ADPRO® XO™

IntrusionTrace™

Video Analytic for Intelligent Perimeter Detection

Design Guide

Honeywell

Disclaimer

The contents of this document are 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.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Honeywell. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Honeywell.

Trade Name Statement

ADPRO, Xchange, FastTrace, iFT, eFT, iFT-E, iFT Gateway, IntrusionTrace, LoiterTrace, XO, iTrace, iCommand, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Honeywell and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Your use of this document does not constitute or create a licence or any other right to use the name and/or trademark and/or label.

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 Honeywell. 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. Honeywell 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 Honeywell 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 Honeywell.

Honeywell 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 Honeywell or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Honeywell 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 Honeywell 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. All rights not expressly granted are reserved.

www.security.honeywell.com

TABLE OF CONTENTS

CHAPTER

1 INTRODUCTION

The IntrusionTrace™ application is designed to provide full outdoor perimeter detection analytics. It provides reliable and predictable detection of intrusion into secure outdoor areas. The system analyses images from strategically placed cameras to detect 'human-like'[1] movement, and if the movement fulfills a number of criteria, alarms are generated. These alarms are handled by the RMVG[2] (Remotely Managed Video Gateway) and can be transmitted to a remote central monitoring station, assessed and managed by experienced security personnel. A well designed, installed, and maintained IntrusionTrace application can remove the need for onsite guards or patrols, or provide an adjunct to local monitoring, improving the effectiveness of the overall site security.

Purpose

The purpose of this Design Guide is to describe the specification, design, installation, commissioning, and maintenance of the IntrusionTrace application. The recommendations presented are designed to achieve optimal system performance and high reliability. Although there are many variations to the recommended scenarios, any departure from these recommendations may result in less than ideal system performance.

This document describes a typical installation scenario for a medium security IntrusionTrace system. To provide a high security installation, where the intrusion is expected to be covert, detailed consultation with Xtralis[3] staff is required.

1. Human-like: a feature that is able to differentiate between human and non-human movement for intrusion detection.

2. The RMVGs include the ADPRO devices of the FastTrace 2 Series, iFT Series, eFT series and Honeywell cameras running Edge analytics.

3. Xtralis is now a part of Honeywell

Scope

The following items are addressed in this Design Guide:

- operational background information on the IntrusionTrace application
- site survey and system design
- equipment installation
- system commissioning
- site and equipment maintenance.

The following items are not discussed in detail in this guide:

- design, installation, configuration or maintenance of complementary detection technologies excepting PIRs supplied by Xtralis (see the other manufacturer's technical and application information)
- installation or configuration of the RMVG (see the documentation of the RMVGs and the XOa/XO software)
- installation or configuration of central monitoring software (see the documentation of these software products)
- additional guidelines for dealing with difficult scenes (see the IntrusionTrace Best Practices
- guide).

Intended Audience

The intended audience for this Design Guide includes the following key stakeholders:

- Security consultants
- System integrators
- System installers
- Facilities/building/site managers.

CHAPTER

2 QUICK GUIDE

This guide divides the implementation of the IntrusionTrace application into four main areas:

- system design
- system installation
- site commissioning
- site maintenance.

The Quick Guide shown in the table below provides an overview of key design considerations allocated in each step and may be used as a quick reference. It should be used in conjunction with the IntrusionTrace and RMVG technical manuals to produce a robust system design.

Area	Key Design Considerations	Reference
Site survey & checklist	Conducting a site survey and what information should be gathered	Site Survey on page 10
Illumination	Illumination selection and location for use with IntrusionTrace	Illumination Requirements on page 25
Cameras	Camera selection and location for use with IntrusionTrace	Camera Selection and Location on page 16
PIRs	Design and installation of PIRs with IntrusionTrace	PIR Installation on page 30
IntrusionTrace configuration	Configuring the IntrusionTrace application for operation	IntrusionTrace Technical Manual
Commissioning and system test	Testing the system and checking the detection performance	Site Commissioning on page 33
System maintenance	Ensuring the system continually operates to the required criteria	Site Maintenance on page 37

CHAPTER

3 THE ROLE OF SECURITY

Security is becoming an increasingly accepted part of everyday living. It is imperative for organizations to consider physical and information security as a fundamentally important element of their overall management strategy. Suitable security must include detailed **Risk Analysis and Management** as well as an awareness of **Business Continuity Management**, ensuring that the system instituted provides the organization with the best approach to achieve on-going success.

The key elements to instituting a security solution are:

- Identify and evaluate risks
- Develop strategy to remove or reduce risks
- Test and monitor strategy.

A typical approach to security is to provide an indication when an intrusion has occurred. Xtralis, however, recognizes the value in being able to immediately identify the cause, evaluate the situation, and respond accordingly.

The combination of on-site detectors, audio/video recording and transmission to monitoring stations, provides security in a wide variety of markets and application areas. The IntrusionTrace application forms an important element of security solutions where automatic detection and verification of an intrusion is paramount. It is ideally suited for security solutions where the risk is illegal intrusion into a high value asset.

The IntrusionTrace application, coupled with other video analytic technologies, can form an important link in responding to different scenarios:

- A remotely monitored perimeter detection analytics provides rapid remote response, with an option for local response follow-up. The response from a remote monitoring station, followed by dispatch of security guards or law enforcement provides a powerful, flexible, and effective solution to many site security problems.
- The presence of an IntrusionTrace application at a site can provide rapid local response. When local notification via standard CCTV monitors is linked to alarm systems for visual and audible notification at a local monitoring station, guards

are able to respond appropriately in a very short time. Automatic monitoring of multiple video channels provides significant security and cost benefits.

CHAPTER

4 SYSTEM CONCEPT

The IntrusionTrace analytic is an image analysis tool able to detect human intrusion in a sterile zone, i.e. a (part of a) scene where human intrusions are not allowed. Good examples of sterile zones are the surroundings of a prison, the surroundings of a nuclear plant, a military or civilian strategic site, etc. The sterile zone should be (nearly) free of obstacles such as cars, trees, etc.

IntrusionTrace analyses video from CCTV cameras to detect movement that is likely to be an intruder. The IntrusionTrace application uses advanced algorithms to maximise target detection and tracking under a wide range of environmental conditions. It therefore has a very low probability of false alarms from animals, clouds, shadows, wind, moving trees, rain, or snow.

IntrusionTrace monitors contrast changes and rate of contrast change within the defined detection areas. This information on contrast changes and rates of change is fed into a number of computational routines that analyze the changes and extract valid targets from the images whilst rejecting changes from background movement. The detected targets are further analyzed to ensure that they meet criteria based on size and speed. If the criteria are met, an alarm is generated.

What is actually considered a target will depend on your particular security requirements. In a high security environment, the maximum horizontal Field of View (FOV) must be less than for that in a medium security environment.

CHAPTER

5 SYSTEM DESIGN

The system design phase consists of three elements:

- **Preliminary information**: Gather general site information and discuss the security requirements with the customer to ensure that the IntrusionTrace application meets the customer's requirements.
- **Site survey**: Conduct a site survey to determine site requirements such as the positioning of cameras and other detectors, lighting, and existing and required communications infrastructure.
- **Equipment selection**: Conduct a comprehensive analysis to determine equipment requirements, such as camera types and lenses, level and type of illumination, and communications and control room equipment.

The system design is critical to ensure that the IntrusionTrace application performs as expected.

A well designed system can deliver exceptional performance, whereas a system that has not had a rigorous design process will not perform to expectations. IntrusionTrace provides a high level of flexibility in its configuration, but is dependent on the quality of video signals and scene content to deliver a high performance solution.

Preliminary Information

Gather site information to determine IntrusionTrace's suitability for the site. If possible, obtain a copy of the site plans to check the layout and suitability of IntrusionTrace.

Assess Site Plans

Assessing the site plans prior to visiting the site allows a quick overview, as knowledge of this is important for a good IntrusionTrace system design. If unable to obtain site plans prior to visiting the site, then once on site prepare a sketch of the site, remembering to include the immediate external environment, such as roads and location of neighboring buildings.

Discuss Requirements

During the preliminary stages, discuss the security requirements and expectations with the customer's representative. Different areas of the site may have varying security requirements and knowledge of the external environment is critical in understanding the customer's requirements and performance expectations from the system. Collect information about the customer's response requirements, such as use of local guards and/or remote monitoring.

Recommendations

If, after the preliminary investigation phase, the site is deemed suitable for IntrusionTrace and the customer's performance expectations can be met, a site survey should be conducted. The following criteria determine the site's suitability for the IntrusionTrace application:

1. Sterility of protected area
    - How well defined is the border surrounding the protected area?
    - Is the area free from general or expected activity?
    - Are there clear areas in which detection can occur?
2. Customer requirements for response (onsite or remote)
3. Customer expectations of system performance, such as false alarms or integration into third- party systems
4. Possible addition of other detection technology, e.g. PIRs.

Site Survey

Once preliminary information is collected and the site considered suitable for protection with IntrusionTrace, a site survey can be conducted. Conduct the site survey taking into account any customer tender or requirements documents to ensure that the survey and subsequent design meet the customer's specifications and requirements. The site survey draws on the preliminary information to design a complete system. Determine all necessary criteria for the system and ensure all relevant information is collected. Where clarification is required, ensure that this is received from the customer (or their representative). Appendix B contains a checklist for a site survey.

