The Boundaries of Security

Global Trends in Perimeter Security

US$300

FFT Future Fibre Technologies™
Light years ahead in sensing and security

PREFACE

This document has been written to help provide security consultants, managers and specialists with a background into the popular perimeter intrusion detection system sensor technologies; their capabilities, limitations, and some basic installation information. It covers the most commonly available sensor technologies with a brief description, the fundamental operating principles, typical applications, strengths, weaknesses, as well as possible causes of nuisance alarms and methods of defeat.

This document does not include information on high level security management systems or operator interfaces. Nor is it intended to provide a complete list of all sensor suppliers or equipment models ever made – just those most commonly available today.

Perimeter intrusion detection sensors, like all technologies are constantly evolving. New and improved equipment is continually being developed around the world and introduced into the marketplace, but rarely do the fundamental detection principles and applications change.

All perimeter intrusion detection systems are based on the same core principle of establishing a steady background state, then continually monitoring it to detect any change to this background state, either above or below a pre-determined threshold, indicating an intrusion event is taking place.

The bulk of intrusion detection system development these days appears to be on reducing the number of nuisance alarms generated – that is, where an alarm condition takes place, but without an actual intrusion occurring. This is typically caused by environmental conditions such as wind, rain, passing traffic, lightning etc. Ongoing nuisance alarms are both inconvenient and expensive to respond to, and will eventually erode all confidence security staff have in the effectiveness and value of the intrusion detection system installed.

In the past, typical techniques employed to control nuisance caused alarms usually involved reducing the sensitivity of the entire detection system during times of high environmental noise. Unfortunately the trade-off for this was reduced sensitivity to intrusions and therefore a reduced probability of detection during adverse weather conditions.

Today we are seeing techniques such as intelligent learning algorithms, neural networks and advanced multi-parameter signal processing employed to dramatically improve the recognition of real intrusion events versus nuisance alarms. This allows systems to minimise nuisance alarms without trading off the sensitivity or probability of detection to a real intrusion event.

Only 2 to 3 years ago these advances were confined to primarily the military and aerospace industries – now they are emerging in the latest generation intrusion detection systems. There is a specific write up within this document that explains how some of these techniques are employed and the dramatic impact they have on nuisance alarm rates.

Table of Contents

PREFACE 2
INTRODUCTION 4
PERFORMANCE CHARACTERISTICS 5
ENVIRONMENTAL CONSIDERATIONS 7
ALARM MONITORING SYSTEMS 7
- ALARM ASSESSMENT 7
- SENSOR INTEGRATION 8
- COMMUNICATIONS 8
- POWER SUPPLIES 9
- COST CONSIDERATIONS 9
- MAINTENANCE COSTS 9
- THE TYPICAL PERIMETER INTRUSION ALARM PROCESS 10

PERIMETER SENSING TECHNOLOGIES 11
- FENCE MOUNTED SENSORS 12
  - FIBER OPTIC FENCE SENSORS 12
    - ZONE-BASED FIBRE OPTIC SENSORS 13
    - INTERFEROMETRIC FIBRE OPTIC SENSORS 16
    - FIBRE BRAGG GRATING SENSORS 18
  - VIBRATION (‘RATTLER’) SENSORS 19
  - TAUT WIRE FENCES 22
  - STRAIN SENSITIVE AND MICROPHONIC CABLES 26
  - ELECTROSTATIC OR CAPACITANCE SENSORS 32
- BURIED SENSORS 35
  - BURIED FIBRE OPTIC SENSORS 35
  - PORTED OR ‘LEAKY’ COAX BURIED SENSORS 37
  - BALANCED BURIED PRESSURE TUBE SENSOR 39
  - BURIED GEOPHONES 41
- VOLUMETRIC SENSORS 43
  - MICROWAVE SENSORS 43
  - ACTIVE & PASSIVE INFRARED DETECTION SYSTEMS 45
- VIDEO SENSORS 47
  - VIDEO MOTION DETECTION 47
  - REFERENCES: 49

INTRODUCTION

The intrusion detection solution selected for any perimeter is normally determined by the physical barriers (the type and condition of the fence, if any, for example), and the perceived level of risk of the site to intrusion. It usually comprises several different but complimentary technologies to form layers of protection.

An intrusion detection solution is typically designed to meet customer specific needs and the unique requirements of the site to be secured - the type of facility to be protected, the nature of the environment, perimeter fence construction, intrusion and security history, along with the perceived threat. Activity in and surrounding the site or facility, the physical configuration of the site to be secured, the surrounding environment, the site weather conditions, as well as advances in intrusion detection technologies are all factors to be considered when planning a perimeter intrusion detection system for a site.

Even the very best sensors available today will deliver less than optimum performance if not correctly tailored to meet the specific site requirements.

The role of any perimeter security system (that is, the perimeter fence and the Perimeter Intrusion Detection System - PIDS) is to act as the first level of site protection – providing both an early warning of intrusion attempts as well as deterring, detecting, documenting and delaying any intrusion into the protected area or facility. This integration of sensors and systems is a major design consideration and is best accomplished as a part of an overall site security plan and not simply as a stand-alone package.

The main elements in the design of an Intrusion Detection System are:

a) The actual Intrusion Detection Sensor(s) installed in the field or on the fence
b) The Alarm Processor that drives and analyses sensor signals
c) The Security or Alarm Management System that notifies security staff of an alarm and the location of the intrusion
d) The communications infrastructure that connects these three elements together and connects the system to the security staff.
e) An established and clearly documented site policy and alarm response procedure.

A critical part of any security plan always has to include appropriately trained security staff and an alarm response mechanism or procedure. Without the right staff to operate, monitor and maintain the system, or a professional response team with an established response mechanism in place, the end result will almost always be unsuccessful regardless of which intrusion detection technology is installed.

The smart intruders generally don't defeat the sensors or intrusion detection systems, but instead rely on poor alarm response procedures and mechanisms to avoid getting caught!

PERFORMANCE CHARACTERISTICS

When evaluating any perimeter intrusion detection sensor, there are at least three key performance characteristics to be considered: the Probability Of Detection (POD), the Nuisance Alarm Rate (NAR), and Vulnerability to Defeat (i.e. typical measures used to defeat or bypass detection by the sensor).

In the ideal world, the ideal Perimeter Intrusion Detection System (PIDS) would exhibit a zero NAR and a 100% POD simultaneously, and cannot be defeated.

Probability of Detection (POD) provides an indication of a systems ability to detect and intrusion within the area protected. Probability of detection involves not only the characteristics of the sensor, but also the environment, the method of installation and adjustment, and the assumed behaviour of an intruder. Any POD figure quoted will be conditional and unique to a site - despite the claims made by some sensor manufacturers. For example a sensor may have quite a high POD for a low level threat such as a teenage vandal who has little knowledge of the system versus a more sophisticated threat such as a professional thief or special operations person where the POD will almost certainly be substantially lower.

Almost any sensor manufacturer can quote and offer you a 99.99% POD under ideal conditions, that is, a large target and sensor sensitivity turned up to the max. Of course, at maximum sensitivity both the confidence level and the NAR may be totally unacceptable. If a manufacturer were to quote you a 99% POD figure, you should be asking them for very extensive test data to verify their claims!

Nuisance Alarm Rate (NAR) indicates the expected rate of alarms not attributable to legitimate intrusion activity. Generally nuisance alarms are caused by known or suspected environmental events such as animals, rain, wind, storms etc. and not by an actual intruder. The newer intrusion detection systems categorise the intrusion in order to distinguish false positives from actual intrusions. A *false alarm* however is an alarm where the cause is unknown, so an intrusion is always a possibility, but analysis after the fact indicates that no intrusion actually occurred. The intrusion detection system has produced an alarm when no attack has taken place. Generally false alarms are generated by the hardware or software supporting the detectors. These days, with the advances in electronics, false alarms are becoming increasingly rare.

Vulnerability to Defeat is another measure of the effectiveness of sensors and system design. Since there is no single sensor which can reliably detect all types of intrusions, yet still have an acceptably low NAR, the potential for defeat can be reduced by designing overlapping sensor coverage using multiple units of complementary technologies.

Each of these three performance characteristics will vary according to the technology selected and the unique site conditions – remember, no two sites are ever the same. Also, when

comparing POD and NAR rates quoted by manufacturers, the two must be considered together as both are inter-related and to some extent can be traded off against each other. Anyone can quote a high POD by winding up the sensor sensitivity, and conversely a low NAR by winding back the sensitivity – what you really need to know is what NAR is associated with what POD or a range of POD's.

You need to understand what the simultaneous POD and NAR figures will be – what you can really expect in the field with a real-world installation (and this will often be site dependent). For example an operator may be willing to tolerate a greater NAR to increase the sensitivity or POD of the system.

Signal Discrimination. In recent years, there have not been any breakthroughs in sensing technologies, but instead there have been major developments and advances in Signal Discrimination and the way sensor information is analysed. This is only possible because of the large amount of multi-parameter sensing information now able to be collected by the newer and much smarter technologies such as fibre optics, and the processing power available from the multiple CPUs in the centrally installed controllers to run signal fingerprint and pattern recognition type software. This amount and level of processing is typically not available from distributed processing architectures – that is multiple microprocessor based sensor controllers installed in the field. The computing required is far more intensive than distributed processors are capable of.

These advanced technologies were originally designed for Military applications, and have made their way into the security arena where they are capable of clearly discriminating between 'real' events and background clutter. This allows the detection system to be made extremely sensitive to intrusions (high Probability of Detection) without the penalty of creating nuisance alarms (low Nuisance Alarm Rate). It minimises the effects of wind, rain, storms, aircraft, traffic, lightning etc. while maintaining the same high levels of sensitivity and intrusion detection.

ENVIRONMENTAL CONSIDERATIONS

Each individual installation has a set of unique environmental factors which must be taken into account when designing the system, selecting the sensors, and performing the installation. Failure to consider all these factors can result in excessive nuisance alarms. The unique environmental factors for a site that may need to be considered, include climate (wind, rain, salt air etc), animal activity, as well as man-made environmental factors such as human activity patterns, electrical fields, lightning, radio transmissions, and nearby vehicle, truck, rail or air movement.

There are other considerations that must be assessed when actually installing sensors to monitor perimeters. If fence mounted sensors are used, the fences themselves should be well constructed and solidly anchored, as loose fences can move in the wind and generate nuisance alarms. In addition to simply dividing the perimeter into a number of independent zones in order to simplify the identification of the intrusion position, consideration should also be given to PIDS that provide actual locations on the perimeter fence where an intrusion attempt has occurred to improve response times for security staff and provide more accurate CCTV surveillance.

Above all else, carefully read the installation manual and follow the sensor manufacturers' installation instructions. After all, they designed their system; they know what works in what environments and what doesn't. If you have any doubts or questions - call them. Failing to closely follow the instructions almost always leads to disaster and substantial cost overruns.

ALARM MONITORING SYSTEMS

In addition to sensor technology discussed in this document, there is also a variety of alarm monitoring systems or operator front-ends available. Although each system is unique in the number and variety of options available, all systems perform the basic function of annunciating alarms, logging alarm details, and displaying the alarm locations in a simple to understand format to the security staff. The front-end (control function) of most of these systems is configured with a PC running Windows. Most of these systems operate with proprietary manufacturer supplied software.

ALARM ASSESSMENT

Alarm monitoring systems provide both a visual and an audible indication of an alarm. The alarm data is typically displayed as symbols overlaid on a map of the site being monitored. Most systems offer multiple levels (scales) of maps which can be helpful in guiding security personnel to the precise location of the intrusion. The urgency of the visual alarm can vary as to the nature of the alarm or the location of the possible intrusion (e.g. high priority versus low priority areas, nuisance alarms versus real intrusions). In most security systems, several of these capabilities are combined to provide security staff with a comprehensive picture of the alarm situation. Many systems offer a CCTV surveillance capability which automatically provides security staff with a real-time view and automatic recording of the intrusion activity.

SENSOR INTEGRATION

From a technology perspective, the integration of sensors into a high level security monitoring or security management system is relatively easy. Typically, most sensor systems have contact outputs, one for each zone, and may have additional contacts or switches to indicate tampering of the field cabinet. Most monitoring systems also provide a means of constantly monitoring the continuity of the wiring to each device, indicating if circuits have been cut or bypassed.

Different but complimentary types of sensors are often be integrated together to reduce nuisance alarm rates, and increase the probability of intrusion detection. Sensor alarm and tamper circuits can be joined together by installing a logic AND circuit. This AND system then requires multiple sensors to indicate an alarm condition prior to the field unit sending an alarm indication. Using a logic AND circuit can reduce nuisance alarm rates but it may also decrease the probability of detection because two or more sensors are required to detect an alarm condition prior to initiating an intrusion alarm. Another down side of this approach is that often it can take many seconds to poll each individual sensor on a perimeter to see if they have an alarm, by which time an intruder could have climbed the fence and run off before the CCTV camera has had a chance to verify the intrusion.

The latest generations of fibre optic intrusion detection systems are more advanced than this, offering much better discrimination and control of nuisance alarms. Alarm outputs to the security management system contain and present far more information than a simple alarm/no alarm relay contact. They can send information such as the location of the intrusion event, what type of intrusion event it is (climbing, cutting, lifting the fence fabric, environmental nuisance alarm etc.), and software commands directly to activate and control CCTV systems, all in real time.

COMMUNICATIONS

Communications between the front-end computer and the field elements (sensors, processors) traditionally employed standard telecommunications protocols such as RS-485, RS-422, RS-232, Frequency Shift Keying (FSK), and Dual Tone Multi Frequency (DTMF), although some manufacturers use their own proprietary communications protocols which can limit options for future upgrades and additions. In order to reduce the tasks required to be handled by the front end computer, some systems have a pre-processing unit located between the computer and the field processing elements, relieving the front end computer of these communications processing overheads.

Newer generation systems are far simpler, faster and far more advanced, using standard computer communication protocols such as TCP/IP allowing high speed bi-directional communications over huge distances using readily available and proven network topologies such as Wide Area Networks (WAN), Local Area Networks (LAN), the Internet, WiFi etc.

POWER SUPPLIES

Regardless of how well a solution is designed and installed, virtually all perimeter intrusion detection systems are vulnerable to power loss. Potential intruders who are aware of this vulnerability may try to cut power if they cannot bypass the system by other means. Therefore it is critical that all elements of the perimeter intrusion detection system have a power backup strategy (UPS, batteries, standby generator etc.) incorporated into the design and operation, to guarantee uninterrupted operation of the sensor on the perimeter, alarm reporting, situation assessment, and security staff response.

So not only do the field components of the PIDS require this, but also the security management system, as well as communications to security staff such as phones, radio etc., CCTV, DVR, etc. Every aspect and element of the security response mechanism needs to have backup power available.

COST CONSIDERATIONS

The true cost of a Perimeter Intrusion Detection System is often very easy to underestimate. Sensor manufacturers often quote just the cost per meter for the sensor system, and this figure is representative of the hardware cost only, and does not include the costs of installation, any associated infrastructure to provide power to the field elements (sensor and controller), communications lines to the field elements, mounting poles, security management system, training or maintenance.

Make sure you work with the total installed cost when comparing systems. With many vendors, the low up-front purchase price of the PIDS hardware is far outweighed by the high costs associated with providing the power and communications infrastructures, and purchasing and installing the assessment and alarm reporting systems. It is not uncommon for these infrastructure and installation costs to be 4-5 times the cost of the actual PIDS hardware!

