The Boundaries of Security 2013

Global Trends in Perimeter Security

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

Future Fibre Technologies Pty Ltd
10 Hartnett Close
Mulgrave
VIC 3170
Australia

email: info@fftsecurity.com

Contents

1

INTRODUCTION

The purpose of this document is to provide security consultants, managers and specialists with basic information and up-to-date general background on commonly available and emerging perimeter intrusion detection sensing (PIDS) technologies, as well as information on the global perimeter security market. It includes a brief description of the fundamental PIDS properties, their differing capabilities, limitations, typical applications, strengths, and weaknesses. Causes of nuisance alarms and methods of defeat are also briefly discussed.

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 the technologies commonly in use today.

Having unprotected perimeters means unprotected assets, unprotected people, and inevitably, security breaches. The ramifications of these breaches can be catastrophic so the threat of intrusion remains a prime concern at all critical infrastructures and major facilities. As most of these perimeters are simply too long for conventional security patrols to cover practically or effectively, advanced perimeter intrusion detection systems have become the only answer.

In the past, perimeter intrusion technologies were prone to nuisance alarms with few systems providing tracking, assessment, or situational awareness capabilities, making it impossible for ground staff to identify the point of intrusion or escape in a timely fashion.

Today there is a diverse range of sensing technologies available for perimeter security, each varying in their effectiveness, affordability, and accuracy. So designing an effective and reliable outdoor perimeter security system these days is rarely a simple exercise. When evaluating any of the available technologies, the major requirements should be:

- system durability/reliability;
- minimal nuisance alarms;
- maximum detection capability;
- minimal maintenance;
- ease of use and understanding;
- ability to quickly and accurately pinpoint the location of intrusion; and
- ability to work with other existing and often complementary technologies.

Perimeter intrusion detection systems are based on the core principle of establishing a steady background state and continuously monitoring to detect any change above or below a predetermined threshold that indicates that an intrusion event has occurred. Like all technologies, these systems are constantly evolving. Although new and improved equipment is continually being developed around the world and introduced into the marketplace, rarely do these fundamental detection principles and applications change.

In recent years, there has been a steady move towards developing more sensitive intrusion detection systems, yielding a higher probability of detection (POD) of an intruder. A number of vendors have introduced fiber optic sensors using a range of detection technologies into their product offerings in an effort to address this demand for higher detection rates.

Of course, along with this increase in sensitivity comes an increase in nuisance alarms. Therefore, a significant amount of development today is on processing these raw alarm signals to reduce the number of nuisance alarms generated, that is, where an alarm condition is reported without an actual intrusion occurring. These nuisance alarms are typically caused by environmental conditions such as wind, rain, passing traffic, and lightning. Frequent nuisance alarms are both inconvenient and expensive to respond to, and quickly erode the confidence security staff have in the effectiveness and value of the intrusion detection system installed.

In the past, techniques employed to control nuisance alarms typically involved reducing the sensitivity of the detection system during times of high environmental noise such as wind and rain. Unfortunately, the significant trade-off by taking this approach is a reduced sensitivity to intrusions and therefore a reduced probability of detection during adverse weather conditions.

Today, techniques such as artificial intelligence (AI), neural networks, and advanced multi-parameter signal processing, are becoming the norm to dramatically improve the recognition of real intrusion events against background noise. This allows systems to minimize their nuisance alarms without trading off the sensitivity or probability of detection of attempted or actual intrusion events.

Don't underestimate the complexity of the signal processing currently being developed or deployed – until recently these technologies were confined primarily to the military and aerospace industries. Now they are emerging in the latest generation of intrusion detection systems. This document also outlines some of the signal analysis techniques employed and the dramatic impact they are having on nuisance alarm rates.

Regardless of the system selected, the need for adequate warning and a response mechanism for an unwanted intrusion is essential. It is not sufficient to simply know that a breach of the perimeter may have occurred, you need to have a system in place to assess and respond to it.

Perimeter security is all about the deterrence, detection, assessment, and delaying of the intrusion for a response to be initiated. Every application is unique in the type of facility to be protected, operating environment, perimeter fence construction, intrusion and security history, and perception of threats.

The protection of the perimeters of individual facilities needs to be tailored to suit the unique requirements of each site. Site layouts, sensitive areas, facility buildings, the surrounding environment, activity in and surrounding the site, local weather conditions, and topography are all factors to be considered when planning a perimeter intrusion detection system. These influence the detection technologies selected and subsequent overall system performance. Often the final intrusion detection solution will consist of several different but complementary technologies to form "layers of protection."

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 together with the perimeter intrusion detection system (PIDS) and the response mechanism – is to act as the first level of site protection. This defines the boundary of the site, providing both an early warning of intrusion attempts as well as deterring, detecting, documenting, and delaying any intrusion into the protected area.

The 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 standalone package. Correctly integrating various detection and assessment methodologies not only strengthens the systems detection and assessment capability, but also provides multiple overlapping security layers that support each other should one layer fail.

The main elements in the design of a perimeter intrusion detection system are:

- the design and construction of the perimeter fence;
- the actual intrusion detection sensor(s) installed in the field or on the fence;
- the alarm processor that drives and analyzes the raw sensor signals;
- the security or alarm management system that promptly notifies security staff of an alarm and the location of the detected activity;
- the communications infrastructure that ties these three elements together and connects the system to the security staff; and
- 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 along with a documented and implemented alarm response mechanism or procedure. Without the right staff to operate, monitor, and maintain the system, or a professional security team with an established response mechanism in place, the end result will almost always be unsuccessful regardless of which particular intrusion detection technology is installed.

Any security system is only as strong as its weakest link. The smart intruders rarely defeat the sensors or intrusion detection systems. Instead, they rely on poor alarm response procedures and mechanisms – the human element – to avoid getting caught.

Despite the economic challenges facing the USA and Europe, the world market for PIDS is expected to continue to grow at a steady rate. As part of this market growth, it is predicted that the increase in efforts and budgets to combat security threats and protect major facilities will also see more large system integrators entering the security market. We have seen a number of organizations forging partnerships with smaller niche product or technology specific companies to offer a broader range of products and greater benefits in the turn-key solutions they provide to the end user.

Intrusion detection technology will continue to advance, but these advances will be more focused around alarm and signal processing software rather than the sensing hardware as manufacturers continue to pursue improved system performance, flexibility, and reliability while reducing nuisance alarms.

We trust that you will find the information contained within this report to be of value and assistance in understanding the landscape of today's perimeter intrusion detection market, and selecting a technology and solution that is most appropriate for your particular application.

Alec Owen

International Client Manager

Future Fibre Technologies Pty Ltd

2

MARKET CHARACTERISTICS

The global perimeter intrusion detection market continues to evolve. The types of facilities to be protected, the current political environment, the perceived level of risk of a site to intrusion, the nature of the perceived threat, previous intrusion and security history, and the cost of insurance premiums continue to have an impact on the size and segmentation of the perimeter intrusion detection market.

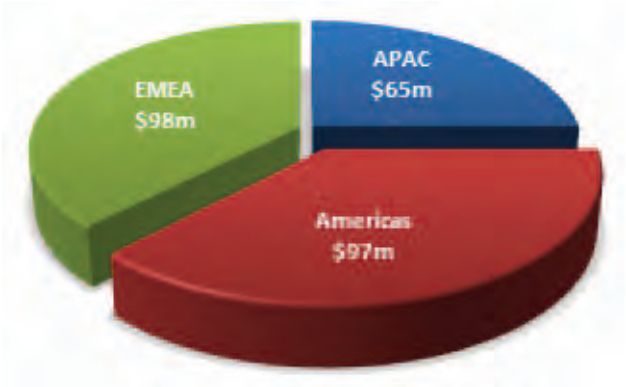
The following provides information on the competitive landscape of vendors, the key drivers fueling the growth in perimeter security, and examples of some of the higher profile perimeter security breaches that have occurred recently.

Three main factors are continuing to drive growth in the perimeter intrusion detection market – the increased threat of terrorist activity, government funding, and government legislation.

Existing nuclear power plants and other critical infrastructure sites typically have perimeter security already installed because of their inherent need for high levels of security. Nuclear plants in the United States and overseas have further increased their levels of security based on the recent NRDC security requirements. Other applications, such as airports, chemical facilities, water treatment plants and borders, have been slower to adopt perimeter intrusion detection on their sites. Government legislation will continue to play a major role in the growth of these applications as they are identified and mandated by Homeland Security as either high risk or critical national infrastructure, requiring enhanced levels of perimeter security.

ESTIMATED WORLD MARKET FOR PERIMETER SECURITY SYSTEMS

Industry revenue forecasts for 2013 are in the vicinity of $400 million for PIDS systems, with fence-mounted sensors accounting for more than 65% of this figure, and expectations are that revenue will continue to grow steadily at around 5% per year.



Industry forecast for fence-mounted PIDS systems by region for 2013

The market split for fence-mounted sensors is around 25% of this business will be in Asia–Pacific, and the remaining 75% evenly split between the Americas and EMEA.

Sales of fiber optic fence-mounted sensors continue to outstrip the sales of copper sensors, and recent announcements of fiber-based intrusion detection solutions by some previously copper only manufacturers further reinforce this market shift.

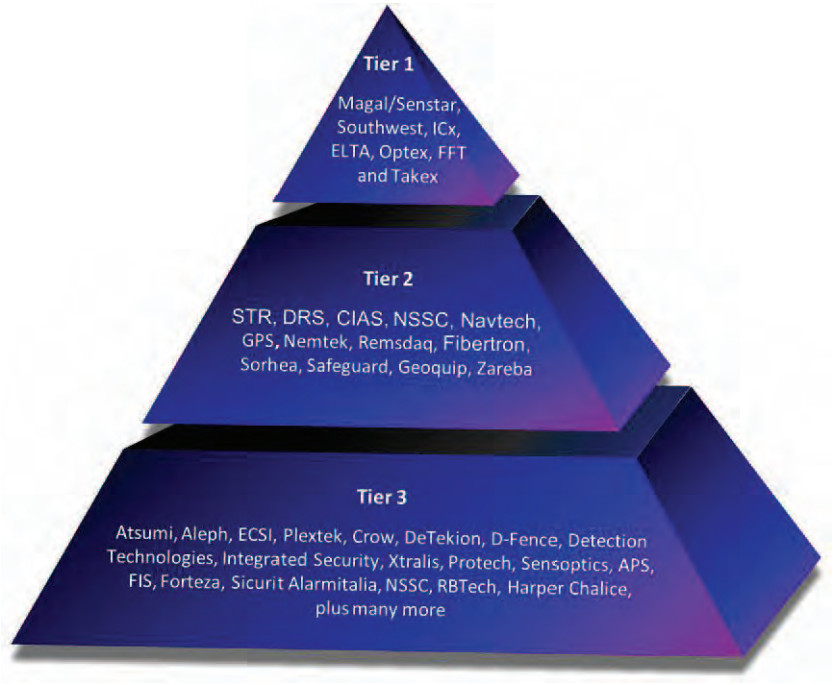
Evolving global politics, the threat of terrorism and various economic factors have all assisted in shaping the size and segmentation of the perimeter intrusion detection market today. As business becomes more competitive and resources scarcer, private industry – especially Oil and Gas – are operating in more remote and difficult geographic regions and higher risk environments, necessitating increased levels of security to protect their workers and equipment.

North America and Europe have traditionally led the way in perimeter security expenditure, however the longer than expected slowdown of these economies has seen reduced opportunities in this predominantly retrofit market, but a gradual increase in commercial construction in the USA over the last year should see opportunities for new installations arise in this market going forward. Growth continues to exist in the rapidly developing economies of Asia and the Middle East, tied mainly to the construction of new critical infrastructure to support their expansion. This growth will not be as strong as previously forecast due to a gradual slowing of the Chinese economy which, of course, will have a global impact. Regardless of the varying global economic situations, security will always remain important.

COMPETITIVE LANDSCAPE

The perimeter intrusion detection market is comprised of a number of companies offering varying ranges of products and services. The last year has seen the merging of several key players as well as cross-product partnerships. This has resulted in an expansion of the range of technologies offered by these vendors to the end user.

- Some manufacturers, such as Future Fibre Technologies (FFT), Detection Technologies, and others are highly specialized, offering just a single technology.
- Some vendors offer two or three technologies which may complement each other. For example, Sorhea offers infrared and laser open area sensors combined with thermal cameras.
- The remaining vendors offer a complete range of technologies, often supplementing their own products with others bought from other manufacturers and rebadged. This group includes companies such as Magal/Senstar, Geoquip, GPS, Optex, and Southwest Microwave.
- A small number of these companies, such as Magal/Senstar, NSSC and Integrated Security Corp, also negotiate with and sell directly to end users, even doing their own installations. This tends to be at odds with the traditional distribution channel strategies in the perimeter security market, at times causing conflict between the manufacturer and their integrators.



Perimeter intrusion detection market in 2013

KEY DRIVERS FUELING GROWTH IN THE PERIMETER SECURITY MARKET

Global social and political instability with the ongoing threat of terrorism will continue to drive the need to both fund and enforce regulation and legislation regarding perimeter security at critical national infrastructure sites including nuclear power stations, water reservoirs, data centers, transportation hubs, and historic landmarks. An increase in organized protest movements (environmental, political, climate, economic and the like) is also heightening the need for advanced perimeter security.

Legislation will continue to play a major role in the growth of perimeter security equipment along with stimulus monies and other regulation. Chemical, petrochemical, and liquefied natural gas (LNG) facilities have been identified as critical national infrastructure and subject to increasing government legislation and regulation in many countries. While the potential growth for perimeter security is large, typical government bureaucracy and delays in rolling out any project means the actual market growth will be at a more moderate and steady pace.

There will be increased demand for newer perimeter intrusion detection systems that require limited or no power in the field, especially for those remote locations and long distance applications where power is not readily available, making these installations more viable than in the past.

Growth in vertical markets is also due to the following:

- Government and military is seeing growth in the number of prisons, increased border protection, and in the number of military bases and camps.
- Recent well-publicized security breaches of airport perimeters around the world, as well as the building of new airports and airport expansion programs.
- Legislation and regulation of the security of petrochemical sites.
- Increased sea port security post 9/11 for illegal people movements and to address the International Ship and Port Facility Code (ISPS Code), although a large portion of the spending will continue to be on container screening.
- As industry demand for power increases, so does the drive to build more nuclear power plants. Each of these has to be protected from potential terrorist activity.
- New LNG production facilities being constructed to satisfy the increasing global demand for non-nuclear power generation especially in the wake of the Fukushima Daiichi nuclear disaster in Japan.
- Water treatment facilities have also been identified as potential risk sites where intentional acts may have a substantial impact on public health and safety.

- Conventional coal or fossil fuel power plants face the risk from activists, whereas solar power generation is subject to the theft of expensive solar panels. Security is also being upgraded on substations and switching yards.
- Other regional drivers such as political instability in the Middle East, increasing oil and gas prices, economic issues in the Eastern European markets as well as an increase in crime, terrorism and other security threats all fuel the growth in perimeter security.

Technological innovation

The last decade has seen new entrants and substantial advancement in perimeter intrusion detection technologies, increasing the reliability and accuracy of probability of detection (POD), lowering the number of nuisance alarms and greatly improving their performance (differentiating between intruders and environmental disturbances).

As the more traditional vendors continue to promote the legacy technologies they have been offering for many years, innovation has been driven by numerous smaller developers and manufacturers of niche technologies. The plethora of intrusion detection sensor systems now on offer and under development includes electromagnetic point sensors, geophone point sensors, fiber optic fence sensors, infrared beams, buried magnetic lines, fiber optic mesh, buried seismic lines, vibration sensors, and video event detection.

Globally, sales of fence-mounted fiber optic intrusion detection systems are estimated to be almost twice those of the traditional copper based microphonic and vibration based systems. This growth is impressive considering the comparatively short time that fiber optic PIDS have been available and the resistance to change within some entrenched sections of the security industry. The majority of growth has been in the newer global markets, with Europe surprisingly having the slowest take up of fibre optic based intrusion detection systems, possibly reflecting their highly conservative nature and entrenched existing manufacturers.

Surprising perhaps because many of these newer fiber optic technologies do not require any power or electronics to be installed in the field. This has made large or remote sites, such as airports, military bases, country borders, etc. that were previously thought to be too expensive to protect, far more economically achievable and within financial expectations.

Increased government spending on security, infrastructure, and alternative energy

To combat the ongoing Global Financial Crisis, governments around the world are continuing in their attempts to spend their respective economies out of a double-dip recession. This is likely to result in additional spending on new infrastructure projects and on the resulting perimeter security needs.

As more countries look toward renewable energy and reducing carbon emissions, solar and LNG power plant construction is forecast to increase. Since the events of 9/11, governments around the world have become aware of the need to protect their critical national infrastructure, which will of course require additional perimeter security equipment both now, and in the future.

RECENT HIGH PROFILE SECURITY BREACHES

NUCLEAR WEAPONS PLANT SECURITY BREACH

USA (July 2012) Before dawn on July 28, three activists, including an 82-year-old woman, entered the Highly Enriched Uranium Materials Facility (Y-12) at Oak Ridge, Tennessee. This security breach has led to a temporary suspension of activities where "all special nuclear materials will be moved to vault-type facilities on site, all nuclear operations will be halted, and contractor security personnel will undergo training and refresher instruction." The NNSA reviewed the incident and identified numerous problems:

- Surveillance cameras, including the camera watching the fence zone that was penetrated by the protesters, were not functioning.
- Despite numerous intrusion alarms, the guards failed to react as intruders cut through three security fences.
- Response by a vehicle patrol was slow.
- When the guards did arrive, they did not respond effectively to the intruders.
- Contractors responsible for security failed to coordinate effectively.

While some of the blame was due to equipment not being fully operational, the bulk of the responsibility comes down to the human element of the security "system".

AIRPORT SECURITY SCRUTINIZED AFTER UTAH BREACH

USA (July 2012) Gaining access to a plane was as easy as using a rug to scale a razor wire-topped security fence at a small Utah airport in the middle of night, slipping past security, and boarding an empty 50-passenger jet.

The Transportation Security Administration doesn't require airports to maintain full-time surveillance of their perimeter fences, leaving airport security largely in the hands of individual facilities. One aviation security expert said, "it might be time to revisit protocols aimed at securing airport perimeters."

"If you defeat one layer of security, there are supposed to be other layers in place to prevent criminal or terrorist attacks. Today, perimeter security at airports, it's just a fence. They're not required to have intrusion protection systems, and they're not required to have closed-circuit TV to monitor the fence because the current level of risk doesn't warrant it. But maybe that needs to be looked at."

WATER TREATMENT PLANTS A TARGET FOR TERRORISTS

USA (March 2012) Security experts say water treatment plants could be a top target of terrorists, but one night two drunken people stumbled past a gate and entered a secured water treatment facility. No alarms were tripped, and no one noticed until the intruders called for help after one of them fell into a water tank.

If they could get inside this 'secured' facility, what would happen if somebody with more sinister motives got in? It was one of only two facilities pumping drinking water to the entire city and certainly on the critical infrastructure list.

SECURITY BREACHES AT ROCKET PLANT TROUBLES SPACE OFFICIALS

Russia (December 2011) Five separate security breaches over the past several months at the state-run Energomash plant, which manufactures motors for civilian and military rockets, have Russian officials demanding change and promising to punish those who let the incursions happen.

A group of Russian bloggers claim they didn't encounter security guards on any of their night-time jaunts on the Energomash grounds. The multiple security breaches of this highly sensitive facility have startled and angered Russian officials, with the Deputy Prime Minister promising harsh punishment of intruders.

GREENPEACE BREACHES FRENCH NUCLEAR PLANT SECURITY

France (December 2011) Environmental group Greenpeace said it had exposed the "vulnerability" of French nuclear sites after its activists broke into an atomic power station near Paris before being arrested. French authorities admitted to security "lapses" after the incident and vowed a full investigation, denouncing the activists as "irresponsible."

The dawn raid saw nine activists sneak past security at the plant. Most were quickly arrested but two managed to evade capture at the plant for nearly two hours, authorities said. "The aim is to show the vulnerability of French nuclear installations, and how easy it is to get to the heart of a reactor," said a Greenpeace nuclear campaigner.

EDINBURGH AIRPORT SECURITY ALERT AFTER HOLE FOUND IN PERIMETER FENCE

UK (June 2011) Edinburgh airport was evacuated and hundreds of passengers delayed after a suspected breach of a security fence. Eleven planes had to wait on the tarmac for over an hour while around 500 people in the terminal were evacuated. Hundreds of incoming passengers were delayed up to 2 hours. Police have confirmed that a hole was discovered in the perimeter fence.

Police and airport security staff worked through the night to check the rest of the fence and to examine the airport grounds and runway for potential threats to aircraft. The hole in the fence was discovered by airport staff on a regular security patrol but they were unable to confirm when the breach had actually occurred.

AIRPORT INTRUDER CLIMBS OVER PERIMETER FENCE UNDETECTED

Australia (August 2010) Australian authorities are investigating a recent security breach at Melbourne Airport. The intruder climbed a barbed wire fence completely undetected before dawn on July 24 into the "airside" security area and then walked to the Virgin Blue hanger. He then pulled on a pair of staff overalls, stole a vehicle and drove for some time within the sterile area of the airport which encompasses the landing strip and terminal areas before being noticed and arrested.

GREENPEACE PROTEST AT SWEDISH NUCLEAR PLANT

Stockholm (June 2010) Swedish police arrested some 50 members of the environmental pressure group Greenpeace on Monday, after they breached security fences and unfurled banners at a nuclear plant in Forsmark, north of Stockholm. At least three activists managed to scale the roof of one of three reactor buildings and held up banners, but no one entered any of the buildings. The protest triggered criticism about security at the plant. Security was raised at this plant and two other nuclear installations in the country following the protest.

But sometimes they get things right …

OFFICERS PUT TRAINING TO WORK AFTER POWER PLANT SECURITY BREACH

USA (April 2012) For the first time in recent memory, someone tried to scale the fence at McGuire Nuclear Station. The plant's emergency protocols immediately went into place and police arrested the intruder.

"As soon as his boots hit the ground, our security officers were aware, immediately responded and apprehended the individual and turned him over to local law enforcement," said a spokesperson.

McGuire officials regularly train to respond to security breaches. In some exercises, experts intentionally work to breach the various levels of security without tipping off anyone at the site.

"This goes right along with their training and they knew exactly what to do and they did that," said the spokesperson.

The key take-home message from this incident is that:

a) the intruder was detected straightaway,

b) the response from the guards was immediate, and

c) they clearly knew the procedures to be followed.

And best of all, they trained regularly for these sorts of events so they knew what steps to take and exactly how to respond when an intrusion such as this did occur.

3

DESIGNING AN EFFECTIVE PERIMETER SECURITY SYSTEM

WHAT MAKES UP A PERIMETER SECURITY SYSTEM?

Designing an effective and reliable outdoor perimeter security system is rarely a simple exercise. Determining the specific site risks, customer expectations, monitoring, and intruder response mechanisms available, and more importantly the customers' security budget must all be taken into account.

While each individual installation will have its own unique characteristics and requirements for outdoor perimeter protection, they still follow the fundamental protection rules known as the Five Ds – define, deter, detect, delay, and detain. An effective perimeter security system will consistently prevent intruders from reaching their target within the site undetected.

The key to securing perimeters is to utilize a multi-layered approach. The more layers or obstacles an intruder needs to get through to reach his target, the more determined he will need to be, the more likely the chance he will be detected, and therefore the more secure the site ultimately is. By taking a holistic approach to site security, each of the individual components or layers that make up the final intrusion detection solution should complement each other, working together to protect against both known and perceived threats.

There is no individual or single technology in the market that will take care of perimeter security on its own. The CCTV cameras, the fence along with the fence-mounted and open area sensors and the response mechanism each play a role in the final solution. The weakest point in any of these layers will ultimately determine the level of security you deliver. So it requires careful planning and a thorough understanding of the site specific characteristics, selection of the individual security elements, and knowledge of how each component or layer plays a role in securing the site.

You need to match the system design to the site profile, and each site will be unique. Of course, the more layers and higher probability of detection, the more expensive it quickly becomes! At a number of points in the design phase there will be trade-offs made, usually associated with price and performance.

PLANNING

Managing the customer

A key element of the planning stage is to manage the customer expectation. Too often the customer reads all the sales hype then decides he needs a system with 100 percent POD of a "special ops" type intruder with zero nuisance alarms, all for the lowest possible price. Customers watch crime drama shows on television showing low-light CCTV images being magically enhanced to identify tattoos etc. on intruders a mile away and somehow believe this can be achieved with a $90 camera. We all know the reality is quite different, but the customer sometimes doesn't!

So set realistic expectations with the customer and get sign-off on an agreed acceptance criteria before you start installing anything. All too often you find a medium-risk site expecting and demanding prison-level performance from their mid-range security system – unfortunately, this generally comes about in the commissioning phase, and not at the design stage, and is usually a very costly mistake for the integrator.

Another area often overlooked in the planning stage are the response mechanisms and procedures required when an intrusion and alarm does occur. Are there security staff on site, or will the system be monitored and responded to remotely? Are there documented procedures to cover this?

No single technology in the market is either undefeatable or infallible. We should remember that the CCTV cameras, the open area sensors and tracking systems, the fence and the sensors are each a part of a layered perimeter security solution and should be used in combination to deliver the most effective results.