The items you need to perform a detailed site survey include:

- digital camera
- tape measure
- workbook
- site plans (accurate engineering drawings of the site).

The different stages of a site survey are described below.

Detailed Site Plan

The production of a detailed site plan annotated with key information (see Appendix C for an example) is the key element in completing a successful site survey. As a minimum, the following information must be included:

1. Location and type of existing illumination, including coverage, to determine its suitability. If necessary specify additional illumination.
2. The location of the equipment room for the installation of the RMVG with the IntrusionTrace application, to confirm cable-run lengths for cameras.
3. If remote monitoring is to be used, confirm the location and type of any existing communications infrastructure.
4. Location of trees and other vegetation that may affect detection performance, camera positioning, and field of view.
5. Type and height of fences or barriers to check where intrusion is likely to occur. Also determine if any concealment of intruders may occur, and what is visible through fences.
6. Any other permanent or semi-permanent structures not already marked on the site plan, e.g. semi-permanent location of large cable drums, which may obscure camera views.
7. Location of any nearby roads, to determine whether street lighting or car lights from any roads nearby may present a lighting problem.
8. Location and description of nearby buildings or structures to understand whether lighting may spill from adjacent properties, or shadows from industrial equipment may affect performance, e.g. a shadow from a moving crane cast across the FOV of a camera may cause nuisance alarms.
9. Location of any existing CCTV cameras or other detectors and their suitability with the IntrusionTrace application, or incorporation as a third-party detector.
10. Special requirements within protected areas, i.e. high security critical areas within the site, or special requirements due to dangerous chemicals and/or service reliability.
11. If audio is considered for offsite response, identify the location of any noisy equipment, e.g. generators, to ensure that the noise does not affect any microphones to be installed. This also relates to onsite audio broadcast equipment, i.e. speakers and horns should be appropriately located and specified with appropriate power.

Site Images

Collect a detailed set of site images covering all protected areas. The site images provide a visual reminder when assessing the site plan offsite. These also provide a reference point during installation and commissioning. Ideally the digital images should be taken under a variety of lighting conditions, i.e. dawn, daylight, dusk, and night. The most challenging lighting conditions for CCTV systems can occur at

dawn and/or dusk. It is vitally important to be aware of the variable lighting conditions under different circumstances and in different seasons. The detailed site survey must consider the likely occurrence of seasonal variations. Shedding or sprouting of new leaves on nearby trees may affect lighting conditions and camera views. Ideally there should be no trees in any camera views, however this is not always possible. Lighting and views change as foliage grows or drops, affecting nuisance alarm rates or detection probability.

The “ideal” scene is looking along a perimeter fence outdoors, without any vegetation, fluttering flags, or moving tree shadows. The following images illustrate some suitable and unsuitable perimeter and area protection scenarios for the IntrusionTrace application.

Suitable Perimeter Conditions and Area Detection Scenes

Unsuitable Perimeter Conditions and Area Detection Scenes

IntrusionTrace is used in perimeter and area protection scenarios. The key to providing a successful solution is installing IntrusionTrace into a scenario that is suited to its requirements. Essentially, the sterility of the area/perimeter to be protected is paramount. It is essential to have clear areas for target observation with minimum continuous or sporadic movement from non-target sources.

Clarify Requirements

The exact requirements for site security must also be clarified through tender documents or engineering specifications. This is vital to ensure that the system design and installation meets the customer's expectations. It is good practice to draft a commissioning schedule to further clarify the system acceptance criteria. Details of system commissioning are described in Site Commissioning.

System Hardware

Appendix D contains a checklist for system design and equipment selection.

Camera Selection and Location

The selection and location of cameras is vitally important for the successful operation of the IntrusionTrace application. The cameras are intrinsically linked with any other detectors in use and the availability of suitable lighting.

Camera and Video Signal Requirements

Using Analogue Cameras

Analogue cameras must adhere to the CCIR/PAL or RS170/NTSC standard for suitable operation with IntrusionTrace. IntrusionTrace only processes the monochrome section of the video signal. Any colour signal present neither adds nor detracts from the performance.

The following conditions must be met for an RMVG to synchronize to an incoming video signal from the camera and to provide good video motion detection:

- The sync amplitude at the video input of the RMVG must be within the range of 0.2 V to 0.4 V.
- The video amplitude (not including sync) at the video input of the RMVG must be within the range of 0.75 V to 1.0 V.

If the video level at the video input of the RMVG is low, cable compensators or line drivers should be installed at the camera end, and adjusted to boost the video signal to within the correct voltage levels. Typically, the best solution is to ensure that the correct grade of coaxial cable is installed to transmit the images over the required distance. Take into consideration impedance and capacitance qualities of the selected cable type to ensure that image degradation is minimised from the outset. The quality of the video is influenced by the cable length. Generally the shorter the cable runs between the RMVG and the camera, the better the quality of the picture. For long cable runs, cable compensators may be required.

Using IP Cameras

Check the list of supported IP Cameras for your RMVG, provided in the *Supported IP Camera List*. Only supported IP cameras that also support an analytics stream will guarantee that the IntrusionTrace application will function as described.

Camera Field of View (FOV)

To achieve high detection probability and effective nuisance alarm rejection, the field of view at the maximum detection distance should be no more than 16.7 times the target size.

For example, to detect a 1.8 m high human target, the recommended maximum field of view (FOV) at the maximum detection distance is: 16.7 x 1.8 m = 30 m (98 ft). If a larger field of view is used, then the detection probability is reduced.

In this scenario, increasing IntrusionTrace's sensitivity can only partially compensate for the reduced detection probability and may lead to an increase in the number of false alarms. It is not recommended.

Setting the correct horizontal FOV of the camera is critical for reliable detection. The maximum horizontal FOV and the required target size to be detected determine the required camera and lens configuration. The following guidelines are important:

- Ensure there is adequate detection area. The default minimum distance is 2 m (6 ft), and it is recommended that the detection area be at least this wide.
- Ensure that the horizontal FOV at the maximum detection range does not exceed the recommended maximum of 30 m (98 ft).
- The tilt of the camera should be such that the FOV does not include large areas of the sky, thereby reducing the detection area of the IntrusionTrace system.
- Ensure the FOV is clear, with minimum views of foliage and obstructions that provide cover for intruders.
- IntrusionTrace uses perspective compensation for its motion detection algorithms, hence it is important that the FOV is not obtuse, i.e. a target in the background on the left edge of the FOV must be the same size as a target on the right edge of the FOV.
- When designing cameras to look along a fence line, the majority of the horizontal FOV of the camera should be on the monitored side of the fence.

Camera Position and Lens Selection

The maximum horizontal field of view and the likely target size to be detected, determines the required camera and lens configuration. The absolute maximum horizontal field of view where detection occurs should not be more than 30 m (98 ft). It is also advised to avoid that large parts of the FOV are not used for detection. Large areas of the sky, or large unmonitored areas render the perimeter detection unreliable.

The IntrusionTrace application functions most effectively when the camera is not mounted too high. The perspective characteristics used in the detection algorithms will not function as expected when the camera is mounted too high. When looking directly down on a cat or a person, their relative sizes are quite similar. Their true sizes can be judged only when viewing at an angle. Place the camera at a height that it is out of reach of intruders. The ideal height is 4.2 m (14 ft), as this allows the detection algorithms to function and is high enough to prevent tampering with the camera.

Analysis of the site plans and information from the site survey determine the FOV of the camera to ensure coverage of all areas requiring protection. Always ensure that the maximum horizontal FOV is no greater than 30 m (98 ft), to prevent compromising detection of small targets.

The tables in Appendix E show the approximate maximum distance between the camera and the target for reliable detection, at a maximum horizontal field of view of 20 m (66 ft), 22 m (75 ft), 25 m (83 ft), and 30 m (98 ft) respectively. The approximate dead zone beneath the camera is also shown, for a camera mounted at 4.2 m (14 ft), although this will vary depending upon the final angle at which the camera is set. These figures should be used for guidance only. Other considerations, such as lighting and external environmental aspects, may dictate the use of different camera/lens combinations.

The formula for determining the distance from camera to target based upon the maximum horizontal FOV is as follows:

Distance between camera and target = (lens focal length × maximum horizontal FOV) /camera format width

Where:

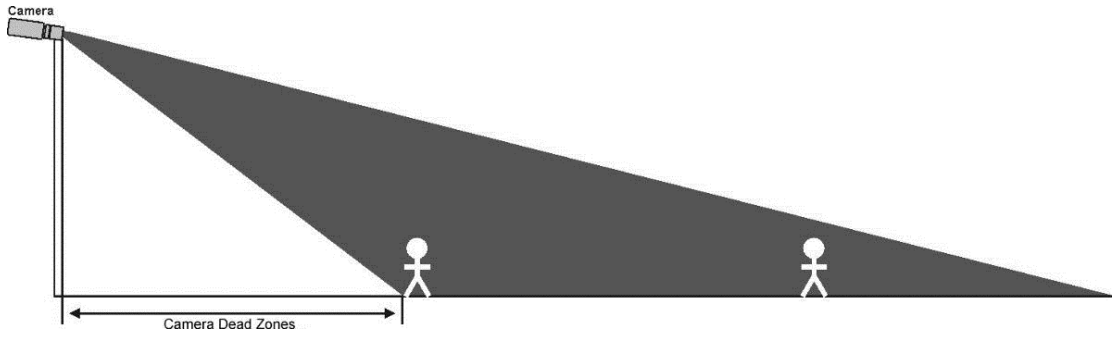
- Distance between the camera and target is in metres
- Maximum horizontal field of view is in metres
- Lens focal length is in millimetres
- Camera format is in millimetres

= 8.8 mm for a 2/3" camera; 6.4 mm for a 1/2" camera; 4.8 mm for a 1/3" camera; 3.2 mm for a 1/4" camera.