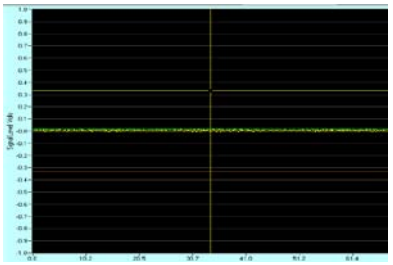
MAINTENANCE COSTS

Ongoing maintenance costs should also be taken into account, as these can be significant over the life of the system. Questions that should be asked:

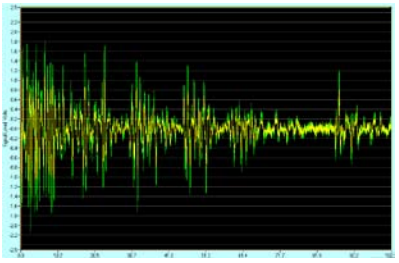
- What is the Mean Time Between Failures (MTBF) of the entire system (not just the parts or individual components of it)?
- How long is the warranty period?
- What is the realistic life expectancy of the system?
- Is there a warranty extension program available?
- What is covered by warranty extension?
- What will be the response times if I have a problem?

THE TYPICAL PERIMETER INTRUSION ALARM PROCESS

The perimeter intrusion detection system is calibrated for ambient background conditions



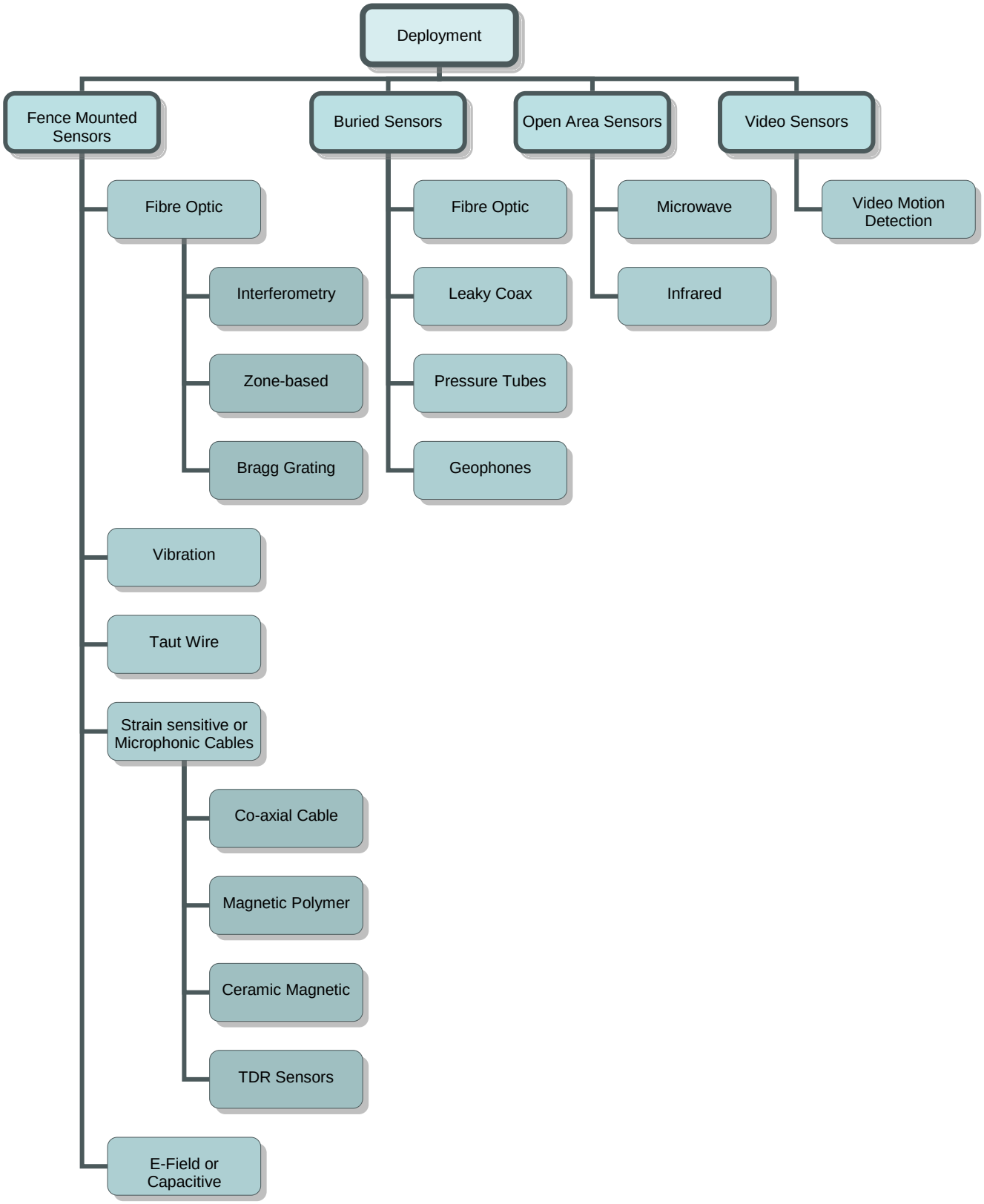
An intruder breaches the perimeter and disturbs this background signal



This signal change is processed and if it meets defined criteria an alarm is sent to the Security Management System

The Security Response Force examines the event on CCTV and/or goes to the intrusion site to investigate

PERIMETER SENSING TECHNOLOGIES



FENCE MOUNTED SENSORS

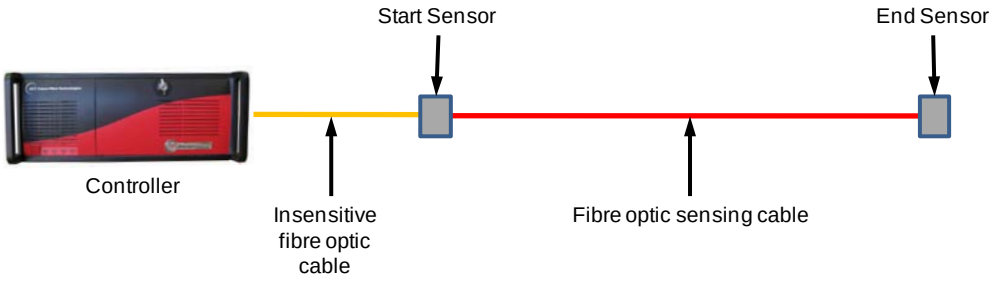
FIBER OPTIC FENCE SENSORS

Description: Fibre optic sensing systems are relatively new detection technologies but have a strong following. The systems are readily available and are highly tuneable to compensate for environmental conditions in the field such as weather and climate characteristics. The sensors are impervious to lightning, electromagnetic interference, radio frequency interference or other electronic signals and can be used over long distances.

Fibre optic sensors use light travelling down a glass fibre rather than electrical signals down wires for transmission and detection, so are ideal for incorporation into existing fences. There are two main types of fibre optic intrusion detection systems – the traditional hardware zoned systems, and the newer more sensitive Interferometric systems that provide the location of an intrusion. Although both of these are fibre optic based, the fundamental principles behind them are quite different, as is the performance and applications. Also included is a brief description of one of the newer emerging technologies – Bragg Grating.

Basic Operating Principle: Optical fibre is a flexible tube of glass that guides light waves from a light source at one end to a detector or a mirror at the other end of the fibre. When the fibre is bent or moves, the characteristics of the light travelling down the fibre are altered. In a perimeter system, light is sent down the fibre attached to the fence and is returned to the controller to establish a steady or ambient background or no-alarm state. When someone attempts to climb the fence, the fibre optic cable moves minutely and the light pattern travelling down it changes. It is this change in the light pattern that is detected, and if it exceeds a predetermined threshold, an alarm is flagged.

As well as being intrinsically safe, the optical fibre itself is immune to Electrical Magnetic Interference (EMI), Radio Frequency Interference (RFI) and lightning



When any motion or vibration acts on the sensing fibre, or anything the fibre is attached to such as a fence, the light is affected and this change is detected at the controller.

ZONE-BASED FIBRE OPTIC SENSORS

Operating Principle: The traditional zone based fibre optic sensing system consists of a microprocessor-based controller installed on the fence line, and a multimode fibre optic sensor cable attached to the fence fabric and connected to the controller. Light from a laser is sent down the fibre, and the returned light is compared to determine if there are any light or "speckle pattern" changes due to the micro bending of the fibre optic cable caused by a disturbance on the fence. While zone lengths of up to 2000 metres are theoretically possible, realistically they are usually limited to 300 metres or less.

With some systems the fibre optic sensor cable has to be installed within a conduit to help control environmental conditions such as rain, or with an anemometer to reduce the sensitivity of the system during windy conditions to avoid nuisance alarms being generated by the wind on the fence fabric. Naturally, when you decrease the sensitivity to wind, you will also decrease the probability of detecting a real intrusion event.

The main disadvantage of this zone based technology is the cost and complexity of getting power to the fence mounted controllers, and also communications back from the field. As there are electronics situated in the field, while the fibre optic cable itself is immune to EMI, RFI and lightning, the electronics are not. For this reason, the latest releases of this detection technology tend to have the controllers housed inside the Security Centre and fibre only outside the building and on the fence.

Application: The fibre optic sensor cables are mounted directly to the fence fabric using cable ties or twist ties. A good quality and stable installation of the fence is necessary for reliable detection as with any perimeter intrusion detection system. Fences free of rattles, loose signs, and vibrations will always maximise system performance. With these zone based systems, the more ambient activity that exists around the fence, the lower the sensitivity setting for the system, and the less likely the system will detect an intruder.

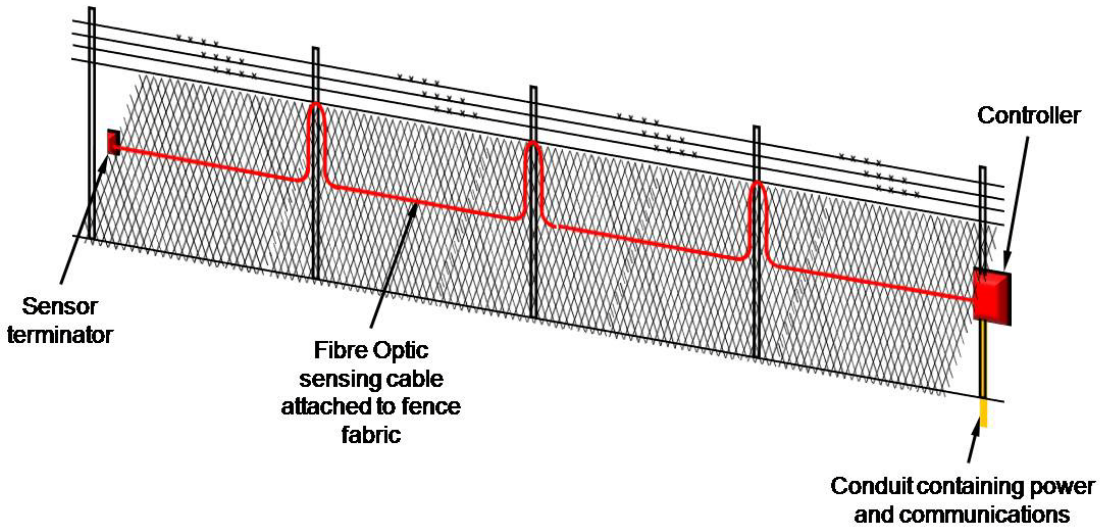
Zone based systems are more suited to smaller sites typically less than 2000 metres, where power is readily available on the perimeter fence or at least close by. The preference should always be to install a system where there are no electronics in the field and the controller is mounted in the Security Centre to maximise immunity to strong electromagnetic events and minimise installation costs.

Strengths: Low purchase cost for small perimeters, simple to install the sensor cable, sensor cable immunity to EMI, RFI and lightning.

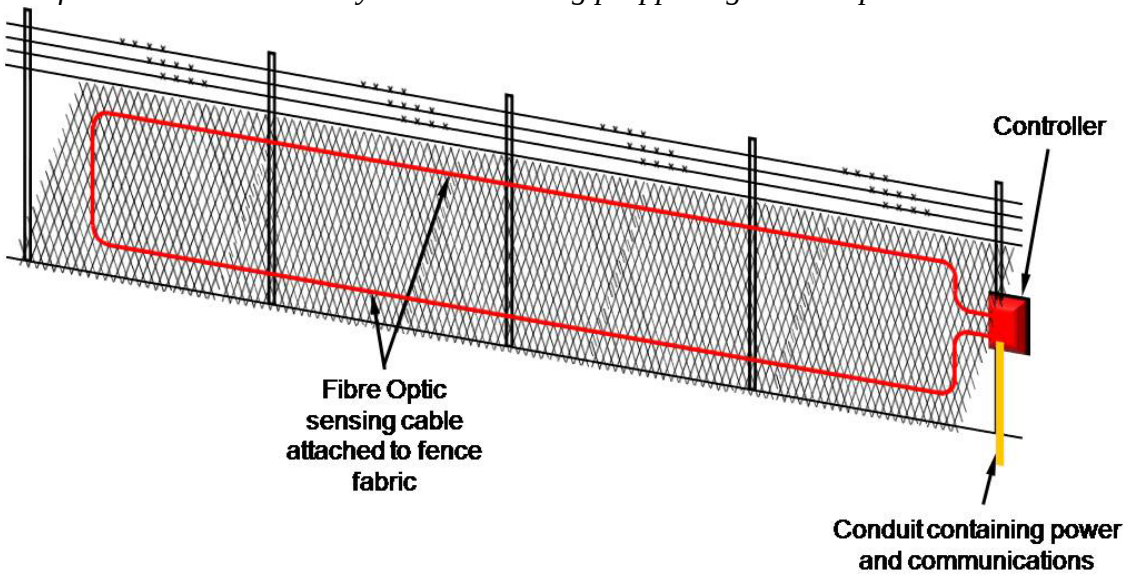
Weaknesses: Installation costs can be high if controllers are situated in the field and power / communications has to be supplied to these. Sensitivity not as high as an interferometric fibre optic sensor.

Potential Causes of Nuisance Alarms: Although the fibre optic cable itself impervious to interference, as with any outdoor electronics, system problems can be created by RFI, EMI and lightning where controllers are installed in the field, as will extreme changes in temperatures. In addition, animal activity coming in contact with the fence can be interpreted as human activity, falsely signalling an intrusion attack

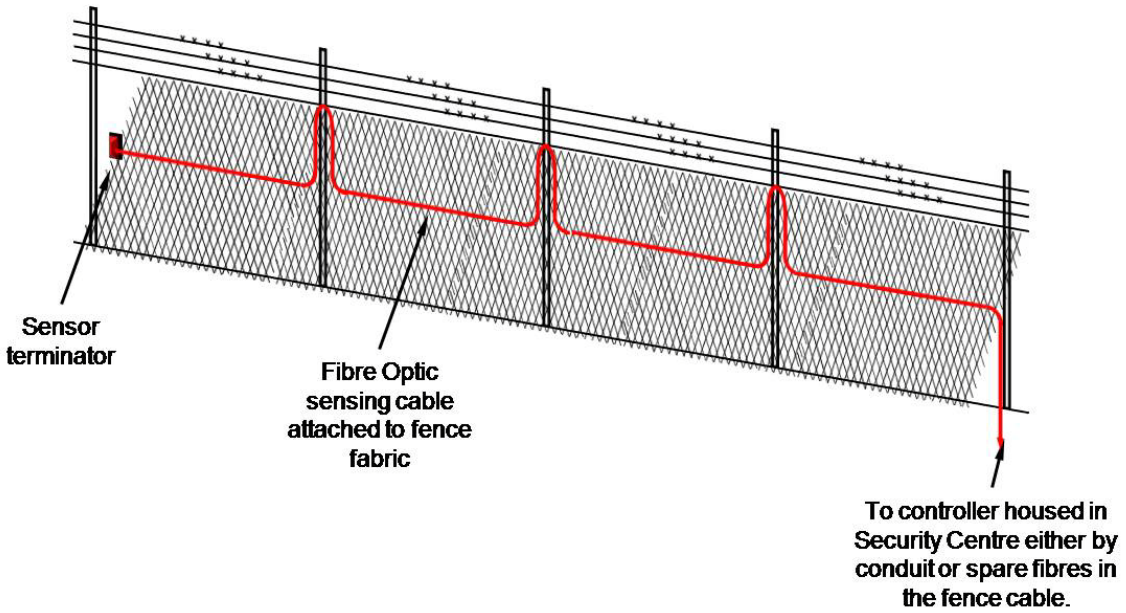
Typical Defeat Measures: Bridging or tunnelling will bypass the fence and, therefore, bypass the sensor. Careful or assisted climbing, particularly at the more rigid turn points, may not produce the activity level required for alarm activation. This can be overcome by using Microstrain technology which is far more sensitive to situations such as propping ladders against a fence.