THE SITE PROFILE AND RISK ASSESSMENT

The first step is risk profiling the site to be protected – that is, defining the facility you are protecting. For example, is this a storage yard or a pharmaceutical plant? Are there buildings (which are potential hiding spots) on or near the perimeter? Is the area open and flat, or undulating? Is it subject to weather extremes like strong winds or snow? Next, profile the types of intruder you may encounter – vandals, petty thieves, trespassers, or professional highly skilled intruders? Next, assess the "attractiveness" or potential targets contained within the site – are there goods of high value or worth on site, or are buildings or workers the target?

Even the very best sensors available today will deliver less than optimum performance if not correctly tailored to meet the specific requirements of the site (for example, microwave sensors used on undulating ground). The role of any perimeter security system (that is, the perimeter fence, the perimeter intrusion detection system, and the response mechanism) is to act as the

first level of protection-defining the boundary of the site, providing both an early warning of intrusion attempts as well as deterring, detecting, documenting and delaying any incursion. The other layers that make up the solution are then used for the verification and tracking of intruders once they have breached the perimeter.

The systems integrator plays a key role in risk assessment – doing a complete site survey and creating a holistic plan for security, despite the temptation for and often pressure from a customer to skip over this step. It has to be an approach that looks at all the vulnerabilities and risks of the protected site and accurately assesses and applies technologies to provide the best levels of detection and protection that are acceptable to the customer. It's a total solutions approach.

Budgets

The true cost of an intrusion detection solution is very easy to underestimate. Sensor and CCTV manufacturers often quote just the cost per meter or per foot for the system, or per camera, and this figure is typically the hardware cost only and does not include the costs of installation, any associated civil work or infrastructure required to provide power to the field elements (sensor and controller), communications lines to the field elements, mounting poles, security management systems, training or ongoing maintenance.

Suppliers tend to downplay the actual installation and commissioning costs, often citing best case scenarios, so it is important to always use a realistic "total installed price" as the basis for comparing systems and technologies. Often the attractive low up-front purchase price of the perimeter intrusion detection system hardware can be far outweighed by the high costs associated with providing a power and communications infrastructure to support it. The cost of providing this infrastructure at say an airport – where you simply can't bury cables – can often be many times the price of the actual perimeter intrusion detection system, making the final installed solution prohibitively expensive. This is covered in more detail in a white paper titled "Selecting a perimeter intrusion detection system" on page 103 at the end of this document.

An important consideration for any intrusion detection system is the dependability and reliability of the solution being offered. Dependability or confidence in the system is critical as security staff must be able to trust that an alarm is really an intrusion event and not a nuisance alarm, and it can quickly guide a response team to the intrusion point. Reliability is also fundamental, so look for systems with a low component count and a high system mean-time between failures (MTBF). Remember the more components you have in the system, the more points of failure and potential of system down-time.

Talk to your customer if you think their security expectation versus budget may be unrealistic. Do what is in their best interests.

SELECTION OF THE INDIVIDUAL ELEMENTS

The fence

The perimeter fence not only defines the boundary of the site but also provides a deterrent and a delay for those attempting to enter illegally. The fence should be in a good state of repair, have adequate lighting and have vegetation cleared from both sides for clear observation. Always remove large trees and overhanging branches that may provide climb points. In addition to defining the boundary of the site, the fence should also provide a sufficient delay to an intruder climbing it to give the intrusion detection system enough time to activate and position a CCTV camera to visually verify the intrusion activity.

Is the fence suitable for the application and potential or expected risks, and will it provide a suitable deterrent for intruders? If teenage vandals and trespassers are the major threat, then a chainlink fence topped with barbed wire is probably adequate, whereas if you are expecting a more experienced thief skilled and equipped to a higher level, then you may want to consider a razor wire topped anti-climb prison-style fence. The higher the fence, the more difficult it is to climb. So a typical 6 feet high (2 meter) fence is used for low-security applications, 9 feet (3 meter) for medium-security, and 20 feet (7 meter) for high-security applications such as a prison. Be aware that a solid wall – as attractive as it sounds – may provide concealment opportunities for an intruder. As chainlink or weldmesh fences often allow for unobstructed observation of an intruder, the fence may actually be a deterrent in itself.

Regardless of the fence type selected, it must be regularly inspected and maintained if it is to retain its deterrent value, and the cost of this maintenance must be taken into account.

There is no point spending more money than you need to on a fence, but conversely, the fence must, as a minimum, match the profiled security risk.

Lighting

Effective perimeter protection begins with a good fence and adequate lighting. In its simplest form, CCTV linked to motion triggered lighting can be a useful low-cost deterrent to opportunistic thieves by providing improved surveillance and observation of suspect activities, but the more determined criminal will not be frightened off at all. Hence the need for multi-layer security systems where lighting forms an integral part.

The perimeter intrusion detection system

The perimeter intrusion detection system (PIDS) attached to the fence will provide the first warning of an intrusion, detecting the fence climb activity and providing the location of the attempted entry in all weather conditions. This information is then passed to the CCTV system to activate specific cameras or views, providing visual verification and tracking of the intruder if video analytics are employed.

There are numerous systems and technologies available to detect intruders climbing fences, however each site will generally have some unique requirements in this regard.

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 the vulnerability to defeat (i.e. typical measures used to defeat or bypass detection by the sensor).

In the ideal world, the perfect perimeter intrusion detection system (PIDS) would simultaneously exhibit a zero NAR and a 100 percent POD, and be undefeatable.

The probability of detection (POD) provides an indication of a systems ability to detect an intrusion within the protected area. The probability of detection depends not only on the characteristics of the particular sensor, but also the environment, the quality of the fence itself, the method of sensor installation and adjustment, and the assumed behavior of an intruder. Any POD figure you are quoted will be conditional and unique to each site and installation-despite the claims made by some manufacturers. For example, a sensor may have quite a high POD for a low-level threat such as a teenage vandal or protestor who has little knowledge of the system, versus a more sophisticated threat from a professional thief or special operations person for whom the POD will almost certainly be substantially lower. It is doubtful that there is any single technology on the market that could not be defeated by experienced people; hence the need for a layered multiple-technology solution where risks are high.

In conjunction with the probability of detection, you must look at the Nuisance Alarm Rate (NAR). A nuisance alarm is defined as being an alarm on the sensor that is not attributable to an intrusion attempt. This is primarily caused by environmental conditions, which may include animals, wind, rain, etc.

Typically there is a trade-off between the POD and the NAR – if you make the system more sensitive (a higher POD) then you will also see an increase in nuisance alarms. Conversely, if you wanted fewer nuisance alarms, then you traded off some sensitivity and had a lower POD. There are however, some exceptions to this rule that have appeared in the market in recent years – systems that use signal signature analysis or artificial intelligence to process alarms with a high degree of discrimination rather than the more simplistic and traditional threshold method. By carefully matching the

unique patterns and characteristics of the intrusion alarm signals, the system sensitivity can be increased (yielding a higher POD) without the penalty of increased nuisance alarms.

Signal discrimination and the way sensor information is analyzed have undergone major developments and advances in recent years. This is only possible because of the large amount of multi-parameter sensing information that can be collected by the newer and much smarter technologies, such as interferometric fiber optic sensors, and the processing power available from multiple CPUs in centrally installed controllers which can run signal fingerprint and pattern recognition type software. This level of processing is typically not available from distributed processing architectures, that is, a number of microprocessor-based sensor controllers installed in the field. The computing required is far more intensive than the capability of these distributed microprocessors.

These advances in technology were originally destined for military applications but have made their way into the security arena where they are capable of clearly discriminating between “real” events and background clutter. This capability 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 minimizes the effects of wind, rain, storms, aircraft, traffic, and lightning while maintaining the required high levels of sensitivity and intrusion detection.

The newer PIDS technologies are also “Ranging” or “Locating”, which means instead of just identifying a zone where an intrusion occurs (which may be several hundred meters long), they give a precise location of the intrusion to within a few meters. This is especially useful when verifying an intrusion event with CCTV.

You also need to look at what and how much hardware you are installing in the field. While each component of the hardware may have an individual reliability or Mean Time Between Failure (MTBF) figure of say 10,000 hours, when you combine many pieces of hardware in a “system”, the “overall system” MTBF will be significantly less due to the high component count and the many points of failure.

Conversely, if you select a system with a “head end unit” or with all of the electronics in a single location for improved reliability, then you need to ensure that there is sufficient redundancy built in to minimize the chance of a system failure.

Open air surveillance and tracking

The next layer of defense will involve the detection and tracking of an intruder once they have penetrated or breached the perimeter fence. This can be done using a variety of technologies, but commonly comes down to PTZ CCTV cameras, but may also include microwave, ground based radar systems or similar open area technologies.

While CCTV cameras with video motion detection (VMD) or Video Analytics are great for visual monitoring, confirmation, and providing forensic evidence, its performance as an intrusion detection system has not lived up to the sales hype put out by many manufacturers. However, what CCTV with video analytics is good at, is its ability to automatically identify, track, and record intruders as they move away from the fence breach to other areas within the protected site, without the operator having to constantly monitor the video or adjust the camera. Linked to a digital video recorder (DVR), CCTV systems also provide forensic video documentation of an intrusion event and the intruder.

As part of the layered solution, when an intruder is detected climbing the fence, an alarm is raised by the fence-mounted PIDS system along with the location of the intrusion. This location information is automatically relayed in real time to the CCTV control system in the format of “select a camera” (or cameras) and “preset view.” The cameras then point to and provide visual verification of the intrusion and location, then track the intruder from that point onwards.

Ground based radar is also good for open area tracking and usually operates in conjunction with cameras – the radar unit providing the location and position of the intruder, and the camera providing the visual verification. Similarly, microwave detectors can be used to monitor movements of an intruder within a site. But bear in mind that both of these technologies are “line of sight” so vehicles, buildings, shrubs, trees and hollows in the ground can provide hiding spots.

The biggest problem with open area solutions used as the only detection system is if you have any movement or traffic within the site, such as cars, trucks, planes, etc. they may provide false positives, as will blowing debris, animals and such. This is why they need to be part of a layered solution.

Integrating the layers

A Physical Security Information Management (PSIM) system connects multiple existing safety and security systems on a site into a single interface that automates the notifications and interactions between systems (such as information from the detectors in the field, detectors on the fence, the CCTV and/or ground based radar). All of this alarm information is then analyzed and prioritized to instantly identify those situations that are legitimate intrusions and require urgent attention. With the advent of Android mobile devices running alarm management software for example, it is now possible to relay this detailed intrusion information live to your mobile security forces in the field.

The aim of a comprehensive security solution such as this is to prioritize and provide a warning that someone has breached the perimeter, visually verify the intrusion, track their movement once they are inside, and delay them long enough for the appropriate security response to take place – all before the intruder can reach their target or achieve their goal. A PSIM can provide a total picture of a security incident and enable the responders to have complete situational awareness of an event and respond in the most effective manner.

The response mechanism

Finally, any security system is only as strong as the weakest link. The smart intruders rarely defeat the actual intrusion detection systems. Instead, they rely on poor alarm response procedures and mechanisms – the human element – to avoid getting caught. It is this human factor – the response mechanisms, the procedures to follow, and adequately trained security staff that are key to a sites security.

In some cases, untrained security staff are not clear on what to do when they actually get an alarm. Some customers wrongly view intrusion detection technology as a cost-saving alternative to having to employ security staff at all!

The response mechanism for a military installation will be quite different to that of a civilian system. Although the technologies may be the same, a military installation typically has mobile, armed security staff on duty 24 hours a day with clear procedures and a clear chain of command in the case of an intrusion. Civilian installations may not always have this clear response mechanism or chain of command – this has to be factored into the site assessment.

Regardless of which solution or technology you finally select, without the right human factors, the odds of success will be low.

4

THE ROLE OF SIGNAL PROCESSING IN INTRUSION DETECTION

There has been an increase in the use of terminologies such as "advanced signal processing," "intelligent signal processing," "artificial intelligence" or AI, "digital signal processing" and the like from perimeter intrusion detection system (PIDS) manufacturers in their marketing material. These terms and the way they are used can become confusing, making it difficult to understand what you are really being offered. The following is intended to give a bit of background into these terms, demystify what they actually mean, clarify what they do, and what benefits they bring to the end user.

Nuisance alarms are typically generated by a broad range of environmental conditions. This can include the wind flapping or rattling the fence fabric; rain or hail directly on the sensors; birds landing on fences; small wildlife including squirrels; lightning strikes or thunder; nearby road, rail and air traffic; children throwing stones or sticks at the fence; this list goes on ... As sure as death and taxes (and in spite of some of the manufacturers' claims!) you will always get some nuisance alarms, but how you deal with them is critical to the overall system performance. How do you eliminate those nuisance alarms without compromising the detection of real intrusion events? How do you transform PIDS performance to deliver improved value to the customer? Better signal processing.

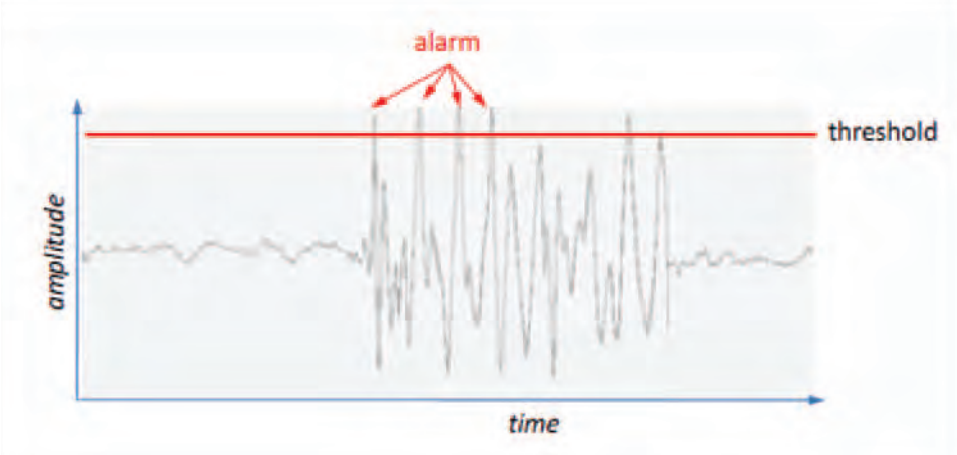
IN THE PAST

Traditional PIDS systems had fairly unsophisticated ways of dealing with nuisance alarms. As the background signal level increased – for example as the wind speed increased or the rain got heavier – the sensitivity of the system was reduced to decrease the number of nuisance alarms. The problem with doing this is that the detection sensitivity and therefore the ability to alarm on a real intrusion event is also reduced a corresponding amount, often to the point of actually having trouble detecting any sort of fence climb. So if you were trying to break into a site undetected, the best time to choose would be a wet and windy night!

So setting up and configuring these traditional systems became a delicate balancing act, trading off sensitivity against nuisance alarms. How many nuisance alarms per day could the customer tolerate in order to maintain sensitivity? Or could they eliminate nuisance alarms but live with only detecting fairly major intrusion events on the perimeter fence?

Some systems needed to be recalibrated each season to allow for differing types and rates of nuisance alarms. Systems even had anemometers connected to them, so that as the wind speed picked up the sensitivity of the system was automatically reduced. A range of creative methods have been employed over the years to recognize and eliminate nuisance alarms – some more successful than others. One example is the use of headphones to have the alarm operator 'listen in' to the alarm signal, then have the operator determine from what he can hear if it was a real fence climb or just environmental noise. So in this case the signal discrimination (deciding what is an alarm and what isn't) is human rather than electronic, and correspondingly (or humanly) highly subjective and inconsistent.

All these systems worked on the same fundamental principle of establishing a base line or ambient signal level and then alarming on any signal that exceeded a preset threshold – be it an alarm or not.



If the signal goes above the threshold line, then it is an alarm.

TODAY

The newer interferometric fiber optic intrusion detection technologies appearing in the market from an increasing number of vendors deliver significant improvements in sensitivity when compared to more traditional fiber optic and copper PIDS systems. This improved sensitivity results in a higher probability of detection (POD) of an intruder, especially when they are carefully trying to defeat the system using techniques such as stealthy climbing, carefully propping ladders and even placing ladders with sponge on the back of them against fences in an attempt to climb over undetected.

But there is a downside to this – this improved sensitivity can lead to increased nuisance alarms. So the key challenge facing manufacturers and developers continues to be how to minimize these nuisance alarms without compromising the system sensitivity to real intrusion events.

As these newer systems also cover much longer distances than in the past – typically many miles rather than just a few hundred feet per controller – you now have far more background noise sources being detected up by a much longer sensor cable in addition to nuisance alarms generated by the increased sensitivity, so traditional methods of handling environmental noise such as filtering and simple thresholds will not work. Far more efficient signal processing is required; signal processing that can clearly differentiate between what is a real intrusion event and what isn't.

This is one reason why the newer technologies typically use a centrally housed processor to manage the entire PIDS system. In addition to the substantial installation cost savings and maintenance benefits of not requiring power or communications to the field anymore, one important advantage of this PIDS architecture is that you now have considerable processing 'horsepower' readily available. This in turn allows you to implement some very advanced processing and identification of the signals – far smarter than just simple threshold or sensitivity levels.

The development and implementation of these advanced signal processing techniques in the PIDS environment is transforming the market. Traditional PIDS systems without this level of signal processing will over time disappear, being displaced and replaced by these high performance systems that offer greater sensitivity, fewer nuisance alarms, lower overall costs, and much simpler set-up.

WHAT THE TERMINOLOGY MEANS AND ACTUALLY DOES

Notwithstanding the technical definitions, in the PIDS market the terms "advanced signal processing", "intelligent signal processing", and "digital signal processing" are often used loosely and interchangeably to represent the same thing – using intelligent algorithms to analyze and identify different events within the raw signal. This technology (comprised of both hardware and software) is employed to digitally process the raw PIDS sensor signal received from the fence, looking at far more characteristics than just the amplitude or frequency of the signal.

The signals are digitally processed by algorithms to isolate and remove events attributed to nuisance alarms yet still retain real intrusion event information. These filtered signals can then be passed through an amplitude threshold type system to determine if it is an alarm, or if it requires further processing.

Artificial intelligence (AI) however takes this one step further by analyzing and classifying the digitized sensor signal, comparing the filtered signal to a known event, and actually making the yes or no decision as in the case of supervised networks. AI can also classify and decide on sensor signals using unsupervised methods such as clustering and unsupervised neural networks.

ADVANCED / INTELLIGENT / DIGITAL SIGNAL PROCESSING

These three terms are generally interchangeable in the intrusion detection business, but are more generally referred to as “digital signal processing” or “DSP” of the raw signal from the perimeter.

DSP has an emphasis on using mathematical algorithms rather than traditional analog filtering techniques for processing the raw perimeter sensor signals. In addition to processing PIDS signals, typical DSP applications include audio and speech signal processing, sonar and radar signal processing, sensor array processing, digital image processing, seismic data processing, etc.

The goal of DSP within a PIDS application is to measure and filter the signals from the sensor on the fence or perimeter and effectively remove those parts of the signal not attributable to a real intrusion event, i.e. ambient or environmental noise. In most cases this signal processing is a multi-step process. The first step in the process is to convert the signal from an analog to a digital form, as the computational requirements for digital signal processing are far simpler than analog. The signals are then converted from time to the frequency domain usually through the Fourier transform. The signal can also be transformed into the time-frequency domain using wavelet or quadratic time-frequency methods to reveal even more information.

The next step is the analysis of signals in the frequency domain, digitally examining the signal properties from the fence sensor to determine which frequencies are present in the input signal for a real intrusion event, passing these through, and blocking those frequencies that are known to be caused by environmental and nuisance events. When blocking the frequency of the environmental noise, advanced signal processing should be considered, as in some cases the pass spectrum of the noise and real intrusions may overlap making it harder to discriminate between the two.

DSP provides much finer filter control than you could ever achieve with analog components, and any dynamic changes required by the filters are done in software rather than in hardware, making them programmable and highly flexible. The downside is the processing overhead required to filter out bands or frequencies that are of no interest, i.e. are not real intrusion events. For this reason, a growing number of DSP applications are now implemented using powerful head-end PCs with multi-core processors.

ARTIFICIAL INTELLIGENCE OR AI

Artificial Intelligence (AI) is different and more advanced in that it builds mathematical models that simulate the human neural decision making processes, replicating in software how your brain makes a decision. It's an electronic version of listening and trying to identify an intrusion signal through headphones, but much faster, much smarter, and far more reliable. This is the next step in the process after the DSP.

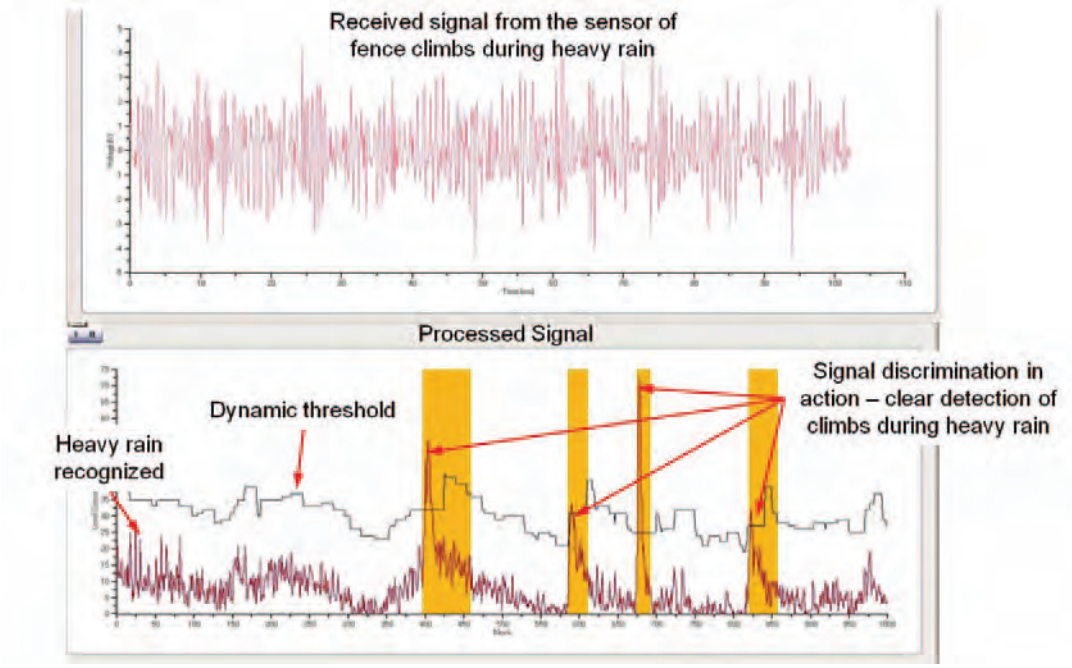
Neural networks, as used in artificial intelligence, are non-linear statistical data modeling or decision making tools based on statistics and signal processing. They can be used to model the complex signals received from the perimeter fence sensor and detect patterns in data. It's these patterns in the alarm data that are specifically of interest and useful to us in eliminating nuisance alarms. What has attracted the most interest in neural networks by far is its ability to "learn" using a set of observations gained from the sensor on the fence, by classifying these data patterns as either real intrusion or nuisance events and then deciding if it is a real intrusion or just a nuisance event.

AI enables the system to recognize and remove background signals such as rain, leaving the intrusion signal untouched without any loss of sensitivity at all, and process this signal further to alarm and locate the intrusion. By employing AI, this nuisance mitigation algorithm adjusts to varying levels of rain (or other sources of nuisance alarms) but, importantly, never reduces the intrusion event sensitivity.

Only a few years ago this leading edge technology was confined primarily to the military and aerospace industries, used in biometric identification systems, biomedical signal analysis, speech recognition, imaging and robotics to name just a few. Now it's become an essential part of the technology industry, providing the heavy lifting for many of the most difficult problems in signal analysis, as seen in the latest generation of intrusion detection systems.

By definition AI is an intelligent self-learning process, but in the PIDS industry it is currently implemented at a basic 'supervised' level, primarily as a decision making process. There is no doubt that self-learning PIDS systems using 'unsupervised' AI methods will appear in the future, but the industry is not there yet.

The most effective PIDS systems currently use a combination of both digital signal processing and artificial intelligence. Digital signal processing does the first pass of the incoming signal to remove those parts of the signal clearly not associated with an intrusion. The remaining signal data is then passed to the artificial intelligence program for further processing that includes features such as signal pattern recognition for example to provide a more refined level of filtering of nuisance events.



How the intrusion signals are clearly extracted from the raw fence signal using both DSP and AI

The result is a clear highly accurate and reproducible yes or no intrusion alarm with very few nuisance alarms.

5

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 (such as wind, rain, and salt air), animal activity, man-made environmental factors such as human activity patterns, electrical fields, radio, or radar transmissions, and nearby vehicle, truck, rail, or air movement.

There are other considerations that must be assessed when installing sensors to monitor perimeters. If fence-mounted sensors are used, the fences themselves should be well constructed and solidly anchored (preferably to recognized industry standards), as loose fences will 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 the 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.