Note: *Consider using cameras with varifocal lenses to meet the lens criteria.*

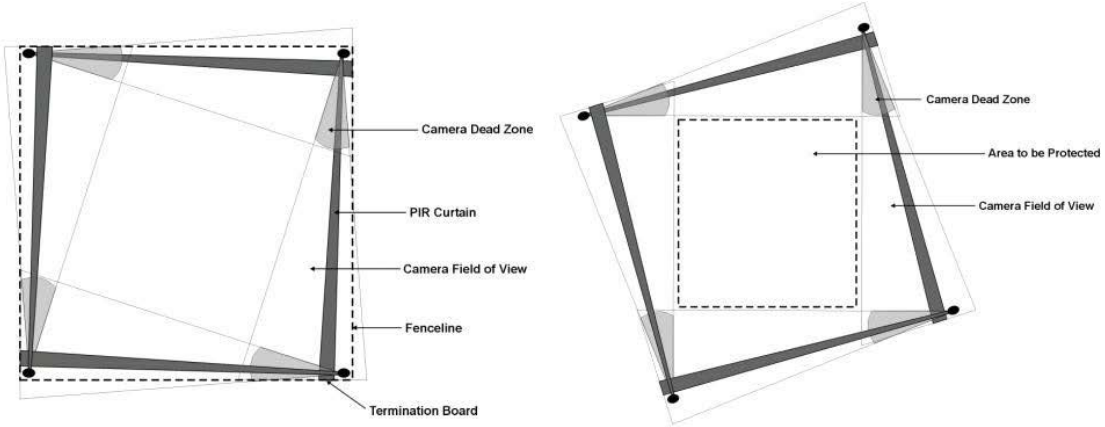
Dead Zones

The 'dead zone' is the area under the camera that the camera cannot view and should be considered during system design. The following figure shows the dead zone area.



Camera positioning should be such that the 'dead zone' of one camera is covered by another camera's field of view. The area just in front of the 'dead zone' can also be vulnerable to fast moving targets. It is a good practice to ensure that the field of

view of the camera covering the 'dead zone' includes the 'dead zone' plus an extra 10% to 15% of the area adjacent to the 'dead zone'. The following diagram shows the camera's FOV and 'dead zone' in both perimeter and area protection scenarios.



Optimal Camera Angle

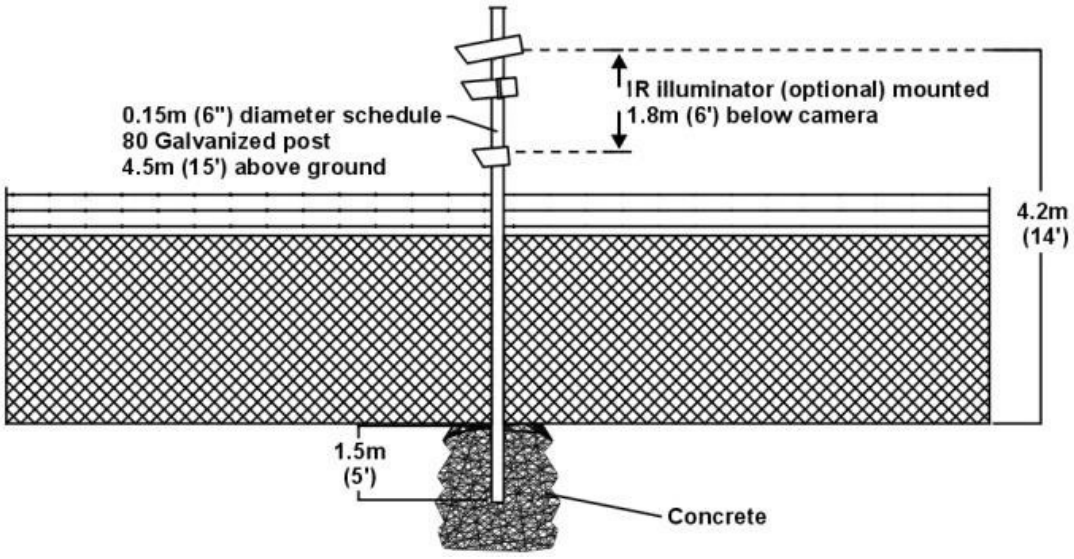
The figure above, which shows the 'dead zone' of a single camera, also shows the optimal camera angle. The target closest to the camera should have its feet at the base of the camera FOV, and the head of the target at the furthest detection distance should be just below the top of the FOV of the camera.

Normal video monitors do not show the full horizontal video available. IntrusionTrace uses all of the horizontal video for detection. Hence when aligning cameras, it is important to take this into account, and if normal monitors are used (as opposed to underscanning monitors), then mask out the extreme left and right hand edges of the image using the detection area selection capability of the IntrusionTrace application.

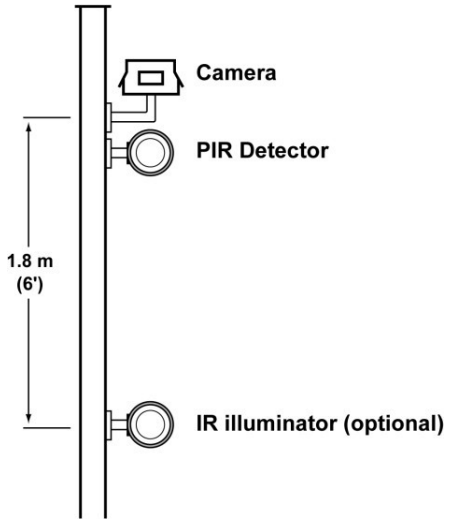
Camera Positioning and Mounting

The position and mounting of cameras is vital to ensure reliable performance from the IntrusionTrace application. The essentials when choosing a position and mount for cameras are:

- Ensure that the camera mount and pole are stable, even in windy conditions. As the lens size increases, smaller movements appear magnified and the stability of the camera mounting becomes increasingly important. Ensure that there are at least three mounting points on the selected camera housing mounting. A camera mounting used for a standard CCTV site implementation may not be suitable, as some camera movement generally does not cause distress to an operator, however the IntrusionTrace relies on steady camera images. Though the algorithms within IntrusionTrace allow for some camera shake, it is advisable to use a heavy duty mounting location or pole. Mount the camera close to the pole, and the PIR on a separate mount, also close to the pole. The following figure shows a typically recommended mounting pole for a camera/PIR combination as well as an infrared illuminator.



- The position of the cameras relative to lighting is extremely important. Do not install cameras close to lights (particularly infrared illuminators) which could attract insects, or face cameras into lights, windows, the sun, or in areas which have a large number of reflections or shadows. When the lighting is below or to the side of the camera, the recommended safe distance is 2 m (6 ft). If the lighting is directly above the camera, then insects flying up towards the light in front of the camera may cause nuisance alarms or obscure the view. If this is the case, ensure that the lighting is well above the camera, in excess of 4 m (13 ft). The previous image of the pole shows the location of an IR illuminator. The figure below shows this in greater detail.



- Do not install cameras facing at trees or plants, which may move in the wind or drop leaves (tree shadows may also move in the wind). In many circumstances this is unavoidable, but should be limited as far as possible. Use the IntrusionTrace detection area selection functionality to mask out areas with foliage.

- Do not install cameras facing into areas where there is likelihood of vehicle headlights at night. The presence of roads near sites is unavoidable, and the positioning of cameras must account for this. The placement of opaque material on fences near roads can alleviate most nuisance alarms from lighting.
- Take into consideration the position of sunrise and sunset, as well as reflections from objects in the FOV to limit any 'blinding' of the camera due to bright light.
- Do not install cameras facing into bright lights or IR illuminators.

Cable Selection

Using Analogue Cameras

Typically RG59 standard cable should be used as a minimum requirement:

- In a monochrome system, the cable length should be restricted to 250 m (800 ft) before cable compensators are installed.
- Signal degradation due to cable length has a far greater effect on colour video, where the coaxial cable should be restricted to 150 m (500 ft) before cable compensators are installed.

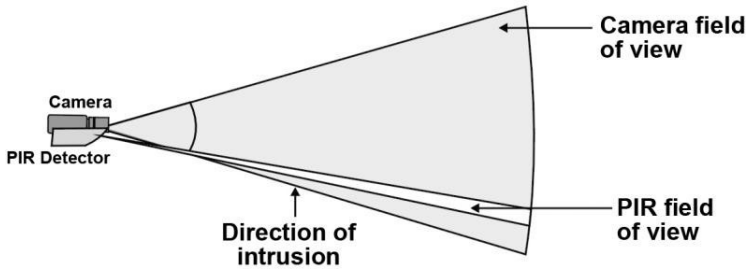
Using IP Cameras

The standard IP camera cabling via network cables (e.g. CAT5E or CAT6) should be used.