Installation Method 1. *Fence mounted controller with a single run of cable looped up the poles for additional sensitivity to ladders being propped against the posts.*



Installation Method 2. *Fence mounted controller with a single loop of cable – provides medium sensitivity but requires additional sensor cable.*



Installation Method 3. *Remotely located controller with a single run of cable looped up the poles for additional sensitivity to ladders being propped against the posts*

INTERFEROMETRIC FIBRE OPTIC SENSORS

Operating Principle: The newer interferometric or Microstrain technologies are far more sensitive than the traditional 'speckle pattern' zone based systems, usually achieved by using a principal of detection called interferometry. They combine the signals from the two single mode fibres within the same fence mounted cable and when an adequate change in the resulting light pattern takes place an alarm is generated. By timing these signals some systems can also calculate and provide the location of an intrusion. The key to this technology is that it utilises highly advanced signal processing and signature analysis carried out in a powerful head end unit located within the Security Centre to maintain the inherently high sensitivity to intrusions without the penalty of increased nuisance alarms.

As Microstrain systems use single mode fibres, a single system can protect a perimeter of up to 80km in length, with uniform sensitivity anywhere along the sensor cable. Rather than having hardware defined zones, this technology allows zones to be easily set in software for improved flexibility and better correlation to fixed perimeter points (gates, buildings, corners, roads) and cameras etc.

Application: Fibre optic fence sensors (actually fibre optic cables) are quickly and easily fixed directly onto the fence fabric in a single pass. A good quality and stable installation of the fence is necessary for reliable detection as with any perimeter intrusion detection system. Fences free of rattles, loose signs, and vibrations will always maximise system performance and sensitivity. The Microstrain system is unaffected by ambient noise and it uses advanced techniques such as signature recognition and pattern matching to determine legitimate intrusion events rather than the more basic signal amplitude threshold of zone based systems.

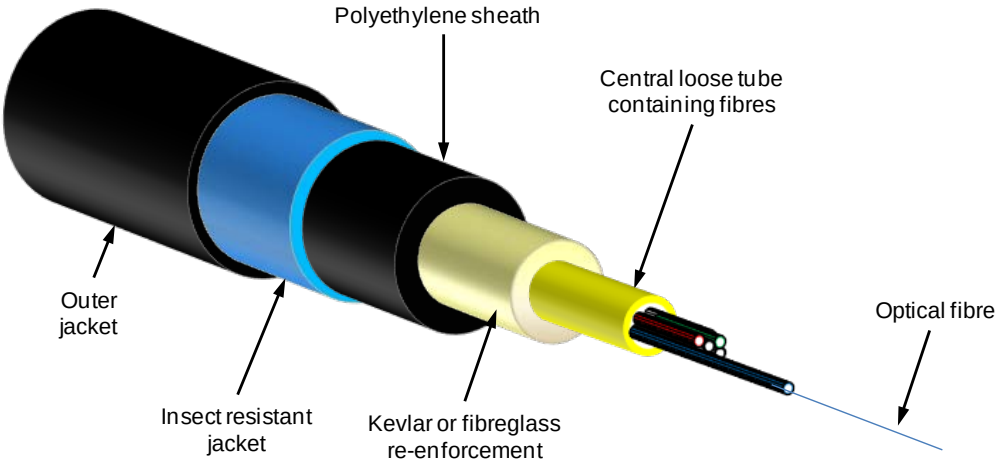
Microstrain systems are more cost effective for perimeter fence lengths of between 2km and 80km which are handled by just the one controller. A single cable is run at the midpoint of the fence and the controller is installed in the Security Centre, making installation extremely cost-effective for these longer distances as no power is required in the field and no electronics are installed in the field.

Strengths: Long distance, highly sensitive, low installation costs, intrinsically safe, immunity to EMI, RFI and lightning, and powerful signal processing. Excellent signal discrimination = very low NAR. Highly reliable

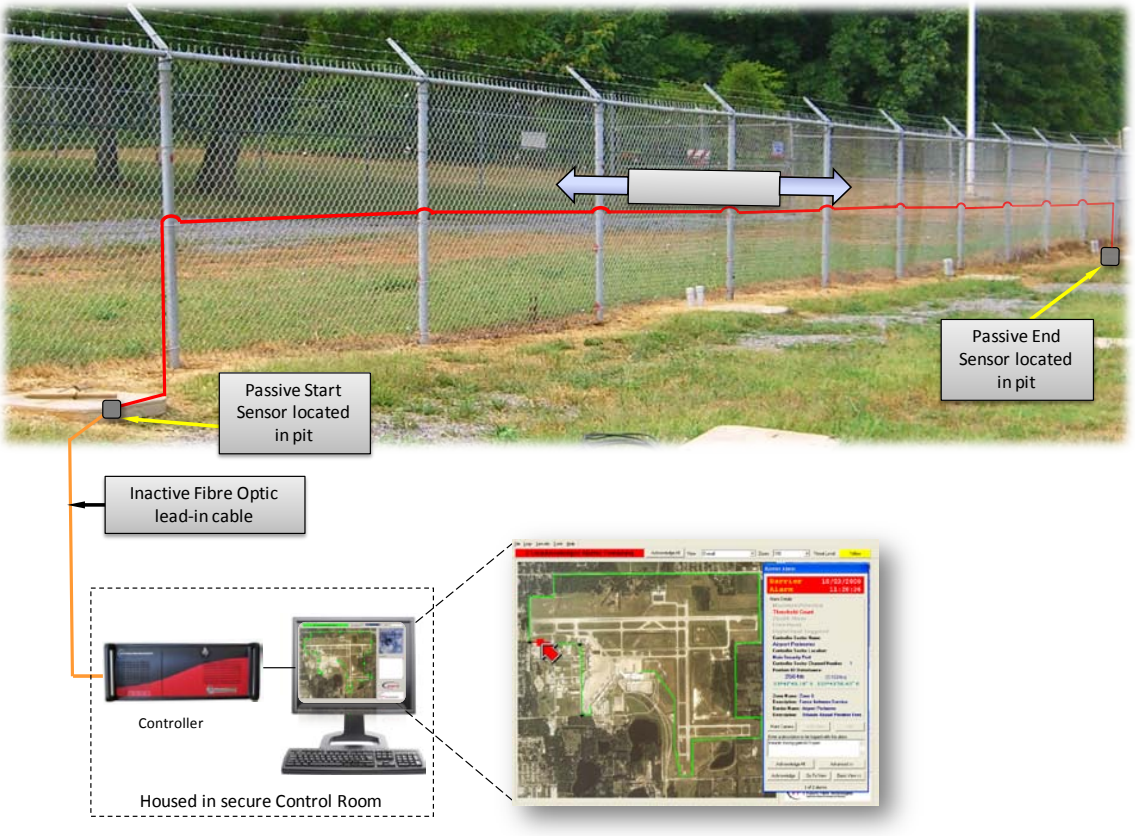
Weaknesses: Not connectorised – requires fusion splicing to join fibres, but there are many telco contractors capable of doing this.

Potential Causes of Nuisance Alarms: As with any fence mounted intrusion detection system, poor fence quality is a common cause for nuisance alarms - when properly installed on a good quality fence in accordance with the manufacturer's instructions, the system is very stable and gives few if any problems.

Typical Defeat Measures: Bridging or tunnelling will bypass the fence and, therefore, bypass the sensor.



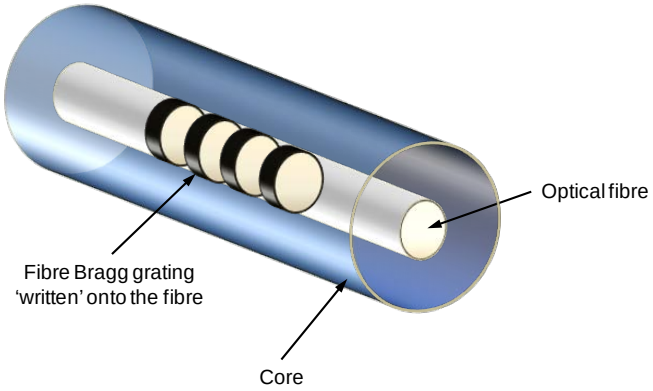
Fibre Optic Sensor Cable Construction



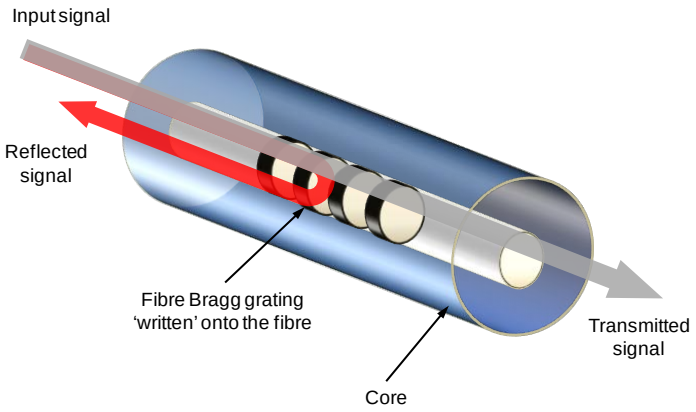
A typical Microstrain Fibre Optic Sensor system installation.

FIBRE BRAGG GRATING SENSORS

Operating Principle: Another of the new breed of emerging and possible future fibre optic sensors is the Fibre Bragg Grating (FBG). FBGs' are an inline optical device that has an alternating refractive index pattern. This pattern is 'written' or implanted into a custom optical fibre.



The Bragg grating works by reflecting back a very narrow wavelength or frequency of light travelling through the fibre, allowing all other wavelengths to pass. In its simplest form, it is an optical filter. However, when the fibre is minutely moved, these tiny grating spaces change slightly, and so the reflected wavelength changes.



Because the behaviour of FBGs changes with strain such as you would see from an intruder climbing a fence or structure the optical fibre is attached to, they can also be used as point sensors or quasi-distributed sensors. As each FBG written on the sensor fibre is different - corresponding to a different wavelength – this system can also potentially determine which grating changed, and therefore provide the location of an event.

Several organisations are researching and promoting this technology, but as yet there are few commercial installations. The FBG sensor cable is expensive to produce and typically the controller has a limited number of gratings that can be processed meaning reduced resolution over longer distances.

VIBRATION ('RATTLER') SENSORS

Description: Fence vibration sensors are mounted directly on the fence fabric and will detect vibrations on the fence including those associated with cutting, climbing or lifting of the fence.

Operating Principle: There are two basic types of fence vibration sensors: Electro-mechanical or inertial sensors, whose signal processor has a pulse accumulation circuit that recognizes momentary contact openings of electromechanical switches; and Piezoelectric, whose signal processor responds to the amplitude, duration, and frequency of the transmitted signal.

Mechanical or inertial sensors consist of a weighted mass that moves as the sensor or fence vibrates. If this movement is of sufficient strength, the weighted mass momentarily opens and closes some contacts as it swings from side to side. The opening and closing of these contacts generates electrical pulses which are sent to the controller.

Piezoelectric sensors convert the mechanical impact forces generated during an intrusion attempt into electrical signals. Unlike the open/close signal generated by electro-mechanical sensors, piezoelectric sensors generate an analogue signal that varies proportionally in amplitude and frequency to the vibration activity on the fence fabric.

Intrusion actions will generate mechanical vibrations in the fence fabric that are different from the vibrations associated with background activity. Fence vibration sensors detect these vibrations and the signals from the transducers are then sent to a signal processor to be analysed. The frequency that the sensor contacts open and close is compared to the ambient background level and triggers an alarm if it exceeds the thresholds set.

Application: These sensors come pre-assembled on a cable at 3 metre intervals, and are installed approximately 150cm above the ground. Recommended zone lengths are typically 100 metres.

Proper installation and spacing of the sensors is critical to reliable detection. Poor quality fences with loose fabric will create too much background activity (flexing, sagging, swaying), initially generating nuisance alarms and eventually transmitting little reliable intrusion activity. Likewise, adverse weather conditions can cause sensitivity settings to be set above or below what is required for reliable detection to occur. Fence corners pose particular challenges for readily detecting intrusion vibrations, because of the increased bracing of the fence posts and more solid foundations typically used at a corner or turn-point.

Because vibration sensors are prone to activation from <u>all</u> types of vibrations, additional sensing equipment is required to reduce the incidence of nuisance alarms. One method is the pulse count accumulator circuit. With this device, sensitivity is determined by counting the number of pulses over time generated by the sensor to create an alarm. Higher sensitivity is achieved by setting fewer pulses over a period of time (and consequently more nuisance alarms) and lower sensitivity by waiting for more pulses.

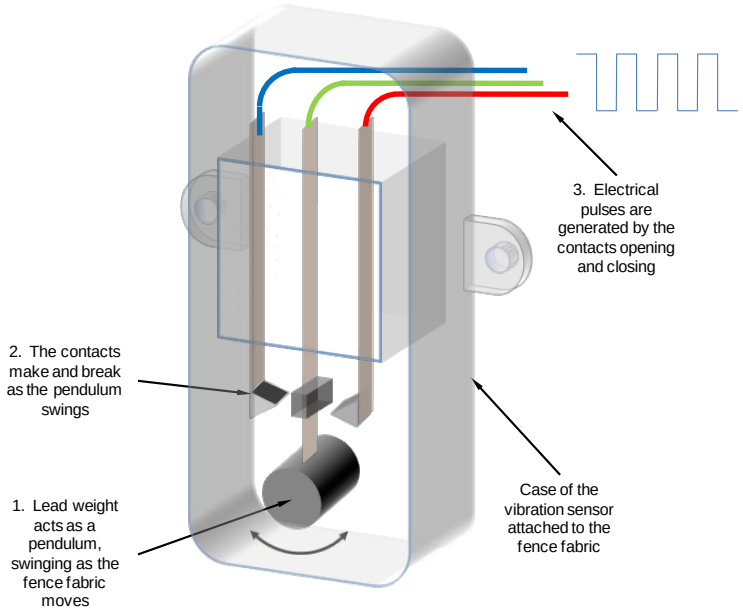
Mechanical vibration sensors should only be used in applications where natural or man-made environmental vibrations are non-existent. Vibration sensors are neither suitable nor reliable in areas where high background vibrations occur, such as close to construction sites, railways, highways and roads.

Strengths: Cheap, simple to attach to the fence, possible to locate by pulsing the signal and measuring reflected signal times.

