect on event detection and the false alarm rate. Contrary to other detection technologies, not only contact-based ladders, but also non-contact ladders or other means of crossing the barrier can be detected.

- **Tunneling**
  It is generally believed that tunneling under a monitored barrier can only be detected by a digging detection system (e.g. burried cable detection system). From a technological point of view, PIR detectors are inherently unable to detect tunneling under a barrier. However, the intruder has to return to the surface in order to complete the intended task. The system can be designed in a way that ensures reliable detection of this type of attack and subsequent passage through the monitored zone. Here again, the right choice of detectors, e.g. volumetric detectors that scan large surfaces, plays an important role.
- **Drive-through**
  Comparable to walking/running, however associated with a higher speed and greater mass and therefore greater energy. As a result, contrary to walking and running, this method can break through a mechanical barrier.
  From a technological point of view, due to the speed, PIR detectors may not necessarily reliably detect a drive-through attack on the barrier. However because the intruder will have to come to a standstill again after penetrating the barrier, the system can be designed in a way that reliably detects this type of attack and subsequent passage through the monitored zone in particular. In this case, the right choice and number of detectors and strategic positioning of those detectors is particularly important.

2.6 False alarms – classification

A false alarm can be classified as follows:

- **Technical alarm (spurious alarm)**
  The detector is faulty or may have been triggered by electromagnetic interference (for example).
- **Alarm triggered with malicious intent**
  An alarm is triggered by an intentional intervention; e.g. changing the alignment of a PIR detector to trigger an alarm.
- **False alarm caused by mistaken identification**
  The detector or alarm system mistakenly triggers an alarm in reaction to phenomena that are similar to a real threat such as large animals, vehicle exhaust gases or environmental effects.

- **Communication errors**
  Communication errors may also be the cause of a false alarm (false assumptions or lack of competency in relation to the area of operation).

2.7 Risks

Many commercial complexes and industrial buildings and the associated external areas such as logistics centers, car dealerships with large yards, goods and machinery storage areas or scrapyards are relatively easy targets for potential criminals if no surveillance system is installed.

Particularly in times of economic crisis, these external areas attract criminals like magnets and become high risk zones if unauthorized persons can gain access without being detected.

Increasing dependency on business processes means that even minor faults can lead to significant financial losses when operations are interrupted. For example, stealing catalytic converters from delivery vehicles or stealing solar panels from solar energy farms.

Threat exposure starts at the legal boundaries of the plot or, in special cases, in front of those boundaries (spying).

2.7.1 Threat analysis

This includes identification of possible threats and perpetrator profiles, analysis of potential damage and an assessment of the likelihood that a damaging event will occur. This imperatively requires involvement of the owners, tenants, financiers, police and fire department and the (future) insurers in the design process.

2.7.2 Threat scenarios

The following scenarios are possible:

- Theft of goods present at factory sites
- Intruder entry into buildings
- Sabotage and vandalism in relation to operating assets and equipment
- Espionage
- Arson

This page is intentionally left blank.

3 PIR detectors

3.1 Introduction

A PIR detector detects temperature differences between moving objects and a stationary background in the perimeter area. The mode of operation is passive, which means that very little power is required. This is explained in greater detail in chapter Passive-Infrared Technology.

The detector alarm thresholds are modified depending on external influences such as environmental conditions and temperature changes and noise interference is filtered out by the intelligent signal analysis feature.

The detector is available in various models. The use of high precision optics results in a nominal range of 21 m to 220 m in length and from 2.9 m up to 30 m in width.

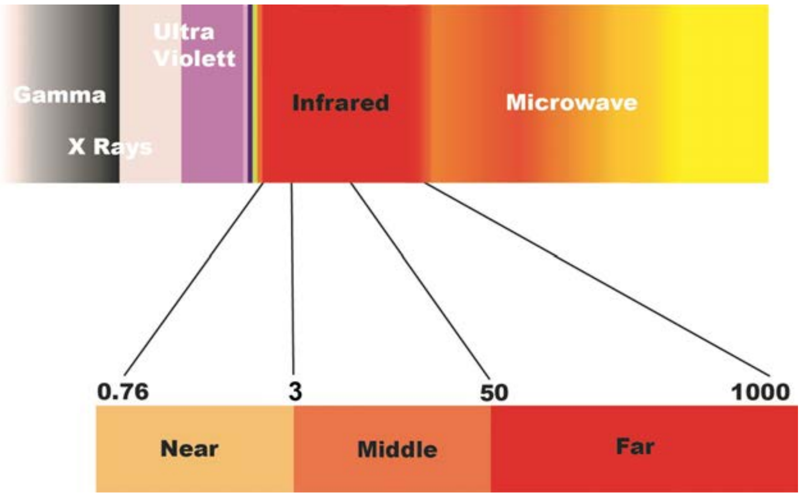
3.2 Passive-Infrared Technology

3.2.1 What is infrared?

All bodies or objects (people, animals, vehicles, etc.) at a temperature above 0 degrees Kelvin (absolute zero) emit infrared radiation (also known as IR) based on Planck's radiation law. In terms of physics, this radiation consists of electromagnetic waves just like visible light, a phenomenon that is familiar to all of us.