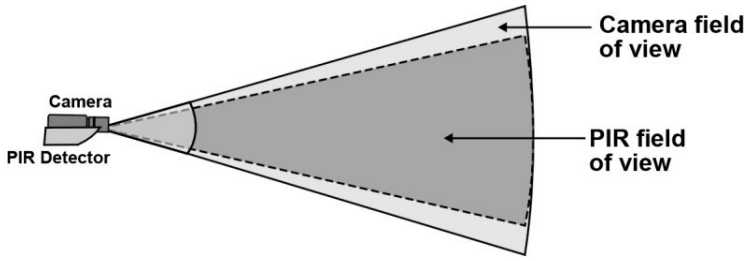
Other Detectors Selection and Location

The rationale behind using an additional detection technology is to provide a system that is not susceptible to any one possible cause for nuisance or false alarms, i.e. using complementary technologies to limit false and nuisance alarms whilst maintaining the highest detection probability. Xtralis recommends using either long-range (for perimeter protection) or wide-angle (for area protection) Passive Infrared (PIR) technology in conjunction with the IntrusionTrace application. In many instances using other detection technologies with IntrusionTrace is extremely beneficial to provide a 'double-knock' scenario. Double-knock installations using a different technology can reduce nuisance and false alarm rates to minimal levels, dramatically increasing the overall effectiveness of the system. The benefit of verifying the nature of the intrusion through video images is paramount, with the additional technology providing an extra level of security. The use of PIR detectors is a well-established and field-hardened method of providing security. The Xtralis range of PIR detectors features long-range and wide-angle detectors suitable for perimeter protection and for area protection respectively. The operable range of the detectors varies from 18 m (60 ft) for the wide angle, up to 150 m (500 ft) for the longest range PIR. Prevailing site conditions determine the effective range. The recommended maximum is 100 m (330 ft).

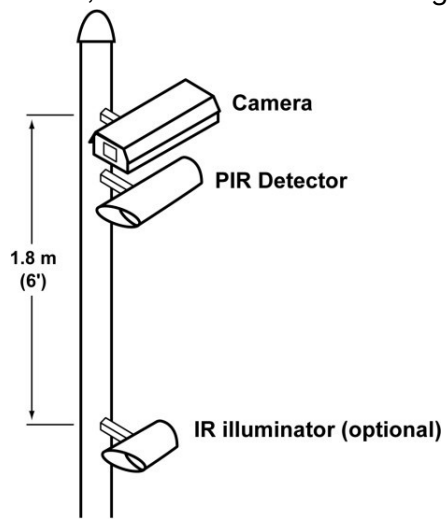
The following diagram illustrates the alignment of a long-range PIR with the camera field of view:



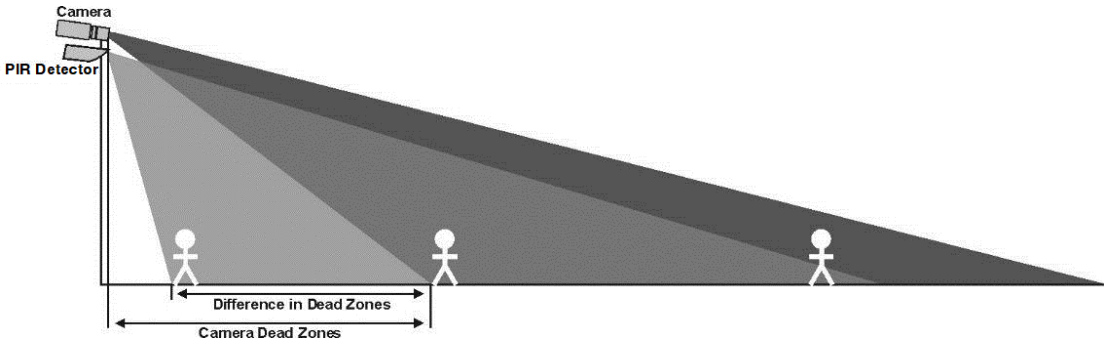
The following diagram illustrates the alignment of a wide-angle PIR with the camera field of view:



To aid aligning the camera and the PIR, it is recommended to mount the PIR as close to the camera as possible, as shown in the following diagram:



The difference in dead zones of the two technologies is an important factor to consider when the PIR/camera combination is used. The PIR may have a very steep downwards angle, whereas a camera may have a much larger dead zone, as illustrated below. This is a very important consideration as a moving target in the camera's dead zone may activate the PIR. The target will not be visible to the camera mounted with the PIR, however the target will be visible to the camera covering the first camera's dead zone. If the PIR/camera dead zones require matching, carefully check the comparative dead zones to ensure that this can be achieved. Also consider mounting the PIR and camera on separate poles.

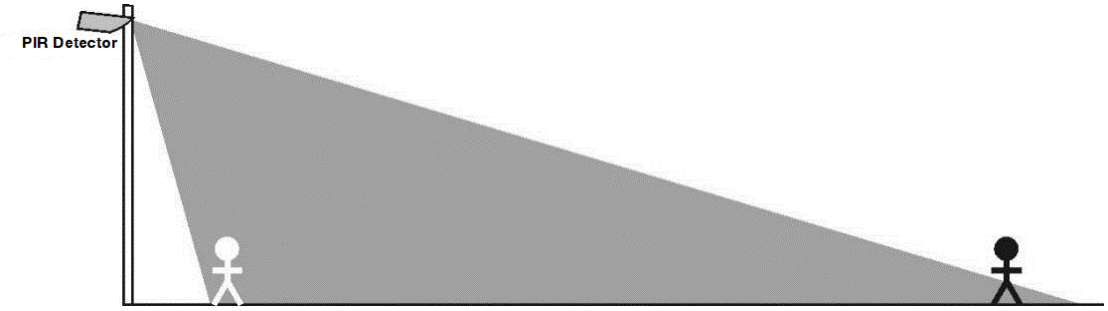


The installation and use of any detection technology must consider:

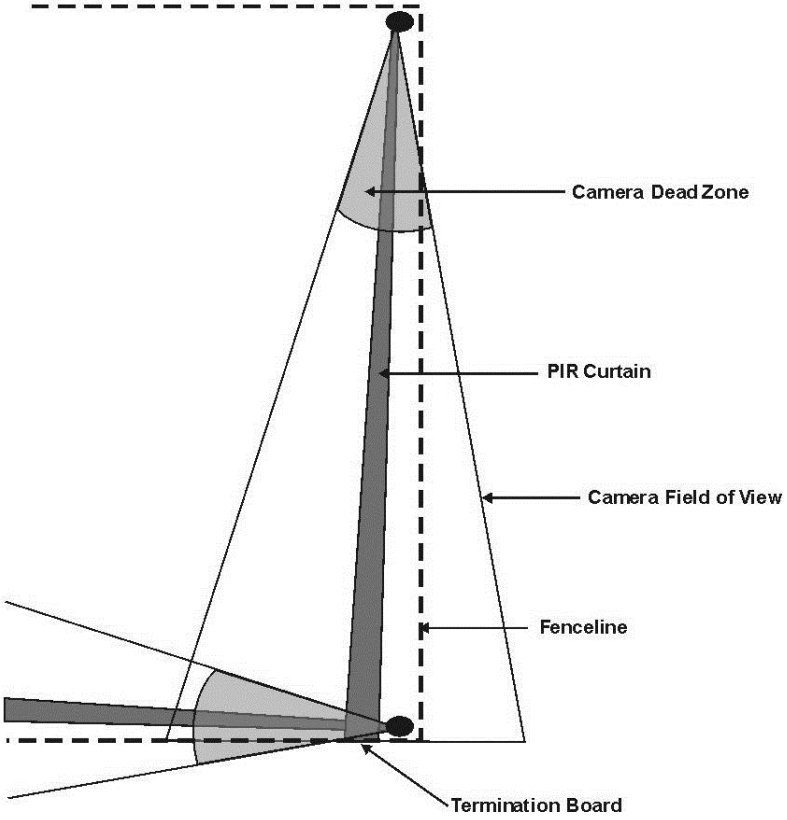
- The angle of elevation and the horizontal alignment with the camera is critical in providing a high degree of performance.
- It is recommended to keep foliage trimmed and grass cut for a clear PIR and camera FOV.
- Termination barriers are important so that targets past the protected area are not detected.
- Minimise reflective material in the FOV to ensure reflections from sunlight do not affect the PIR.
- Minimise facing PIRs in the direction of sunrise or sunset.
- PIRs also require a maintenance program to clean the lenses and to regularly check performance and alignment.

PIR Alignment

For good PIR performance ensure PIR and camera alignment match. The following figure shows the optimal PIR placement angle, where the top of the curtain is approximately 1 m (3 ft) high at the maximum detection range.



When using a long-range PIR next to a fence line, it is important that the PIR curtain is aligned approximately 0.5 m (2 ft) inside the fence line, as shown in the next figure.