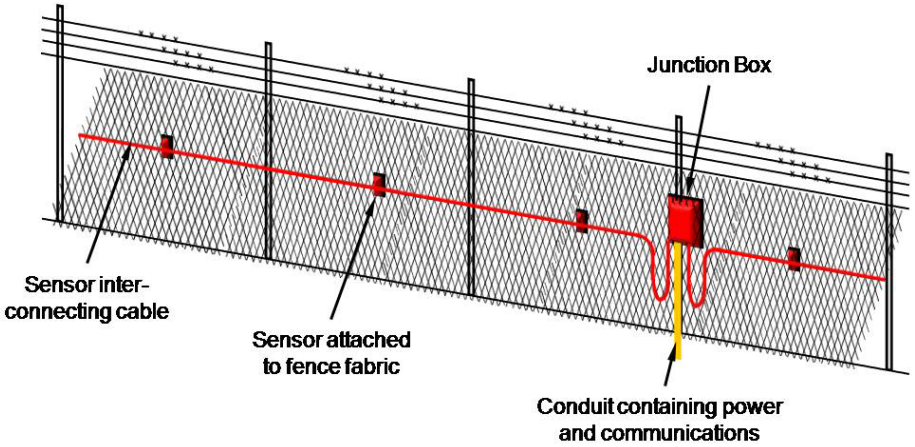
Weaknesses: Very little signal discrimination = high NAR. Susceptible to environmental vibrations and lightning. High installation costs as it requires controllers, communications, and power infrastructure to be installed in the field.

Potential Causes of Nuisance Alarms: Poor quality fence construction, tree branches, animals and adverse weather – in fact anything that can cause the fence to vibrate or rattle will trigger the sensors. In areas with high wind or many animals, vibration sensors should never be used.

Methods of Defeat: The most common defeat method is to avoid contact with the fence by bridging it or by careful removal of fence fabric. Although less common, tunnelling is always a possible defeat method.



Principal of Operation of Mechanical Sensor



Typical Installation method

TAUT WIRE FENCES

Description: A Taut Wire intrusion detection system typically combines many strands of horizontal barbed wire fencing with micro-switches or strain gauges to detect changes in tension (an intruder) on the actual barbed wires which form the physical barrier.

These are one of the most expensive types of perimeter fence intrusion detection systems available because of the complex installation and on-going seasonal maintenance required. However, as a definite pressure is required on the barbed wire for activation, they do offer high detection rates and very low nuisance alarms.

Operating Principle*:* The taut wire sensor is actually a series of micro-switches or strain gauges connected to tensioned barb wires installed on either the top of a chain link fence or barbed wires installed horizontally as the fence or barrier itself. The micro-switch itself typically consists of a movable centre plunger suspended inside a cylindrical conductor. In the rest position, the centre plunger is in the middle of the cylinder, and does not touch the outer edges. Increasing or relaxing the tension of the wire, which would happen if an intruder attempted to climb, spread or cut the wires, makes the centre plunger touch the wall of the cylinder closing the circuit, and an alarm is activated.

If a strain gauge is used, rapid changes in wire tension cause a change in the resistance of the strain gauge which is monitored.

The taut wire sensors are generally not susceptible to wind conditions (unless there is debris such as plastic bags caught on the wires), and quite a firm force is needed to activate a switch. The Taut Wire design is intended to activate an alarm on the very first contact, as this may be the only indication of an intrusion attempt or penetration taking place. Regular seasonal tensioning of the system is critical to ensure the system continues to perform as intended.

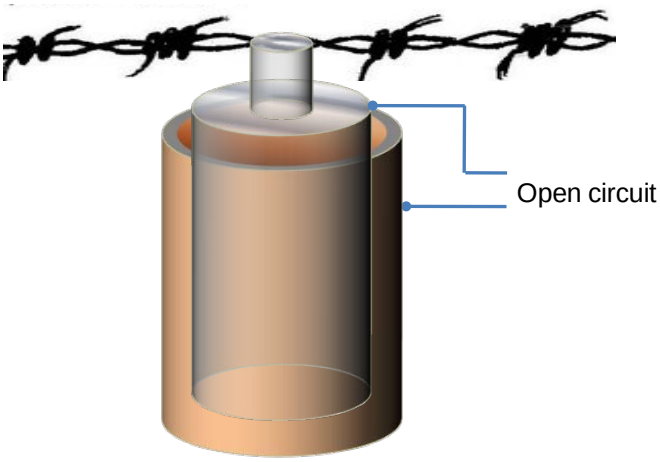
Application: Taut wire sensor systems can be installed as a stand-alone barbed wire fence creating a dual-purpose physical barrier as well as a detection system; added to an existing fence; or used as a barbed wire outrigger on top of a wall or fence. Because of the very high costs associated with a taut wire system, they are typically only installed at high risk facilities, and even then, not for long distances – usually less than 1km.

Strengths: High POD with a very low NAR. Difficult to defeat, so ideal for very high security sites such as prisons etc. Simple technology.

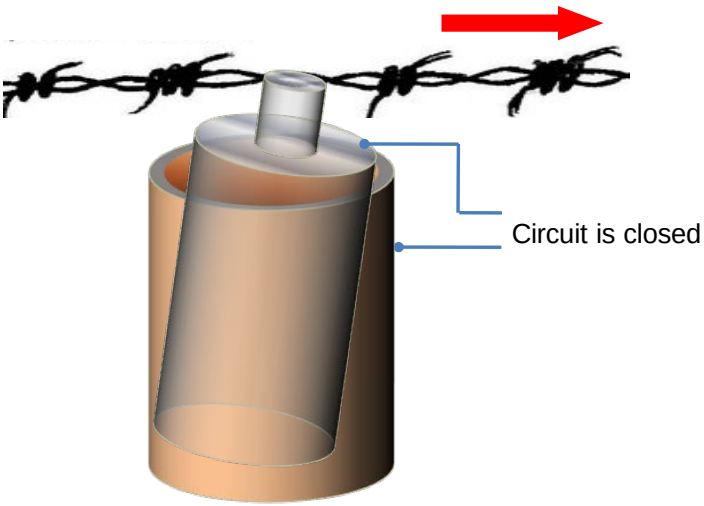
Weaknesses: Expensive to purchase, install and maintain. Requires seasonal adjustments and has many points of failure.

Potential Causes of Nuisance Alarms: Taut Wire is one of the more reliable fence-based detectors, as it is less susceptible to environmental conditions and small animals. Poor seasonal maintenance of the fence or incorrect tensioning of the barbed wires will lead to unreliable operation.

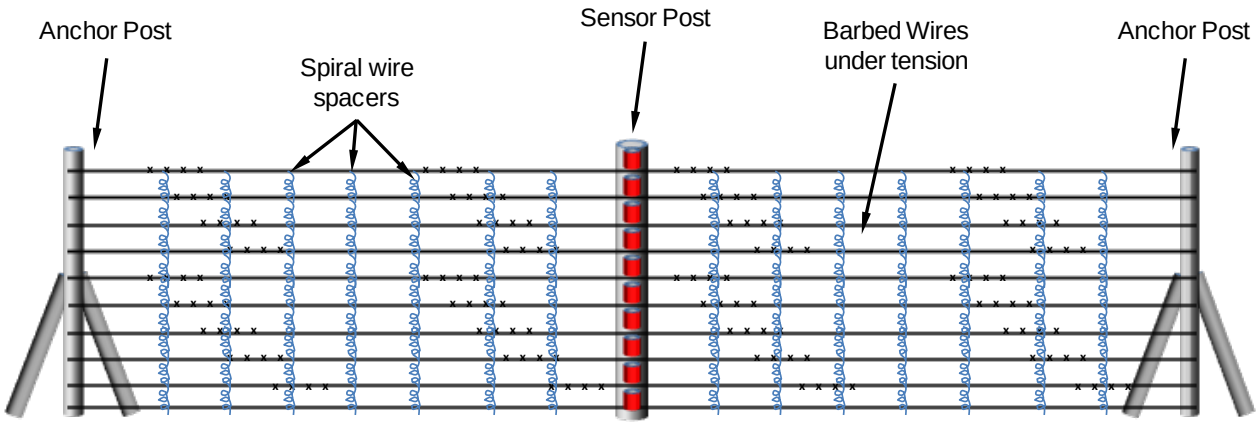
Methods of Defeat: Tunnelling under or bridging over the fence itself, with the most likely locations being those areas not under visual surveillance.



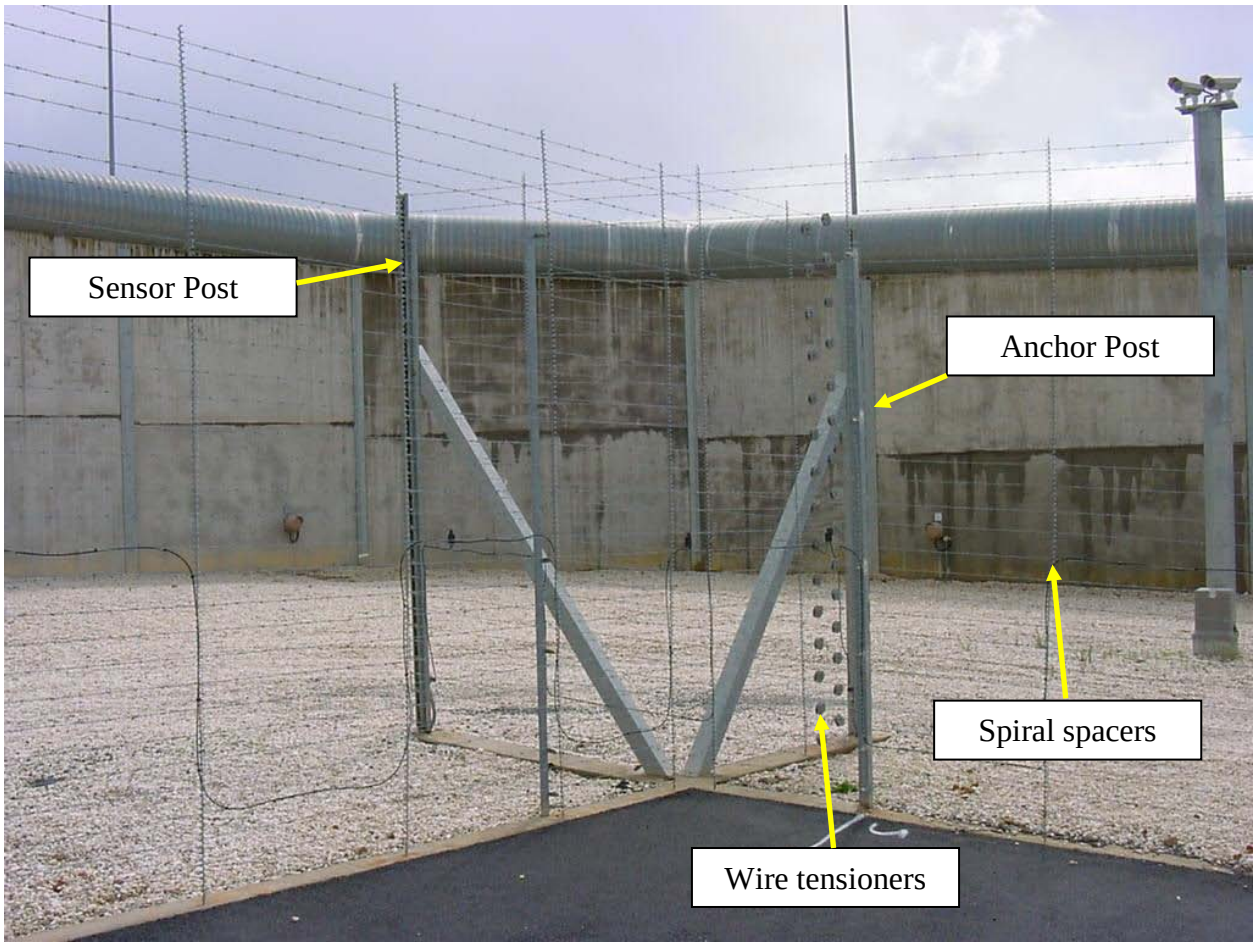
In the steady non-alarming state, the centre plunger does not touch the outer cylinder.



When an intruder attempts to cut or spread the barbed wire, the wire moves in one direction, causing the centre plunger to contact the outer cylinder and set the alarm.



Each sensor post houses one micro-switch or strain gauge attached to each of the horizontal barbed wires, and sits between two anchor posts. The spiral spacers are to prevent the wires flapping against each other in the wind and also make it more difficult to spread the wires without generating a horizontal pull to trigger the micro-switch.



Taut wire installation showing the anchor posts in a corner configuration, the wire tensioners and the spiral wire spacers installed every metre.

STRAIN SENSITIVE AND MICROPHONIC CABLES

Description: Strain sensitive cables (also known as Microphonic cables) are transducers that maintain uniform sensitivity over the length of the sensor or zone. The system consists of a sensing cable attached to the fence fabric and a signal processor mounted on the fence line. The sensor cable runs from the field installed signal analyser to a termination resistor, which is constantly monitored and will generate an alarm if an intruder attempts to bypass the sensor cable.

Operating Principle: When attached to a fence, the strain sensitive cable has the vibrations from the fence mechanically coupled to it. These vibrations or strains generate an electrical signal in the cable proportional to the mechanical stress resulting from a movement in the fence – associated with cutting, climbing, lifting etc. These generated signals are sent to the signal processor installed on the fence for analysis and if the signal is determined to be hostile, an alarm is generated. The processor provides for adjustments such as signal gain or sensitivity, the number of signal cycles required to generate an alarm, and duration of the disturbance.

With microphonic sensing systems a terminal voltage or charge is produced when the sensor cable is vibrated or deformed by an intruder in proximity. Some manufacturers use a coaxial cable that rely on the triboelectric effect - where a small cable terminal voltage is produced when the cable attached to the fence is vibrated by an intrusion etc. Other vendors use the piezoelectric effect, or are based on magnetic materials for detection.

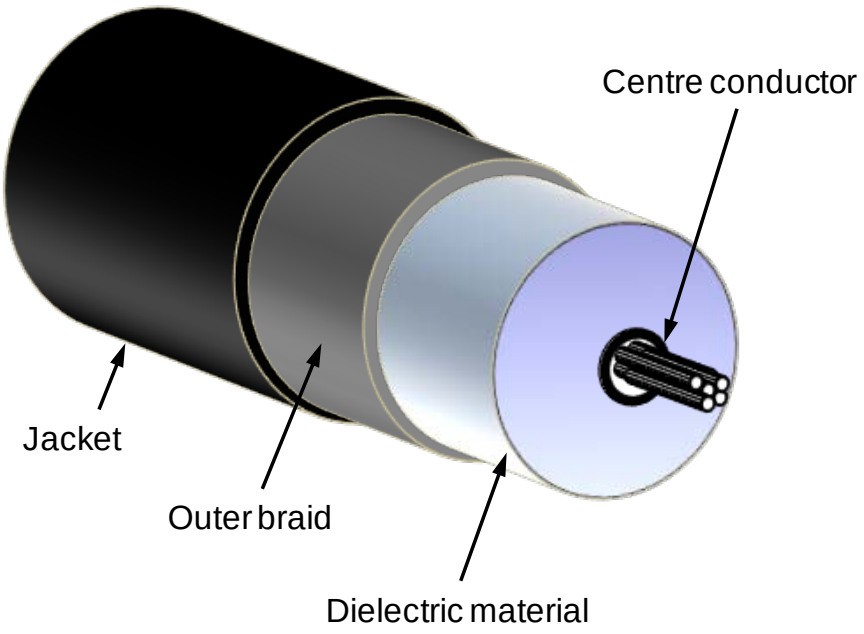
As this type of sensor is effectively a microphone, an audio monitoring capability can be incorporated, enabling the operator to hear noises along the fence line and manually determine, assess, or verify what caused the alarm. However, this requires very low levels of background noise, considerable training of staff, and constant real-time human monitoring. It also introduces delays in responding due to indecision or wrong decisions. Other technologies do not require this 'human signal discrimination' and decision making – signal discrimination software now does this task far quicker, more reliably and consistently, without any human intervention at all.