The frequency range for IR radiation lies between 300 GHz and 400 THz , which corresponds to a spectral bandwidth of 780 nm up to 1 mm and is virtually undetectable to the human eye.

X-rays, for example, are characterized by a much shorter wavelength at a higher frequency and therefore possess greater radiant energy. The radiant energy level of IR radiation is relatively weak.



As the graph shows, infrared radiation can be broken down into three categories: near-infrared (IR-A: 0.78…1.4 µm / IR-B: 1.4…3.0 µm, mid-infrared (IR-C: 3…50 µm) and far-infrared (also IR-C: 50…1000 µm).

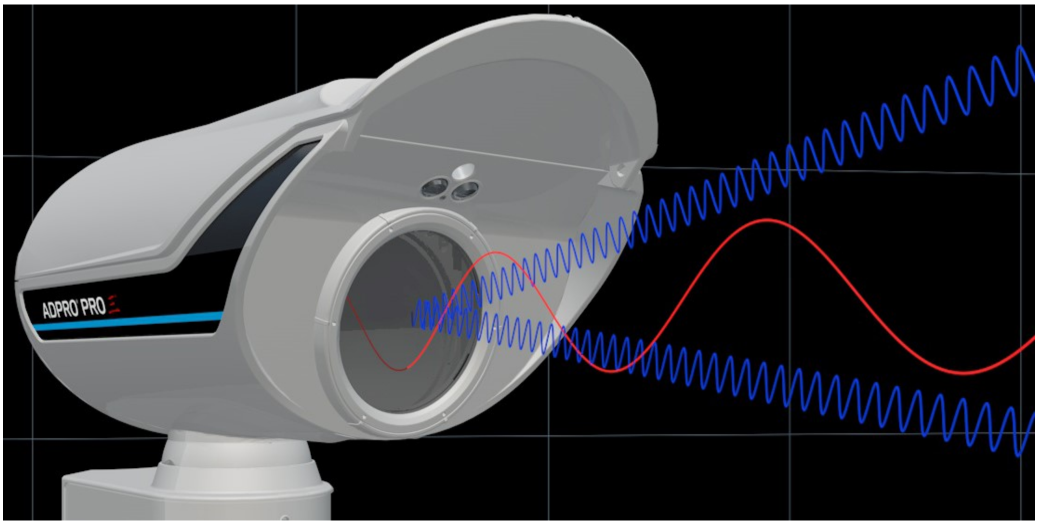
On the one hand infrared light is reflected by surfaces such as glass, mirrors, water, dew on meadows or trees, etc. but absorbed on the other hand by other surfaces (mist, snow, hail, etc.).

3.2.2 What do PIR detectors register?

Passive-Infrared (PIR) detectors in the ADPRO PRO E series detect temperature changes in the spectral band for long wave mid-infrared radiation with a wavelength from 8 µm to 14 µm.

This spectral bandwidth is achieved through high-precision double filtering.

The detector's window is used as the first filter. Both the HDPE foil and the wafer disc only allow the "right“ radiation through. A second filter is present directly on the pyroelectric element.



People and animals emit infrared radiation at a wavelength of approximately 10 micrometers (µm). The sensor circuitry and sequence of software algorithms in the detector are calibrated in a way that ensures recognition and analysis of these wavelengths only. They also detect the temperature differences in a defined detection area between the background and the moving object.

3.2.3 Detector components that determine quality

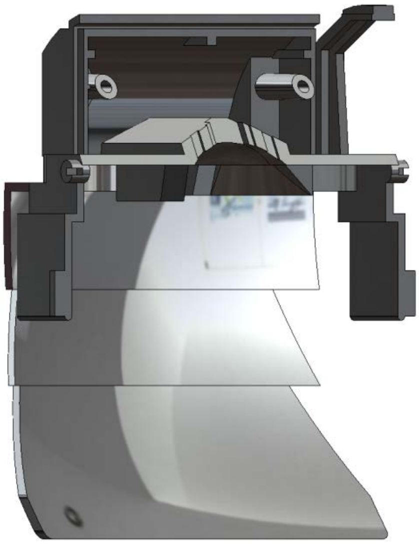
The detector additionally includes many further components that provide protection against environmental interference factors or sabotage. However only four essential components are required in order to register a person's infrared radiation:

3.2.3.1 ADPRO PRO E-detectors are digital

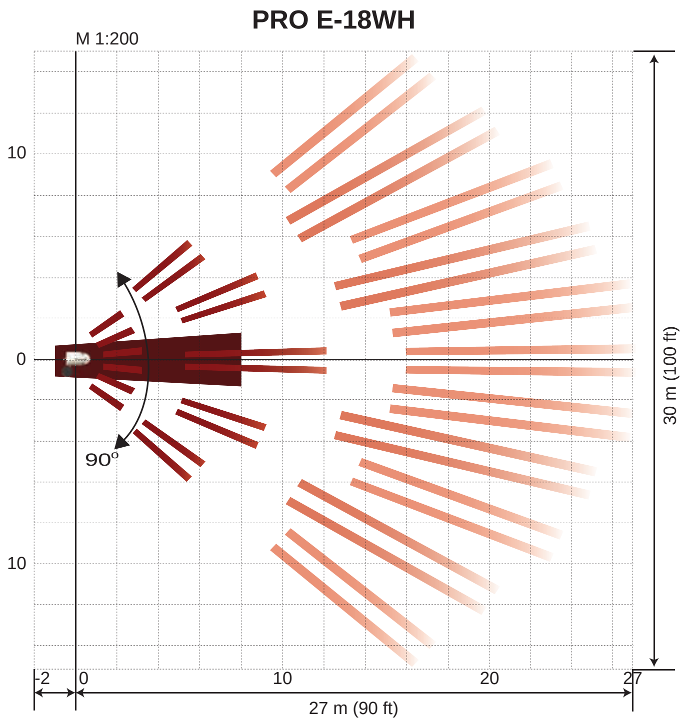
The pyroelectric sensor in PIR detectors recognizes fluctuations in the mid-infrared range and converts them into electrical signals, which are immediately digitized. This significantly increases the detector's electromagnetic immunity.

3.2.3.2 Optical components in the PIR detector

The detector's optics play a key role. The IR radiation, which has been pre-filtered by the detector window, is concentrated into a bundle by a mirror and projected onto the pyroelectric element. Depending on the geometry, the detector may therefore also be able to "see“ into the target zone.

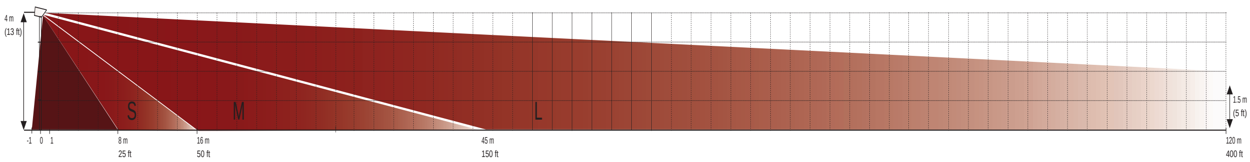


This zone can be shaped like a curtain or barrier for perimeter monitoring or as a broad fan for monitoring a large surface or volume. The optical system splits the IR radiation into several axes according to the desired geometry of the monitored zone (in comparison, a camera or a telescope has only one axis).



This leads to further small zones (fingers) inside the main zone.

These sub zones can be separated from each other and used to identify the exact origin of the IR radiation, i.e. the position of the body.



The high-precision mirror optics used by Xtralis, which even consist of a glass mirror in part, use this capability to determine the detection zones in terms of size and sensitivity.

3.2.3.3 Sensor components

The IR radiation that is captured and bundled by the high-precision mirror is directed at a special pyroelectric element. This pyroelectric element converts the radiation into electrical signals, which it also digitizes immediately. These components absorb the energy of the infrared light (i.e. heat) and convert it into electrical energy, i.e. electrical signals. This only occurs however when the IR radiation (the energy) fluctuates.

The sensor circuitry is therefore passive; i.e. it reacts to change rather than continuously measuring the value. As a result, the sensor circuitry does not generate signals when nothing happens in the monitoring zone.

Xtralis uses decoupled pyroelectric element technology in order to prevent false alarms produced by highly sensitive detectors reacting to background heat or extreme non-human heat.

This achieves significantly better accuracy in terms of analysis and setting sensitivity.

3.2.3.4 Signal processing components

These components process the digital data generated by the pyroelectric element to deliver the desired functionality. In addition to a very high threat detection rate, a further characteristic of a high-quality system is a minimal percentage of false alarms.