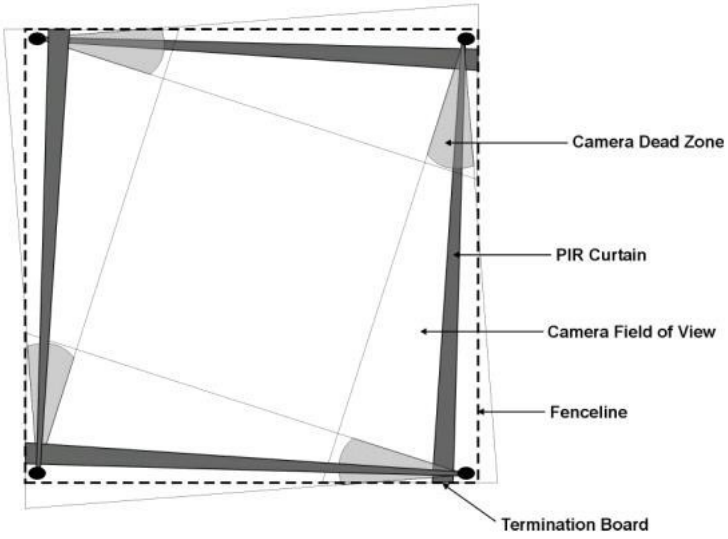


PIR Termination

If PIRs are being used on the site, then their detection curtain must be terminated suitably, in a similar fashion to blocking out lights from nearby roads. Referring to the figure under the PIR alignment section (see page 23), the detection curtain should be terminated by a suitable material at the boundary of detection. Suitable materials include privacy mesh that can be woven into chain link fences, plywood, heavy landscaping cloth, or plastic facades. The use of steel is not recommended, as it may heat to a temperature that a PIR may incorrectly detect as a human body.

Camera/PIR Alignment

The camera alignment relative to the boundary and other cameras is paramount in ensuring that there are no 'blind spots' on the site. Align each camera to cover the dead zone of the next camera, and to adequately cover the area under protection. If, due to practical limitations, external areas not requiring detection are included in the camera view, use the detection area selection feature in IntrusionTrace configuration to mask out such areas. The following figure shows camera alignment and PIR alignment around the perimeter of a facility.



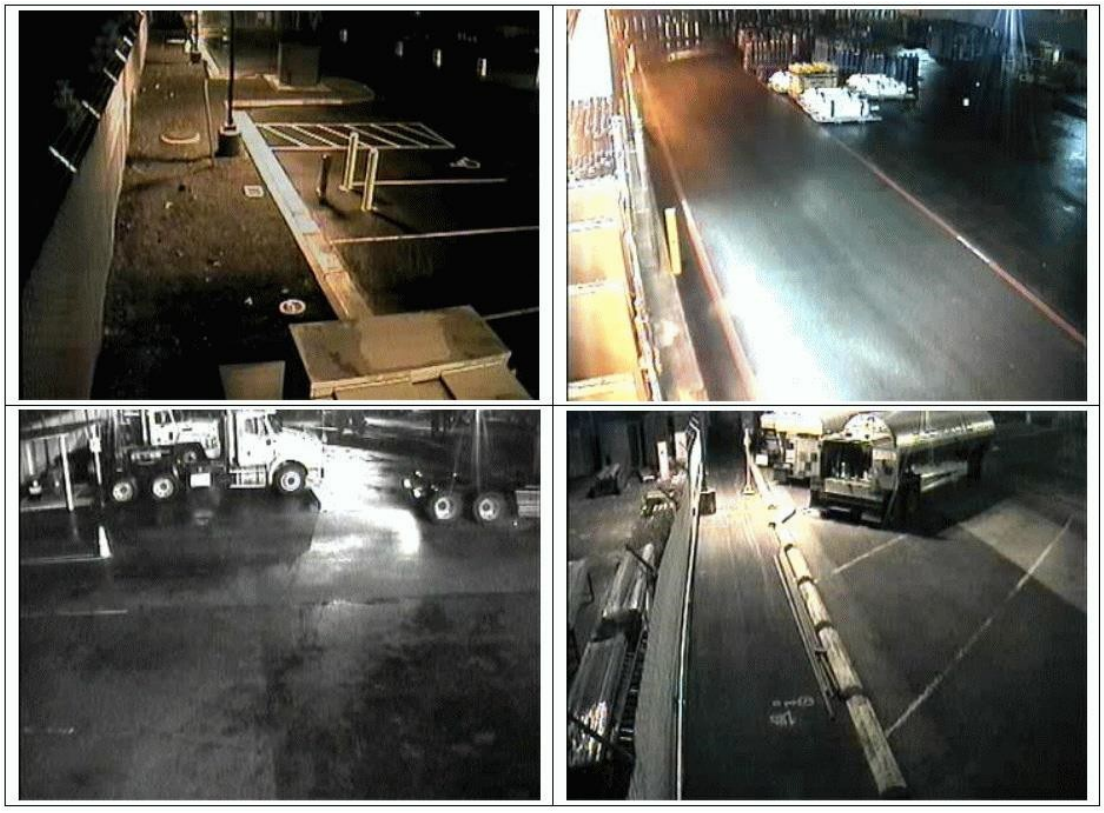
Illumination Requirements

Ideally, the illumination around the site should be even, with no major contrast changes caused by shadows at all times of the day and night. Typically, to provide a more even illumination, it is better to use high levels of ambient lighting throughout the field of view of the camera rather than subjective lighting systems. To ensure continuous monitoring by IntrusionTrace, the lighting (or illuminators) should be on at all times during hours of darkness (typically photocell controlled).

Switching illuminators on at the point of alarm in order to deter intruders is not effective because if illumination levels are too low, IntrusionTrace may not detect the intrusion. If the scene contrast is poor, and no additional lighting can be installed, then the contrast can be increased by adding stripes to walls and pathways, by painting the background surfaces a light color or by laying strips of different colors of gravel. Determining the required lux level from a mathematical calculation can be difficult. There are references available that describe this process in detail. Check these references, or other sources for a mathematical approach in determining the lux level required at a site to provide adequate illumination for the cameras selected. Lux meters are available for checking the illumination level at a site and to relate the measurements to camera specifications. A good rule of thumb is, if the target is clearly visible to the human eye at the maximum range under the worst lighting conditions, then a camera can detect it.

The following are some key considerations in determining the best illumination method:

- The requirements will dictate if IR illuminators or visible lighting is used. The cameras used with IR illuminators must be either B&W or day/night cameras capable of automatically switching between color/B&W depending on the conditions. Visible lighting must be used for color cameras. The level of lighting required is higher for colour cameras as these have less sensitivity compared to B&W cameras.
- The sensitivity of the cameras determines the required level of illumination. When visible illumination is used, the lighting should be sufficient for the human eye to see targets at the maximum detection range. When using IR illumination, verify the intensity by viewing the camera output on a monitor.
- It is important to ensure that areas where lighting casts shadows do not provide dark areas for intruders to utilize.
- Illuminators (visible or IR) should not be positioned to face directly into a camera.
- Typically, the best type of visible lighting is closest to normal daylight, i.e. a white light source rather than a colored light source such as sodium vapor.



Equipment Room

The equipment room for mounting the RMVG equipment should meet the following requirements:

Environmental Requirements

The equipment room should meet the following environmental specification:

- Temperature: 5–40 °C (41–104 °F)
- Humidity: 20–93% non-condensing.

Power Supply

Depending upon security requirements, consider using a backup power supply (such as a UPS). To ensure total system reliability in the event of power failure, a backup supply would also need to provide power for all the cameras and other detectors, as well as any communications equipment. See the manuals for the respective equipment for their power consumption details.

Access Requirements

Access to the equipment room should be limited to authorised personnel. An access control system may be used to limit access to the equipment room.

Equipment Mounting

If the RMVG is mounted in a 19" racking system, allow spacing equivalent to 1U between different equipment in the racking to ensure proper cooling. Consider providing cooling within the rack if the rack has a significant amount of equipment.

Monitoring Equipment

An IntrusionTrace application may be remotely monitored via an Xtralis or a third-party Central Monitoring Station (CMS) equipment management platform.

For remote monitoring, suitable communications infrastructure must be provided. There is a range of communications media choices available for use, such as PSTN, ISDN, ADSL, GPRS, 3G, 4G, and Ethernet. The type of communication link depends upon a number of criteria:

1. Existing infrastructure: To provide a cost-effective solution, consider using any existing communications infrastructure at the site, subject to it meeting required bandwidth and other operational requirements.
2. Backup communications: Under some circumstances, a secondary communication link may be required if the primary method is negated (redundancy).

3. Availability: Consider the availability of different telecommunications options, as not all telecommunication solutions will be provided by a single provider, or site requirements may exclude certain types of communications.
4. Installation and operational cost: The installation and operational cost are a major factor in deciding the type of communications infrastructure selected. The cost is generally linked to the bandwidth provided on the link.
5. Bandwidth requirements: The expectation of bandwidth, which ultimately drives how quickly video information can be transmitted, is extremely important to ascertain. Links with throughput of 33.6 kbps or higher (a minimum of 256 kbps is recommended) are available. Xtralis video transmitters are optimized for operation over low-bandwidth links, however they also provide outstanding operation over higher bandwidth links.

CHAPTER

6 SYSTEM INSTALLATION

Install the IntrusionTrace application and associated hardware in accordance with appropriate CCTV installation practices. Ensure adherence to any local, legal or mandatory requirements for electrical or telecommunications infrastructure.

Appendix I contains a flowchart providing an overall view of the installation and commissioning process. It can be used as a guide for the installation and commissioning sequence of events.

Camera Installation

Alignment

Confirming the FOV of the camera is very important. The initial design must ensure that the perimeter (or area) is completely protected and no dead zones are present. Adherence to the design during installation ensures there will be no dead zones or blind spots in the protected area.