There are four main types of strain sensitive or microphonic cables: ***Coaxial***, which uses a custom coaxial cable where the centre conductor carries a permanent electrostatic charge; ***Magnetic Polymer***, which uses two semicircular magnetic polymer conductors separated by an air gap containing two uninsulated wires; ***Ceramic Magnetic*** consisting of a magnetic core containing two freely moving active conductors; and ***TDR*** consisting of a coaxial cable with two additional grooves containing sense wires.

Coaxial Cable:

The system comprises of two main parts, the sensor cable and the analyser. In the event of an intruder attempting to force entry by either cutting or climbing the fence, the vibrations caused by this intrusion are detected by the sensor cable and sent to the analyser.

On receipt of this signal the analyser determines a level of activity. If the level of activity is over a certain threshold the analyser will switch into alarm mode sending alarm and audio signals to the control.



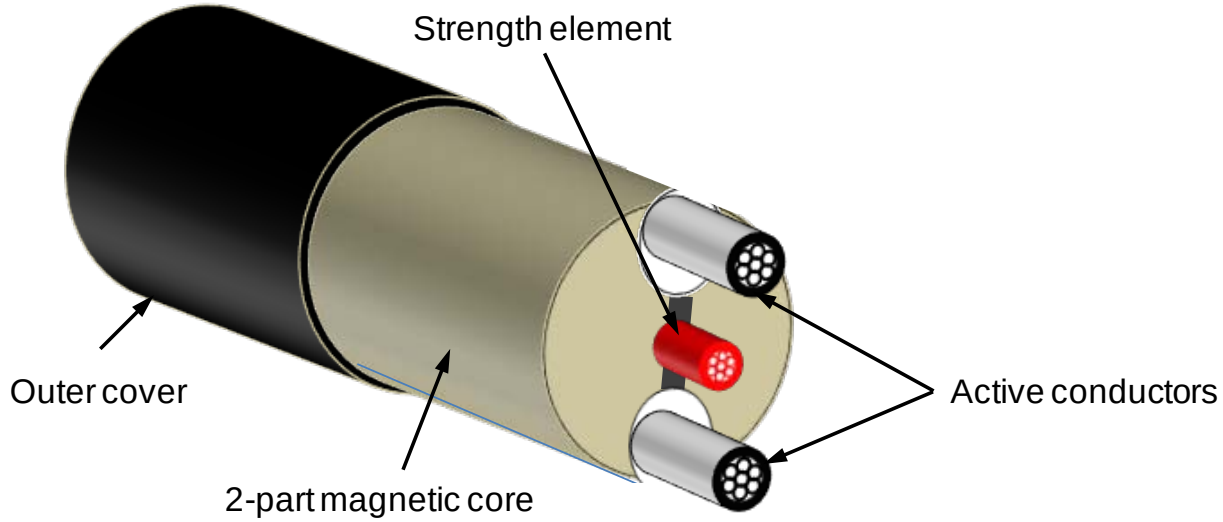
This typically works by means of the triboelectric effect. A steady permanent electric charge is placed on the centre conductor of the coaxial cable.

When an intrusion is attempted and the cable flexes, the friction associated with relative motion between the inner electrical conductor, the dielectric material, and the outer conductor causes an electrical charge to be transferred between the inner and outer conductors. This charge varies in response to movement of the cable.

Magnetic Polymer:

The strain sensitive magnetic polymer cable consists of a two part magnetic polymer core (that works like a linear magnet) and two free floating insulated wires (active conductors) in grooves 180° apart within the paired core. These wires move freely in response to vibrations and stress on the fence fabric. The movement of these wires within the grooves of the magnetic field created by the magnetic polymer core generates minute electric signals.

The processor then compares the signals and generates an alarm if it's outside the pre-calibrated parameters.

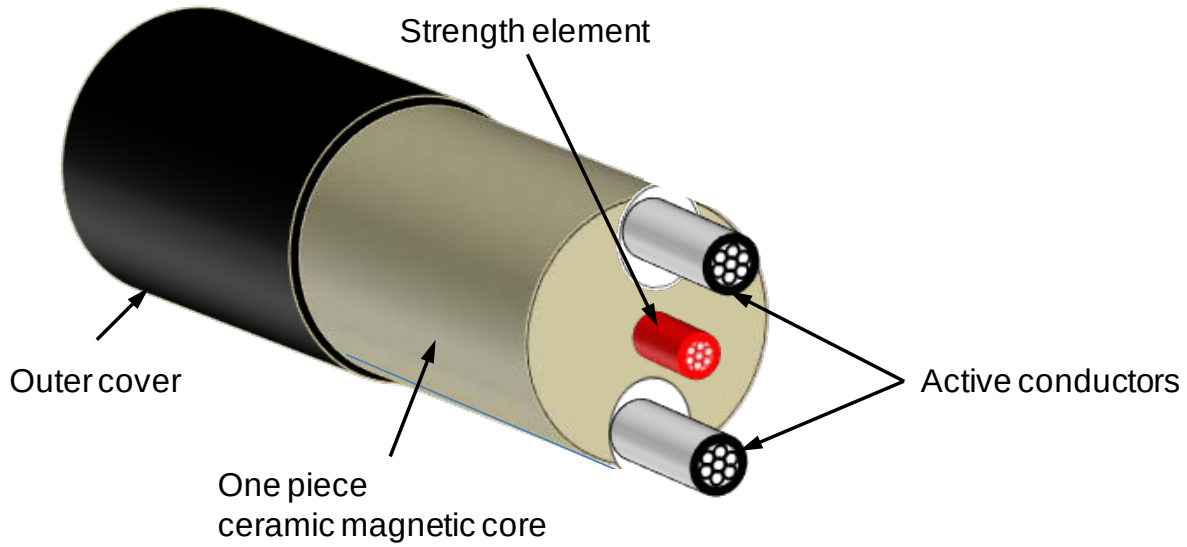


The system also functions as a microphone, with a "listening" operation implemented in the system, allowing the operator to audibly interpret the activity taking place at the fence line. But the reality, like all of the "listen-in" type systems, is that it requires very low levels of background noise, considerable training of staff, and constant real-time human monitoring to be of any value.

Ceramic Magnetic:

The strain sensitive ceramic magnetic cable operates in a very similar fashion to the Magnetic Polymer system. However, instead of a two part magnetic polymer centre core, it uses a single piece ceramic magnetic core, and two insulated wires (active conductors) in grooves 180° apart in the core. These wires move due to the vibrations and stress on the fence fabric, and the movement of the wires within the grooves of the static magnetic field created by the ceramic magnetic core generates minute electric signals.

The processor then compares the signals and generates an alarm if it's outside the pre-calibrated parameters.



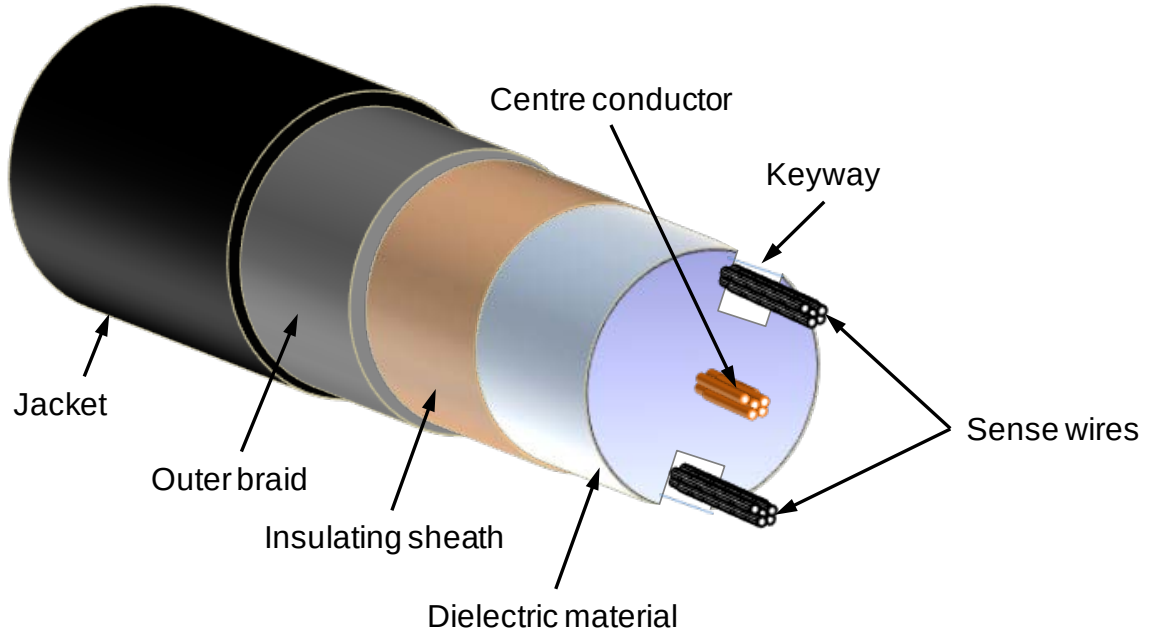
The system also functions as a microphone, with a "listening" operation implemented in the system, allowing the operator to audibly interpret the activity taking place at the fence line. But the reality, like all of the "listen-in" type systems, is that it requires very low levels of background noise, considerable training of staff, and constant real-time human monitoring to be of any value.

TDR or Time Delay Reflectometry:

The centre conductor and the braided outer conductor form a regular coaxial cable. Narrow keyways are formed into the dielectric material and two small sense wires are inserted into those keyways. These sense wires move freely in the keyways, and so move relative to the centre and outer coaxial conductors corresponding to the vibrations and stress on the fence fabric that the cable is attached to, such as when an intruder climbs the fence.

A short rise time pulse is transmitted down the coaxial cable through the centre conductor. If the sensor cable is of uniform impedance and properly terminated, the entire transmitted pulse will be absorbed in the far-end termination and no signal will be reflected. However, any movement of the sense wires with respect to the centre conductor changes the cable impedance causes some of the incident signal to be reflected back to the controller. This is similar in principle to radar.

When there is a disturbance on the cable such as an intrusion, the movement of the sense wires will cause a change in the energy reflected, and this can be measured as a changing signal from ambient or background levels to detect the disturbance. How much energy is reflected will depend on the position of the sense wires in their slots. Locating the disturbance is achieved by measuring the time difference between transmitting and receiving reflected pulses from the cable to localise the disturbance.



Applications: Can be used on a range of fence types including chain link, weldmesh, palisade and anti-climb fencing. The sensor cable is usually fixed to the fence using UV resistant cable ties around the midpoint between the top and bottom of the fence. These sensors can also be fixed to perimeter walls to detect intruders breaking through the wall.

Zone lengths can be up to 350 metres, but realistically should be in the 100-200 metre range.

Strengths: Very sensitive. Easy to install with a high POD on a range of fence types. TDR system can locate the point of intrusion.

Weaknesses: Highly sensitive to EMI, RFI and Lightning in the proximity of the sensor. The microphonic feature is of questionable value. All of these sensors rely on the free movement of the sensing wires within the cable. Anything causing these wires to bind or not move freely – excessive heat, moisture, tight installation, etc. will dramatically reduce the sensitivity of the system. All require electronics and power to be installed in the field, adding considerably to the installed cost.

Potential Causes of Nuisance Alarms: Poor quality fence construction, tree branches, animals and adverse weather such as wind; rain, snow etc; – in fact anything that can cause the fence to vibrate or rattle can trigger the sensors. Sensor runs parallel to power cables or other sources of EMI such as transformers, high current switches, electric motors, high power cables etc. may cause interference and nuisance alarms.

Methods of Defeat: As with most other fence-based sensors, bridging over or tunnelling under will bypass the sensor. Careful or assisted climbing, particularly at the more rigid turn points, may not produce the activity level required for alarm activation. An intruder with knowledge of the system and its limitations may be able to climb the fence undetected.

ELECTROSTATIC OR CAPACITANCE SENSORS

Description: Electrostatic or Capacitance sensors generate an electrostatic field around a series of parallel wire conductors. Sense wires installed parallel to the field wires then detect any disturbance of this electrostatic field caused by someone approaching or touching the fence. These are volumetric sensors that detect intruders before they reach the fence.

Operating Principal: The sensor consists of an AC (Alternating Current) field generator which creates an electrostatic field on a series of field wires that run parallel to the ground. Some of these wires are used to create the field, and some of the wires are used as the sense or detection elements. Whenever an intruder enters the field, his or her body capacitance creates an imbalance in the electrostatic field; the processor detects this change in signal from ambient conditions through the sense wires and generates an alarm. The wires can be mounted on free standing poles, walls, roofs, fences and other structures to provide a high, narrow field of detection.

To reduce false alarms, typically three parameters must be met to indicate an alarm: consisting of amplitude change (the size of the intruder), the rate of change (how fast the intruder is moving) and the time the intruder is in the detection field. Once all of these conditions are met, the processor then generates an alarm to the security management system.

Application: The field disturbance sensors are mounted on either freestanding posts, standoffs attached to an existing fence, or on the top of a fence or wall (most commonly on outriggers). All the wires are mounted parallel to each other and to the ground, to achieve uniform sensitivity along the fence length. Special springs are used at the connectors to ensure excessive wind vibrations do not cause false alarms.

As this type of system is effectively a proximity sensor, in some cases bridging and tunnelling can be detected depending on how large the generated field is, and how close the activity is to the sensor wires. However, the increased sensitivity required for this typically has a trade-off with increased nuisance alarms. This type of sensor should be considered if bridging or tunnelling are expected intrusion tactics.

Good earthing of the system and insulation of the sense wires is critical to reduce nuisance alarms. Nearby metal objects such as the fence fabric must also be grounded; poor or intermittent grounds will cause nuisance alarms.

Adverse weather conditions such as rain, snow and lightning can disturb the generated field and create problems. Vegetation and animal movement along the fence line will also cause alarms.

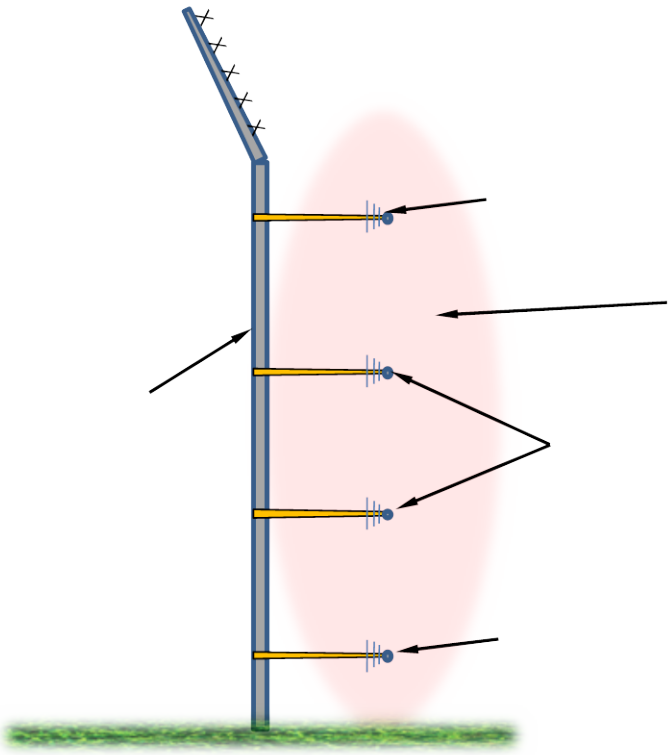
Strengths: Resilient to wind and ambient noise, low maintenance, can be mounted on fences, walls & roofs, or stand-alone, and has a high probability of detection. Detects intruders before they reach the fence.

Weaknesses: Expensive to install and high maintenance. Requires power, communications, and electronics to be installed in the field.