Adaptive triggering threshold discrimination (ATD) can be activated in Xtralis ADPRO PRO E-detectors as they obviously also detect smaller signals, e.g. those caused by animals. These smaller signals are designated as noise. If the ATD function is left switched off, aggregation of the signals over time will result in a low signal-to-noise ratio. This in turn can lead to false alarms. In effect, the system becomes oversensitive.

When the ATD function is switched on, these signals are analyzed using complex algorithms and the alarm threshold level is automatically adapted to an adequate degree. However, in order to prevent the system from becoming completely insensitive, this only takes place up to a factory-set maximum value. This function eliminates false alarms highly effectively and achieves an optimum detection rate.

Further detector functions, which determine the reliability and quality of a PIR detector system can be found in the manual entitled "26571_01_ADPRO_PRO E_PIR_System Setup Manual".

3.3 Monitoring characteristics

Note: To ensure maximum clarity, not all views are shown precisely to scale. As a result, some dimensions such as the installation height, the relationship between person/mast/detector or the creep zones may appear disproportionately large.

Either monitoring of surfaces is required, or more linear monitoring of clear defined limits, or both. Several fundamental monitoring characteristics are available for this:

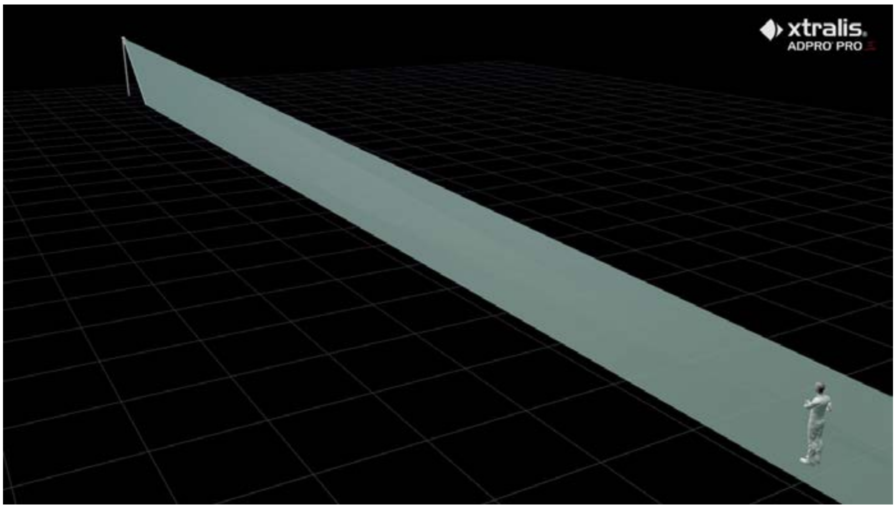
- Barrier detectors
- Volumetric detectors
- Combinations of both types

In order to allow effective combination of these detectors when designing systems, Xtralis offers an extensive range of both types of detector:

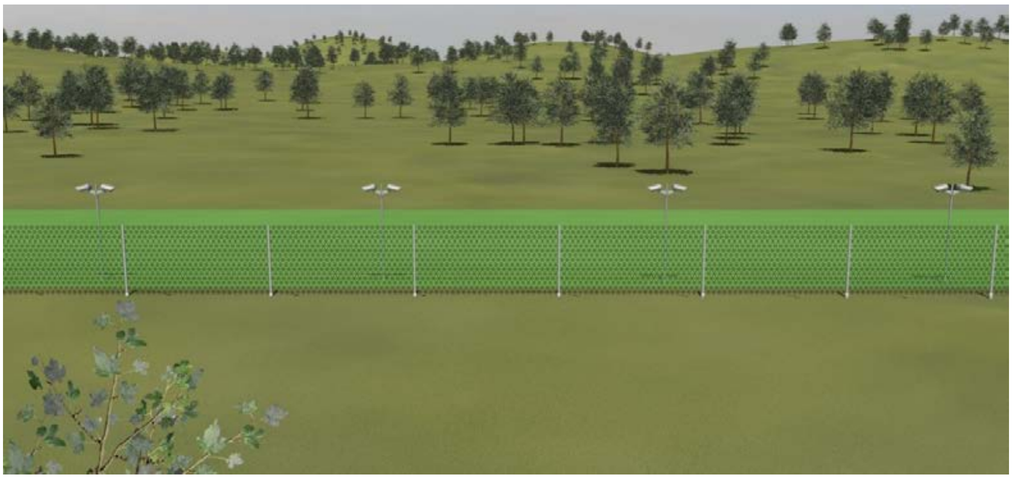
- Barrier detectors with a wide detection angle and a medium nominal range
- Barrier detectors with a narrow detection angle and large nominal range
- Volumetric detectors with a wide detection angle and short nominal range
- Volumetric detectors with a very wide detection angle and medium nominal range
- Volumetric detectors with a wide detection angle and large nominal range
- Barrier detectors with additional creep zone detection

Please refer to the product summary for details of the nominal range, monitoring angle and the resulting detection width or detection surface area.