Placing traffic cones or markers at the edges of the expected detection areas (foreground and background) provides a mechanism to initially align the camera and ensure that the FOV is as per requirement. Alternatively have one person watch a monitor and direct another (use a walkie-talkie) to walk the site. Last but not least, use the Xtralis iPhone/ iPad application, iTrace, over 3G communication to achieve “one-person” camera alignment.

Installation Tips

When installing cameras in camera housings, the following tips will prevent some nuisance alarms.

- Apply insect-repellent material, such as pest control strips or surface spray, to reduce any nuisance alarms caused by insects or spiders in or near camera housings.

- Place a bead of silicone across the top of the shield or housing near the front. This prevents that water droplets fall in front of the camera off the front of the sun or rain shield of the housing. When water hits the bead, it diverts to the side and does not collect along the front of the housing.
- Rain or sun shields can catch the wind, causing significant camera shake. To restrict camera movement, appropriately increase the strength of the fixing hardware as the size of the shield increases.

Interference Caused by High Voltage or Ground Loops

Take care to preserve the signal integrity. There is significant potential for interference in some installations, particularly on sites with high-voltage infrastructure, such as electricity substations. High 'ground loop' currents are produced between equipment earthed at different points around the site. Depending on the level and type of interference, ground loop currents may cause nuisance alarms or a reduced detection rate, if they cause interference on the video signal (i.e. the picture displayed on the monitor) or data corruption on IP connections.

Furthermore, high voltages and currents that may be present due to incorrect earthing, can damage equipment.

During the design stage, carefully consider the likelihood of interference or damage from high voltage or ground loops. Factor counter measures into the design, such as floating earths, and isolation transformers on video signals.

Installation Adjacent to Roads

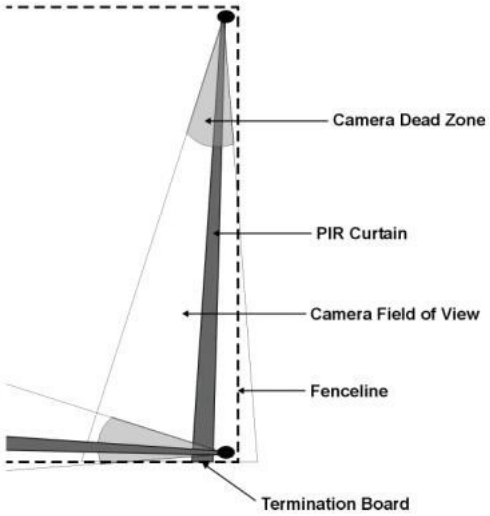
Headlights sweeping across the area under surveillance have the potential to cause nuisance alarms. If the area is near a road and has the likelihood of headlights sweeping over it, consider some sort of light barrier to ensure the headlights do not cause nuisance alarms. The options for light barriers include solid panels such as plastic or metal facades placed on fences next to the road, high opacity shades or greenhouse/landscaping cloth, or privacy mesh interwoven on chain link fences.

PIR Installation

Aligning the PIR with the camera is critical for good performance. There are a number of ways of checking PIR alignment.

- A slot in the top of some of the Xtralis range of PIRs can be used as a simple method to align the PIR. Looking through a drinking straw in the slot, or resting a laser pointer in the slot can help with alignment.
- Xtralis offers an alignment telescope for aligning PIRs across the full range.
- A cordless walk tester (CT 45) is available. During a walk test it indicates a detector alarm with a beeper and an LED.

- It is also possible to use the Xtralis iPIR (iPhone/iPad application) walk test, which is a one- person walk test. Please consult the iPIR user manual for more information.
- In addition, a tester and software available for each type of Xtralis PIR provides a very accurate method of aligning the PIR detector. The tester provides an output showing the IR activity that the PIR is sensing. This requires two people, where one acts as a target while the other adjusts the alignment of the PIR to cover the required detection area.



It is important that the PIR curtain is aligned approximately 0.5 m (2 ft) inside the fence when a long-range PIR is used next to a fence line (the previous figure illustrates this). The PIR can be aligned using previously described methods. Confirm correct alignment, with a walk test performed immediately adjacent to the fence, ensuring that detection does not occur in the 0.5 m (2 ft) area directly next to the fence.

It is important to ensure that the extents of the PIR detection are within the FOV of the camera, i.e. if a wide-angle type PIR is used, the camera FOV must overlap the PIR detection area. To confirm this, the alarm output status (or the test output using the PIR tester software) of the PIR should be monitored as a person walk tests the site. Ensure the person remains within the FOV of the relevant camera.

Instrument Racks and Cabling

There are a number of standard procedures that should be followed while installing any electrical equipment:

- Ensure that all local safety regulations regarding installation of electrical equipment are followed.
- Route all cables neatly and hold them in place using routing trays, channels, or ties.
- Label all cables for future reference, and mark the identifiers on cabling diagrams or plans.

- Allocate adequate space between equipment in racks to provide ventilation.

Once all equipment has been installed and is operating in the rack, monitor the temperature in the rack to check that the equipment is operating within specified limits (operating range 0–40 °C).

Even though equipment may be operating within specified limits, reducing the temperature will increase the operable life of all equipment in the system.

CHAPTER

7 SITE COMMISSIONING

The commissioning phase consists of the following steps:

- IntrusionTrace configuration
- Detection tests
- Soak tests
- Monitoring tests.

Appendix F contains a commissioning checklist for each IntrusionTrace channel.

IntrusionTrace Configuration

The first element of Site Commissioning is to configure the IntrusionTrace application in the XO software that runs on your RMVG. See the IntrusionTrace Technical Manual for instructions.

Performance Assessment

Detection Tests

IntrusionTrace, as a detection system, should initially be configured to ensure detection occurs effectively, and then corrective action can occur to limit any nuisance alarms. Whilst performing the detection tests, it is important to ensure that the tests are adequately documented and described for proper on-going maintenance. A subset of the tests should be performed on a regular basis to confirm correct operation. The detection tests should also be annotated on a site plan to highlight the areas where the tests are performed. See Site Maintenance on page 37 for a description of the necessary maintenance procedures.

Appendix G contains a table for documenting the detection tests performed and their outcome. For each detection area, the following should be performed:

- Check that the detection area covered by each camera connected to IntrusionTrace matches the design, and that the detection areas programmed for IntrusionTrace are correctly aligned within the field of view of the camera.
- Check that any PIR detector is aligned as initially designed. This may require using the PIR tester and software to ensure that the angle of the tilt is correct, i.e. approximately 1 m (3 ft) high at the maximum detection distance, as well as the horizontal alignment of the PIR, using another person as an IR target when required.
- Determine the level of intrusion to be detected, such as a casual opportunistic intruder, or a well planned and executed covert intrusion. Design and document tests based around the security level and scene content. Factors that may vary include the speed of target, the size of the target and the location in the scene. The following describes how to perform the tests, and is suitable for both the PIR and IntrusionTrace detection testing:
    - Tests should be performed at three separate locations: the foreground FOV, the middle of the scene, and the maximum FOV.
    - The target should move to the point where intrusion would expect to start. If this is within the detection area, then once the target has moved to the start point, the target should stay motionless for one minute to allow IntrusionTrace to settle.
    - The target should then perform the detection test. As a minimum, a walk test and a run test should be performed at each distance. More tests can be performed as required in each individual scene, but most importantly all possible intrusion points must be tested.
    - For size discrimination testing, you can use a small target, such as a basketball rolled across the scene, to check that small targets are or are not being detected by IntrusionTrace as required.
- Execute tests in each detection area based on the type of intrusion, and where possible differing environmental conditions, e.g. day/night/dusk/dawn. Ensure that the alarm activation is reported as expected at the IntrusionTrace system, and also that any third-party system triggered from the IntrusionTrace system receives an alarm notification.
- If the system is installed in a high-security installation, then also perform tests with different types of camouflaged clothing.

Soak Tests

Once the system has been installed and the detection tests performed, then the system must be monitored for its performance in relation to the ambient environment. Changes in environmental conditions or just routine actions can produce nuisance alarms. The system should be monitored on a daily basis prior to going 'live' to highlight issues of concern, and then adjust the IntrusionTrace and RMVG parameters as required. Every time detection parameters are modified, detection tests should be performed again to ensure the detection performance has not

been compromised. Once the performance of the soak tests has reached an acceptable level, and the detection performance is as required, the system can go 'live'.

System Tests

The integration and performance of IntrusionTrace as a component of a larger system must be verified to ensure the complete system behaves as required and expected. There are a number of areas to check:

- For remote monitoring, ensure that generated alarms are successfully transmitted to the Central Monitoring Station (CMS).
- If any functions are being used within IntrusionTrace, test that the behaviour meets expectation and the system generates alarms when it is armed.
- If the IntrusionTrace application is integrated into a larger matrix or CCTV system, ensure that any inputs/outputs to/from the larger CCTV system function as expected.

Recording System Configuration

Once you have configured all the IntrusionTrace channels, you must save the configuration of your RMVG. Once the complete configuration has been saved, you can reload it in the case of a system malfunction, or use it to configure another RMVG.

For details on storing system configurations, see the ADPRO XO Client Software User Manual.

CHAPTER

8 SITE MAINTENANCE

This section covers the following five areas of system maintenance and management:

- routine maintenance
- routine site maintenance
- routine equipment maintenance
- routine detection tests
- maintenance to regulatory requirements.