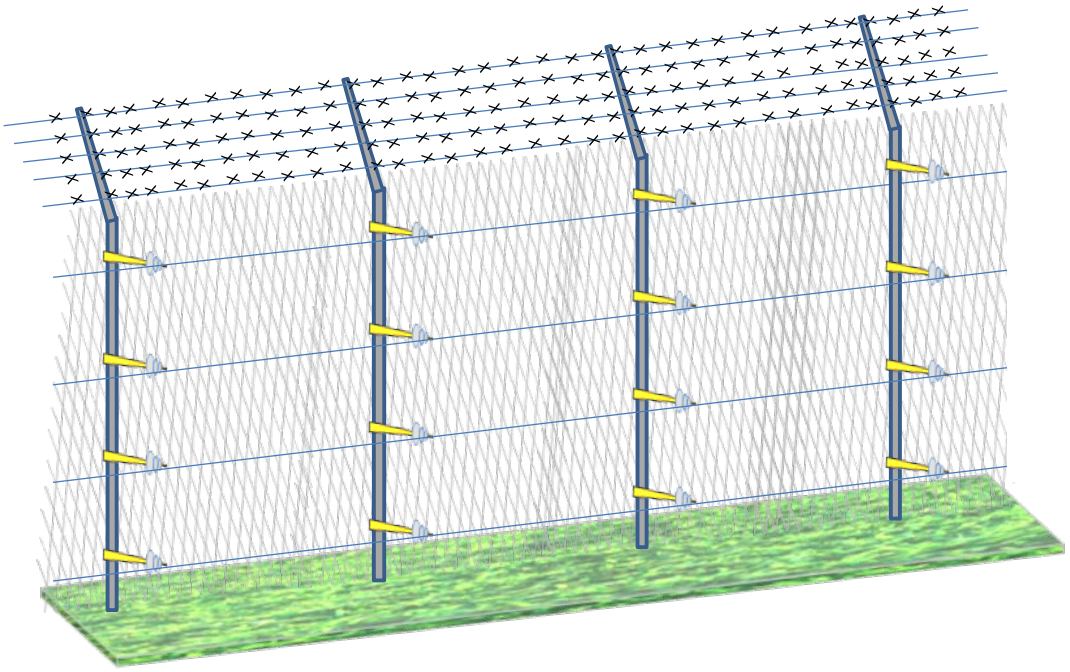
Potential Causes of Nuisance Alarms: Anything causing excessive fence movement such as wind; rain, snow etc; as well as birds and animals, or vegetation that impinges on the electrostatic field or lightning. If there is a public path or road on the outside of the fence, pedestrians or traffic may cause nuisance alarms if the field is sufficiently large.

There is a high level of maintenance required to assure the capacitive characteristics of the fence remain within specification – specifically changes in the insulation of the wires due to dust, moisture etc.

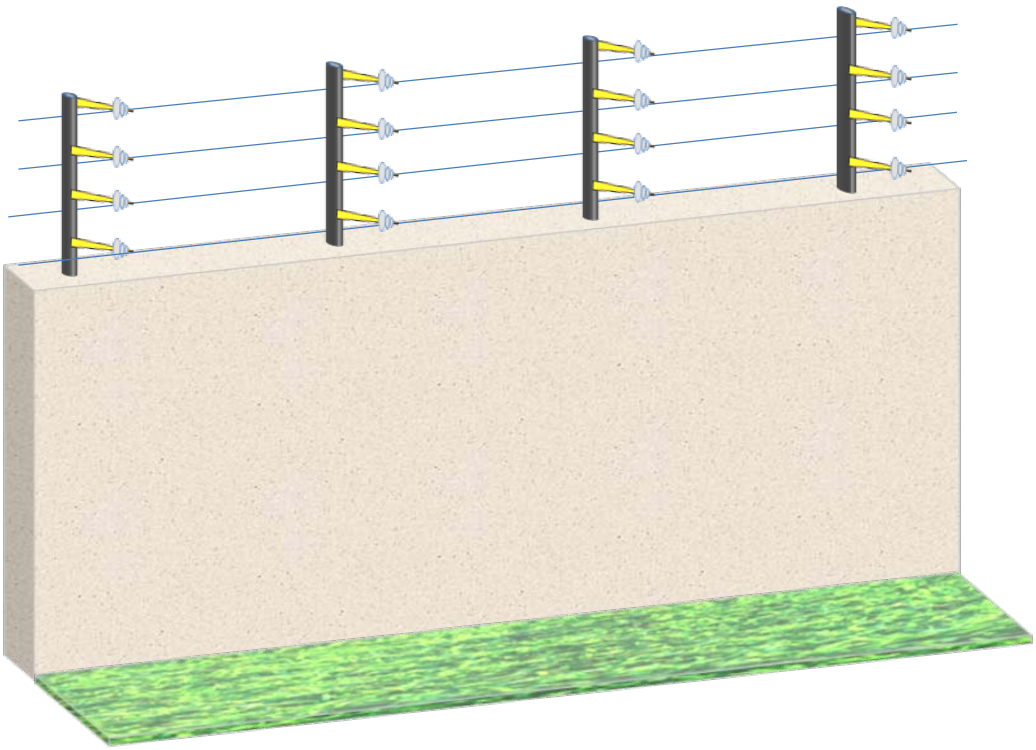
Methods of Defeat: Tunnelling below or bridging over the fence.



How it works



A typical fence mounted installation



A typical wall mounted installation

BURIED SENSORS

BURIED FIBRE OPTIC SENSORS

Description: Passive fibre optic sensors can also be used as a buried pressure-sensitive detection system. To ensure the intruder treads on the ground above the fibre and is detected, the fibre is often woven into a grid or laid in a serpentine pattern, and buried just below the surface at a depth of a few centimetres.

Operating Principle: There are two main technologies currently employed for this application – 'Speckle Pattern' systems and Microstrain systems.

With 'Speckle Pattern" technology, light from a laser is sent down a single multimode fibre, and the returned light is compared to determine if there are any "speckle pattern" changes due to the micro bending of the fibre optic cable caused by external pressure on the cable such as somebody walking over it.

The newer Microstrain technologies are more sensitive than 'Speckle Pattern' systems, achieved by using a principal of detection called interferometry. They combine the signals of two single mode fibres within the same buried sensor cable and when an adequate alteration in the resulting light pattern takes place such as when someone walks above it, an alarm is generated. By timing these signals some systems can also calculate and provide the location of an incursion rather than just the zone. With interferometric based buried systems, the cable is normally laid in a serpentine pattern rather than attached to a grid, reducing installation time and costs.

Applications: Deploying a buried fibre optic intrusion detection system involves a number of steps to ensure a reliable system with optimal performance is delivered – planning, installation and configuration. This technology is sensitive to ground vibrations and seismic events, so either avoid those installations where these occur such as close to major roads, trees, light pole, railways, construction sites etc. or install the sensor cables in gravel to isolate them from these ground based seismic events.

Try and avoid burying the cable directly in soil, as when the soil compacts over time, the sensitivity and thus the POD will decrease. When the sensor cable has to be buried in soil or under a lawn, very little motion or pressure is transmitted to it. Intruders must step directly on top of the cable in order to be detected.

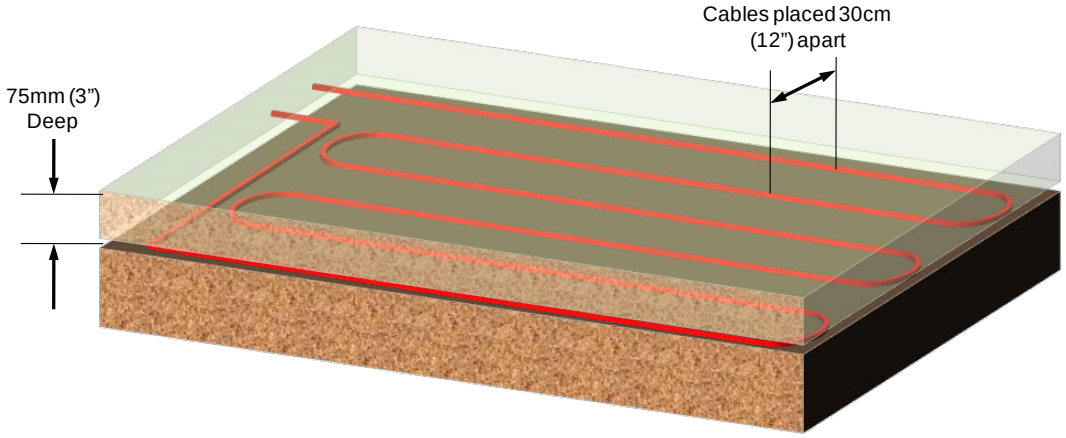
The installed area must be well drained to prevent pooling of water that may freeze in winter, or compaction of the soil that will reduce sensitivity. Wind and water erosion may either expose the cables or bury them deeper than is optimal for good sensitivity. The most effective application for this technology is buried in gravel in a sterile zone between two fences.

Strengths: Covert protection, difficult to defeat, and low maintenance requirements.

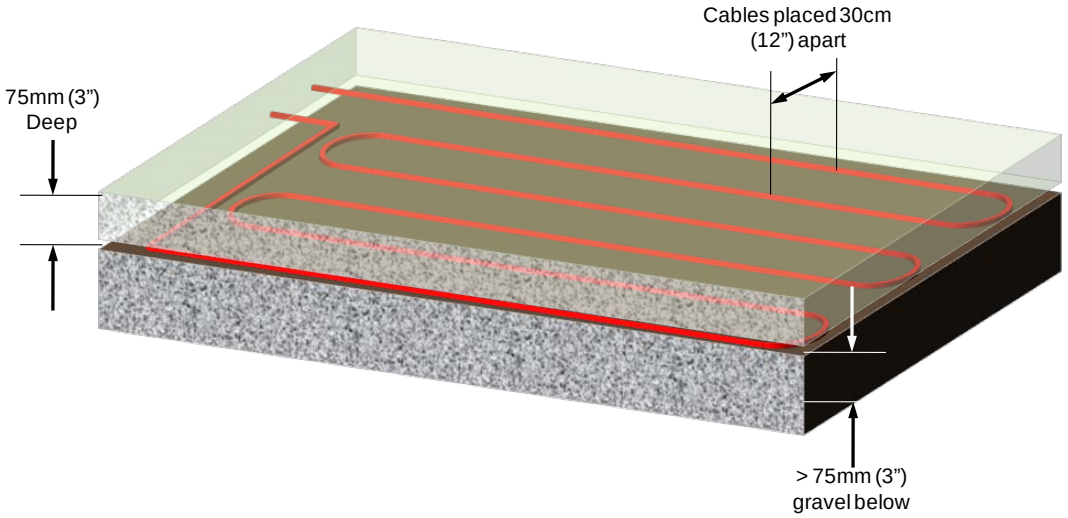
Weaknesses: Heavily dependent on the soil conditions for performance. In other than gravel, you virtually have to tread directly on top of the sensor cable to be detected. Requires power an electronics to be installed in the field for some systems.

Potential Causes of Nuisance Alarms: Seismic vibrations, large animals crossing, or animals digging in the detection area.

Methods of Defeat: Bridging over the protected area will bypass the system.



Installation in Soil – Speckle Pattern



Installation in Gravel – Speckle Pattern

PORTED OR 'LEAKY' COAX BURIED SENSORS

Description: Ported or 'leaky' coax sensors are coaxial cables that have small, closely spaced holes or slots constructed in the outer shield. In one cable, these openings allow electromagnetic energy to 'leak' and radiate a short distance, while the other cable acts as a receiver. These emissions generate an electromagnetic field which is disturbed when an intruder approaches.

Operating Principle: The system requires two ported coax cables - one to transmit and the other to receive (although some systems incorporate both sensors in a single cable - the two cable system has a bigger detection field, whereas the single cable system requires just a single trench). The cables are normally laid 1-2 metres apart and will provide a detection zone up to 2 metres wider than this and about 1 metre above the ground. Processors send either a pulse or continuous stream of RF energy through one of the cables creating an electromagnetic field, and receive it through the other. The speed at which the pulse travels is constant, creating a standard amplitude signature that is picked up by the signal processor. This signature is stored and continually updated to account for gradual changes in the soil and environment.

When an intruder or vehicle disturbs the field an alarm is generated. Intelligent signalling processors eliminate many causes of false alarms such as small animals etc.

Applications: Where covert detection is required and where fence mounted protection would be unsuitable. The cables are normally buried in the ground to a depth of about 25cm, and depending on the soil density, creates a field approximately 1 metre above the ground and around 3 metres wide. The size of the detection zone will vary depending on cable separation distance and the characteristics of the soil - soils with a high salt or metal content will reduce the sensitivity and therefore the detection zone size. With this sensor cable, zone lengths can extend up to 200 metres.

Never install cables under metal fences, reinforced concrete or other objects. If water pipes, electrical cables or other utilities must travel through the detection field, then they should be buried at least one metre below the ported coax cable. When installing the cables parallel to metal fences or near metal light poles, the cables must be positioned 4 metres away from these objects to minimise nuisance alarms caused by the motion of these in the wind.

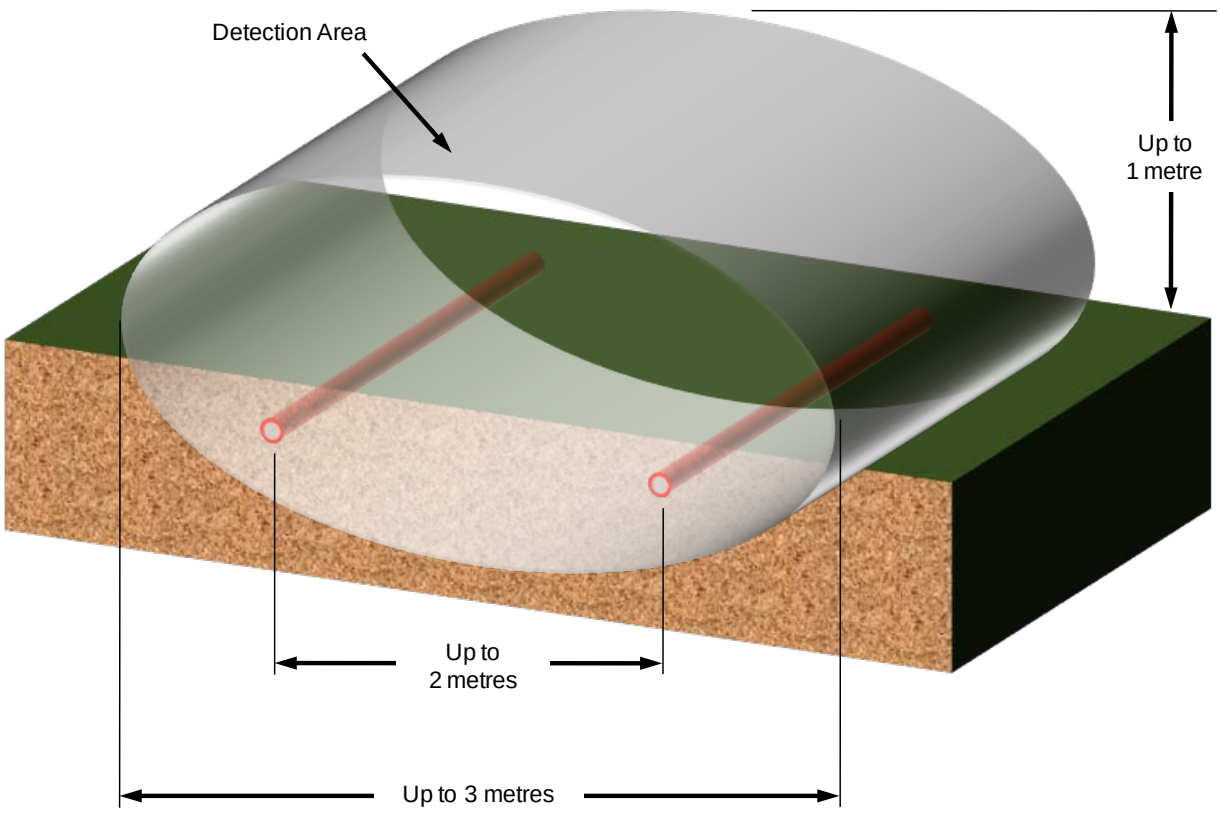
Pools of water above the cables may also cause nuisance alarms – especially as the wind blows and the water ripples. The ground surrounding the sensor cables should be carefully graded to eliminate water pooling and provide adequate runoff. The trenches must have very consistent spacing and depth.