If your installation is in a coastal or other corrosive environment, the type of perimeter intrusion sensor you select needs to take this into account. For example, copper sensors or communications cables will rot out quite quickly in salt air and so should be avoided, and any electronics or controllers installed in the field should be completely sealed to prevent corrosion and subsequent reliability issues. Anything metallic, such as camera housings, electronic enclosures, and junction boxes, should be avoided altogether or be constructed of UV-stabilized plastic or marine grade stainless steel instead.

If your installation is in an area subject to winds, then you need to make sure you select an appropriate intrusion detection system that has adequate signal processing to prevent wind from generating nuisance alarms. You want more than a system that just desensitizes the sensor as the wind picks up – this legacy solution will reduce your probability of detection significantly, and may leave the perimeter unprotected in windy or rainy conditions. You want to eliminate the effects of wind yet maintain full sensitivity to an intrusion, so look for intrusion detection systems with some sort of advanced signal processing that takes care of this.

Above all else, carefully read the installation manual and follow the sensor manufacturer's installation instructions. After all, they designed their system; they know what works in what environment and what does not, and should be contacted if there are any concerns or questions.

Failing to closely follow the manufacturer's instructions almost always leads to substandard system performance and substantial cost overruns.

6

PERFORMANCE MEASUREMENTS

Calculating a realistic measurement of performance for outdoor Perimeter Intrusion Detection Systems (PIDS) is not simple due to the highly interactive and closely coupled relationship that exists between the detection of intrusions and unwanted nuisance alarms.

Detecting every intrusion on your perimeter is the expectation of any system, but equally important is the confidence that your security staff have in the system. Too many false or nuisance alarms will seriously erode confidence in the system, often to the stage where all alarms – real or not – are dismissed or ignored by security staff.

Vendors often quote only the raw detection rates for their technologies without any sort confidence factor or compensation for nuisance alarms – so it's unlikely to be the level of performance you can realistically expect to achieve on your site. Vendor testing is usually carried out in a controlled environment where they typically increase sensitivity to do the detection tests, record this figure, then reduce the sensitivity down to a level to eliminate nuisance alarms and record this figure – both in isolation of each other. The reality is that due to the highly interdependent nature of these results, both of need to be evaluated together in order to come up with a meaningful intruder detection measurement.

How a PIDS system will actually perform on your site is often markedly different from the expectation set by the raw detection rate figures (sometimes quoted as the POD). No two sites are ever the same with numerous external and site specific factors impacting on this figure to reduce the quality of the overall system performance. A more detailed explanation of this topic is in the White Paper "Calculating the Quality of Performance of a Perimeter Intrusion Detection System" on page 107 of this report.

7

ALARM MONITORING SYSTEMS

In addition to the 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 Microsoft Windows. They may operate as a stand-alone system or in a client–server configuration. Most of these systems operate with proprietary software supplied by the manufacturer.

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 overlaid maps which can be helpful in guiding security personnel to the precise location of the intrusion. The urgency of the visual alarm can vary according to the nature of the alarm, which particular sensors or layers are triggered in which sequence, or the location of the possible intrusion (for example, high-priority versus low-priority areas, and 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 to constantly monitoring the continuity of the wiring to each device, indicating if circuits have been cut or bypassed.

Different but complementary types of sensors are often integrated with the aim of reducing nuisance alarm rates and increasing the probability of intrusion detection. These different sensors can be joined together by installing a logic "AND" circuit. The 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 now two or more sensors are required to detect an alarm condition prior to initiating an intrusion alarm. Using a logic "OR" will have the opposite effect – increased chance of nuisance alarms but an improved POD and response time. The overall system POD will be dictated by the POD of the weakest device. Another downside of this approach is that often it can take many seconds to poll each individual sensor on a perimeter to see if it has 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 fiber optic intrusion detection systems are more advanced, 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 (such as climbing, cutting, lifting the fence fabric, environmental nuisance alarm) and software commands directly to activate and control CCTV systems, SCADA and Modbus devices all in real time.

COMMUNICATIONS

Communications between the front-end computer and the field elements (sensors and 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 severely limit the options for future upgrades and additions. 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 communication processing overheads. Unfortunately, this adds another layer of system complexity and additional points of failure.

Newer generation systems are far simpler, faster, and far more advanced. Standard computer communication protocols such as TCP/IP allow high-speed bidirectional communications over huge distances using readily available and proven network topologies such as wide area networks (WAN), local area networks (LAN), the Internet, and Wi-Fi. Be aware though, while Wi-Fi networks can solve certain challenges, it is far riskier to deploy, use and maintain than a hard-wired network. Wi-Fi systems are vulnerable to jamming and interference so should never be the sole communications link – you will need a backup link for it. Wi-Fi can also potentially create issues when used in an environment such as an airport as it may interfere with ILS aircraft landing systems, and conversely may be affected by nearby radar or radio signals, buildings, and in populated areas, by other Wi-Fi or cordless phone systems.

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 (such as UPS, batteries, and standby generator) incorporated into their design and operation to guarantee uninterrupted operation of the sensor on the perimeter, alarm reporting, situation assessment, and security staff response.

Not only do the field components of the PIDS require backup power, but so do the security management system, as well as communication devices used by security staff, such as phones, radio, CCTV, and DVR. 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 foot for the system, and this figure is typically 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, and maintenance.

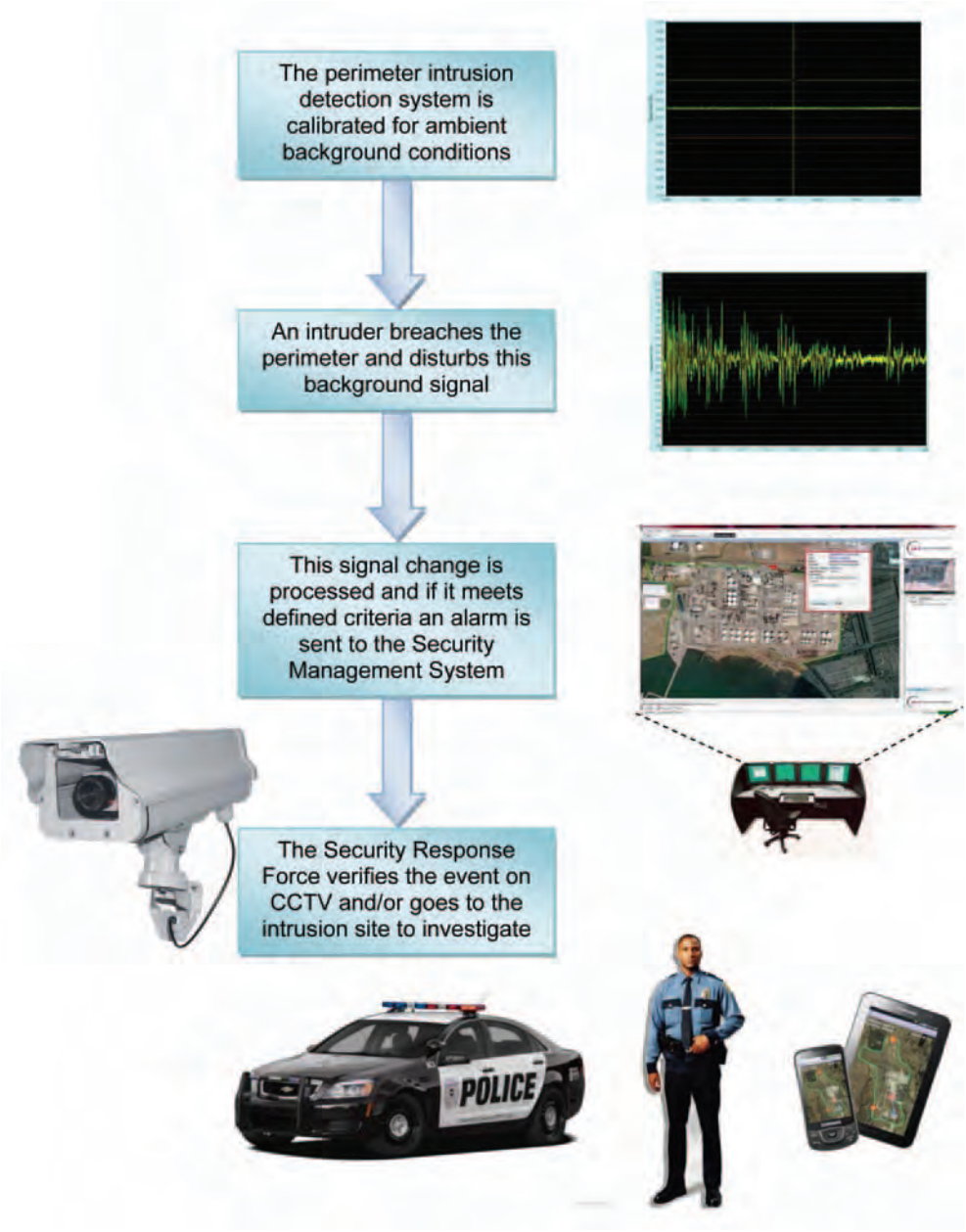
Suppliers tend to downplay the actual installation and commissioning costs involved, often using best case scenarios. It is important to always use a realistic “total installed price” as the basis for comparing system costs. The low up-front purchase price of the perimeter intrusion detection system hardware can be far outweighed by the high costs associated with providing the power and communications infrastructure. It is not uncommon for these infrastructure and installation costs to be four to five 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 include:

- What is the mean time between failure (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?
- Local support – what will be the response times if I have a problem?

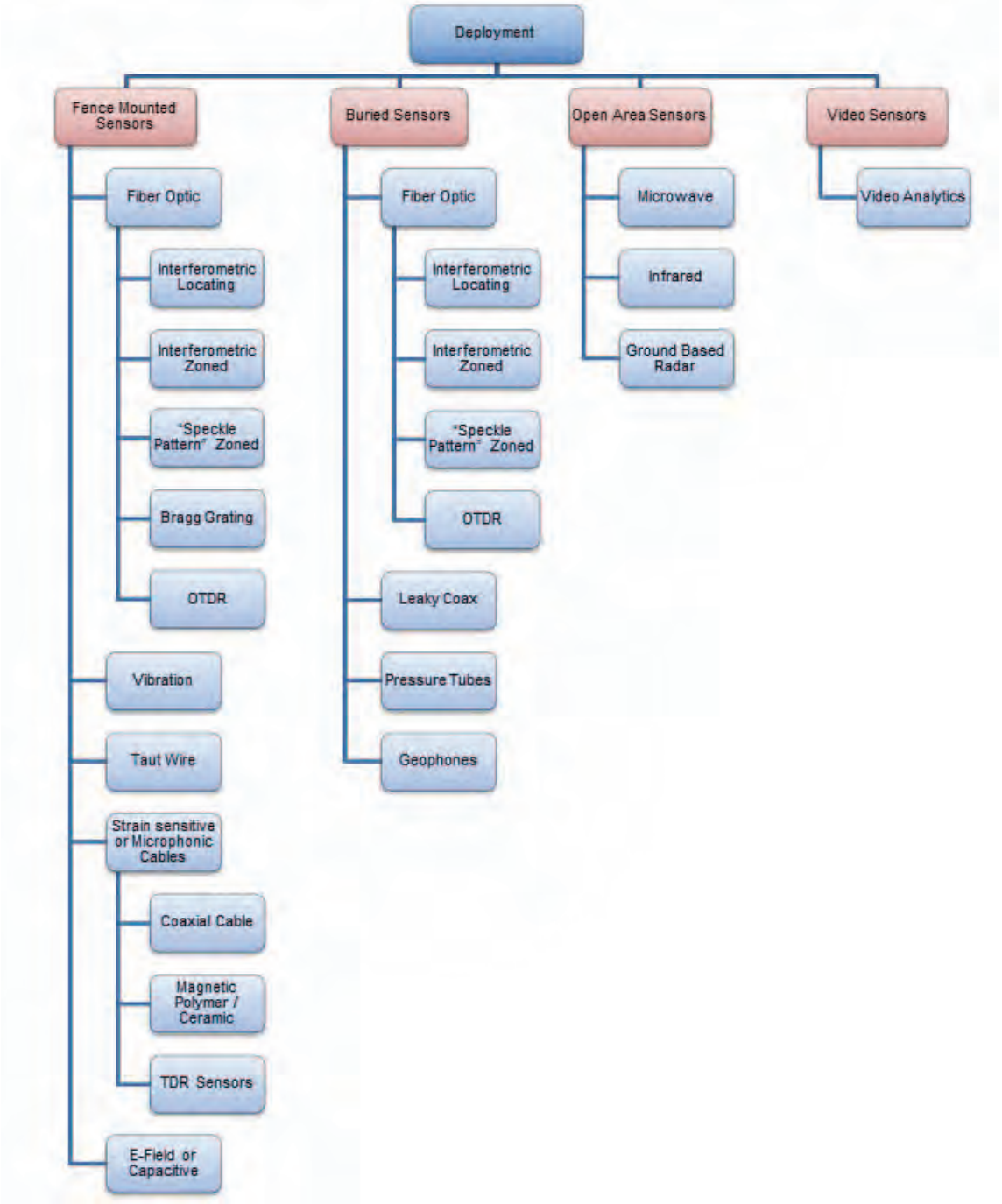
TYPICAL PERIMETER INTRUSION ALARM PROCESS



8

PERIMETER SENSING TECHNOLOGIES

CLASSIFICATION OF PERIMETER SENSING TECHNOLOGIES



FENCE-MOUNTED SENSORS

Fiber optic fence sensors

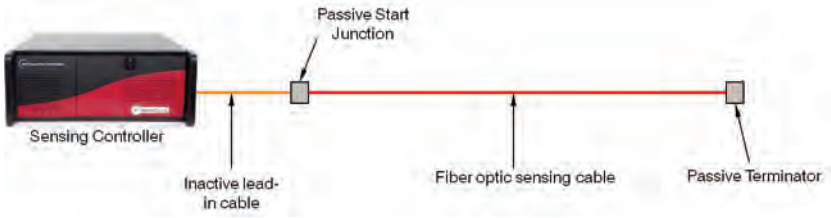
Description: Fiber optic sensing systems are well established in the market with a strong following based on its world proven reliability and performance over the last decade and more. These systems are readily available and are highly tunable to compensate for environmental conditions in the field, such as weather and climate characteristics. The sensors do not require power, are impervious to lightning, electromagnetic interference, radiofrequency interference or other electronic signals, and can be used over long distances.

Over the last year in particular, there has been a noticeable shift in the market towards fiber optic sensing technologies. A number of PIDS vendors who previously discounted fiber optic sensing technologies have seen the market demand and witnessed the performance advantages of fiber-based systems and are now either developing their own technologies and/or have formed alliances with the key fiber optic developers. Some are now even promoting fiber as their lead intrusion detection technology.

Fiber optic sensors use light traveling down a glass fiber rather than electrical signals down wires for transmission and detection, so are ideal for incorporation into existing fences. There are two main types of fiber optic intrusion detection systems: the traditional hardware-zoned systems and the newer more sensitive interferometric systems that can also provide the actual location of an intrusion. Although both of these are fiber optic based, the fundamental principles behind them are quite different, as is the performance and applications. Also included is a brief description of several of the newer emerging technologies – Fiber Bragg Gratings and OTDR.

Basic operating principle: Optical fiber 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 fiber. When the fiber is bent or moves, the characteristics of the light traveling down the fiber are altered. In a perimeter system, light is sent down the fiber 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 fiber optic cable moves minutely and the properties of the light traveling down it change. It is this change in the light that is detected, and if it exceeds a predetermined threshold or meets set criteria, then an alarm is flagged. The properties of light which can be monitored for change include power, phase, wavelength, polarization, and scattering.

As well as being intrinsically safe, the optical fiber itself is immune to electromagnetic interference (EMI), radiofrequency interference (RFI), and lightning.



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

ZONE-BASED "SPECKLE PATTERN" FIBER OPTIC SENSORS

Operating principle: The traditional zone-based fiber optic sensing system consists of a microprocessor-based controller installed on the fence line, and a multimode fiber optic sensor cable attached to the fence fabric and connected to the controller. Light from a laser is sent down a multimode fiber, and the returned light is compared to determine if there are any light or "speckle pattern" changes due to the micro bending of the fiber optic cable caused by a disturbance on the fence. While zone lengths of up to 6,500 feet or 2,000 meters are theoretically possible, realistically zones are usually limited to a more manageable 650 feet (200 meters) or less. This zone length can be halved depending on the quality and range of the CCTV camera being used to visually assess the intrusion.

In some systems, the fiber 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 the sensitivity to wind is decreased, the probability of detecting a real intrusion event is also decreased.

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 to the control room. While the fiber optic cable itself is immune to EMI, RFI, and lightning, the electronics situated in the field are not.

Application: The fiber optic sensing 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 maximize system performance. With zone-based systems, the more ambient activity that exists around the fence, the lower the sensitivity setting for the system, and the less likely it will be that the system will detect an intruder.

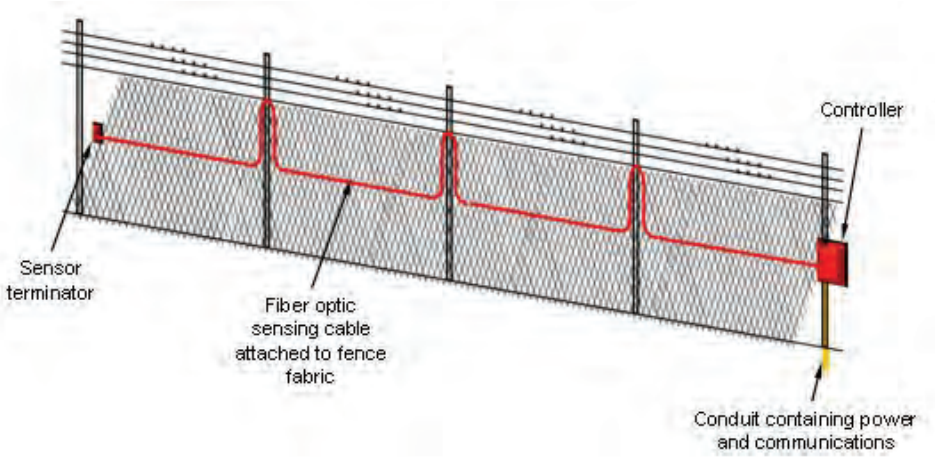
Zone-based systems are more suited to smaller sites, typically less than 6,500 feet or 2,000 meters, where power is readily available on the perimeter fence or at least close by. The preference should always be to install a system where there are no electronics in the field and the controller is mounted in the security center to maximize immunity to strong electromagnetic events and minimize installation and infrastructure costs.

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

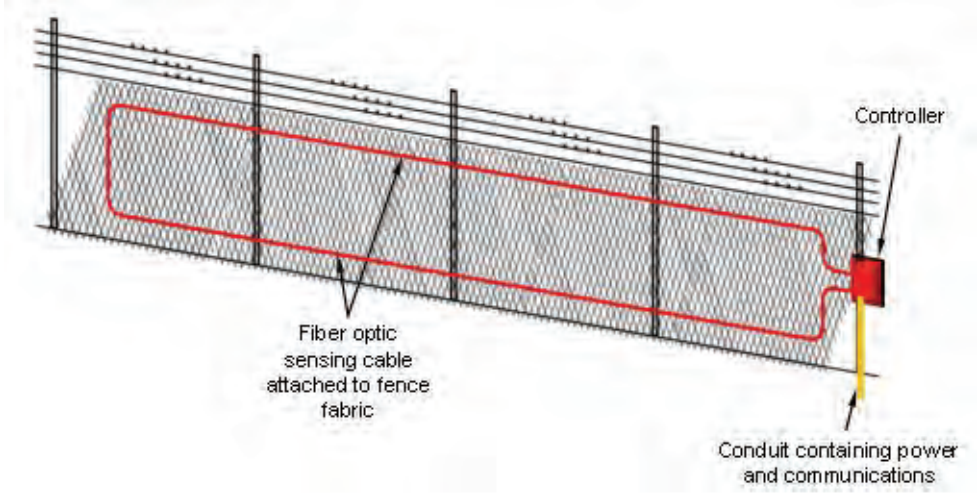
Weaknesses: Installation costs can be high due to the controllers situated in the field and the associated costs of providing power/communications to them; sensitivity, nuisance alarm mitigation, and the distance it can protect is not as high as for an interferometric fiber optic sensor. Nor does it provide the precise location of an intrusion.

Potential causes of nuisance alarms: Although the fiber optic cable itself is impervious to interference, as with any outdoor electronics where controllers are installed in the field, system problems can be created by RFI, EMI, lightning, salty or corrosive environments, and extreme changes in temperatures. In addition, animals coming in contact with the fence can be interpreted as human activity, falsely signaling an intrusion attack.

Typical methods of defeat: Bridging or tunneling 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 interferometric or 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 to high level of sensitivity but requires additional sensor cable*

ZONE-BASED INTERFEROMETRIC FIBER OPTIC SENSORS

Operating principle: Unlike the traditional zone-based fiber optic sensing systems with controllers installed on a fence line, interferometric zoned systems are far more sensitive. Typically, they have the controller housed inside the security center and fiber only outside the building and on the fence (but often still have the option of a field-installed controller configuration if required).

A singlemode fiber optic sensor cable is attached to the fence fabric and connected to the controller. Light from a laser is sent down the fiber, and the returned light is compared to determine if there are any changes due to the micro bending of the fiber optic cable caused by a disturbance on the fence.

Detection zone lengths are typically around 500 meters or 1600 feet, but the big advantages of this technology are the long insensitive lead in cable lengths supported – often up to 10 kilometers or 6 miles – allowing the controller to be installed remotely from the fence. The system is so sensitive and the controllers have such good environmental alarm mitigation software in them that cables do not have to be installed in conduit. This delivers a significant cost saving overall.

The simple installation architecture, plus the relatively low cost for a system with such high levels of sensitivity makes this technology extremely attractive for those smaller sites in the range of 2000 meters (6500 feet) or less.

Application: The fiber optic sensing 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 maximize system performance.

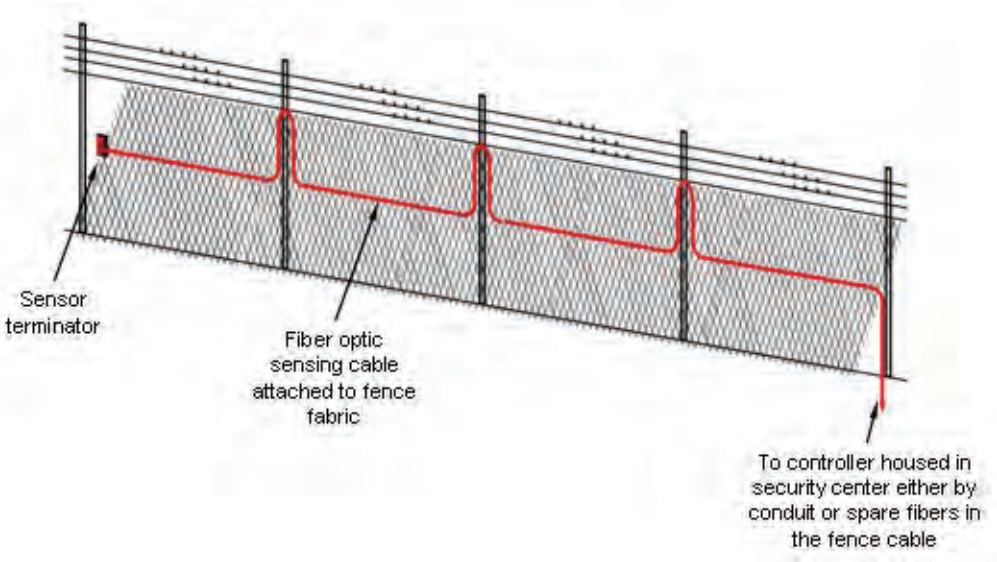
Zone-based systems are more suited to smaller sites, typically less than 6,500 feet or 2,000 meters, where the controller can be housed remotely from the perimeter fence. The preference should be to install a system where there are no electronics in the field and the controller is mounted in the security center to maximize immunity to strong electromagnetic events and minimize installation and infrastructure costs.

Strengths: Low purchase cost for small perimeters; simple to install the sensor cable; high sensitivity; the complete system can be immune to EMI, RFI, and lightning.

Weaknesses: Often not connectorized, requiring fusion splicing of the fibers, but most Telco contractors are experienced in doing this. Does not provide the location of an intrusion – just the intrusion zone.

Potential causes of nuisance alarms: As with any fence-mounted intrusion detection system, poor fence quality is a common cause of 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 methods of defeat: Bridging or tunneling will bypass the fence and, therefore, bypass the sensor.



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 LOCATING OR RANGING FIBER OPTIC SENSORS

Operating principle: The newer interferometric or Microstrain technologies are far more sensitive than the traditional "speckle pattern" zone-based systems, and are based on the well-established principles of interferometry. They combine the signals from two singlemode fibers 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 utilizes highly advanced signal processing and signature analysis carried out in a powerful head-end unit located within the security center to maintain the inherently high sensitivity to intrusions without the penalty of increased nuisance alarms.

As Microstrain systems use single mode fibers, a single system can protect a perimeter of up to 50 miles or 80 kilometers 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 far simpler correlation to fixed perimeter points (such as gates, buildings, corners, roads) and cameras.

Application: Fiber optic fence sensors (actually fiber 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 maximize system performance and sensitivity. The Microstrain system is less affected by ambient noise as 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.