Routine Maintenance

On many sites, IntrusionTrace will be used in conjunction with other detection technologies. The respective maintenance and testing procedures for the other products should be used in conjunction with this information to ensure overall site security is maintained at the required level. Maintenance of the Xtralis PIR detectors is also covered in this section.

To perform maintenance in a repeatable and consistent manner, it is suggested that a table of tests and checks to be carried out in each inspection/maintenance cycle be drawn up, which should have been done as part of the commissioning phase. This will ensure that the system is tested in a similar fashion each time, particularly if sufficient detail is provided for each test.

These tables should include the following information for each camera, PIR, and/or detection area:

- date/time/person conducting tests
- description of test or maintenance to be performed
- results of test or maintenance performed
- any maintenance or site issue that needs to be addressed
- date/time for next maintenance/test.

In addition, copies of site plans annotated showing camera locations as well as location of any other detector technologies should be used to document detection areas and the path of detection tests.

Appendix H contains examples of tables for tracking maintenance procedures and outcomes.

Routine Site Maintenance

Regular site inspections, preferably on a monthly basis, that check the listed site conditions should occur as a minimum. These conditions can impact on the performance of IntrusionTrace or on the level of security provided, but they are by no means an exhaustive list. If a very significant change occurs, then a site re-evaluation may be required to ensure optimum performance.

Foliage can impact IntrusionTrace in a number of ways, and must be kept controlled so that the following scenarios do not occur:

- masking areas where detection should occur
- nuisance alarms where foliage has grown and has become visible in the field of view
- blocking lighting of areas during the night
- removal of foliage causing changed lighting conditions, such as removal of shrubs along a fence line allowing multiple vehicle headlights to sweep across a camera's field of view
- moving shadows from wind-blown foliage in the field of view of the camera causing nuisance alarms.

Lighting is an essential element of the performance of IntrusionTrace. Lighting should be checked to ensure that all areas are adequately lit at all times, and in particular structures or foliage are not blocking lights.

There are other environmental factors that can have an impact on the performance of IntrusionTrace or the level of security provided. These include:

- Changes to adjacent premises, such as the erection of temporary or permanent structures, can alter lighting, provide a path for intruders to access the site, or change activity levels expected around the site.
- Changes within the premises, such as the erection of temporary or permanent structures, facilities maintenance activities, or new operating procedures.

Routine Equipment Maintenance

There are a number of regular maintenance tasks that should be performed monthly to ensure that the IntrusionTrace application continues to perform as expected.

- General inspection of all cabling, conduit, connectors, glands, and housings to ensure that they are all in good working order and not suffering deterioration.
- General inspection of the RMVG chassis, ensuring that it is dust free and the fan mounted on the power supply is not obstructed in any way.
- If the RMVG is equipped with fan filters, check whether they require cleaning or replacing.
- Regular cleaning of camera housing windows with lens cleaner and a lint-free cloth to ensure that the performance of the system is not prejudiced by poor image quality.
- Check that any heaters, blowers, washers, or wipers installed on camera housings are operating as expected.
- Regular cleaning of the window on any Xtralis PIR. Clean the window with lens cleaner and a lint-free cloth. If the window is showing signs of deterioration or peeling, please contact your Xtralis supplier for replacement details.
- Where insects or spiders can be a problem in or near camera housings, apply insect-repellent material, such as pest control strips or surface spray, to reduce any nuisance alarms.

Routine Detection Tests

Regular site detection tests should be performed at least once per month, but preferably weekly, to check whether the IntrusionTrace application detects unauthorised intrusions. The detection tests used as part of the maintenance program should follow the tests performed as part of the initial installation and commissioning. The descriptions of these tests should have been documented in tables.

For each detection area, the following should be performed:

- Check that the detection area covered by each camera connected to IntrusionTrace matches the initial design and commissioning, and that the detection areas programmed for IntrusionTrace are still aligned within the field of view of the camera.
- Check that any PIR detector is still aligned as initially designed and commissioned.
- Execute a test in each detection area based on the type of intrusion, such as a walking target for opportunistic intruder. Ensure that the alarm activation is reported as expected at the IntrusionTrace application, and also that any third-party system triggered from the IntrusionTrace application receives an alarm notification.
- Repeat the tests under the different lighting conditions, e.g. day or night. Conducting tests at dawn/dusk should also be considered as the lighting conditions at these times can provide the most challenging environment for detection.

It is also important to check that detection is not occurring in areas where detection should not occur. In each detection area, check that detection does not occur in areas that should be masked out, or should not be aligned with Xtralis PIRs or other detection technology. With the PIRs in particular, check that detection does not occur past the defined maximum detection point.

Maintenance to Regulatory Requirements

Regular maintenance and testing of security systems may be mandated by internal organisational requirements, but in some industries, specifically high-risk industries such as nuclear power generation, there may be statutory requirements for maintenance and testing. Please check with the appropriate government agencies to determine whether any such criteria apply in your industry area.

APPENDIX

A FALSE AND NUISANCE ALARMS

Ultimately no security system is perfect, generally through generating false or nuisance alarms. As a security system is made more sensitive to detecting intrusions, the false and nuisance alarm rate can increase. False or nuisance activations limit the effectiveness of a security system, as operators become used to receiving alarms that are not valid, and may miss valid alarms assuming that the alarm is just another false or nuisance alarm.

- A **false alarm** can be defined as an alarm activation that is reported, but the cause of which cannot be identified.
- A **nuisance alarm** can be defined as an alarm activation that is reported, but the cause of the alarm can be verified and no further response is required.

The goal in designing a security system is to provide the highest rate of successful detection, traded off against the lowest rate of false and nuisance alarms. Using an application such as IntrusionTrace allows for removing nuisance alarms, as the alarm must be verified remotely at a monitoring centre before dispatching personnel.

The use of a second detection technology/device (e.g. PIR, microwave detector, or fence sensor) may also be useful in minimising false alarms. The second device may be 'ANDed' with IntrusionTrace to provide double-knock alarm generation.

In addition, a well-designed and correctly installed system can limit the generation of false alarms significantly. The capability to reduce the impact of false/nuisance alarms greatly enhances the utility and suitability of the IntrusionTrace application to a number of scenarios.

APPENDIX

B SITE SURVEY CHECKLIST

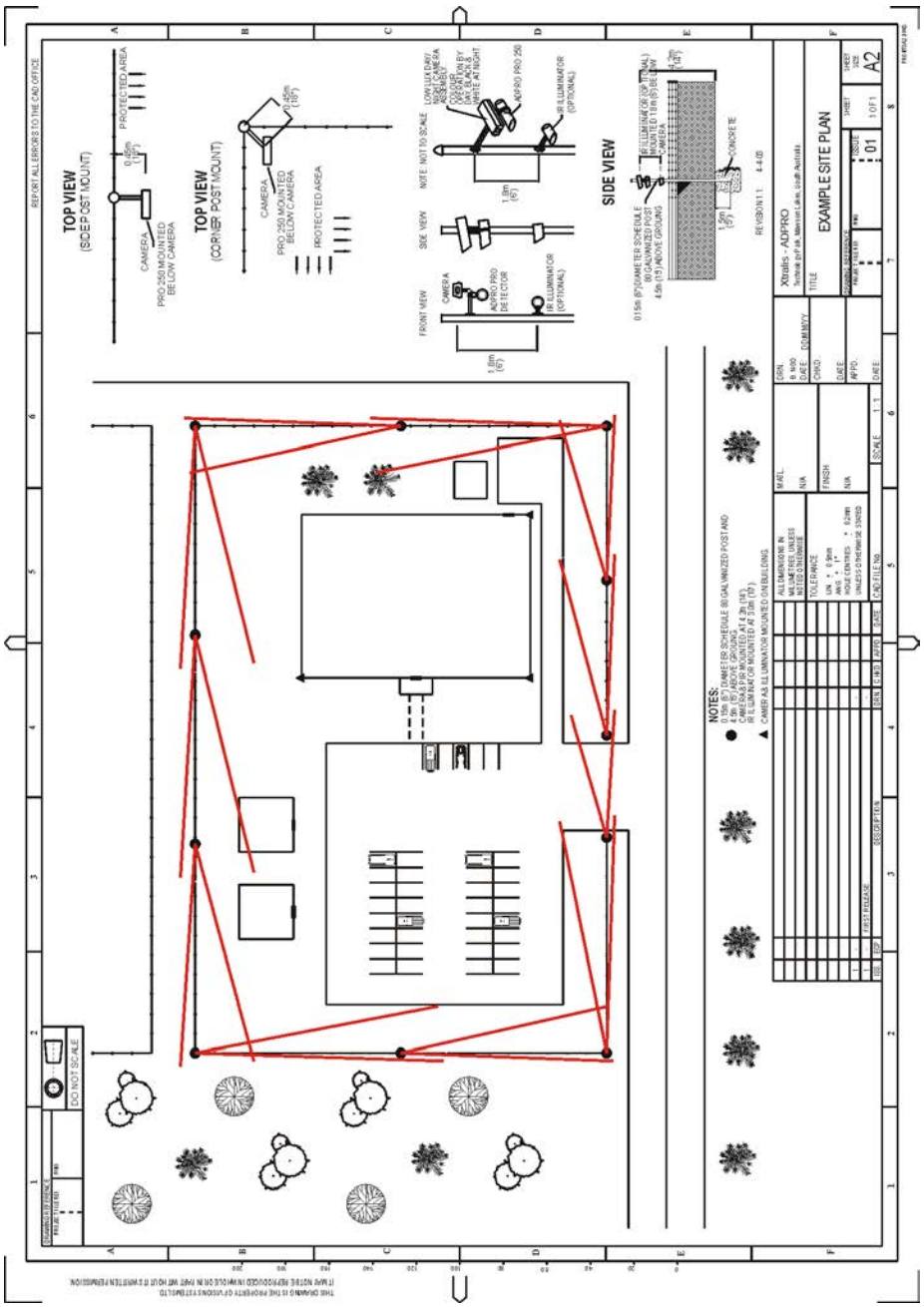
Company: **Date:**

Location: **Surveyed by:**

Site Plan Annotation	Checked
Location of lighting	
Location of equipment room	
Communications infrastructure identified	
Trees identified and marked	
Location of fences and barriers	
Location of nearby roads	
Location of adjacent structures	
Location of existing CCTV systems or other detectors	
Location of all structures	
Other Requirements	
Site images acquired	
Clarification of customer and security expectation	
Clarification of any special security requirements	
Location of noisy equipment (only if using audio)	