Strengths: Covert volumetric protection, high POD, low maintenance requirements and few nuisance alarms if installed correctly. It is not sensitive to ground vibrations. The cables can be buried in any medium such as soil, sand, clay, concrete or asphalt.

Weaknesses: Sensitive to nearby pools of water, metal objects, and electromagnetic interference. Needs to be installed at least 5 metres from passing traffic, and 3 metres from fences and pedestrians. Controllers installed in the field require power and communications links.

Potential Causes of Nuisance Alarms: Large animals, metal fences, signs or other moving objects in the detection field, underground streams, flooding, nearby vehicles, and pools of water. Being an active radiating device, ported coax sensors will be affected by RFI, and EMI emanating from sources such as electrical equipment, power generation, or electrical sub stations and should not be used in close proximity to these.

Methods of Defeat: Deep tunnelling (below 1m) or bridging.



Typical installation and coverage for a Leakey Coax system

BALANCED BURIED PRESSURE TUBE SENSOR

Description: A balanced buried pressure line sensor is a passive in-ground system that detects low frequency vibrations and ground pressure. These pressure waves are typically caused by an intruder or vehicle moving across the area where the sensors are buried.

Operating Principle: This technology is based on the detection of differential pressure. The pressure sensors consists of 2 or more soft parallel tubes buried along the perimeter, filled with liquid and a system for regulating and monitoring the differences in pressure between them. Attempting to cross the protected area creates a difference in pressure between the tubes that is detected. Differential sensing helps reduce nuisance alarms caused by background events.

When an intruder passes over the detection zone, the ground compresses slightly under their weight. This creates a small difference in pressure between the two buried tubes that is detected and processed by the pressure sensing unit. It detects this pressure differential in both tubes and generates an electrical output that is proportional to the pressure exerted. When the differential between the two tubes exceeds a predetermined threshold, the analyser generates an alarm signal.

Application: The detection area is created by burying the parallel tubes approximately 1 metre apart. Depending on the nature and composition of the soil, it will give you a detection zone about 3 metres wide and up to 100 metre long. The depth at which the tubes are placed depends on the composition of the medium in which the tubes are placed. Normally, 25cm is sufficient for earth and sand. When installed, they are covert.

Soil with an asphalt covering requires tubes to be placed at a more shallow depth of 10 – 20cm. When working with a concrete surface/area, the sensor tubes should be buried just below the base of the concrete. Installing under concrete will definitely reduce the sensitivity, possibly to a level where only vehicle and not pedestrian traffic is detected.

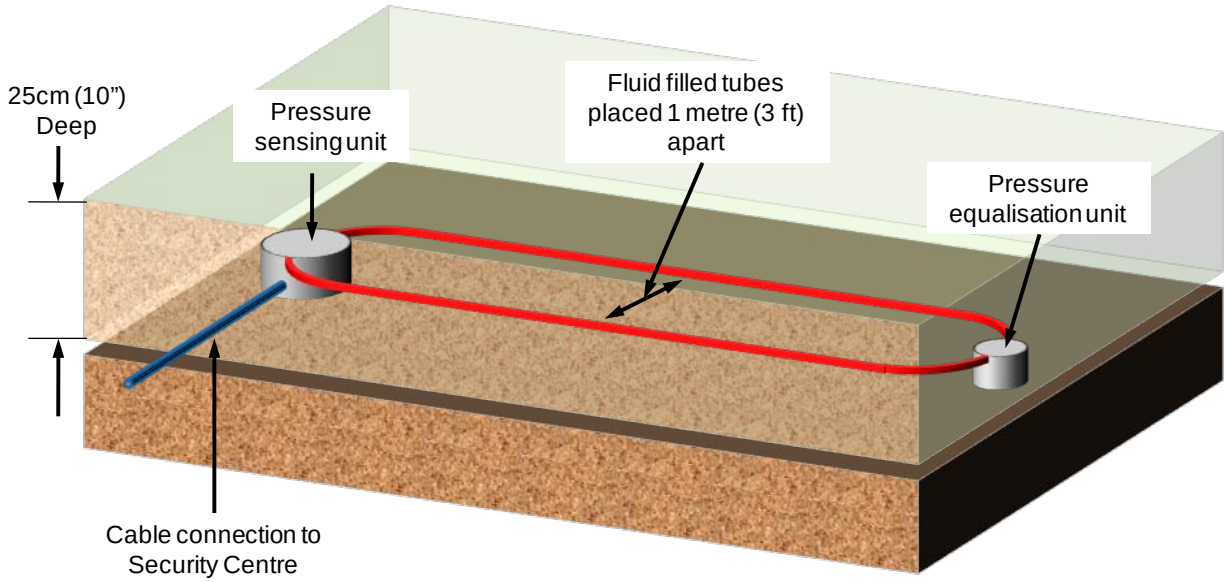
The system has a high degree of immunity to typical environmental noise and weather conditions. However, areas with heavy snowfall (and/or shifting sand) may have trouble with the system properly detecting, depending on the depth and composition of the snow/sand.

Strengths: Largely unaffected by environmental noise and weather.

Weaknesses: Nearby trees, fences, light poles, and telephone poles can pose nuisance alarm problems when moving in high winds. Requires power to be installed in the field.

Potential Causes of Nuisance Alarms: Improper installation or calibration can cause background activity to be interpreted as intrusion. Also, proximity to heavy traffic or seismic activity can cause nuisance alarms.

Typical Defeat Measures: Avoiding the detection area or bridging over the detection area with a plank.



Typical installation of a pressure tube sensor

BURIED GEOPHONES

Introduction: A buried geophone converts ground movement or low frequency vibrations into electrical voltage. Measuring the variations in the electrical current determines the intensity of the vibration. Any deviation of this measured voltage from the background level is called a seismic response and corresponds to someone or something crossing through the detection area above the sensors.

Operating Principle: A single geophone consists of a permanent magnet suspended by a spring in a conductive coil. Any vibration or movement causes the magnet to move relative to the coil, and generates an electrical voltage proportional to the velocity of the magnet. A processor will then analyse this voltage, and if it exceeds predetermined background levels, will cause an alarm.

Application: For perimeter intrusion detection applications, single geophones are rarely used. Instead, they are typically installed in a string or array of between 20 and 50 geophones. They are buried 15 to 35cm deep and are usually spaced around 2 to 4 metres apart in stable, compacted soil. Preferably geophones should be installed between layers of compacted sand, as compact sand is a very good conductor of vibrations. Loose or inconsistent soil causes significantly reduced sensitivity

Any installation comprises two elements - a signal processing unit, and a string of geophone sensors. The geophone sensors detect the vibrations created by walking above its location, and send these signals to the processor for analysis. When the characteristics of the signal satisfy the criteria, an intrusion alarm is generated.

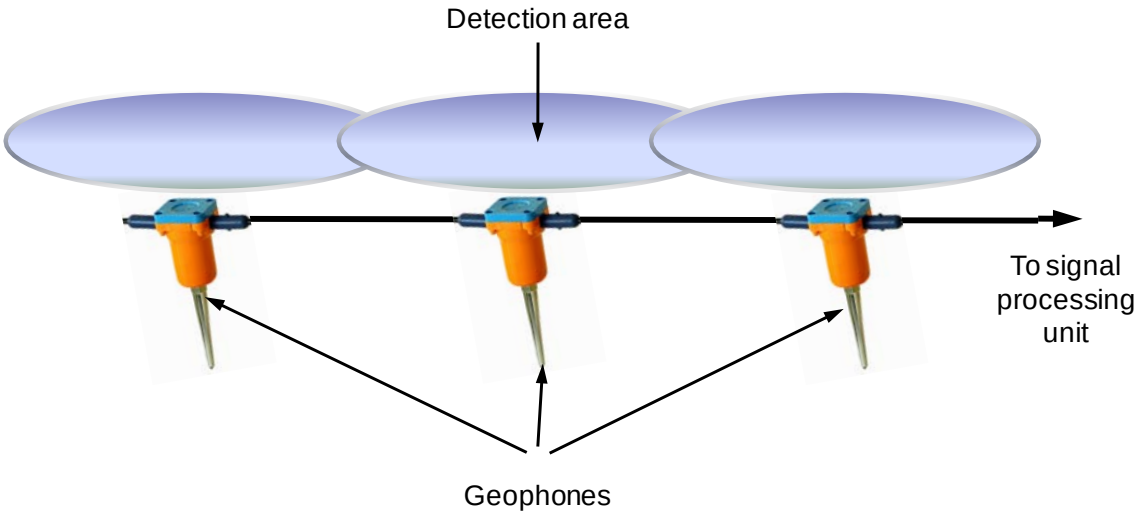
Strengths: Can detect very low levels of seismic energy so can be used where a high detection probability is required

Weaknesses: Nearby trees, fences, light poles, and telephone poles can pose nuisance alarm problems when moving in high winds. Also, proximity to heavy traffic or other seismic activity can cause nuisance alarms. Requires power and communications infrastructure in the field.

Potential Causes of Nuisance Alarms: As geophones can detect very low levels of seismic activity, nearby trees, fences, light poles, and telephone poles can pose major nuisance alarm problems when moving in high winds. For these reasons, geophones should be installed at least 10 metres from trees, 3 metres from fences, and at a distance equal to the height of any nearby poles. Also, large animals passing through the detection zone can generate a nuisance alarm.

Methods of Defeat: Bridging over the sensors will bypass the system.

A single Geophone device



Geophones installed in an array to protect a perimeter

VOLUMETRIC SENSORS

MICROWAVE SENSORS

Description: Microwave sensors are volumetric motion detection devices that flood an area with a high frequency field. Any movement within this area disturbs this field and sets off an alarm.

There are two basic types of microwave sensors - monostatic sensors, which have the transmitter and receiver encased within a single housing to protect a well-defined detection zone, and bistatic sensors, where the transmitter and receiver are housed in separate units. Bistatic sensors protect larger areas than a monostatic unit, and are typically used where multiple sensors are deployed. However, Bistatic units are somewhat limited by poorly defined detection patterns.

Operating Principle: Microwave sensors transmit microwave signals in the "X" band up to 150 metres in an uninterrupted line of sight. The detection of an intrusion is directly related to a change in the received frequency caused by any movement within the field of coverage (known as the Doppler shift effect). Most sensors are tuned to measure the Doppler shift between 20 Hz and 120 Hz to detect the movements of humans. Intrusions that fail to produce a signal or produce a signal outside this programmed frequency range are ignored. Any intrusions that fall within this range will generate an alarm signal.

Application: Microwave sensors can be used to monitor an open area or along the inside of a perimeter fence line. In situations where a well-defined area of coverage is needed, monostatic microwave sensors should be used. However, monostatic microwave sensors are limited to around 150 metres coverage, whereas bistatic sensors can extend up to 500 metres.

Typically microwave sensors would be employed either along a sterile zone between two fences, on the inside of a perimeter fence in a long narrow beam, or protecting open areas inside the fence line in a broad 3-dimensional fan shaped beam. Some models are also suitable for a rapid deployment or temporary PID solution around parked aircraft for example.

It is important to understand that Microwave sensors require an open area, so do not use these in areas where vehicles may park as the vehicle movement will generate an alarm, and the vehicles will also provide a microwave shadow that will allow intruders to go undetected.

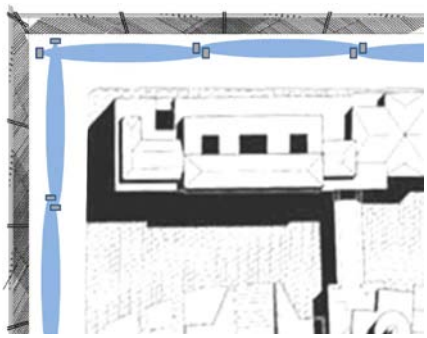
Video Motion Detection (VMD) equipment or another type of complimentary sensor system is often installed to verify intrusions, giving security staff the ability to better assess alarms and discriminate actual intrusions from nuisance alarms.

Strengths: Large area (up to 500m with a Bistatic sensor), volumetric protection, difficult for potential intruders to determine the exact area being protected, and quick to deploy.

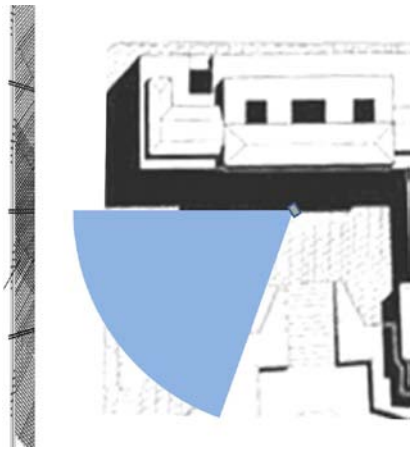
Weaknesses: Potential for blind spots and reflections off nearby objects. Sensitive to both EMI and RFI. Not suitable for uneven terrain. Requires power and communications to each device.

Potential Causes of Nuisance Alarms: External sources of RFI (Radio Frequency Interference - radio transmitters etc.) or EMI (Electromagnetic Interference - large electric motors or generators, power plants etc.), moving objects and debris in the detection field especially if windy conditions exist, movement of mounting posts the sensors are attached to, and reflections off nearby metal or solid objects. Pools of standing water for bistatic sensors

Methods of Defeat: Slow rate of movement through the field; blind spots caused by uneven terrain, hollows, or shielding; tunnelling beneath the protected area or bridging above the field.



Typical perimeter security coverage using bistatic microwaves. Note how each of the coverage areas (in blue) overlaps to prevent dead zones and to protect the microwave equipment in the adjacent zone from being tampered with.



Typical security application and coverage using a monostatic microwave unit. Note the coverage area in blue.

As you can see in this picture, the parked truck will create a blind spot for a Microwave system placed on the inside of this perimeter fence

ACTIVE & PASSIVE INFRARED DETECTION SYSTEMS

Description: Passive infrared sensors detect energy generated by external sources, particularly the thermal energy emitted by people in the far-infrared range. Active infrared sensors generate a beam of modulated infrared energy and react to a change in the modulation of the frequency, or an interruption in the received energy when an intruder passes through the area protected by the beam.

Operating Principal: Passive infrared simply detects the thermal energy of an intruder, much like a thermal camera and alarms on the movement of the thermal image.

An active infrared sensor system however is made up of two basic units, a transmitter and a receiver. The transmitter generates a multiple frequency *straight line beam* to the remote receiving unit, creating an infrared fence between the transmitter and the receiver. The receiver converts this infrared energy to an electrical signal. The receiving unit monitors the electrical signal and generates an alarm when the signal drops below a preset threshold for a specific period of time. As an intruder passes through the field of detection he will interrupt the infrared signal, cause it to fall below the threshold value and generate an alarm signal.

Application: Active infrared sensors are line of sight devices that require the terrain between the two units to be level and clear of all obstacles or obstructions that could block the IR signal. Low areas in the terrain will create blind spots in the surveillance pattern while obstacles or obstructions will disrupt the coverage pattern. Typically, active infrared sensors are used in conjunction with a barrier fence which defines the perimeter to be covered. Sensor zone lengths can extend up to 350 metres each.