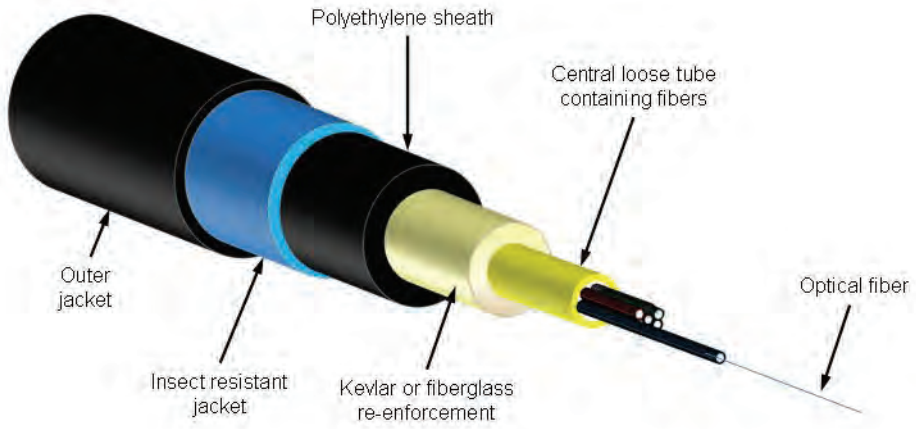
Microstrain systems are more cost-effective for perimeter fence lengths of between 1.2 miles and 50 miles (between 2 and 80 kilometers), which are handled by just the one controller. A single cable is fixed at the midpoint of the fence and the controller is installed in the security center, making installation extremely cost-effective for these longer distances as no power is required in the field and no electronics are installed in the field. For improved sensitivity to difficult to detect events such as ladder props, loop the sensor cable up the posts.

Strengths: Long distance; highly sensitive; pinpoints the location of an intrusion; low installation costs; intrinsically safe; powerful signal processing; immunity to EMI, RFI, and lightning; excellent signal discrimination and, therefore, very low NAR; highly reliable; low maintenance.

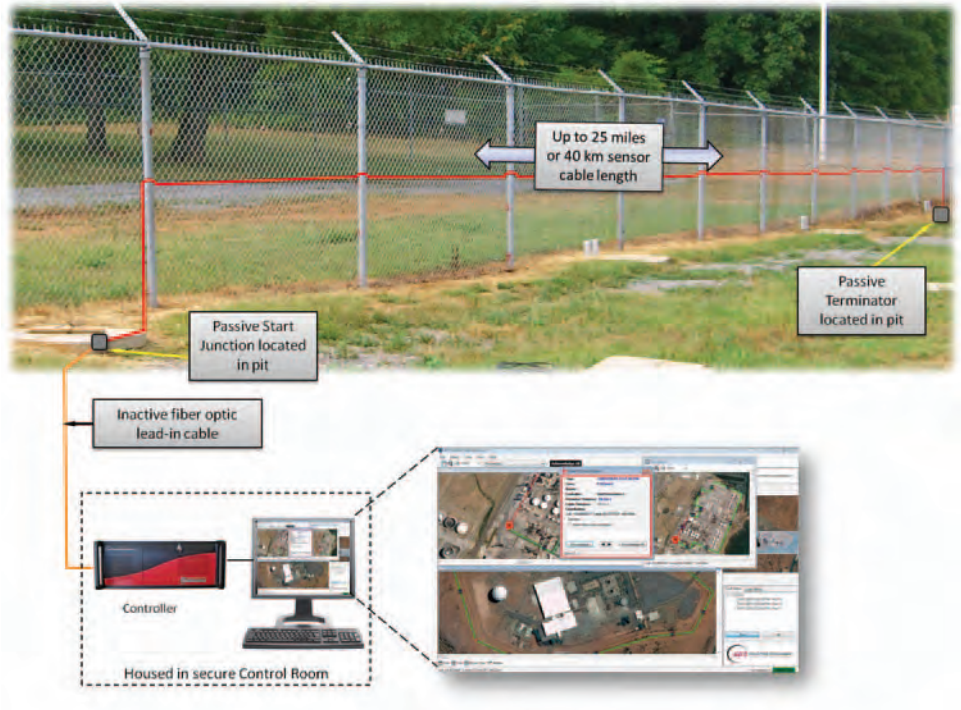
Weaknesses: Not connectorized, so requires fusion splicing to join fibers, but this is common practise these days, and most telco contractors are capable of doing this.

Potential causes of nuisance alarms: As with any fence-mounted intrusion detection system, poor fence quality is a common cause of 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 methods of defeat: Bridging or tunneling will bypass the fence and, therefore, bypass the sensor.



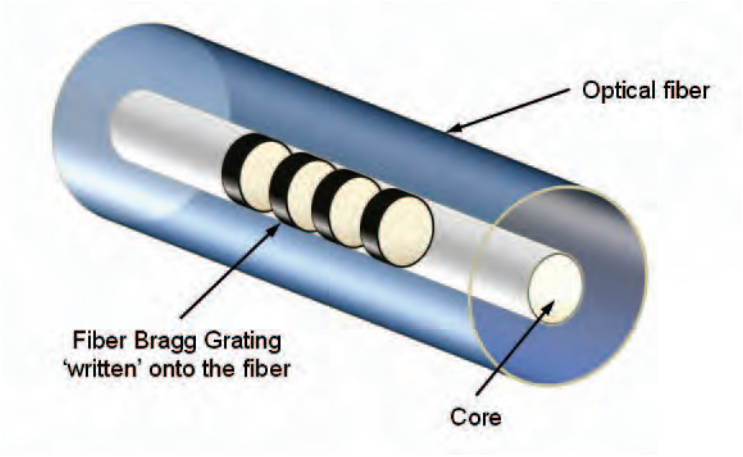
Fiber optic sensor cable construction



A typical Microstrain fiber optic sensor system installation

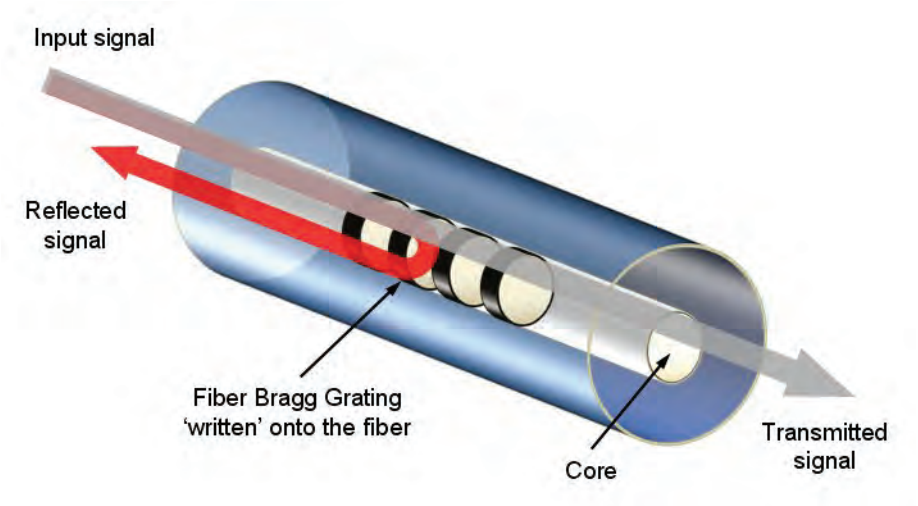
FIBER BRAGG GRATING SENSORS

Another of the new breed of emerging and possible future fiber optic intrusion detection sensors is the Fiber Bragg Grating (FBG). An FBG is an inline optical device that has an alternating refractive index pattern. This pattern is "written" or implanted into a custom optical fiber or manually spliced in.



Configuration of a Bragg Grating

Operating principle: The Bragg Grating works by reflecting back a very narrow wavelength or frequency of light traveling through the fiber, allowing all other wavelengths to pass. In its simplest form, it is an optical filter. When the fiber is moved or strained minutely, these tiny grating spaces change slightly, and so the reflected wavelength changes.



Bragg Grating showing a particular wavelength being reflected

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

Several organizations are researching and promoting this early stage technology, but as yet there are really no commercial installations. The FBG system is expensive to produce and typically the controller has a limited number of gratings that can be processed, meaning reduced location resolution over longer distances.

Strengths: Short to medium distance; highly sensitive; give a close location of an intrusion; intrinsically safe; immunity to EMI, RFI, and lightning; reliable. If the sensor cable is cut, can work up to the point of the cut. High sensitivity makes it more suitable for buried applications.

Weaknesses: A largely unproven technology in perimeter intrusion detection. Currently poor or underdeveloped signal discrimination against environmental effects so much higher than expected nuisance alarm rates. Sensor cables with the Bragg Gratings "written" or physically spliced into it can be expensive to manufacture. Location accuracy is determined by the number and spacing of the Bragg Gratings.

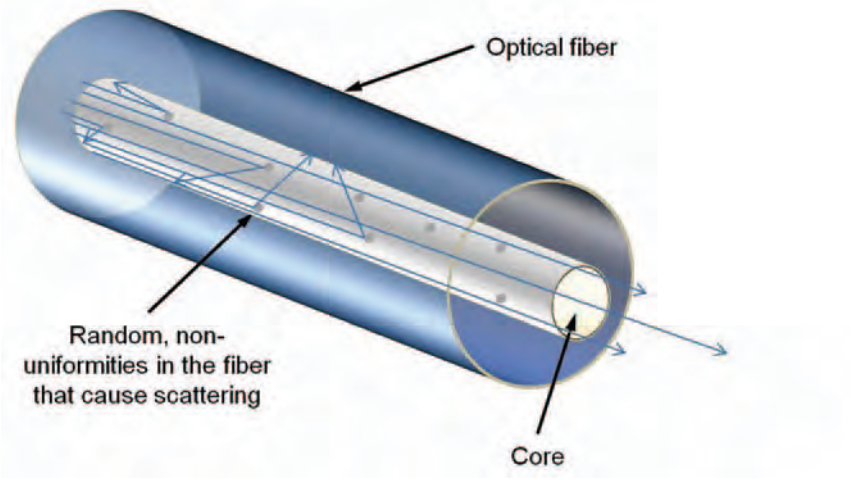
Potential causes of nuisance alarms: As with any fence-mounted intrusion detection system, poor fence quality is a common cause of nuisance alarms. Some temperature related problems in the field as the gratings expand and contract with thermal changes on the fence.

Typical methods of defeat: Bridging or tunneling will bypass the fence and, therefore, bypass the sensor.

OTDR

Another fiber optic intrusion detection technology showing great potential is Optical Time Domain Reflectometry (OTDR), which works on the well-known principle of Rayleigh Scattering. There are a number of variants, which are generally classed as either Phase sensitive OTDR (P-OTDR) or Coherent OTDR (C-OTDR), depending on how the light is sent down the fiber and how the returned light signal is processed.

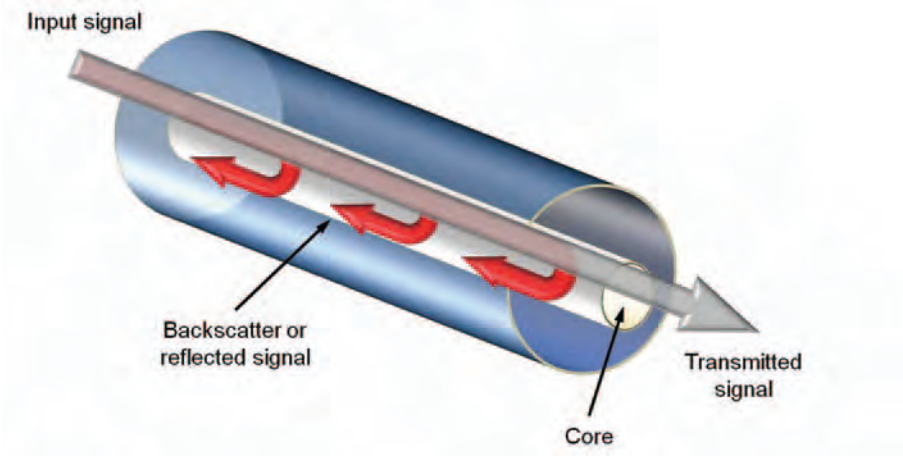
Operating principle: Much like radar, the controller generates an encoded light pulse which is sent down a standard single mode fiber optic cable. As it travels down the fiber, a portion of this injected light will be scattered (Rayleigh backscatter) or reflected back from the microscopic non-uniformities frozen into the glass fiber during manufacture. With no disturbance, the pulse continues to the end of the sensor cable and the steady backscattered light signal sets the baseline or ambient conditions.



Silica fibers are not quite perfect materials, thus their composition varies, on a microscopic scale.

When the fiber optic sensor cable is disturbed, the characteristic of the light reflected back to the controller (or backscattered) changes. This change in the characteristics of the returned signal is analyzed by the controller to verify if it is an alarm or not. The controller also divides the sensor cable into 30-foot or 10-meter segments by timing the backscattered signals of the encoded pulses. So the controller determines which segment the alarm is in to provide the actual intrusion location.

OTDR is currently expensive, and at this stage has been successfully trialed as a fence-mounted sensor. It requires further work on the signal processing software to fully utilize this sensitivity yet minimize the rate of nuisance alarms. It is proving to be potentially useful in some buried applications where higher levels of sensitivity are required.



Backscattering or reflection of light due to impurities or characteristics of the fiber

While offering very good sensitivity there are still trade-offs regarding signal discrimination and the effective elimination of nuisance alarms. Also, due to the large amount of signal information to be analyzed, plenty of computing power and a large data bandwidth are required for some systems.

Strengths: Long distance; highly sensitive; pinpoints the location of an intrusion; intrinsically safe; immunity to EMI, RFI, and lightning; reliable. If the sensor cable is cut, it can work up to the point of the cut. The high sensitivity makes it very suitable for buried applications.

Weaknesses: A largely unproven technology in fence-mounted perimeter intrusion detection. Currently underdeveloped signal discrimination, so higher nuisance alarm rates. Presently it is expensive, but you can expect the cost of this technology to come down over time as it matures.

Potential causes of nuisance alarms: As with any fence-mounted intrusion detection system, poor fence quality is a common cause of nuisance alarms. The high sensitivity of this system works against it as there are large numbers of nuisance or non-intrusion related alarms generated that need to be processed and filtered out. This requires additional development to be done in the area of signal discrimination to get fence nuisance alarms to an acceptable level.

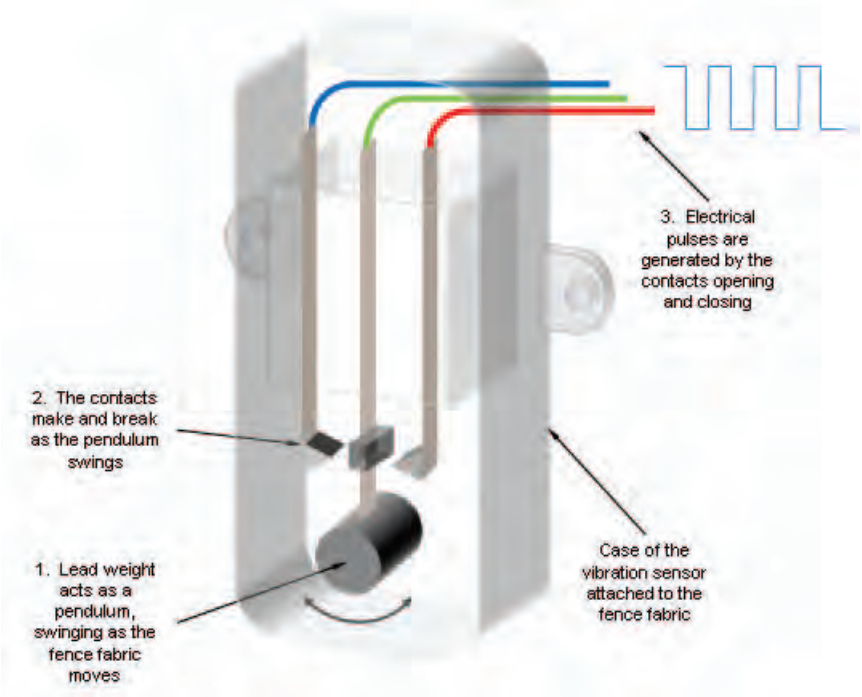
Typical methods of defeat: Bridging or tunneling will bypass the fence and, therefore, bypass the sensor.

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: electromechanical 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 that are sent to the controller.



Principle of operation of mechanical sensor

Piezoelectric sensors convert the mechanical impact forces generated during an intrusion attempt into electrical signals. Unlike the open/close signal generated by electromechanical sensors, piezoelectric sensors generate an analog 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 pick up these vibrations and the signals from the transducers are then sent to a signal processor for analysis. The frequency with which 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 legacy sensors come pre-assembled on a cable at 10 feet or 3 meter intervals, and are installed approximately 5 feet (1.5 meters) above the ground. Recommended zone lengths are typically 330 feet or 100 meters.

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 all types of vibrations, additional sensing equipment is required to analyze the signals in order 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.

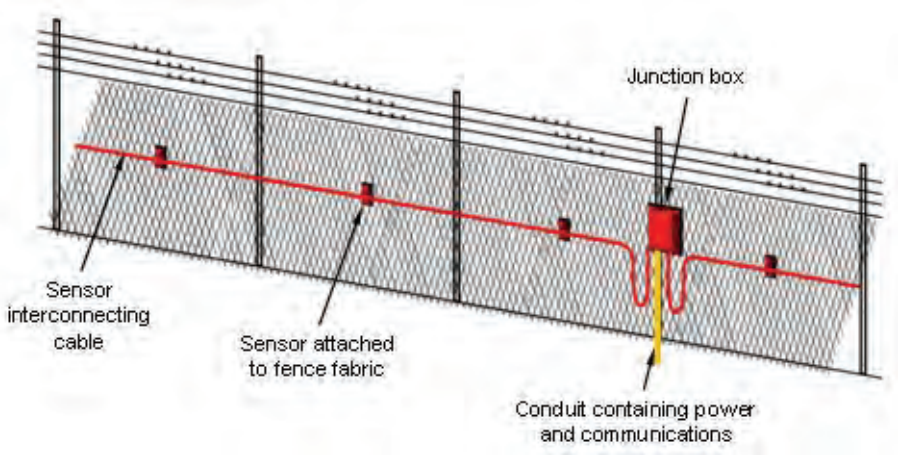
Mechanical vibration sensors should only be used in applications where natural or man-made environmental vibrations are non-existent. Vibration sensors are neither suitable nor reliable in areas where high background vibrations occur, such as airports, close to construction sites, railways, highways, 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. Often an anemometer is required 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 the sensitivity to wind is decreased, the probability of detecting a real intrusion event is also decreased.

Potential causes of nuisance alarms: Poor quality fence construction; tree branches; animals; 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.

Typical 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. Careful or assisted climbing, particularly at the more rigid turn points, in many cases will 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. Although less common, tunneling is always a possible defeat method.



A typical "rattler" 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.

This is one of the most expensive types of perimeter fence intrusion detection systems available because of the complex installation and ongoing 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 barbed wires installed on either the top of a chainlink fence or barbed wires installed horizontally as the fence or barrier itself. The micro switch typically consists of a movable center plunger suspended inside a cylindrical conductor. In the rest position, the center 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 center 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.

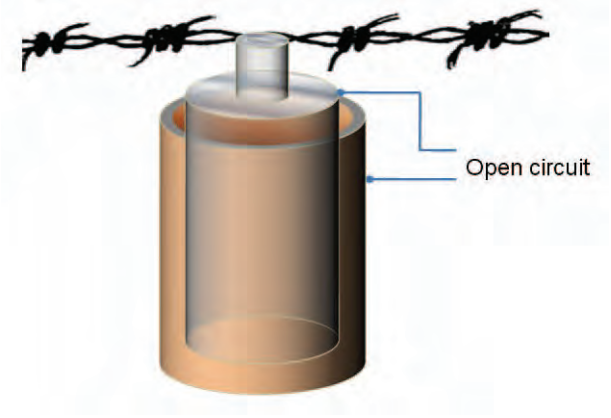
Application: Taut wire sensor systems can be installed as a standalone barbed wire fence creating a dual-purpose physical barrier as well as a detection system; added to an existing fence; or used as a barbed wire outrigger on top of a wall or fence. Because of the very high costs associated with a taut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

Strengths: High POD with a very low NAR; difficult to defeat, so ideal for very high-security sites such as prisons; simple technology.

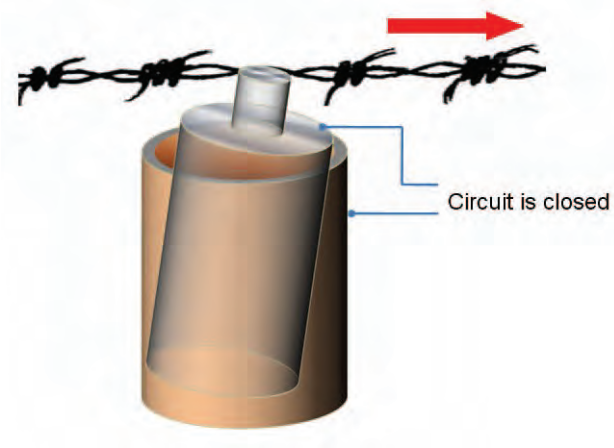
Weaknesses: Expensive to purchase, install and maintain; requires seasonal adjustments; has many points of failure. Slow spreading of wires attached to strain gauges over a period of time may go undetected, hence the ongoing popularity of micro switch systems.

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.

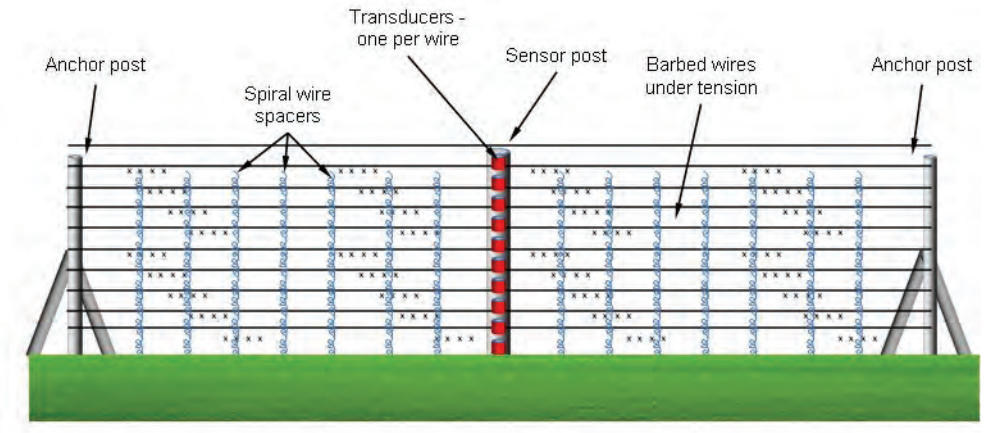
Typical methods of defeat: Tunneling under or bridging over the fence itself, with the most likely locations being those areas not under visual surveillance.



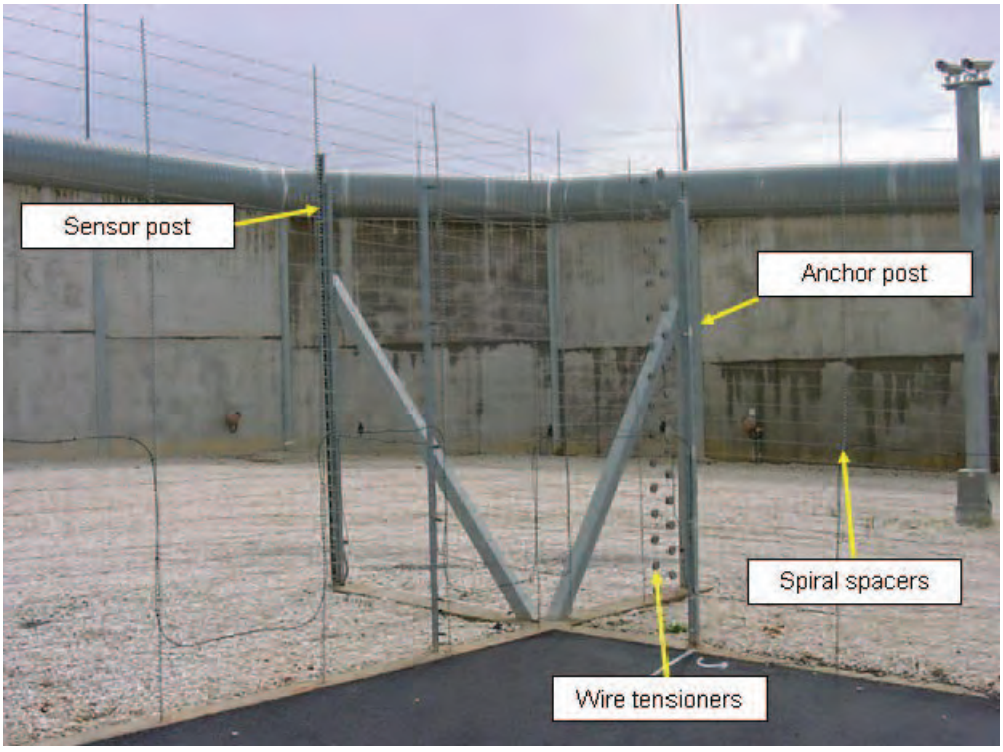
In the steady non-alarming state, the enter plunger does not touch the outer cylinder.