3.3.1 Barrier detectors



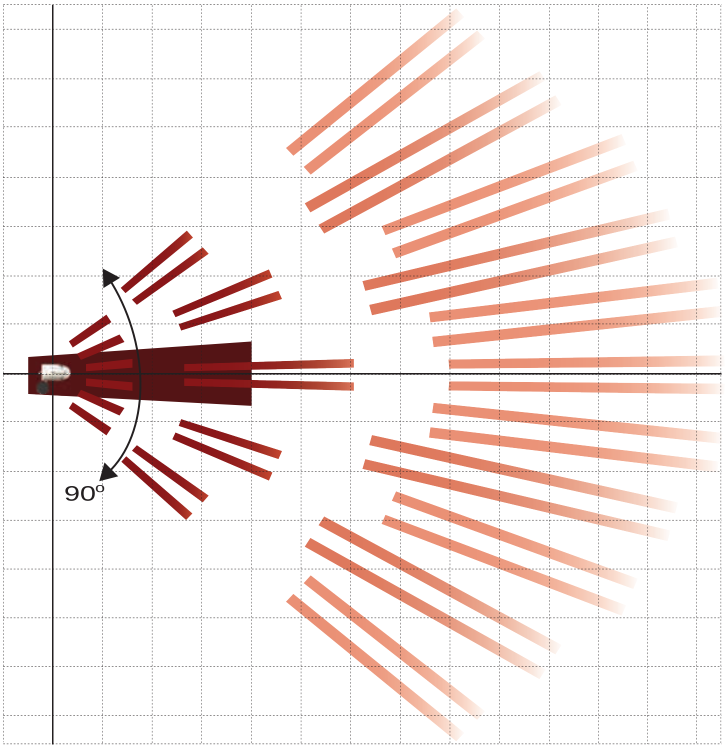
This type of monitoring is characterized by a detection zone that extends for a significant distance across a narrow width. Barrier detectors are specified when the main priority is to monitor clearly defined boundaries. As this type of detector is also capable of detection within its narrow monitoring zone that extends for a significant distance, it is also referred to as a volumetric detector. For clarity's sake however, it is referred to as a barrier detector in Xtralis documentation.



Depending on the site situation, i.e. the distance to the boundaries of the plot that require monitoring or the distance to obstacles (buildings, bushes, containers, etc.), the most suitable XtralisADPRO PRO E-detector is selected

- from the extensive range of products
- based on the nominal detection distance, number of zones (fingers) and monitoring angle
- and the resulting nominal monitoring width.

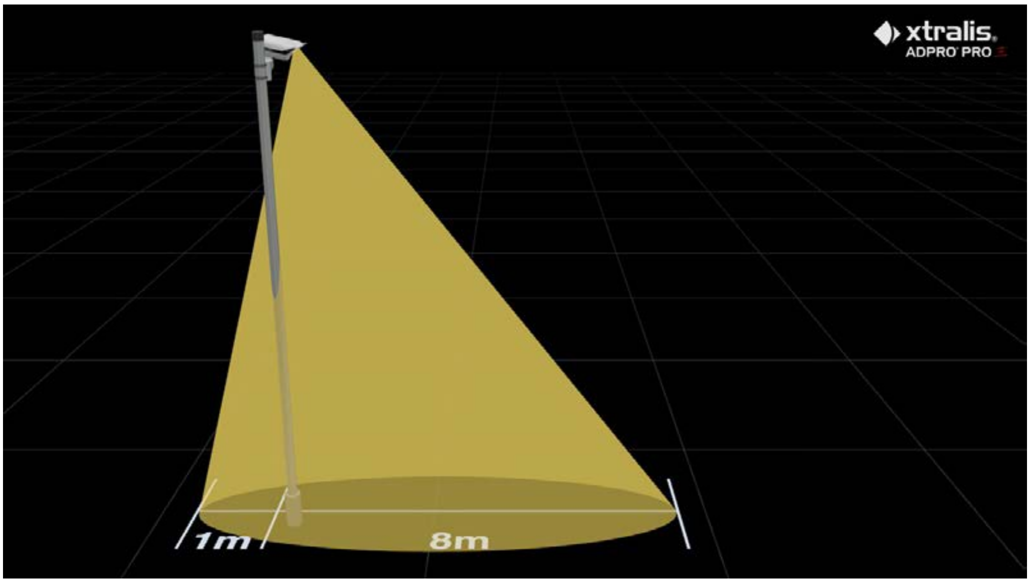
3.3.2 Volumetric detectors



Volumetric detectors are specified if the monitoring activity primarily focuses on covering a large surface. The most suitable ADPRO PRO E-detector can be selected accordingly from the extensive product range based on the nominal detection distance, number of zones (fingers) and the monitoring angle.