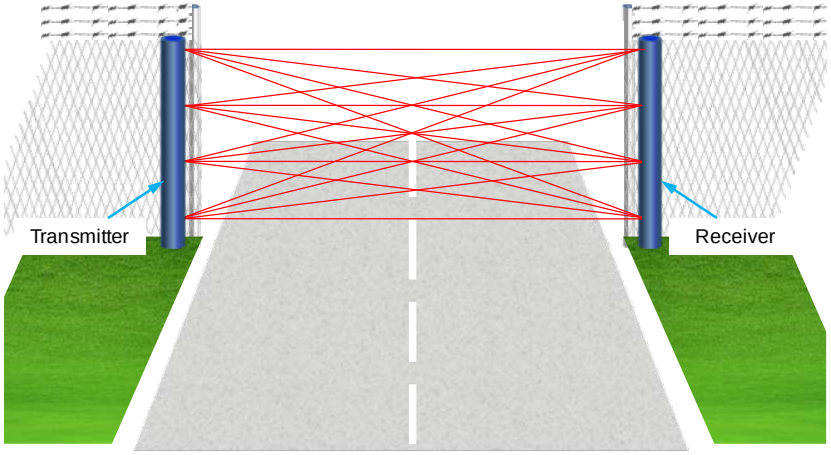
Infrared sensors are typically used to provide protection to opening gates and other fence openings in a multi beam configuration (for more reliable operation).

Strengths: Low cost, easy to deploy & maintain.

Weaknesses: Regular alignment of beams is required for optimal performance, and grass or other vegetation between the IR posts needs to be trimmed short on a regular basis. Have detection problems in fog and heavy rain. Requires power and communications to each post.

Potential Causes of Nuisance Alarms: Precise alignment of the transmitter to the receiver is critical for reliable performance. The detection beam is relatively narrow and requires regular calibration/realignment for optimal performance. Overgrown vegetation, stray animals, fog, heavy rain, snow, sand storms, moving objects, animals, birds and debris, movement of mounting posts, severe temperature changes can all cause nuisance alarms.

Methods of Defeat: The most common method of defeat is bridging over or tunnelling under the detection beams. As infrared detectors are line of sight devices, ensure that any dips or gulley's between the transmitter and receiver are filled to prevent blind spots where intruders can pass undetected.



An active infrared system would be used across a gate or fence opening.

To protect longer distances, active infrared sensors such as these are used.

Passive infrared sensors effectively ‘see’ the thermal image of the intruder. They alarm on movement of this thermal image.

VIDEO SENSORS

VIDEO MOTION DETECTION

Description: Video Motion Detection or VMD enables you to use a good quality CCTV camera to provide both intrusion detection capability, and as a means for security staff to observe intruders once they are detected.. Linked to a Digital Video Recorder (DVR), CCTV systems also provide video documentation of an intrusion event and the intruder. Higher quality systems also include an image tracking feature which can monitor a number of separate intruders simultaneously by drawing a different coloured line around each of them and leaving a trail line of where they have been.

***Operating Principle*:** Video Motion Detectors monitor the video signal being sent from the camera and detect changes in the monitored area by comparing the current scene with a pre-determined ambient scene of the area. When a sufficient change in the image pixels is detected - caused by some sort of movement in the field of surveillance - an alarm signal is generated, and the intrusion scene is displayed at the monitoring station.

When activated, most systems allow security staff to manually control the camera, (zoom, tilt and pan etc.) to better identify, verify and capture the intrusion activities.

Application: VMD can be an excellent addition to other detection systems especially for covering large or difficult areas. However, correct camera positioning, lighting conditions, and stability of cameras and the poles they are mounted on are all factors to be considered, as should striking a balance between the deterrent value of visible cameras and the monitoring value of concealed cameras - both have their merits. Often a complete installation will involve a mix of both visible and concealed cameras.

Areas with poor lighting or extended periods of darkness may give unreliable detection. Under these conditions either Infrared or Low Level Light cameras are recommended. In all applications, vegetation and obstructions in the field of view offer both a hiding point for intruders and potential sources of nuisance alarms. They must be eliminated or reduced to a point where they do not affect the probability of detection or performance of the system.

Strengths: Can be used with existing cameras without additional field wiring, can cover a wide field of view, helps security staff track intruders even in low light conditions, relatively low cost, easy to maintain.

Weaknesses: Lighting is required for 24 hour operation. Requires good quality cameras. Further development required to reduce the nuisance alarm rate before deploying at high security sites.

Potential Causes of Nuisance Alarms: Natural light sources including sun rise or sun set, sudden brightness variations caused by fast moving clouds, windblown debris, severe weather conditions, large animals, flocks of birds, blown debris, vibration of the camera or movement in the camera pole. Man-made light sources such as vehicle headlights, traffic lights, and security lighting switching on and off can also cause nuisance alarms.

Methods of Defeat: Tunnelling, blind spots within or moving beyond the cameras field of view, very slow movement, attack on or the blinding of camera.

Steady state picture of car park

Intruder appears and is recognised by the VMD due to the change in pixels and recording begins.

REFERENCES:

Perimeter Security Sensor Technologies Handbook 1997 – NISE East.

ALARM RECOGNITION AND DISCRIMINATION FOR FIBRE OPTIC INTRUSION DETECTION SYSTEMS

Dr. Jim Katsifolis
Chief Technology Officer
Future Fibre Technologies

Background

The success of any intrusion detection system is judged on three important parameters: the probability of detection (POD), the nuisance alarm rate (NAR) and the false alarm rate (FAR).
The most fundamental parameter, POD, is normally related to a number of factors which include: the event of interest, the sensitivity of the sensor, the installation quality of the system, and the reliability of the sensing equipment.

A nuisance alarm is any alarm which is not generated by an event of interest and by definition can include false alarms[1]. Nuisance alarms are typically generated by environmental conditions such as rain, wind, snow, lightning, wildlife and vegetation, as well as man-made sources such as traffic crossings, industrial noises and other ambient noise sources.

While the terms ‘false alarm’ and ‘nuisance alarm’ are often used interchangeably, an important distinction needs to be made. A false alarm refers to a type of nuisance alarm which is generated by the equipment itself rather than an event (intrusion or environmental) on the sensor. This essentially means that the system is generating an alarm when there is no event acting on the sensor and is usually a result of faulty or poorly designed equipment. While in some of the literature false alarms are categorised separately from all other nuisance alarms, for the purpose of this discussion, a false alarm will be considered to be a type of nuisance alarm.

Intuitively, it makes sense to have the ultimate sensitivity in an intrusion detection system to maximise the POD. Historically, this has led to an increase in the nuisance alarm rate as well, since the latter also depends on the sensitivity of the system leading to a performance trade-off between POD and the nuisance alarm rate of an intrusion detection system.

Traditionally, intrusion detection systems dealt with this trade-off by reducing sensitivity, or employing basic filtering and other simple algorithms in the presence of strong nuisance environments such as torrential rain, nearby traffic or strong winds. While this reduces the nuisance alarm rate, it also compromises the POD and the performance of the system especially when trying to detect an intrusion event that occurs simultaneously with a nuisance event. An example would be trying to detect someone climbing or cutting a perimeter fence during torrential rain or strong winds.

A more effective way to tip the balance in favour of the POD while maintaining low NAR/FAR rates is to employ advanced signal processing techniques such as event classification and nuisance mitigation whereby the performance and sensitivity of a system is not compromised to reduce nuisance alarms. This requires the intrusion detection system to be able to recognise the occurrence and nature of different events and be able to classify and discriminate between them.

The general area of signal recognition and signature analysis is a rich one and offers many possible techniques and tools. Many techniques are already in use commercially as has been demonstrated with biometric identification systems, biomedical signal analysis, speech recognition, imaging and telecommunications to name a few. It is important to understand that the key to signal recognition in intrusion detection systems is the signature analysis techniques used, that is, identifying unique features in an event signal to accurately classify it and discriminate it from other event signals.

FFT Microstrain Locator Technology

Future Fibre Technologies Pty. Ltd. (FFT) develops and manufactures advanced intrusion detection systems for the security industry. These intrusion detection systems employ standard optical fibre cables as truly distributed sensing devices.

Figure 1 FFT Secure Fence system

FFT's core products comprise the following advanced fibre optic intrusion detection systems: *FFT Secure Fence* for fibre optic perimeter intrusion detection systems (see Figure 1)*; FFT Secure Pipe* for oil and gas pipeline third-party interference detection; and *FFT Secure Link* for data communications security. FFT's intrusion detection systems have been employed in well over 100 sites worldwide and include such sites as military bases, government installations, petrochemical plants, refineries and many other high-value assets.

At the heart of FFT's core products is its field-proven Microstrain/Locator (M/L) technology. FFT's Microstrain/Locator technology is based on a distributed fibre optic MZ interferometer where the two interfering arms can be incorporated within the same or separate standard optical fibre cables (see Figure 2). The one sensing system performs both real-time detection and location of an intrusion event to within 75 feet for maximum lengths up to 50 miles long. It also includes an insensitive lead-in and lead-out fibre which can also be incorporated in the same or separate cables. This allows for maximum flexibility in sensing configurations.

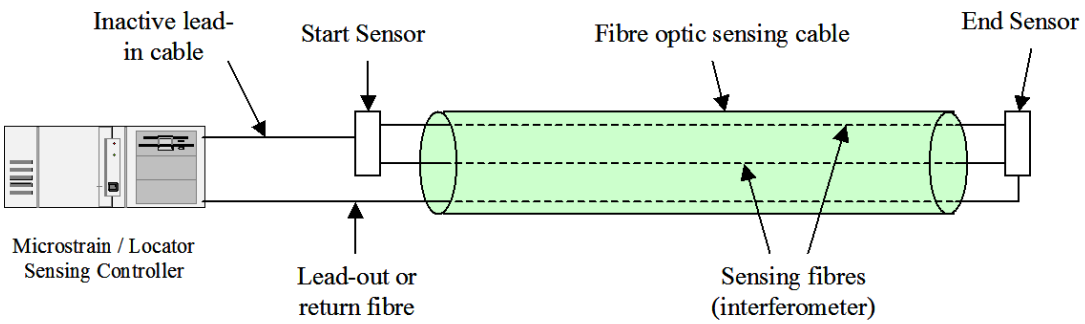


Figure 2 Block diagram of FFT Microstrain/Locator system

Implementing intrusion detection systems with optical fibre technology offers a number of distinct advantages over other technologies including being intrinsically safe, no power required in the field, being simple to install, offering high reliability and zero in-field maintenance, consistent over very long distances, and total immunity to EMI / RFI and lightning strikes.

Minimising Nuisance Alarms in FFT's Intrusion Detection Systems

By leveraging the advantages of using fibre optic sensing technology and combining them with over 10 years of commercial experience in designing and manufacturing reliable and high performance intrusion detection equipment, FFT provides intrusion detection systems which have a zero false alarm rate. This means alarms will only be generated when an event occurs on the sensing fibre.

To mitigate against environmental nuisance events, such as tropical downpours, FFT's intrusion detection systems are also capable of recognising a continuous nuisance signal, and automatically changing its alarming criteria to eliminate any nuisance alarms. This has repeatedly been demonstrated with numerous installations of FFT's Secure Fence system in areas with torrential tropical downpours in excess of 4 inches/hr.

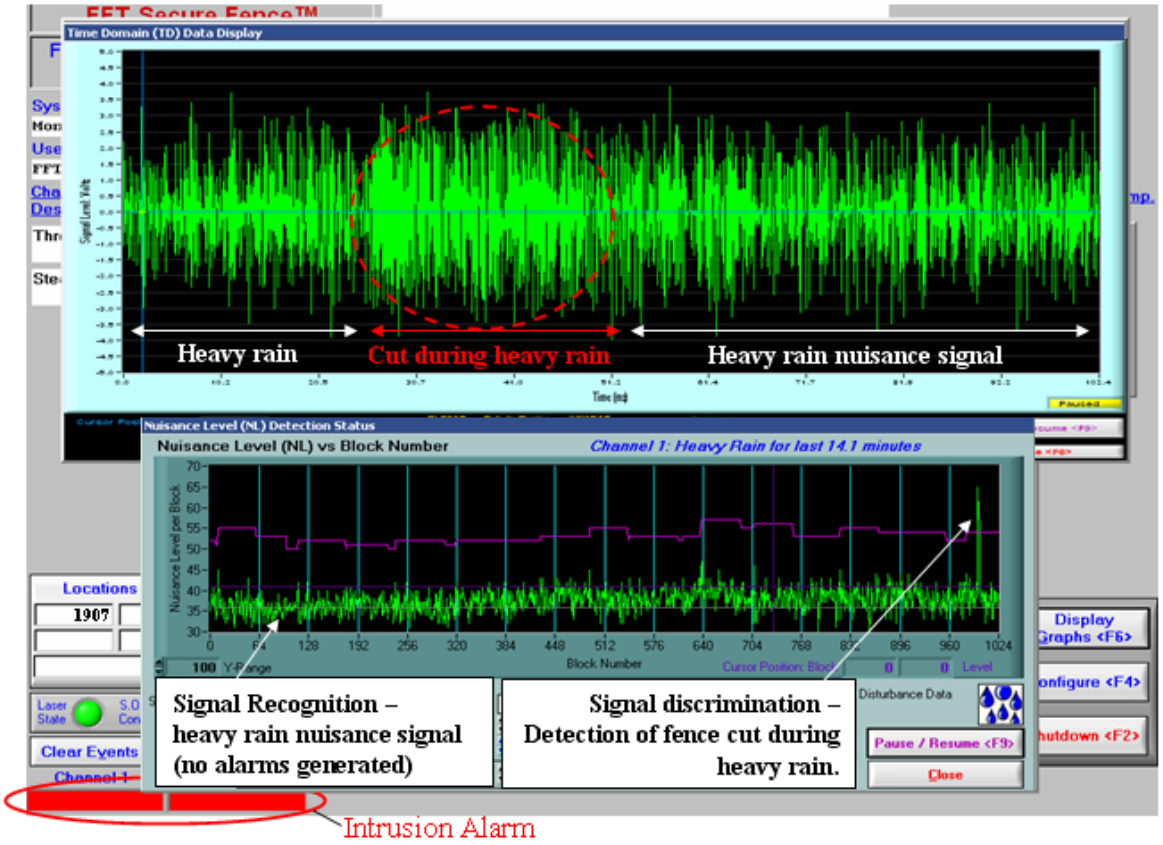


Figure 3 FFT Secure Fence Sensing Controller GUI showing the adaptive rain mitigation algorithm at work for a 2km fence perimeter during 4 inches/hr rain.

As can be seen in Figure 3, by recognising a signature in a 'rain' signal, FFT Secure Fence systems will arm themselves into rain mitigation mode and ignore a continuous nuisance signal. At the same time it maintains its capability of picking out a true intrusion signal during heavy rain without any loss of sensitivity, and processes this signal to alarm and locate the intrusion.

This nuisance mitigation algorithm is also adaptive and will adjust to varying levels of rain (or nuisance levels) but, importantly, does not lower the intrusion event sensitivity. Once the rain stops, the FFT Secure Fence is system able to recognise this and returns to its normal mode of operation. Using this technique rain-induced nuisance alarms can be minimised or even eliminated.

On Going Development in Event Classification and Nuisance Mitigation

FFT has a strong ongoing program for further developing new intrusion detection techniques and algorithms. It is continuing to develop algorithms for identifying and discriminating between different intrusion and non-intrusion events which will be integrated into future releases of their intrusion detection system controller software over the next 12 months.

For more information on Future Fibre Technologies go to www.fftsecurity.com

www.fftsecurity.com