When an intruder attempts to cut or spread the barbed wire, the wire moves in one direction, causing the center 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 yard

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 analyzer 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, and lifting. 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 relies on the triboelectric effect, where a small cable terminal voltage is produced when the cable attached to the fence is vibrated by an intrusion or similar event. Other vendors use the piezoelectric effect or are systems based on magnetic materials for detection.

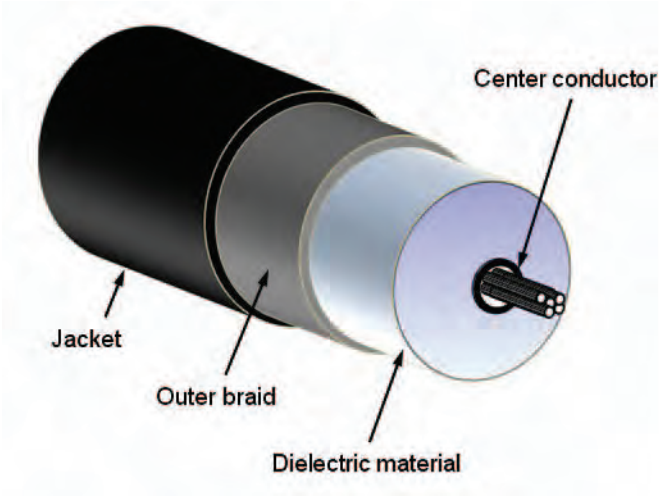
As this type of sensor is effectively a microphone, an audio monitoring capability can be incorporated, enabling the operator to hear noises along the fence line and manually determine, assess or verify what caused the alarm. However, this requires very low levels of background noise, considerable training 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 three main types of strain sensitive or microphonic cables: ***coaxial***, which uses a custom coaxial cable where the center conductor carries a permanent electrostatic charge; ***magnetic polymer or ceramic magnetic***, which uses two semicircular magnetic conductors separated by an air gap containing two uninsulated wires; and ***TDR*** consisting of a coaxial cable with two additional grooves containing sense wires.

COAXIAL CABLE

The system is comprised of two main parts: the sensor cable and the analyzer. 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 analyzer.

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



Coaxial cable

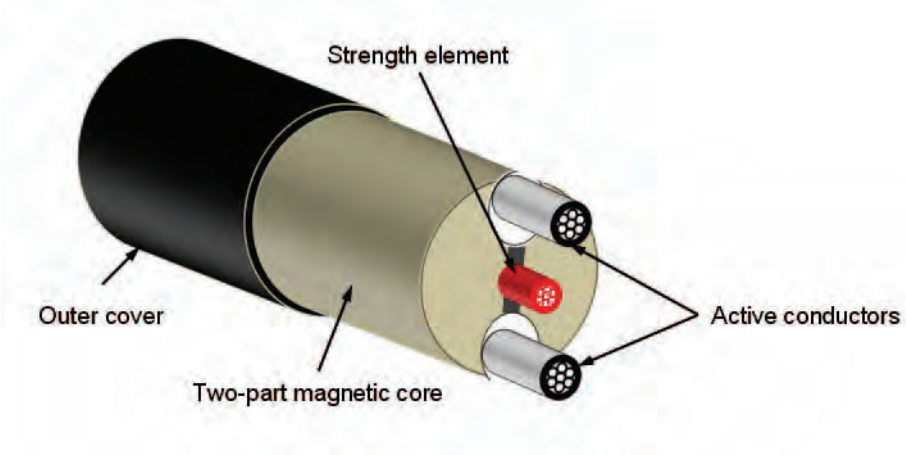
This typically works by means of the triboelectric effect. A steady, permanent, electric charge is placed on the center conductor of the coaxial cable.

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 magnetic polymer or ceramic magnetic cable consists of a two-part magnetic core that works like a linear magnet with two free-floating insulated wires (active conductors) in grooves 180 degrees 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 or ceramic magnetic core generates minute electric signals. The processor then compares the signals and generates an alarm if it is 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. "Listening-in" is really a poor human substitute for the lack of signal discrimination or elimination of nuisance alarms in the processor.



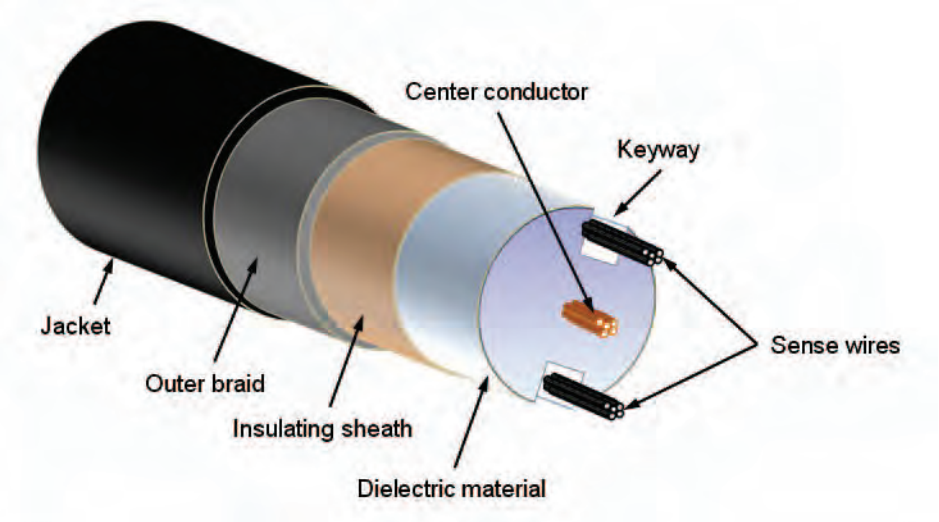
Two-part magnetic core

TIME DELAY REFLECTOMETRY (TDR)

The center 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 center 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 center 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 center 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. The amount of 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 localize the disturbance.



TDR cable construction

Applications: Can be used on a range of fence types, but primarily galvanized chainlink. Weldmesh, plastic-coated chainlink, palisade and anti-climb fencing may give reduced sensitivity. 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 1,000 feet (300 meters), but realistically should be in the 300 to 600 feet (100 to 200 meter) range.

Strengths: Very sensitive; easy to install with a high POD on galvanized chainlink fences; TDR system can locate the point of intrusion.

Weaknesses: Highly sensitive to EMI, RFI, and lightning in the proximity of the sensor; microphonic feature is of questionable value; all of these sensors rely on the free movement of the sensing wires within the cable, so anything causing these wires to bind or not move freely such as excessive heat, moisture, mishandling of cables in the field, and tight installation 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.

Manufacturing tolerances must be kept tight in order to maintain consistent sensitivity along the entire cable.

As with any copper-based system, these strain sensitive or microphonic technologies may be unsuitable for use in marine or coastal environments due to salt corrosion of the sensing cables, connectors, and the electronics.

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

Typical methods of defeat: As with most other fence-based sensors, bridging over or tunneling 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 principle: The sensor consists of an alternating current (AC) 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 are used as the sense or detection elements. Whenever an intruder enters the field, his or her body capacitance creates an imbalance or variation in the electrostatic field; the processor detects this change in signal from ambient conditions through the sense wires and then generates an alarm. The wires can be mounted on freestanding poles, walls, roofs, fences, or other structures to provide a high, narrow field of detection.

To reduce false alarms, typically three parameters must be met to indicate an alarm: 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 tunneling 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 tunneling 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.

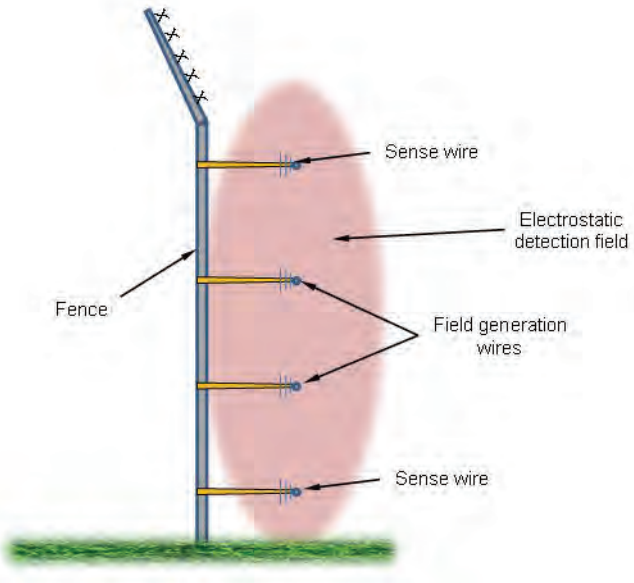
Strengths: Resilient to wind and ambient noise; low maintenance; can be mounted on fences, walls, and roofs, or standalone; has a high probability of detection; detects intruders before they reach the fence.

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

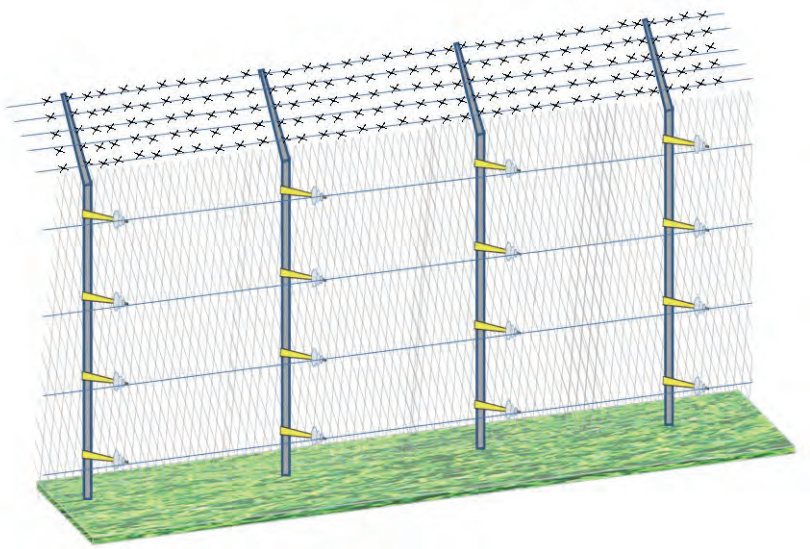
Potential causes of nuisance alarms: Anything causing excessive fence movement, such as wind, rain and snow, birds and animals or vegetation that impinges on the electrostatic field, and lightning. If there is a public path or road on the outside of the fence, pedestrians or traffic may cause nuisance 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 and moisture.

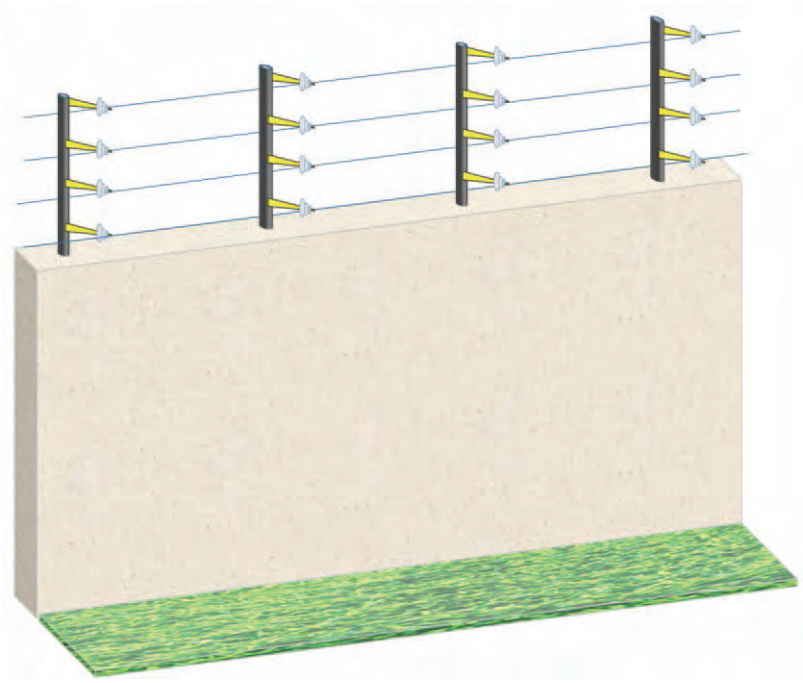
Typical methods of defeat: Tunneling below or bridging over the fence.



How electrostatic or capacitance sensors work



A typical fence-mounted installation



A typical wall-mounted installation

BURIED SENSORS

Buried fiber optic sensors

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

Operating principle: There are two main technologies currently employed for this application: "speckle pattern" systems and interferometric systems. Recently emerging is a third OTDR technology, which has good sensitivity, but is still expensive and susceptible to nuisance alarms. No doubt these costs will come down and the performance will improve as this technology matures.

With "speckle pattern" technology, light from a laser is sent down a single multimode fiber, and the returned light is compared to determine if there are any "speckle pattern" changes due to the micro bending of the fiber optic cable caused by external pressure on the cable such as somebody walking over it. The cable is normally laid in a serpentine pattern and/or attached to a metal or plastic grid to enhance sensitivity.

The newer interferometric or Microstrain technologies are more sensitive than "speckle pattern" systems. They work by combining the signals of two singlemode fibers within separate buried sensor cables, 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.

OTDR works on the principle of optical time domain reflectometry. Much like radar, the controller generates an encoded laser pulse which is sent down a buried single mode fiber optic cable, and due to the nature of the fiber a portion of this light will always be backscattered. With no disturbance, the pulse continues to the end of the sensor cable and the backscattered light signal sets the baseline or ambient conditions. When somebody walks above or close by the sensor cable, the characteristic of the light that is reflected back to the controller (backscatter) changes and an alarm is generated. The controller then determines which segment it is in to provide a location. This detection technology is very sensitive, so the cable is simply buried in a single pass – there is no need for complex serpentine patterns.

Applications: Deploying a buried fiber optic intrusion detection system involves a number of steps to ensure a reliable system with optimal performance is delivered – planning, installation, and configuration. As this technology is sensitive to ground vibrations and seismic events, those installations close to major roads, trees, light pole, railways, construction sites and suchlike should be avoided, or the sensor cables should be installed in gravel to isolate them from these ground-based seismic events.

Try to avoid burying the "speckle pattern" sensing 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.

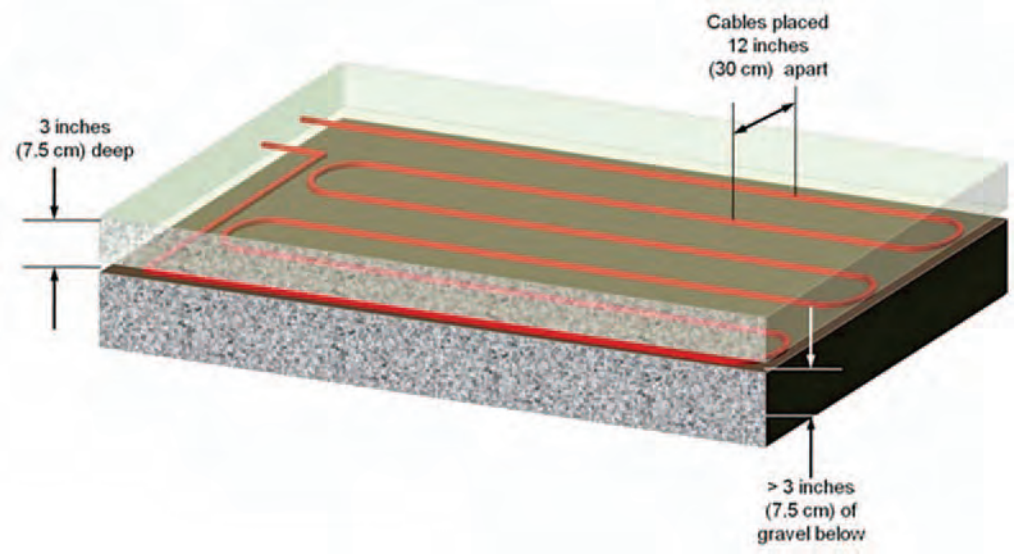
OTDR sensors are far more sensitive and will detect intruders some distance away. They do not rely on pressure on the cable to detect; instead they work by detecting vibrations in the ground.

Strengths: Covert protection; difficult to defeat; low maintenance requirements. OTDR has broad detection coverage with simple installation.

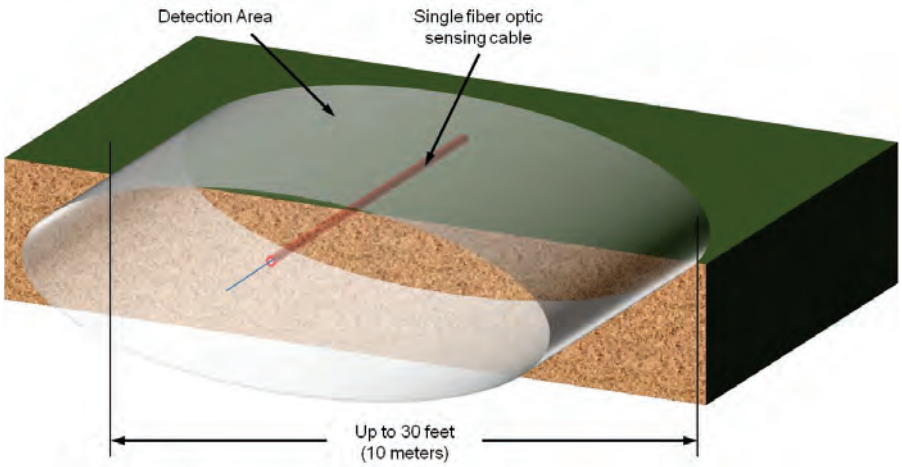
Weaknesses: Heavily dependent on the soil conditions for performance. With the exception of OTDR, in other than gravel, intruders virtually have to tread directly on top of the sensor cable to be detected; requires power and electronics to be installed in the field for some systems. OTDR is currently expensive and requires more development in its signal processing to better manage nuisance alarms.

Potential causes of nuisance alarms: Seismic vibrations; large animals crossing; animals digging in the detection area.

Typical methods of defeat: Bridging over the protected area will bypass the system.



Installation in gravel – "speckle pattern"



Typical installation and coverage of an OTDR system in soil

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 coaxial 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 3 to 6 feet (1 to 2 meters) apart and will provide a detection zone up to 6 feet (2 meters) wider than this and about 3 feet or 1 meter 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. Signal processors eliminate many causes of false alarms such as small animals.

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 10 inches (25 centimeters), and depending on the soil density, create a field approximately 3 feet or 1 meter above the ground and around 10 feet (2 meters) wide. The size of the detection zone will vary depending on cable separation distance and the characteristics of the soil – soils with high levels of moisture, salt, or metal content will reduce the sensitivity and therefore the detection zone size. With this sensor cable, zone lengths can extend up to 650 feet or 200 meters.

Cables should never be installed 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 3 feet (1 meter) below the ported coax cable. When installing the cables parallel to metal fences or near metal light poles, the cables must be positioned 12 feet or 4 meters away from these objects to minimize 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 run-off. The trenches must have very consistent spacing and depth.

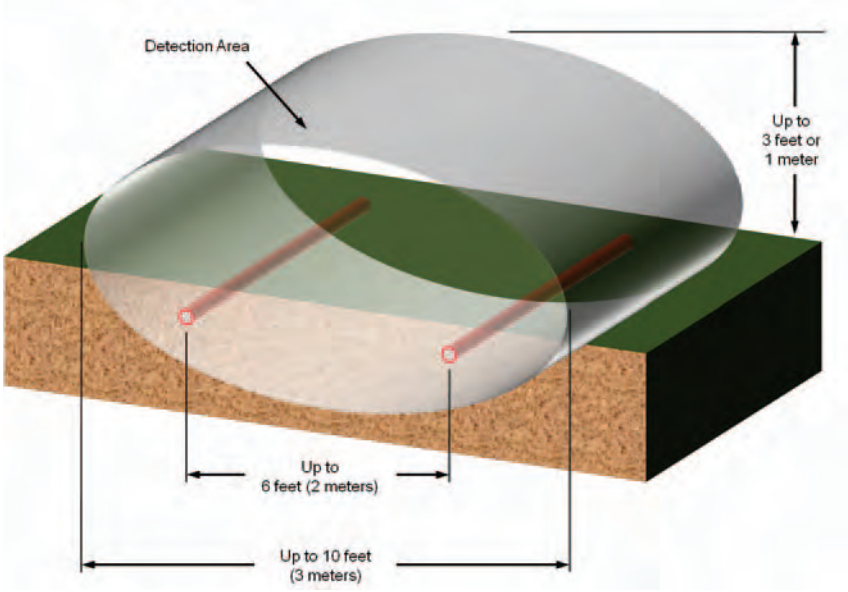
Strengths: Covert volumetric protection; high POD; low maintenance requirements; few nuisance alarms if installed correctly; not sensitive to ground vibrations; cables can be buried in any medium such as soil, sand, clay, concrete, or asphalt.

Weaknesses: Sensitive to nearby pools of water, metal objects and electromagnetic interference; needs to be installed at least 16 feet (5 meters) from passing traffic, and 10 feet (3 meters) from fences and pedestrians; controllers installed in the field require power and communications links.

This technology has a small detection envelope height, making it potentially easy to bridge or vault over to avoid detection. Requires extensive trenching and site preparation to ensure proper drainage.

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 substations and should not be used in close proximity to these.

Typical methods of defeat: Deep tunneling (below 3 feet or 1 meter), bridging, or as the detection height is only around 3 feet (or 1 meter), careful jumping will avoid detection. Can also be defeated by using wooden stilts.



Typical installation and coverage for a "leaky" coax system

Balanced buried pressure tube sensors

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 two 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. The unit detects this pressure differential between 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 analyzer generates an alarm signal.

Application: The detection area is created by burying the parallel tubes approximately 3 feet or 1 meter apart. Depending on the nature and composition of the soil, it will give a detection zone about 10 feet (3 meters) wide and up to 100 yards (100 meters) long. The depth at which the tubes are placed depends on the composition of the medium in which the tubes are placed. Normally, 10 inches or 25 centimeters is sufficient for earth and sand. When installed, they are covert.

Soil with asphalt above it requires tubes to be placed at a more shallow depth of 4 to 8 inches (10 to 20 centimeters). 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 vehicular traffic is detected and not pedestrian traffic.

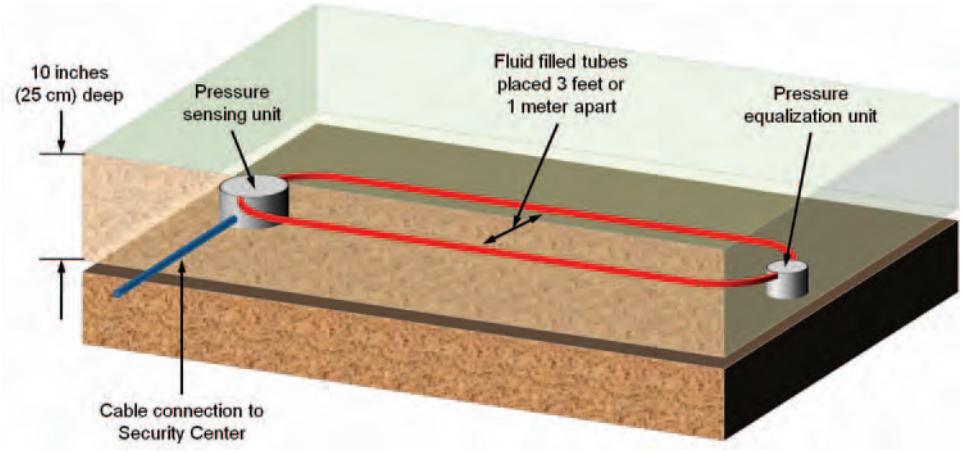
The system has a high degree of immunity to typical environmental noise and weather conditions. However, areas with heavy snowfall (and/or shifting sand) may have trouble with the system properly detecting, depending on the depth and composition of the snow or sand.

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 methods of defeat: 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 analyze this voltage and, if it exceeds predetermined background levels, will cause an alarm.

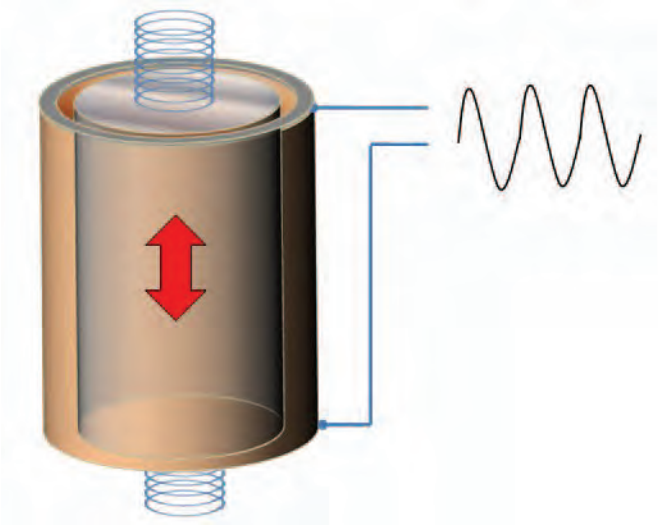
Application: For perimeter intrusion detection applications, single geophones are rarely used. Instead, they are typically installed in a string or array of between 20 and 50 geophones. They are buried 6 to 14 inches (15 to 35 centimeters) deep and are usually spaced around 6 to 12 feet (2 to 4 meters) 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.