3.3.3 Detectors with creep zone detection

In addition to the normal detection area, all Xtralis ADPRO PRO E-detectors are equipped with an additional optical system for monitoring the creep zone. This feature dramatically improves the detector's built-in protection against sabotage.



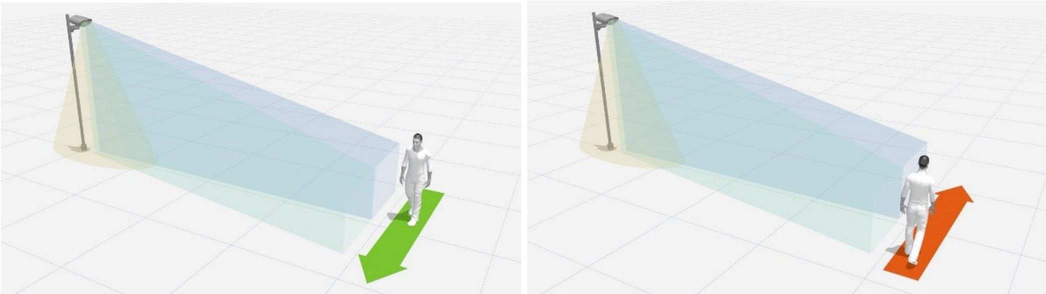
The detectors provide dedicated monitoring of the creep zone, particularly in corners and geometrically complicated applications. The creep zone is covered additionally by a second detector on the bottom face of the housing.

Depending on the conditions of use and detection range, this feature allows cost-effective project design as a single detector can be used to monitor the mast as well. This eliminates the need for a second detector in order to monitor the creep zone.

Depending on the geometry of the perimeter area, the number of detectors can be reduced, resulting in lower project costs. Obviously, the second detector can also be switched off via the software if required by site conditions.

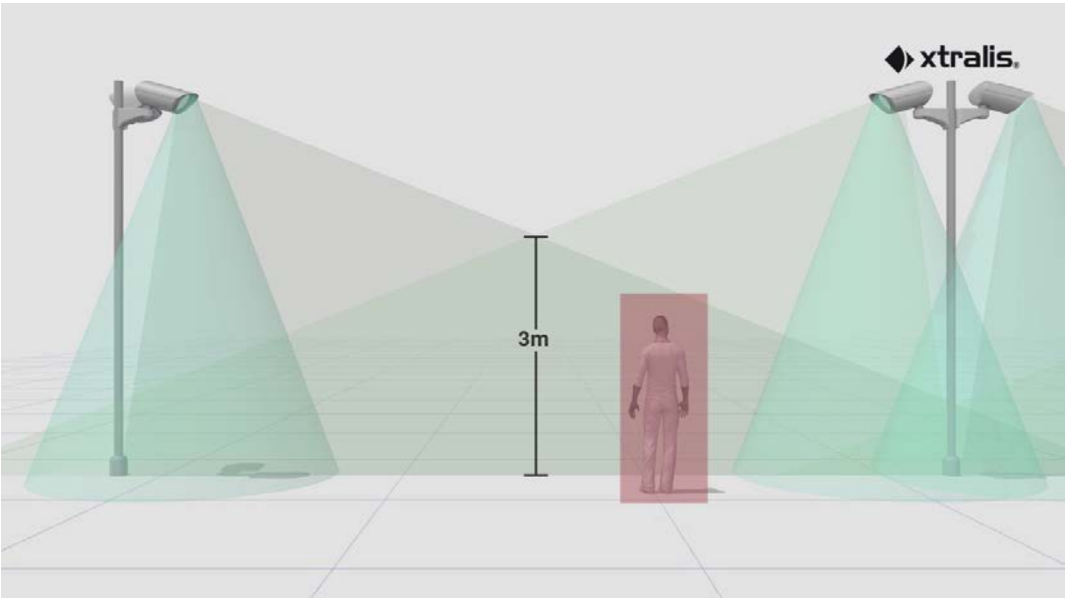
3.3.4 Detector with directional sensitivity

This function allows monitoring of a detection zone in specific directions, reduces false alarms and improves detector performance. In addition, movements from left to right and from right to left can also be detected. For example, if an authorized person crosses the detection area by accident when moving from the interior to the exterior, the directional sensitivity feature can be used to prevent a false alarm. On the other hand, an alarm is triggered if an unauthorized person crosses the detection area moving from the outside to the inside.