APPENDIX

C EXAMPLE SITE PLAN



APPENDIX

D EQUIPMENT CHECKLIST

Company: **Date:**

Location: **Designed by:**

Channel No.	Camera selected	Lens selected	Field of view OK	Lighting OK	Other detectors	Camera mounting	Cabling distance

Any special requirements:

APPENDIX

E CAMERA/LENS SELECTION

Horizontal FOV – 20 Metres (66 Feet)

Lens focal length (mm)	1/4" camera format				1/3" camera format				1/2" camera format			
	Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)	
4.8	30	98	6	19	20	65	3	10	14	48	2	5
6.0	37	123	8	25	25	81	4	15	18	60	3	9
8.0	50	164	10	35	33	109	7	22	25	81	4	15
12.0	75	247	16	53	50	164	10	35	37	123	8	25
16.0	NR	NR	NR	NR	67	220	14	47	50	164	10	35
25.0	NR	NR	NR	NR	NR	NR	NR	NR	78	257	17	55

Horizontal FOV – 22 Metres (75 Feet)

Lens focal length (mm)	1/4" camera format				1/3" camera format				1/2" camera format			
	Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)	
4.8	33	108	6	20	22	71	3	11	16	53	2	6
6.0	41	135	8	26	27	90	5	15	20	67	3	10
8.0	55	181	11	35	36	120	7	22	27	90	5	15
12.0	NR	NR	NR	NR	55	181	11	35	41	135	8	26
16.0	NR	NR	NR	NR	73	242	15	48	55	181	11	35
25.0	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR

Horizontal FOV – 25 Metres (83 Feet)

Lens focal length (mm)	1/4" camera format				1/3" camera format				1/2" camera format			
	Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)	
4.8	37	123	6	20	25	81	3	11	18	60	2	6
6.0	47	154	8	26	31	102	5	16	23	76	3	10
8.0	62	206	11	36	41	137	7	23	31	102	5	16
12.0	NR	NR	NR	NR	62	206	11	36	47	154	8	26
16.0	NR	NR	NR	NR	NR	NR	NR	NR	62	206	11	36
25.0	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR

Horizontal FOV – 30 Metres (98 Feet)

Lens focal length (mm)	1/4" camera format				1/3" camera format				1/2" camera format			
	Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)		Max. distance (metres/feet)		Dead zone (metres/feet)	
4.8	45	148	6	21	30	98	4	12	22	73	2	7
6.0	56	185	8	27	37	123	5	17	28	92	3	11
8.0	75	247	11	38	50	164	7	24	37	123	5	17
12.0	NR	NR	NR	NR	75	247	11	38	56	185	8	27
16.0	NR	NR	NR	NR	NR	NR	NR	NR	75	247	11	38
25.0	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR

Note: *Detection ranges with NR in the table are Not Recommended, as the longer focal length lenses tend to amplify the effects of camera movement in the image, which may lead to false alarms. Camera mounting height = 4.2 m (14 ft).*

APPENDIX

F COMMISSIONING CHECKLIST

Company: **Date:**

Location: **Commissioned by:**

Channel No.	Detection Test	Detection Test Documented	Soak Test	Parameters Recorded
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

APPENDIX

G SITE DETECTION TESTS

Caution: Perform the detection tests at least twice: once during the day, and once at night.

Company: **Date:**

Location: **Tested by:**

Detection Test Description

Detection Area (Camera Name and No.)	Test Number	Test Conditions (day/night/dawn/dusk)	Test Description

Detection Test Performance

Detection Area (Camera Name and No.)	Test Number	Test Due	Test Performed	Signed	Detection Pass/Fail

APPENDIX

H SITE MAINTENANCE TABLES

Company: **Date:**

Location: **Tested by:**

Camera Maintenance Table

Camera Name and Number					
Maintenance Due					
Maintenance Performed					
Signed					
Cleaned Window					
Housing Condition					
Cable Condition					
Heater or Blower functioning					
Correct Alignment					

Company: **Date:**

Location: **Tested by:**

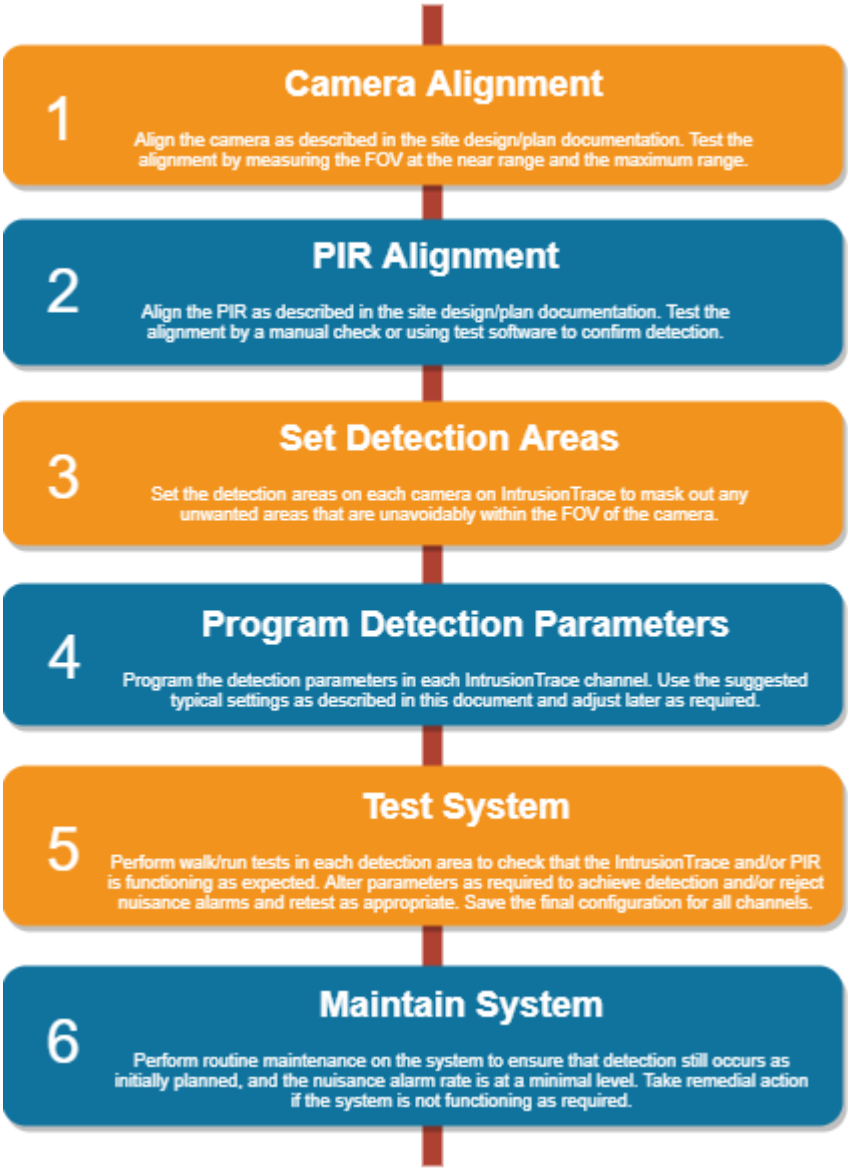
PIR Maintenance Table

PIR Location					
Maintenance Due					
Maintenance Performed					
Signed					
Cleaned Window					
Window Condition					
Cable Condition					
Correct Alignment					

APPENDIX

I INSTALLATION QUICK REFERENCE

The quick reference diagram for installing an IntrusionTrace application:



APPENDIX

J DOS AND DON'TS

Do	Don't
Walk test at day/dusk/night	Install cameras looking into lights/IR illuminators
Trim foliage regularly	Change parameters without testing the system
Use PIR terminations barriers	Use a FOV of greater than 30 m (98 ft)
Check alignment of cameras	
Check alignment of PIRs	
Regularly clean camera windows/lens	
Regularly clean PIR windows	
Route cables neatly	
Spend time performing a thorough survey	
Use barriers to prevent light spillage from roads	
Account for dead zones in site layout and camera/lens selection	
Check target sizes at the foreground and background	

www.security.honeywell.com