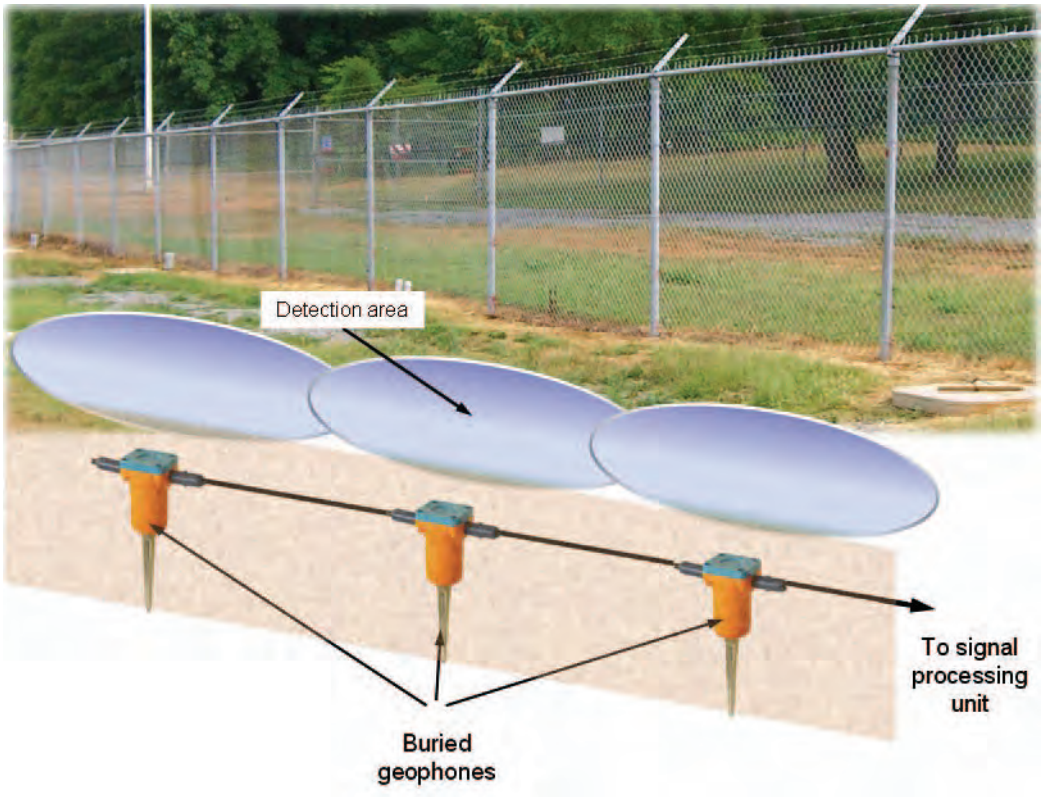
Weaknesses: .Potential causes of nuisance alarms: as geophones can detect very low levels of seismic activity, nearby trees, fences, light poles, and telephone poles can pose major nuisance alarm problems when moving in high winds. For these reasons, geophones should be installed at least 30 feet or 10 meters from trees, 10 feet or 3 meters from fences, and at a distance equal to the height of any nearby poles. Also, proximity to heavy traffic, large animals, or other seismic activity can cause nuisance alarms. It also requires a buried power and communications infrastructure in the field.

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



As the suspended magnet passes through the wire coil as a result of a seismic event, an electrical signal is generated.

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 400 feet or 120 meters 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 hertz and 120 hertz to detect the movements of humans. Intrusions that fail to produce a signal or produce a signal outside this 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 400 feet or 120 meters coverage, whereas bistatic sensors can extend up to 1500 feet or 460 meters.

Typically, microwave sensors would be employed 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 three-dimensional fan-shaped beam. Some models are also suitable for a rapid deployment or temporary PID solution, for example, around parked aircraft.

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

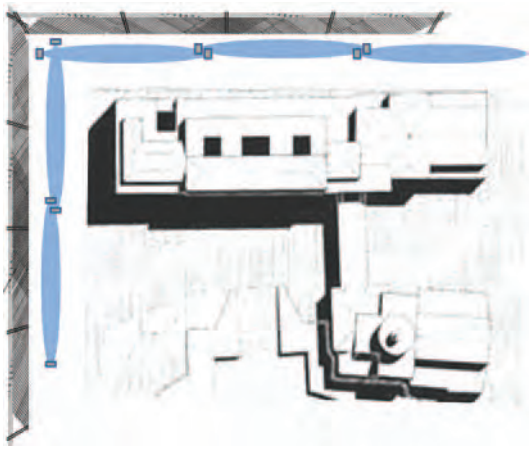
Video Motion Detection (VMD) equipment or another type of complementary sensor system is often installed to verify intrusions, giving security staff the ability to better assess alarms and discriminate actual intrusions from nuisance alarms.

Strengths: Large area (up to 1500 feet or 460 meters with a bistatic sensor); volumetric protection; difficult for potential intruders to determine the exact area being protected; 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.

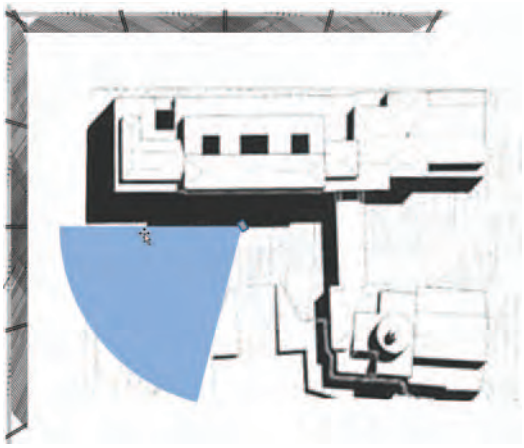
Potential causes of nuisance alarms: External sources of RFI (radiofrequency interference from radio transmitters and suchlike); EMI (electromagnetic interference from large electric motors or generators and power plants); moving objects and debris in the detection field, especially if windy conditions exist; movement of mounting posts the sensors are attached to; reflections off nearby metal or solid objects; pools of standing water (bistatic sensors).

Typical methods of defeat: Slow rate of movement through the field; crawling close to the transmitter or receiver; blind spots caused by uneven terrain, hollows or shielding; tunneling beneath the protected area or bridging above the field.



Typical perimeter security coverage using bistatic microwaves

Note how each of the coverage areas (shown 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 area of coverage shown in blue.

Microwave "shadow"

In this situation, the parked truck will create a blind spot for a microwave system placed on the inside of this perimeter fence.

Active and 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 principle: 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. An intruder passing through the field of detection 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 1200 feet or 370 meters each.

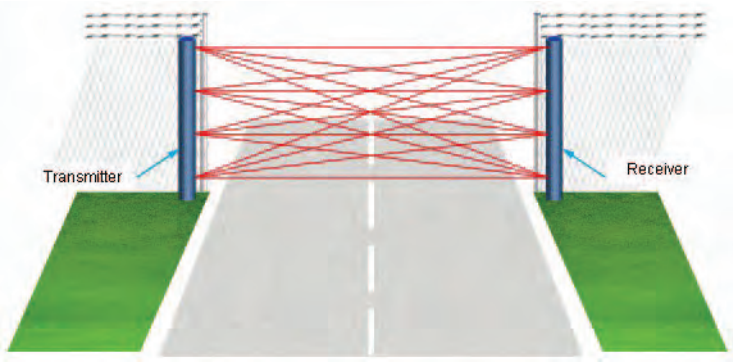
Infrared sensors are typically used to provide protection to opening gates and other fence openings in a multi-beam configuration (for more reliable operation).

Strengths: Low cost; easy to deploy and maintain.

Weaknesses: Passive infrared requires a significant thermal contrast between the background and an intruder – in high temperatures, the POD will decrease substantially. Regular alignment of beams is required for optimal performance; grass or other vegetation between the IR posts needs to be trimmed short regularly; 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, debris, movement of mounting posts, and severe temperature changes can all cause nuisance alarms.

Typical methods of defeat: The most common method of defeat is bridging over or tunneling under the detection beams. As infrared detectors are line-of-sight devices, ensure that any dips or gullies between the transmitter and receiver are filled to prevent blind spots where intruders can pass undetected.



Active infrared system

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

Active infrared sensor

Active infrared sensors such as these are used to protect longer distances.

Thermal imaging

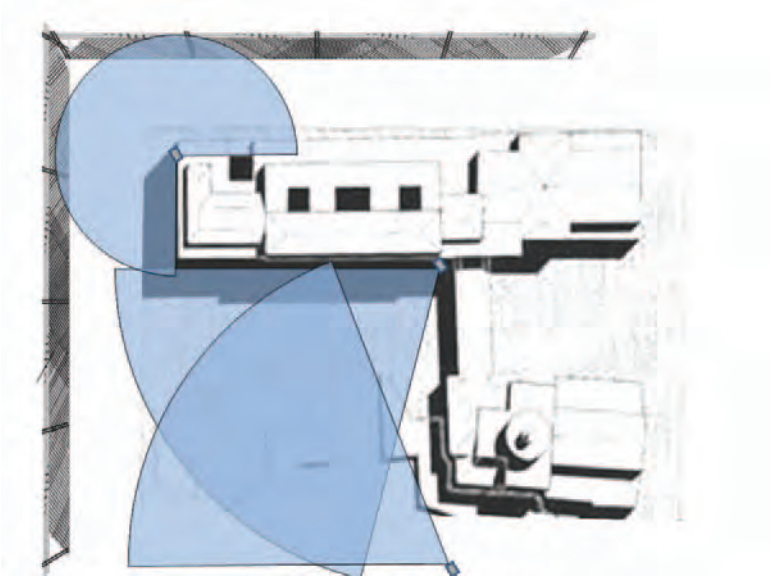
Passive infrared sensors effectively “see” the thermal image of the intruder. They alarm on movement of this thermal image.

Ground-based radar

Description: Like microwave, ground-based radars continuously scan large open areas, detecting movements within a defined perimeter. It is rarely used as a stand-alone intrusion detection system, but mostly in conjunction with intelligent tracking cameras. The ground-based radar is used as the initial detection device with the CCTV camera as the verification and/or tracking device.

Operating principle: Radar is based on the principle of sending pulses of long wavelength radiation from an antenna, and then detecting the energy that it bounces off a remote target. By calculating the speed of the radio waves and the time it takes for the signal to bounce off the object and hit the receiver, you can gauge the distance between the antenna and the object. Having multiple radars spaced apart covering the one area enables the system to receive multiple returns. All of these individual reflections are combined to estimate the size of the object or objects being struck in three dimensions.

However, all ground-based radar can do is notify you that something (hopefully an intruder) is there, but not what that something is. It also suffers from a lot of background 'clutter' or noise from stationary objects and environmental effects, such as trees swaying, passing traffic, etc. For this reason, ground-based radar is rarely used on its own, but mostly in conjunction with high-quality tracking cameras to verify any detection in an open area security solution. The ground-based radar is the detection device, with CCTV as the verification and tracking device which automatically locks onto and follows a target.



Ground-based radar / CCTV area coverage

Due to their high sensitivity and wide area coverage, these radars usually generate substantial background 'noise' or 'clutter', especially when operating adjacent to populated areas. To reduce such noise, radars are optimized to cover shorter ranges, and implement special filtering algorithms which improve their performance in populated areas.

Application: Combined ground-based radar/CCTV systems can provide an effective intrusion detection system for large flat open spaces – applications include airports or sites facing water – especially those difficult areas where you don't want a physical barrier, or cannot install one, such as over water or on a coastline. These combined systems have a maximum detection range of typically 600 to 3,000 feet (200 to 900 meters).

Coverage and protection is line-of-sight only, so normally not suitable for sites with buildings; sites with shrubs, bushes and trees; parked vehicles; or where the terrain is not perfectly flat, as each of these scenarios creates radar 'shadows' where intruders can hide undetected.

Strengths: Provides an 'electronic' perimeter, where physical fences or barriers aren't possible. Depending on the combination of day, night and thermal cameras selected, can operate in all weather and light conditions and can detect a variety of targets, including people, vehicles or boats over water. Has the potential to be used as a rapid deployment or portable system.

Weaknesses: Cost – it is expensive to install and set up as you need both the radar systems and an intelligent CCTV system, but in some cases you may be able to utilize existing cameras if suitable. Requires infrared cameras if the area is subject to fog or rain. Needs an infrastructure to provide power and communications interface (often TCP/IP). Installation and configuring to find the right balance between good detection and low numbers of nuisance alarms can often be extremely complex and time consuming.

Potential causes of nuisance alarms: Problems with background noise or clutter, heavy rain, wildlife, moving vehicles, etc. For example, a group of ducks on a waterway may be seen as one large object by the radar, or a dog walking up to the perimeter fence can appear to the system to be a human crawling.

Typical methods of defeat: These are similar to microwave systems, blind spots caused by uneven terrain, hollows or shielding behind vehicles, buildings or equipment; tunneling beneath the protected area or bridging above the field.

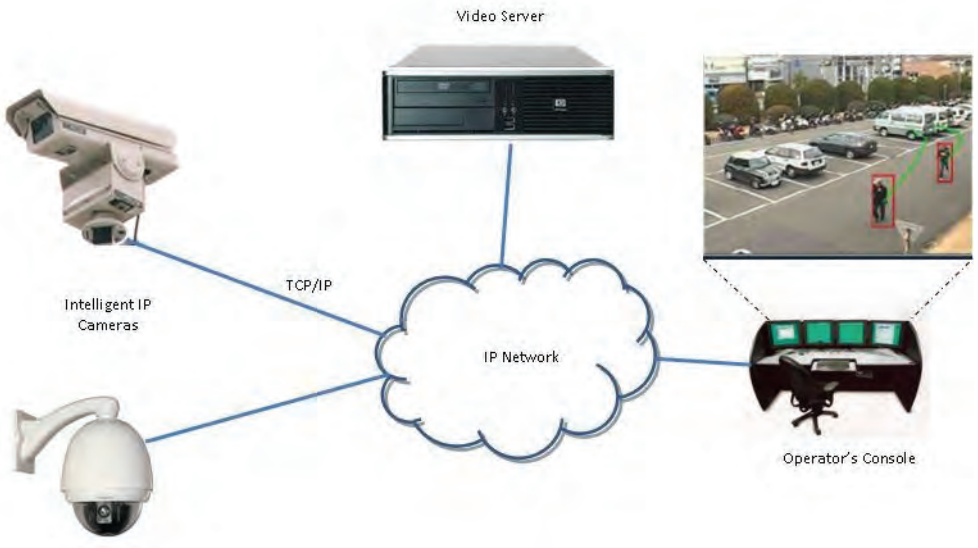
VIDEO SENSORS

Video analytics

Description: Video analytics is the practice of using computers to scan incoming video feeds and automatically identify items of interest without an operator having to constantly monitor the video. The most common uses of video analytics are intrusion detection, monitoring traffic, monitoring people, and license plate recognition.

For intrusion detection, video analytics enables security staff to use a good quality CCTV camera to provide both detection and a means of observing and monitoring intruders once they are detected. Linked to a digital video recorder (DVR), CCTV systems also provide forensic video documentation of an intrusion event and the intruder.

Operating principle: Video analytics is a technology that is used to analyze the video received from a camera for specific changes and behavior in the monitored area by comparing the current scene with a predetermined ambient scene of the area. When a sufficient change in the image pixels and/or image behavior is detected by the video analytics algorithms, such as that caused by a specific type of movement within the field of surveillance – an alarm signal is generated and the intrusion scene is displayed at the monitoring station.



IP video analytics system layout

There have been many advances in video analytics and intelligent video in recent years. Higher quality systems now include an image tracking feature that can monitor a number of separate intruders simultaneously by drawing a different colored line around each of them and creating a trail line of where they have been.

Initially, this video analysis was carried out in the camera, but more recently there has been a move to a "hybrid" type approach that splits the actual video analysis role between the camera and the video server. When the camera triggers a potential event, the frame rate of the system is increased and the amount of video that gets captured and stored is also increased. The sophisticated centralized video analytic servers then run through this captured video and perform more computer-intensive video analysis applications. This allows you to run video analytics on a broader range of cameras due to the lower processing power and intelligence required at the camera. Even though a dedicated server is required, an individual server can handle many cameras.

Application: Not to be confused with the traditional video motion detection (VMD) systems that have been in the market for many years, video analytics 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.

IP cameras are generally predicted as being the future of video surveillance at the expense of traditional analog systems. IP cameras connect to a standard computer network, allowing multiple cameras to transmit to a video server located anywhere on the network. If you have an existing analog camera installation and you want to replace or expand using IP cameras, the migration path is often a complex and costly process.

There is a trade-off between camera resolution and storage requirements. High resolution "megapixel" cameras are preferable for daytime image clarity, but the more high resolution cameras you have, the more storage required – often leading to the purchase of a dedicated storage cluster at considerable cost. This extra cost may make it difficult to justify high-resolution cameras for most applications.

Strengths: Can often 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. IP cameras connect to a standard computer network thereby reducing cabling.

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.

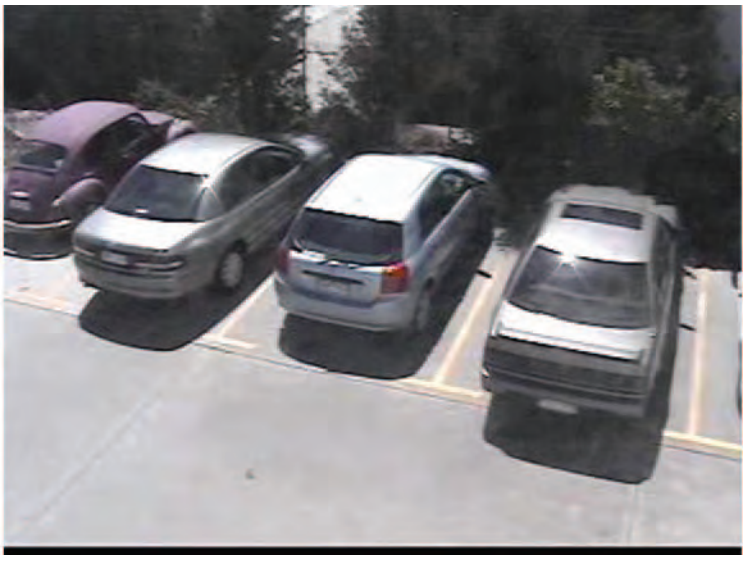
While video analytics holds great promise, there are still many questions regarding the viability of using video analytics in the real world. In the last few years, support for this technology has diminished with the key issues being nuisance alarms, with many video analytic systems generating dozens of nuisance or false alarms each day; system maintenance (both hardware and software) is an often overlooked and somewhat hidden issue in video analytics; and finally the high installed cost of a system with minimal nuisance alarms. Unfortunately, the high cost then encourages people to select cheaper systems that are more likely to generate nuisance alarms, exacerbating the situation even further.

As more and more cameras video servers and storage solutions move from analog to become IP based, integrators now require staff with significant IT skills to be able to set up and maintain complex networks both in the field and at the monitoring point.

There is still not a clear set of standards for IP-based cameras, and the industry is slow in addressing this. This lack of industry standards means many DVRs offer little or no support for IP cameras at all.

Potential causes of nuisance alarms: Natural light sources including sunrise or sunset; sudden brightness variations caused by fast-moving clouds, wind blown debris, severe weather conditions, large animals, flocks of birds, vibration of the camera or movement in the camera pole; man-made light sources such as passing vehicle headlights, traffic lights, and security lighting switching on and off.

Typical methods of defeat: Tunneling; blind spots within or moving beyond the cameras field of view; very slow movement; physical attack on, or the blinding of the camera.



Steady state picture of car park

Intruder appears and is recognized by the change in the image and the behavior of this change, an alarm is set, intruder tracking and recording begins

9

White Papers

FIBER OPTICS – A PRIMER

Dr Jim Katsifolis
Chief Technology Officer
Future Fibre Technologies Pty Ltd

INTRODUCTION

Optical fibers have become the standard communications carrier of choice having penetrated most levels of communications networks ranging from long-distance trunk lines and metropolitan area networks (MAN), to shorter distance local area networks (LAN) and, more recently, fiber-to-the-home (FTTH) systems.

Whilst optical fibers are best known for their applications in the telecommunications industry, they also find applications as sensors in a range of industries, which includes security.

HOW DO THEY WORK?

Typically, an optical fiber is a solid rod of high-purity glass which is made up of a central core region and a surrounding cladding. Plastic versions of optical fibers also exist, however, the glass optical fiber is the most commonly used.

Light is "guided" down the core of an optical fiber via total internal reflection at the core-cladding interface. This is achieved by designing the fiber such that the cladding has a slightly lower refractive index than the core.

A bare fiber is about the width of a human hair (about 0.004 inch) and is coated with a plastic covering called the "buffer coating" that protects it from moisture and other damage. Additional layers of protection are then added to achieve a ruggedized cable. A variety of cable configurations exist where multiple optical fibers are housed in loose and/or buffered tubes.

TYPICAL DIMENSIONS OF AN OPTICAL FIBER

Core diameter (single mode fiber) = 9 μm

Core diameter (multimode fiber) = 62.5 μm

Cladding diameter = 125 μm

Buffer diameter = 250 μm

1 μm = 0.001 mm

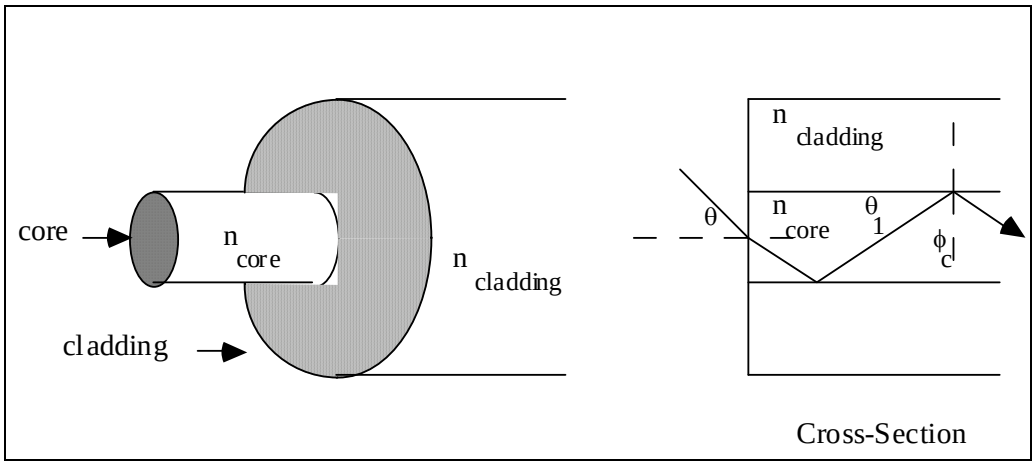


Fig. 1 *Light path through an optical fiber*

TYPICAL CABLE CONFIGURATIONS

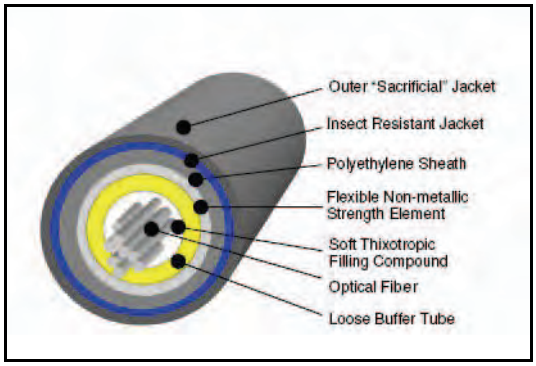


Fig. 2 *Single loose tube multi-fiber cable*

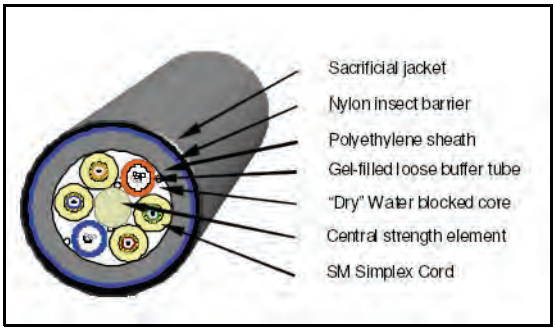


Fig. 3 *Multi-tube fiber cable*

(Source: Secure Fence and Secure Pipe cable datasheets,
Optimal Cable Services Pty Ltd)

TYPES OF OPTICAL FIBER

There are two categories of optical fibers – multimode (MM) fiber and single mode (SM) fiber.

MM fiber

MM fiber has a relatively larger core than single mode fiber (e.g. 62.5 µm versus 9 µm). When light is injected into a MM fiber, thousands of modes are excited and they simultaneously propagate. As an approximation, each mode can be thought of as a separate light-ray path propagating through the fiber. Depending on the design of the fiber these can be straight-line paths or curved paths, as in Fig. 4.

Remembering that light is an electromagnetic wave, a mode is more accurately described by the wave theory of light, and is essentially a standing-wave pattern for the electric field component of the light traveling through the fiber.

The larger cores of MM fibers allow easier light injection into the fiber from LED and laser sources, however, the existence of large numbers of modes leads to transit time differences between lower and higher order modes known as intermodal dispersion, a form of pulse spreading. This restricts MM fibers to low-speed to medium-speed communication systems for short-haul to medium-haul applications (typically, < 1 km @ 500 Mb/s,
< 5 km @ 100 Mb/s).