3.3.5 Intelligent 2-detector dependency

False alarms can also be prevented by use of the 'double knock' configuration, also called 2-detector dependency.



A main alarm is only triggered when two or more detectors generate an alarm signal. Use of this option requires precise analysis and project design. If implementation is not optimal, there is a risk that no alarms will be triggered, i.e. very thick fog between the two detectors.

3.3.6 Highly integrated 3-detector dependency

Integration in a video management system is the most reliable way of preventing false alarms due to mistaken identification and other false alarms.

Xtralis ADPRO PRO E-detectors are specifically designed to allow seamless integration with the ADPRO product range of video management systems such as the FastTrace 2E, IntrusionTrace™, Xchange™, VideoCentral Platinum and iTrace™ systems.

- Intelligent communication with the FastTrace 2E system via RS-485 bus
- PRO E-PIR combined with IntrusionTrace PLUS™ for 'triple knock' protection
- iTrace App offers at-a-glance viewing functionality on a smartphone/tablet and can directly receive the different alarms via remote transmission.
- iPIR-App for wireless PIR configuration

Seamless integration is also possible with the HeiTel product range including CamDisc HNVR, CamDisc VG and CamServer VG.

3.4 False alarms

3.4.1 Causes and avoidance of false alarms based on mistaken identification

- **Inadequately stable masts**
  When planning installation, consideration must always be given to providing a solid base in the form of a stable and vibration-free mast or a similar structure.
  If the unit is mounted to a mast, it must be ensured that no or only very slight movement occurs at the top end of the mast in unfavorable weather conditions, particularly in high winds. The wind load is a further essential factor that must be considered. Above all when further security components such as cameras, LED spotlights, distribution boxes, IP switches and so on are also mounted to the mast, thereby resulting in a higher wind load.
  Xtralis ADPRO PRO E-PIR detectors generate a low wind load as they are light in weight and feature a streamlined housing design that deflects wind.
- **Inadequately anchored fencing**
  In practice, mechanical barriers (generally fences) are a common cause of false alarms as they are often not adequately inspected and maintained. Fences in general, but wire-mesh fences in particular, come loose as a result of the effects of weather and start to move around in windy conditions. This causes signal noise, which still reduces system performance in spite of compensation by the ADT function. For this reason, it is imperative that branches or bushes protruding into the fence be removed. Wind-borne objects, such as sheets of plastic or plastic bags, which often also get caught in the mesh, can cause noise as they flutter in the wind and adversely affect the quality of the PIR detector system.
- **Heat sources in the detection zone**
  A further very common problem is that insufficient consideration is given to external sources of interference outside the perimeter when analyzing the site and subsequently designing the project.
  For example, powerful fans used in air-conditioning systems, diesel-powered generators, exhaust gas flues, chimneys, etc. are overlooked, particularly when these only operate sporadically or possibly either result in hot air haze or other effects that can trigger false alarms.
- **Physical enclosure is not possible**
  If physical enclosure is not possible for aesthetic or cost reasons, this must be taken into account when designing the project and, at a later stage, when aligning the detectors. Firstly, consideration must be given to creating a generous overlap between the monitoring zones of the individual detectors. In addition, an intelligent link can be created at that location by connecting an anti-intruder system or a security management system.
- **Walls and other man-made barriers**
  Walls are ideal range marker boundaries. Are no walls are present, retrospectively installed plates or an IR-blocking foil can also be used to good effect. While the use of IR-blocking foil or sheet is primarily a low-cost solution, it is not generally advised as regular inspection and maintenance are required.