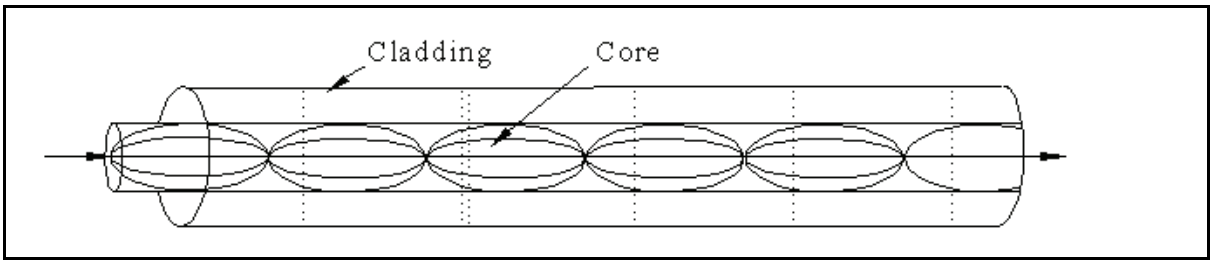


Fig. 4 *MM fiber*

SM fiber

SM fiber has a much narrower core and allows only one mode of light to propagate through the core. It is typically used for medium-haul and long-haul applications, such as telephony, data communications and CATV, but also finds applications in many shorter haul communication systems.

The existence of only one mode minimizes the amount of spreading (or dispersion) of a light pulse traveling through a fiber. This optimizes the SM fiber for use in high-speed digital communication systems (> 10 Gb/s) making it the most used type of fiber worldwide. The trade-off with smaller core diameters is an increase in difficulty when injecting light into the fiber, however, these challenges are easily overcome by using correct optical source coupling design.

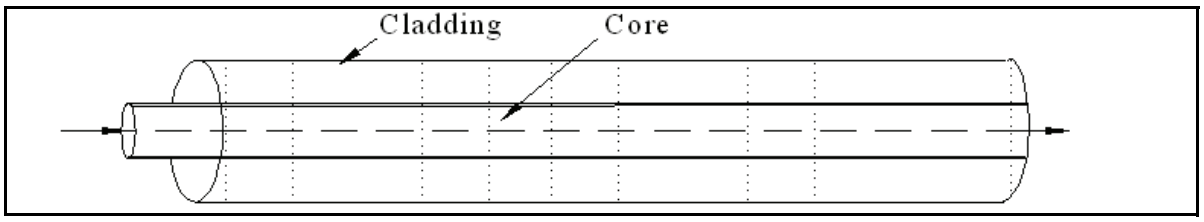


Fig. 5 *SM fiber*

OPTICAL FIBERS AS SENSORS

With a few exceptions, most communications systems employ digital optical signals and are, therefore, normally concerned with distinguishing the amplitude of received light pulses from the background noise. There are, however, other properties of the propagating light in an optical fiber which can respond to a number of stimuli such as temperature, strain, pressure, and vibration.

By monitoring and detecting changes in a light wave's property, such as a change in intensity, attenuation (loss), phase, or wavelength, an optical fiber can be used as a sensor. An added advantage is that because the wavelength of light is in the order of millionths of a metre (micrometres), the sensitivity of fiber sensors is very high. Even the smallest perturbations will cause a change in some of the light's properties. Fiber sensors can be used to directly measure strain, vibrations, temperature, pressure, rotation, and even magnetic fields. Applications which employ optical fibers as sensors include hydrophones, gyroscopes, temperature monitoring and profile, security, and electrical current sensing to name a few.

WHY USE OPTICAL FIBERS AS SENSORS?

When it comes to perimeter security systems, optical fibers offer distinct advantages over conventional sensing technologies. Because they are made of non-conducting materials they are intrinsically safe and require no power in the field. Importantly, they are immune to electromagnetic interference (EMI and RFI) and lightning. Other advantages include ease of installation, consistency over long distances, and high reliability with negligible in-field maintenance.

MICROSTRAIN/LOCATOR TECHNOLOGY – A PRIMER

Dr Jim Katsifolis
Chief Technology Officer
Future Fibre Technologies Pty Ltd

INTRODUCTION

Future Fibre Technologies Pty. Ltd. (FFT) was established in 1994 and develops and manufactures highly advanced intrusion detection systems for the security industry. These world leading intrusion detection systems employ standard optical fiber cables as distributed sensing devices.

FFT's core products comprise the following advanced fiber optic intrusion detection systems:

- *FFT Secure Fence* for fiber optic perimeter intrusion detection systems
- *FFT Secure Pipe* for oil and gas pipeline third party interference detection
- *FFT Secure Link* for data communications security.

FFT's intrusion detection systems have been deployed in hundreds of sites worldwide protecting military bases, government installations, LNG plants, petrochemical plants, refineries, and many other high-value assets and critical infrastructure.

Fig. 1 *FFT Secure Fence system*

At the heart of FFT's products is its field-proven Microstrain/Locator (M/L) technology. The M/L technology is based on optical interferometry which is realized using optical fibers. Interferometry is a well-established and proven highly sensitive detection technique.

OPTICAL INTERFEROMETRY

The most basic optical interferometers are typically achieved by splitting a light signal into two paths and then recombining them to create an interference pattern. The interference pattern is a result of coherently mixing or "interfering" the two light signals. If the two light signals are in phase they will constructively interfere to give a maximum output. If they are 180 degrees out of phase, they will destructively interfere to give a minimum. The interference signal can, therefore, be related to the difference in phase between the two interfering signals. A change in phase in one or both light paths can be caused by an effective change in path length.

An optical interferometer can be achieved in free space using a laser with bulk optics devices such as beam splitters/combiners and mirrors. A laser beam is split into two paths. The interference of the two beams produces an interference fringe pattern which is a series of alternating dark and bright bands. The most common types of optical phase interferometers are the Mach Zehnder (MZ), Michelson, and Sagnac interferometers (not shown here). Examples of a free-space MZ and a Michelson interferometer are shown in Fig. 2, and Fig. 3 on page 90. Note the use of 50:50 beamsplitters/combiners and mirrors which have to be precisely aligned.

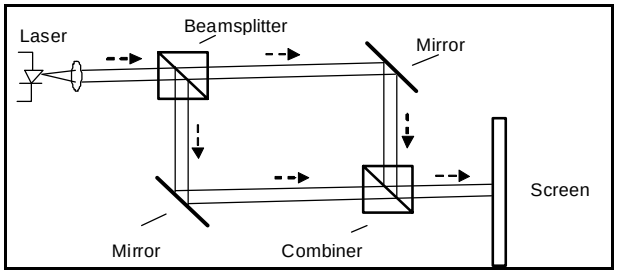


Fig. 2 *Free-space Mach Zehnder interferometer*

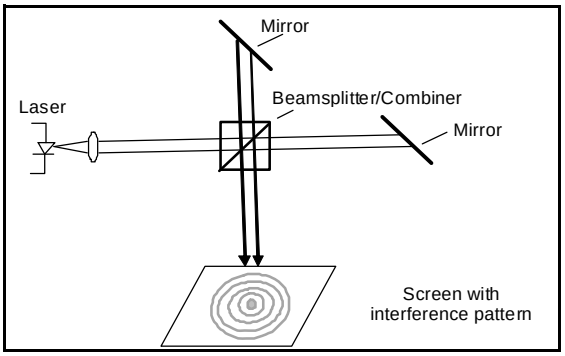


Fig. 3 *Free-space Michelson interferometer*

Free-space interferometers, however, are not feasible for realizing practical intrusion detection sensors. The use of a confining optical guide is required to allow for the most flexibility in design and application. This can be achieved by using a fiber-based interferometer where the free-space light paths described earlier are replaced with standard telecommunications-grade optical fibers, and the bulk optics devices with fiber-based equivalents. Beamsplitters and combiners are replaced with fiber couplers, whilst the optical paths are confined within single-mode optical fibers. Examples of equivalent fiber optic Mach Zehnder and Michelson interferometers are shown in Fig. 4 and Fig. 5.

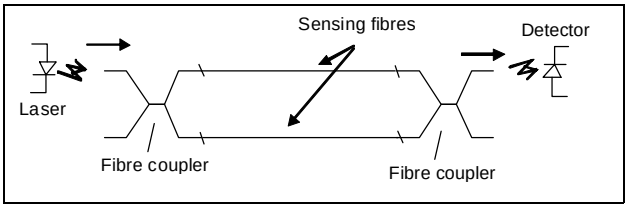


Fig. 4 *Basic fiber optic Mach Zehnder interferometer*

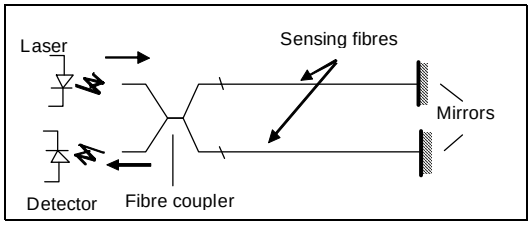


Fig. 5 *Basic fiber optic Michelson interferometer*

The detected signal is an electronic representation of the free-space interference pattern which is effectively a sinusoidal intensity signal which varies with the phase difference between the arms. A perturbation to either or both of the sensing fibers which causes a change in the phase difference between the arms will cause a change in the intensity received by the detector.

WHY ARE INTERFEROMETERS SO SENSITIVE?

Fiber-optic interferometers exhibit a high sensitivity to vibrations, strain, and other physical disturbances which act upon the sensing fibers. Their high sensitivity can be accounted for by the fact that light is used to perform the interferometry. The wavelength of light typically used in these applications is in the order of a millionth of a metre (micrometers). Any sub-wavelength path length mismatch between the two interfering arms will lead to a significant phase difference. Sub-wavelength changes in path lengths can be readily caused by physical perturbations on the optical fiber arms, such as vibrations, strain, or temperature. The interferometer is, therefore, very sensitive to small vibrations or disturbances.

FFT MICROSTRAIN/LOCATOR

FFT's Microstrain/Locator technology is based on a distributed bidirectional fiber optic MZ interferometer where the two interfering arms can be incorporated within the same or separate standard optical fiber cables. The one sensing system performs both real-time detection and location of an intrusion. It also includes an insensitive lead-in and lead-out fiber which can also be incorporated in the same or separate cables. This allows for maximum flexibility in sensing configurations.

The detection of an intrusion event of interest is achieved by processing the interference signal during a perturbation. This involves a combination of signal processing techniques in both the time and frequency domains and applying advanced signal recognition and discrimination techniques.

The location of an intrusion event is determined simultaneously with its detection, and is achieved by measuring the time difference between the received counter-propagating signals. Both the detection and location of the intrusion event can be determined in real-time to better than 30 yards.

Whilst historically most conventional MZ sensors have been short in sensing length, FFT's sensing technology applies the MZ sensor to much longer lengths, in some cases up to 50 miles in optical path length. This makes them ideal for use as an intrusion detection sensor for a wide variety of applications including long-distance perimeters and pipelines.

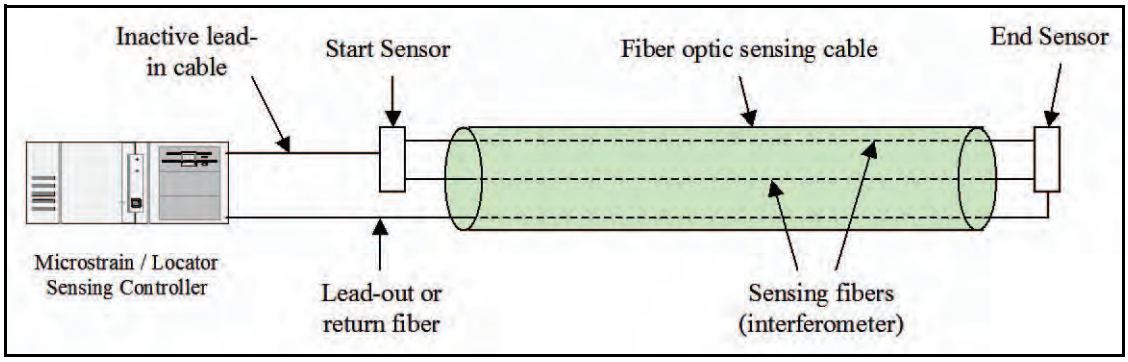


Fig. 6 *Block diagram of FFT Microstrain/Locator system*

FROM THE LAB TO THE FIELD

While with the right equipment a functional fiber optic interferometer can be easily assembled in the laboratory, achieving a fully functional interferometer in the field is vastly more complex. One of the real challenges in developing a fiber optic sensor for security applications is taking this technology from the lab to a practical application in the real world. Given its high sensitivity, a fiber optic interferometer will be sensitive to a large number of parameters other than real intrusion events, such as environmental factors like temperature, rain, and wind, as well as a range of ambient noise sources. This requires the use of advanced signal processing techniques to eliminate these non-intrusion events.

FFT's Microstrain/Locator technology has been engineered into a number of solutions which meet customers' requirements and specifications for intrusion detection systems:

i) **Stable and repeatable performance** The most important aspects of any fiber optic sensor are its stability and repeatability of performance. This arises mainly from the sensor's high sensitivity and susceptibility to environmental factors. This includes such factors as varying fiber birefringence which affect the light's polarization and the system's sensitivity and accuracy. FFT's Microstrain/Locator technology employs suitable optoelectronics hardware and software control algorithms for maintaining system stability and repeatability to provide consistent detection and location accuracy.

ii) **Ranging operating conditions** Intrusion detection systems are required to operate over a large range of environmental conditions. FFT has engineered its Locator products to provide stable and repeatable performance for a range of environments and conditions. This is a testament to FFT's decades of experience in applying fiber optic sensing systems to real-world sensing applications.

iii) **Event Recognition and Discrimination** One of the important challenges of any intrusion detection system is to maintain a high detection rate whilst minimizing the nuisance alarm rate. Most systems typically achieve this by simply reducing the overall sensitivity of a system to cope with increases in nuisance events and signals. The downside of this is that an actual intrusion may be missed.

FFT's Microstrain/Locator technology has been engineered into a number of solutions which meet customers' requirements and specifications for intrusion detection systems:

iv) **Stable and repeatable performance** The most important aspects of any fiber optic sensor are its stability and repeatability of performance. This arises mainly from the sensor's high sensitivity and susceptibility to environmental factors. This includes such factors as varying fiber birefringence, which affect the light's polarization and the system's sensitivity and accuracy. FFT's Microstrain/Locator technology employs suitable optoelectronics hardware and software control algorithms for maintaining system stability and repeatability to provide consistent detection and location accuracy.

v) **Ranging operating conditions** Intrusion detection systems are required to operate over a large range of environmental conditions. FFT has engineered its Locator products to provide stable and repeatable performance for a range of environments and conditions. This is a testament to FFT's decades of experience in applying fiber optic sensing systems to real-world sensing applications.

vi) **Event Recognition and Discrimination** One of the important challenges of any intrusion detection system is to maintain a high detection rate whilst minimizing the nuisance alarm rate. Most systems typically achieve this by simply reducing the overall sensitivity of a system to cope with increases in nuisance events and signals. The downside of this is that an actual intrusion may be missed.

FFT's Microstrain/Locator technology employs a far superior approach by using advanced event recognition and discrimination techniques. At the heart of these techniques is FFT's Alarm Recognition and Discrimination (ARaD) algorithms which allow for the recognition of nuisance events, and clear discrimination between nuisance and real intrusion events. This is crucial for minimizing nuisance alarm rates whilst maximizing intrusion detection rates. For example, FFT has consistently demonstrated in a large number of Secure Fence systems the successful suppression of nuisance alarms during torrential rainfall levels exceeding 4 inches/hour whilst simultaneously detecting and locating attempted intrusions.

Fig. 7 *FFT Secure Fence system on US–Mexico border. The fiber sensor is embedded within a conduit.*

ELIMINATING NUISANCE ALARMS THROUGH THE USE OF ARTIFICIAL INTELLIGENCE

Alec Owen
International Client Manager
Future Fibre Technologies Pty Ltd

INTRODUCTION

Lightning, storms and other environmental conditions are definitely not the security industry's friend, creating many nuisance alarms. But you no longer have to put up with these types of nuisance alarms as today there is the technology available to eliminate them.

As an example of the effectiveness of Artificial Intelligence in analyzing and eliminating nuisance alarms, these sorts of environmental conditions are experienced on a regular basis along the perimeter of a major gas turbine power station in one of the most lightning prone regions in the world.

This coastal site is regularly subjected to extreme weather conditions, including cyclonic winds, year-round temperatures in the mid to high 30 degree range (Celsius), and very high levels of tropical rainfall – in excess of 4 inches or 100 mm per hour at times. It also has one of the world's highest incidents of lightning, recording more than 30,000 lightning strikes every year. Yet nuisance alarms are not a problem for them.

The perimeter intrusion detection system they selected incorporates Artificial Intelligence (AI) in the signal processing, which overcame the problems of nuisance alarms that plagued traditional intrusion detection solutions in this type of application. Artificial Intelligence employs signature recognition and advanced signal processing to clearly identify what is an environmental event and what is an attempted intrusion, thus avoiding nuisance alarms.

You no longer need to put up with nuisance alarms – the technology is available to separate:

- intruders from lightning
- terrorists from wind and rain
- teenage vandals from wildlife.

The aim of this white paper is to give you a better understanding of how Artificial Intelligence (AI) eliminates nuisance alarms, and the significant benefits it brings to intrusion detection systems. You will then be armed with the right information and questions to put to your vendors. Only then can you know if you are getting the right answers and selecting the best intrusion detection technology.

EVALUATING INTRUSION DETECTION TECHNOLOGIES

Like any technology, intrusion detection systems continue to evolve. Although new and improved hardware is continually being developed around the world and introduced into the marketplace, rarely do the fundamental detection principles and applications change.

The bulk of the development work today appears to be not on new intrusion detection technologies, but rather on reducing the number of nuisance alarms generated, that is, where an alarm condition is reported without an actual intrusion occurring. These nuisance alarms are typically caused by environmental conditions such as wind, rain, passing traffic, and lightning. Frequent nuisance alarms are both inconvenient and expensive to respond to and ultimately erode any confidence security staff have in the effectiveness and value of the intrusion detection system installed. Nuisance alarms can also mask or hide real intrusion events, leaving your critical assets open to unnecessary risk.

Three important performance parameters you need to look at when evaluating the performance of any intrusion detection system are the Probability of Detection (POD), Nuisance Alarm Rate (NAR), and the False Alarm Rate (FAR).

The POD is determined by the sensitivity and design of the detection sensor, and also by the quality of the actual installation itself. The experience, knowledge and skills of the intruder also play a role – for example, a teenage vandal will give a much higher POD than a highly trained special-operations person.

Nuisance alarms are intrusion alarms generated on the sensor by non-intrusion events. The NAR is generally determined by environmental conditions such as wind, rain, wildlife, vegetation, traffic, etc. but also by the system sensitivity. Nuisance alarm rates and the probability of detection are different for each installation and definitely site specific. While it is possible to use manufacturer quoted figures as a rough guide, the final figures can only be determined on site as part of a formal test regime, not in a lab or at the manufacturer's test site.

False alarms on the other hand are alarms generated by the intrusion detection system itself and not by the field sensor.

How intrusion detection systems worked

Almost all intrusion detection systems to date, regardless of whose or what particular technology is employed, are based on the same core principle of establishing a steady background state and then continually monitoring it to detect any change above or below a predetermined threshold which indicates that some sort of an event (hopefully an intrusion) has occurred on the perimeter fence.

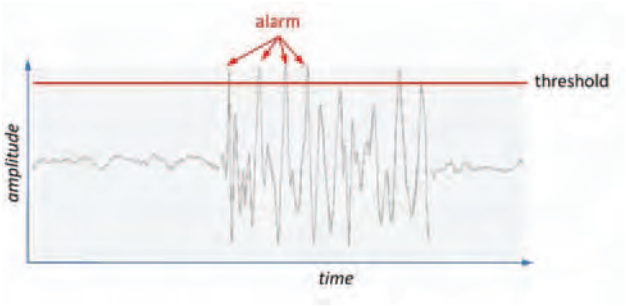


Fig. 1 *If the signal goes above the threshold line, then it is an alarm*

The most basic perimeter intrusion detections systems available use a simple threshold method. If the signal detected on the sensor crosses this threshold line, then it is an alarm If it is below the line, then it is not an alarm.

If you get nuisance alarms or want to reduce the sensitivity of the system, simply move the threshold level higher. And if the system is not sensitive enough, move the threshold lower.

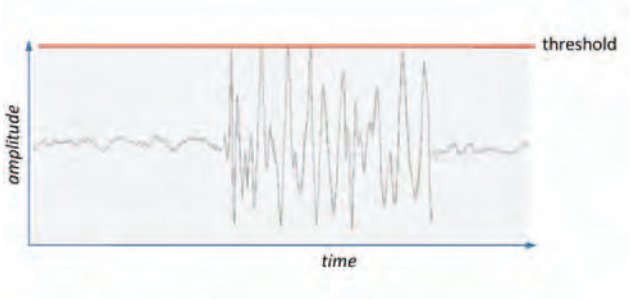


Fig. 2 *If the threshold is set too high, then there is poor sensitivity*

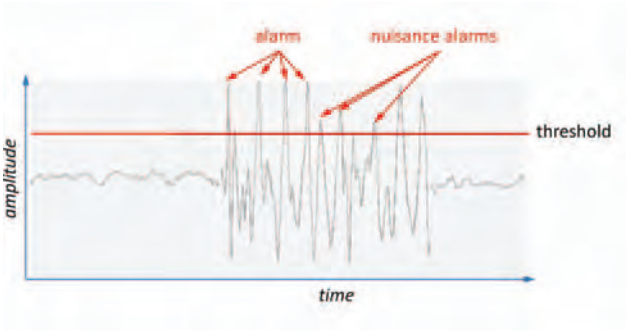


Fig. 3 *If the threshold goes too low, then you will get nuisance alarms*

While this may appear to work OK in a static or controlled environment, unfortunately it does not perform well in the dynamic "real" world. As the wind increases, for example, so does the background signal level, as it will for events such as heavy rain, traffic, vegetation blowing on the fence as well as a multitude of other environmental causes. These changes in background levels make accurate detection of a real intrusion event much harder, and masking of an intrusion far more likely.

There have been attempts to make this threshold dynamic by attaching an anemometer (a wind measuring device) or a weather station, so that as the wind speed increased, the threshold would also increase. While this and similar techniques may possibly reduce the number of nuisance alarms due to wind, it can also simultaneously reduce the system's sensitivity to real intrusion events or the POD.

There have also been some fairly rudimentary attempts at signal processing, such as counting how many of these peaks or pulses exceed the threshold over a set period of time. While this may have helped with the one-off short duration events, such as a stone thrown at a fence, it then

became a problem trying to detect someone cutting the fence one wire at a time.

Unfortunately, the trade-off for this is a reduced POD when trying to detect an intrusion event that occurs simultaneously with a nuisance event. An example of this would be trying to detect someone climbing or cutting a perimeter fence during torrential rain or strong winds.

Simple analog frequency filtering is another method used to try and separate nuisance alarms from intrusions, but often these two events share the same frequency band, so eliminating nuisance alarms also results in a reduced POD.

So you can see, in the past there have been a lot of trade-offs going on in order to reduce nuisance alarms whilst attempting to maintain a sensitivity level high enough to detect legitimate intrusion events.

As we all know, it makes sense to have the ultimate sensitivity in any intrusion detection system to maximize the probability of detection (POD). However, in the past this increased sensitivity has led to a corresponding increase in the nuisance alarm rate (NAR), leading to the eternal performance trade-off between POD and the nuisance alarm rate of an intrusion detection system.

These days, there are far more sophisticated methods available to reduce nuisance alarms on intrusion detection systems. Gone are the old moving thresholds and counting pulses, replaced instead by powerful and highly advanced signal processing and Artificial Intelligence (AI). The goal continues to remain the same as it has always been – to identify and then completely eliminate nuisance alarm signals, yet still maintain sensitivity to intrusions – just the techniques available to achieve this have advanced. Significantly.

Artificial Intelligence

AI, incorporating neural networks and advanced multi-parameter signal processing, dramatically improves the recognition and detection of real intrusion events against a background of nuisance events. This allows intrusion detection systems to minimize nuisance alarms without trading off the sensitivity or probability of detection to a genuine intrusion event.

The following picture is a fairly dramatic example of an actual intrusion detection occurring at the same time as a nuisance event – in this particular case, torrential rain. Normally this intrusion would remain undetected, and your asset would be at risk.

The requirements for the ideal perimeter intrusion detection system in torrential rainfall areas are that it:

- automatically identifies the presence of rain and minimize its effects.
- discriminates between an intrusion event and torrential rain.
- detects an intrusion during torrential rain.

But by using AI, we can allow full system sensitivity to be maintained and effect of nuisance event (in this case rain) to be suppressed.