3.4.2 Deficit of alarms

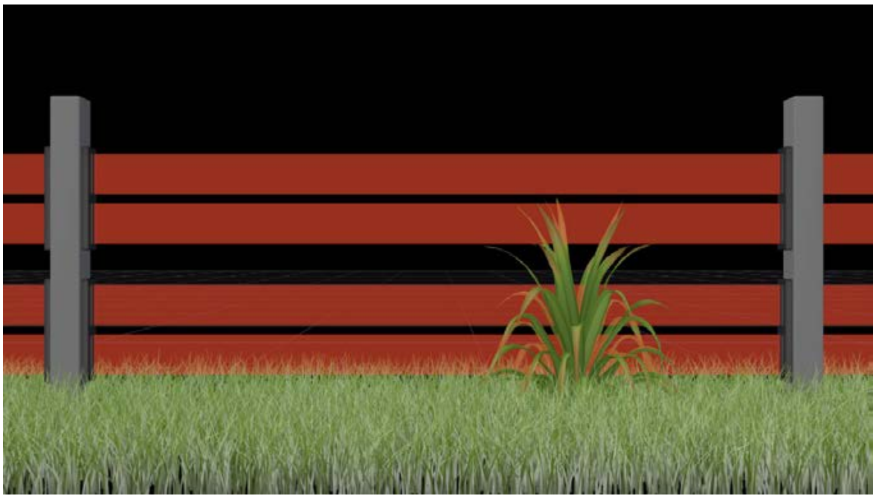
- **Missing alarms: Failure to trigger an alarm**
  Contrary to false alarms based on mistaken identification, failure to trigger an alarm can also have an adverse effect on the quality of a perimeter security system.
  Besides environmental effects such as weather, design errors and/or ineffective programming can also result in an unfavorable detection rate.
- **Low sensitivity**
  The sensitivity of the detectors must be drastically reduced in order to reduce alarms based on mistaken identification caused by various sources of noise.
  When snowfall, rain or even thick fog are factored into the equation, even an optimally configured system may fail to trigger because the signal strength is no longer sufficient, or the alarm threshold is too high. In this case, the system must be successively adapted during a set period of time.

4 Advantages of PRO E-detectors in comparison to other technologies

The ADPRO® PRO E-detectors from Xtralis offer excellent value for money compared to other technologies in terms of their barrier or volumetric monitoring performance. PIR detectors are a versatile solution for the most diverse topographic situations. They function reliably whatever the surfacing; asphalt, paving, gravel, grass, flowerbeds or roof structures.

- Volumetric Xtralis ADPRO PRO E-detectors offer extensive spatial coverage.
- Long-distance detectors, on the other hand, cover a narrow area but are capable of recognizing objects at a significant distance.
- PIR detectives are most commonly used for perimeter security and exterior shell protection. Even so, the detectors can also be used for interior monitoring, in large factory buildings for example.
- The preparation work required for installing the system at the site is relatively undemanding as most of the existing camera or light masts can be used for detector installation.
- The operating and maintenance costs are also comparatively low, as the systems require very little maintenance when designed and operated correctly.
- Possible modifications required due to seasonal effects or operational demands can easily be programmed remotely if the detectors are connected to each other via a data bus, e.g. in an Xtralis management system or video gateway set-up.
- The ADPRO PRO E-detector housing with the integral mounting bracket and tamper-proof, concealed cable management feature is sabotage-resistant, UV-stable and impact-resistant.
- All PRO E-housings are IP65 as standard.
- A universal detector arm allows simple mast or wall mounting.
- Effective cable management, including installing pre-manufactured cable looms, is guaranteed by the patented "Kidney-Seal“ feature.
- Complete protection against sabotage: mechanical and optoelectronic detection of tampering with the housing, including detection of removal from the mounting surface (standard!).

- Active infrared systems such as light barriers are easily circumvented and trigger false alarms in the event of inadequate terrain maintenance. In contrast, ADPRO PRO E systems react to temperature fluctuations and not to the interruption of a light beam.



- In comparison to active infrared detectors with a transmitter and receiver, sunrise and sunset have little effect on the detector if it has been positioned correctly and adjusted to the right angle.
- Xtralis ADPRO PRO E barrier detectors can also be installed at the maximum distance of 1.5 m from a physical enclosure such as a fence or wall and still offer effective detection over a large nominal range. Particularly in surface detection projects for photovoltaic plants, long-range PRO E-detectors offer significant cost benefits in comparison to microwave or active infrared systems.
- In addition, based on their geometry, the PIR motion detector zones are a particularly effective solution for hilly landscapes. Active infrared detector technology is limited to the use of linear beams. Consequently, intruders can creep under the beams or simply walk underneath them in irregular terrain.
- PRO E-PIR detectors operate passively and are therefore very energy-efficient. Completely wireless solutions operate reliably for many years.
- ADPRO PRO E-detectors are equipped with intelligent energy management. This means that a source of renewable energy (e.g. a solar panel) can be connected to the detector in order to significantly extend the lifespan of the batteries.
- ADPRO PRO E-detectors can optionally be equipped with an IP module to allow direct connection to a security IP network. The power required by the unit is drawn directly from the network via Power-over-Ethernet (PoE).

Note: Clearly illustrated, detailed information is available in the ADPRO PRO E presentation for customers on www.xtralissecurity.com

Notes

This page is intentionally left blank.