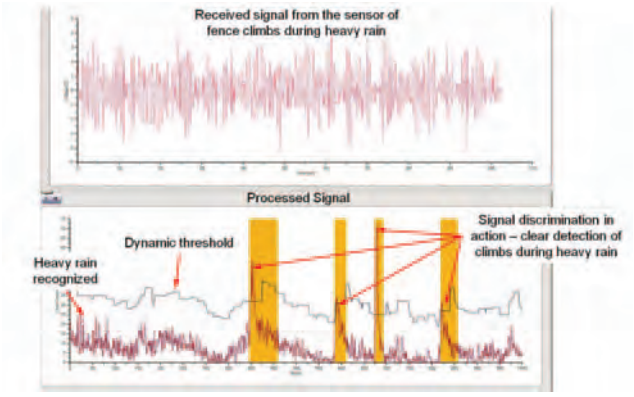


Fig. 4 *An example of intrusion detection during simultaneous nuisance event*

As can be seen in the image above, by recognizing a signature buried within a "rain" signal, the system will ignore the continuous nuisance or background signal caused by rain in this case. At the same time it still maintains its capability of picking out a single true intrusion signal occurring simultaneously during this heavy rain without any loss of sensitivity at all, and processes this signal to alarm and locate the intrusion.

By employing AI, this nuisance mitigation algorithm adjusts to varying levels of rain (or other sources of nuisance alarms) but, importantly, never reduces the intrusion event sensitivity. Once the rain stops, the system recognizes this and dynamically returns to its normal mode of operation. Using this technique, rain-induced nuisance alarms, as in this example, can be minimized or even eliminated.

This is AI in action. Without AI, the system would be either continually alarming, or the cutting and subsequent intrusion activities would remain completely undetected.

Only a few years ago this technology was confined primarily to the military and aerospace industries, and used in biometric identification systems, biomedical signal analysis, speech recognition, imaging, and telecommunications to name just a few.

Now it has become mainstream in the latest generation of intrusion detection systems.

Using Artificial Intelligence to Analyse Signals

Traditionally, intrusion detection systems flagged an alarm to the security staff, who then look at the alarm information, the environmental conditions, maybe listen in to the signal on the fence, have a look with the CCTV, and use their experience to decide if this is a real alarm or not. This process is notoriously inconsistent, slow, highly subjective, and relies heavily on the experience of the operator.

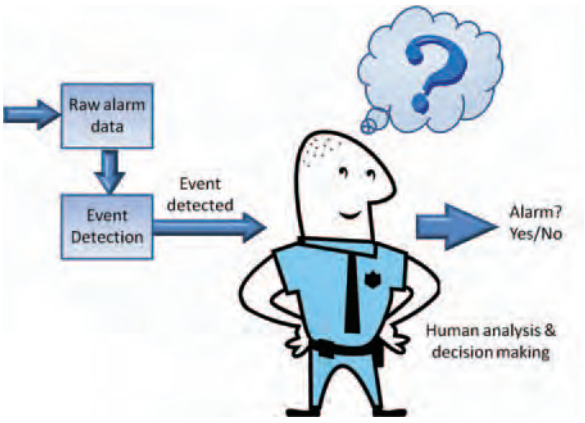


Fig. 5

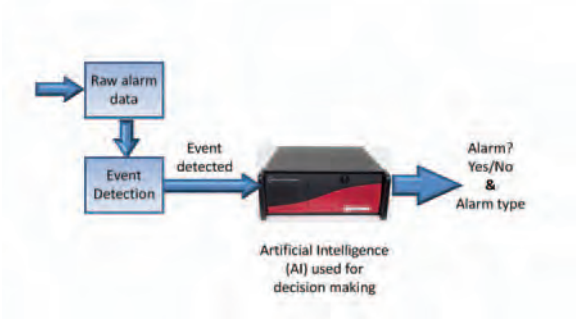


Fig. 6

Artificial Intelligence, however, not only performs this task automatically, but in a far more detailed manner by analyzing all of the available raw alarm data, much quicker – in fractions of a second – far more consistently, and yielding far more reliable results than a human brain. It requires no operator intervention at all to analyze the signal to determine of it is a genuine intrusion event or a nuisance alarm. Not only do you get a simple consistent and reliable YES/NO answer, but it can also perform event recognition to identify and notify you of the type of intrusion that is happening, such as cutting the fence, climbing the fence, throwing a stone on the fence, etc.

How does it work?

Artificial Intelligence builds mathematical models that simulate the human neural or thought processes. In simple terms, AI replicates in software how your brain makes a decision.

Neural networks, as used in artificial intelligence, are non-linear statistical data modeling or decision-making tools based on statistics and signal processing. They can be used to model complex relationships between inputs and outputs or to find patterns in data. It is these patterns in the alarm data that are of specific interest and useful for intrusion detection.

What has attracted the most interest in neural networks by far is its ability to “learn” using a set of observations gained from the sensor on the fence, and then making a decision if it is a real intrusion or a nuisance event.

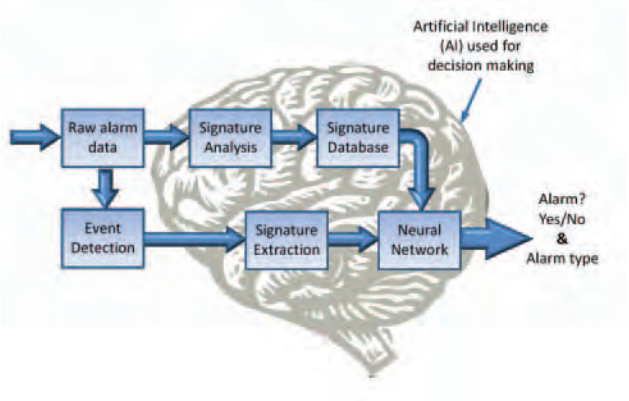


Fig. 7

The simplest way to explain AI is to look at how your own brain recognizes the difference between, for example, a dog and a cat using “human intelligence.”

As a child, you were trained by your parents to identify what is a dog and what is a cat. Although they may seem very similar in size and appearance, where both have four legs, both have a tail, both have fur and ears, etc. there are some subtle differences or features – the shape of the face, type of fur, size and shape of the ears, the sounds they make, behavior, and so on. Your parents implanted this information into your mind as a child – training your brain to recognize and differentiate between these two types of animals.

Fig. 8

Now whenever you see an animal, you can use this training to identify or classify if the animal you are looking at is a dog or a cat or some other sort of animal. The more unique features you can identify the more accurate your classification of the animal will be.

AI does exactly the same thing, but in this case not with cats and dogs, but with real intrusion events and nuisance events.

The Training Path

Just as with the human mind, there are two main parts to AI – the training or learning path, and the processing or classification path.

The training stage involves the analysis of captured raw signals from the sensors in the field. The unique signatures or parameters of different intrusion events are identified through multi-parameter signal analysis, such as level crossings, time–frequency analysis, wavelets, harmonic frequency, etc. These signatures (or features) can then be used to develop algorithms for the real-time classification of intrusion and nuisance events by the neural network.

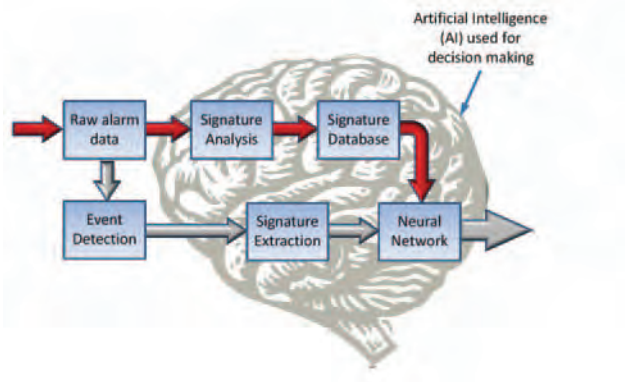


Fig. 9

This is the equivalent of a child learning about dogs and cats by recognizing their unique features.

This training is quite simple to do and is carried out as a part of the commissioning of the system, adding the signatures of specific environmental, and fence features that are unique to each site into the signature database.

This way the AI is tailored or trained for a specific site, and not just a "one size fits all" approach, as no two sites ever have the same environmental conditions.

The Processing or Classification Path

This is what happens once the system has been trained and is now operational.

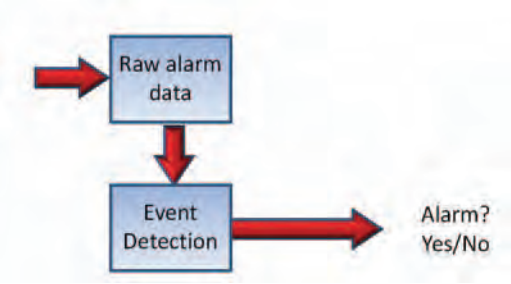


Fig. 10

The raw alarm signal or data is analysed in the Event Detection stage to carry out a first pass to see if there is an event of interest. This could be a real alarm, a nuisance alarm, or just something we are not sure of at this stage. This is the equivalent of the child saying I know there is an animal there, but I am not sure if it is a cat or a dog.

This is fundamentally how traditional intrusion detection systems work, but they fail to go much further than this with the signal analysis, instead relying on security staff to analyze the event and make a decision. This is like the child having to ask Mum or Dad if it is a cat or a dog.

We use this event detection or event of interest as just the starting point for the AI process.

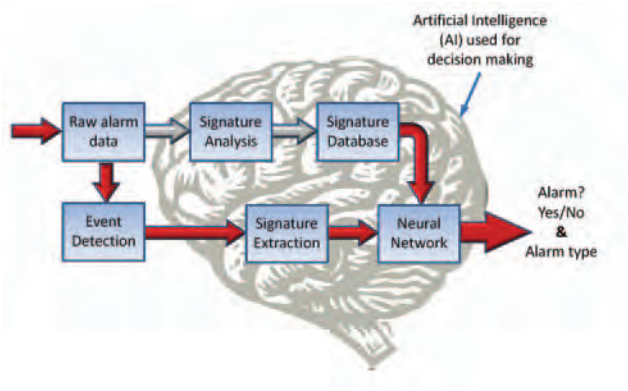


Fig. 11

The unique features or 'signature' of the events detected are extracted from the raw alarm data, and fed into the Neural Network part of the AI. The Neural Network actually does the decision making by taking the extracted signature and data from the signature database and then 'decides' using mathematical algorithms if they are a match and therefore an alarm or not. The Neural Network classifies these events or signatures in real-time. So not only will it provide a simple Yes/No for an alarm, but it can also tell you what caused the alarm. Instantly.

The key to signal recognition in intrusion detection systems is the signature analysis techniques used, that is, identifying the unique features within an event signal to accurately classify it and then discriminate it from other non-intrusion event signals.

This is the equivalent of you identifying what is a dog and what is a cat, in a range of environment conditions, such as during rain or at night, as well as identifying what the breed of dog is regardless of the size or color – without having to ask Mum or Dad.

WHERE AI CAN BE A SIGNIFICANT HELP

Even the best can sometimes get it wrong. Site-specific environmental conditions combined with the wrong choice of perimeter intrusion detection technology can pose a serious problem for the integrator and the customer. The more challenging the environmental conditions the sensing technology has to operate in, the more difficult it is to manage and control nuisance alarms – often to the stage where the system will simply not pass customer acceptance after months of testing. The sensors can trigger nuisance alarms, alerting when it's too windy, rainy, or a squirrel gets too close.

As older legacy technologies using thresholds as the trigger points are simply unable to differentiate between an environmental alarm and an intrusion. They alert you that the signal from the perimeter has exceeded the base level – but not what actually caused it. With an AI solution, the results can be completely different. AI-based perimeter intrusion technology can effectively identify and handle nuisance alarms in situations such as these.

CONCLUSION

When evaluating any perimeter intrusion detection system, 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) – the Holy Grail – would exhibit a zero NAR and a 100% POD simultaneously, and be completely undefeatable.

The probability of detection (POD) provides an indication of a systems ability to detect an intrusion within the protected area. The POD depends not only on the characteristics of the particular sensor, but also the environment, the method of installation and adjustment, and the assumed behavior 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 from a professional thief or special operations person for whom the POD will almost certainly be substantially lower.

Almost any sensor manufacturer can quote and offer a 99.99% POD under ideal conditions, that is, a large target and sensor sensitivity set to maximum. Of course, at maximum sensitivity both the confidence level and the NAR may be totally unacceptable.

This is why it is important to understand what the simultaneous POD and NAR figures will be, that is, what can realistically be expected in the field with a real-world installation (this will often be site dependent) and how it matches the customer expectation. For example, an operator may be quite willing to tolerate a greater NAR to increase the sensitivity or POD of the system.

Signal discrimination and the way sensor information is analysed have undergone major developments and advances in recent years. This is only possible because of the large amount of multi-parameter sensing information that can be collected by the newer and much smarter technologies, such as interferometric fiber optic fence-mounted sensors, and the processing power available from the multiple CPUs in the centrally installed controllers to run AI, signal fingerprint and pattern recognition type software. This amount and level of processing is typically not available from distributed processing architectures, that is, where you have multiple microprocessor-based sensor controllers installed in the field. The amount of computing required is typically far more intensive than distributed microprocessors will ever be capable of.

Around half of the human brain is used in acquiring and processing visual information. To have an AI-based intrusion detection system emulate this, you need to obtain as much information as possible from the sensor in the field. Like the human eye, the more you can see, the better the result, so the quality of the intrusion detection sensor and the information available from it is also critical to the system performance. No amount of AI can overcome a fundamentally poor sensor technology.

Advanced Artificial Intelligence technologies allow the detection system to be made highly sensitive to intrusions without the penalty of nuisance alarms. It's this type of technology that will help you deliver first class security, and it's this type of technology you should expect vendors to recommend.

This leads me to suggest three key questions to ask your intrusion detection system vendors:

1 Does your system utilize advanced signal processing techniques?

2 Does your system employ Artificial Intelligence to eliminate nuisance alarms?

3 Do you use centralized CPUs for signal processing?

Regardless of who your vendor is, look for a tick in each of these boxes. If they can't provide all three ticks, then look for another product. It's that simple.

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

ALARM RECOGNITION AND DISCRIMINATION FOR FIBER OPTIC INTRUSION DETECTION SYSTEMS

Dr Seedahmed Mahmoud
Senior DSP Engineer
Future Fibre Technologies Pty Ltd

Dr Jim Katsifolis
Chief Technology Officer
Future Fibre Technologies Pty Ltd

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. 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 categorized 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 maximize 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 does reduce 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 favor 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 recognize 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 fiber cables as truly distributed sensing devices.

Fig. 1 *FFT Secure Fence system*

FFT's core products comprise the following advanced fiber optic intrusion detection systems: FFT Secure Fence for fiber optic perimeter intrusion detection systems (as shown above); 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 fiber optic MZ interferometer, where the two interfering arms can be incorporated within the same or separate standard optical fiber cables (as shown in Fig. 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 fiber which can also be incorporated in the same or separate cables. This allows for maximum flexibility in sensing configurations.

Implementing intrusion detection systems with optical fiber 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.

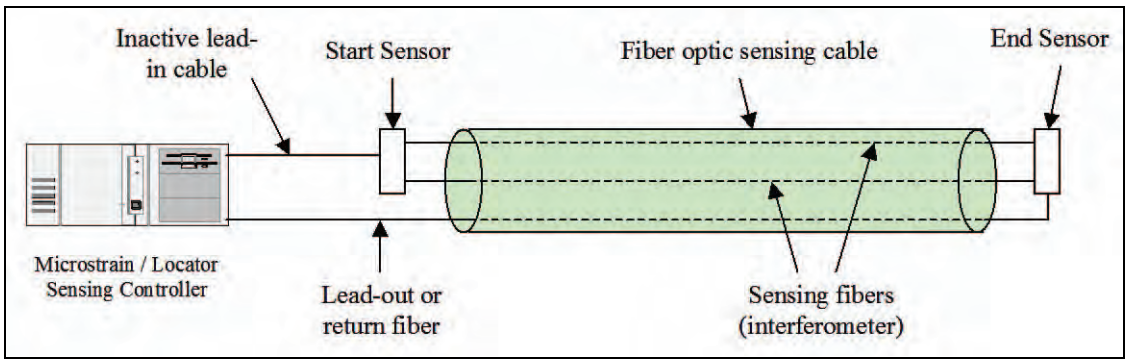


Fig. 2 *Block diagram of FFT Microstrain/Locator system*

MINIMIZING NUISANCE ALARMS IN FFT'S INTRUSION DETECTION SYSTEMS

By leveraging the advantages of using fiber 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 fiber.

To mitigate against environmental nuisance events, such as tropical downpours, FFT's intrusion detection systems are also capable of recognizing 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/hour.

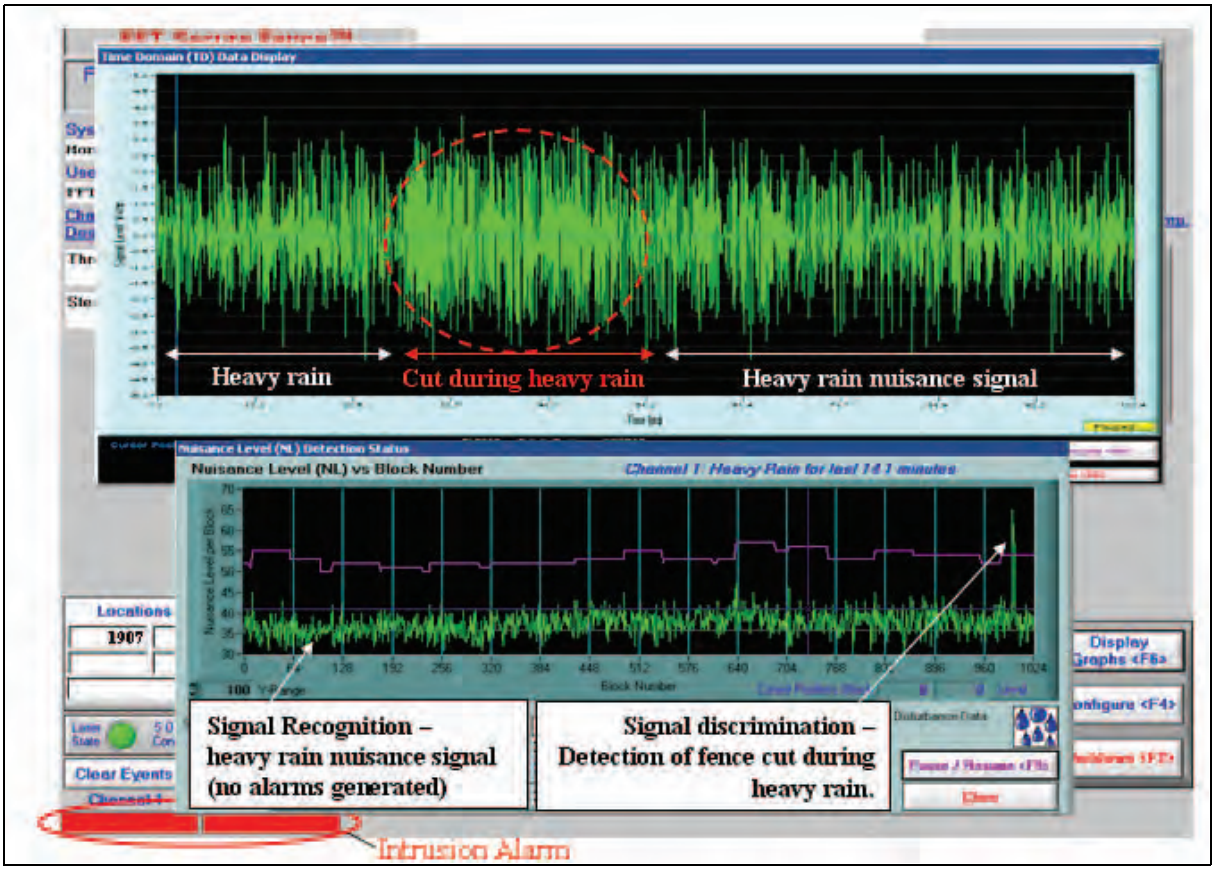


Fig. 3 *FFT Secure Fence Sensing Controller GUI showing the adaptive rain mitigation algorithm at work for a 1.2 mile fence perimeter during 4 inches per hour of rain*

As can be seen in Fig. 3, by recognizing 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 recognize this and returns to its normal mode of operation. Using this technique, rain-induced nuisance alarms can be minimized or even eliminated.

ONGOING DEVELOPMENT IN EVENT CLASSIFICATION AND NUISANCE MITIGATION

FFT has a strong ongoing program for further developing new intrusion detection techniques and algorithms for all its products. It is continuing to develop algorithms for identifying and discriminating between different intrusion and non-intrusion events which are continuously being integrated into its intrusion detection system controller software.

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

SELECTING A PERIMETER INTRUSION DETECTION SYSTEM

Alec Owen
International Client Manager
Future Fibre Technologies Pty Ltd

Unprotected perimeters mean unprotected assets, unprotected people and inevitably, security breaches. The ramifications of these breaches can be catastrophic so the threat of intrusion remains a prime concern at all major facilities. As most of these perimeters are simply too long for conventional security patrols to cover practically or effectively, installing advanced perimeter intrusion detection systems have become the only answer. The challenge is selecting the right system.

THE FUNDAMENTALS

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 together with the perimeter intrusion detection system (PIDS) and the response mechanism, is to act as the first level of site protection. This defines the boundary of the site, providing both an early warning of intrusion attempts as well as deterring, detecting, documenting and delaying any intrusion into the protected area. 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 a perimeter intrusion detection system are:

- the actual intrusion detection sensor(s) installed in the field or on the fence;
- the alarm processor that drives and analyses the raw sensor signals;
- the security or alarm management system that notifies security staff of an alarm and the location of the intrusion;
- the communications infrastructure that connects these three elements together and connects the system to the security staff; and
- 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 security team with an established response mechanism in place, the end result will almost always be unsuccessful regardless of which particular intrusion detection technology is installed.

Any security system is only as strong as its weakest link. The smart intruders rarely defeat the sensors or intrusion detection systems. Instead, they rely on poor alarm response procedures and mechanisms – the human element – to avoid getting caught.

A typical perimeter security solution will consist of a number of layered elements. What makes up these layers is going to be highly dependent on the customer expectation, the perceived threats and the potential intruders. It is important that a holistic approach to site security is taken, so that the elements of a layered security solution are complementary and work together in unison to provide a strong security regime which protects against both known and perceived threats. These layers may include a fence, a fence-mounted intruder detection system, some open area or volumetric sensors, some CCTVs, and of course, security staff and appropriate procedures (Rapid Incident Management System or RIMS) to respond to a situation in a timely manner.

In order to provide an appropriate level of protection that meets customer expectations and budget, a clearly defined set of criteria for customer and system acceptance is required. Too many times ‘scope creep’ on a project or a misunderstanding between the customer and installer of what is expected from the security solution occurs, for example, a chainlink fence and fence-mounted sensor around an electricity substation being expected to comply to prison test standards.

Firstly, you need to have a physical barrier or a fence. Not only does the fence define the boundary of the property or site, it will also deter an intruder (especially if it

has razor or barbed wire on top). Importantly, it will also delay them as they attempt to climb over or cut through it. Selecting the appropriate fence is critical – you need to match the fence to the individual site needs as well as the perceived threat level. For low- to medium-risk sites, such as an airport perimeter, you may be looking at a chain-mesh or weldmesh style of fence; for higher security needs such as a prison or pharmaceutical factory, you may be looking at an anti-climb fence. There is no value in cutting costs by installing a chainlink fence in a high-security environment, and conversely, it is poor value to install an expensive anti-climb fence at a low-risk site. Any security system is only as strong as its weakest link and the type of fence should suit the site.

The Technologies

In the past, perimeter intrusion technologies were prone to nuisance alarms with few systems providing tracking, assessment or situational awareness capabilities, making it impossible for ground staff to identify the point of access or exit in a timely fashion. Today, there's a diverse range of sensing technologies available for perimeter intrusion detection, varying greatly in their effectiveness, affordability and accuracy. However, this broad range also makes selecting which system to deploy for your perimeter security increasingly complex.

When evaluating or comparing perimeter intrusion detection systems, the major requirements include:

- a proven technology;
- successful installation track record;
- system durability/reliability;
- minimal nuisance alarms;
- maximum detection capability;
- minimal maintenance;
- ability to pinpoint the location of intrusions;
- able to work with complementary technologies; and
- the total cost of ownership of the system.

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 perfect perimeter intrusion detection system (PIDS) would simultaneously exhibit a zero NAR and a 100% POD, and be undefeatable.

The probability of detection (POD) provides an indication of a systems ability to detect an intrusion within the protected area. The POD depends not on only the characteristics of the particular 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 from a professional thief or special operations person for whom the POD will almost certainly be substantially lower.

It's doubtful that there is any single technology on the market that could not be defeated by experienced people, hence the need for a layered multiple technology solution where risks are high.

The Risks

You need to minimize your technology risks by ensuring that the perimeter intrusion detection systems you are evaluating have a proven technology with track record of successful installations in environments similar to yours. Too often a manufacturer's brochures and advertising will paint an emerging technology as mature, with little or no mention of the technical or operational risks involved. The technical risks are that the intrusion detection system does not even work in a basic manner, let alone as described in the literature. The operational risks include the system failing to work with or integrate to your existing systems or hardware.

Another end user risk is that the system creates so many nuisance or false alarms that it ends up being abandoned, ignored, or completely switched off. Often, these high levels of nuisance alarms are associated with the wrong technology selected for the application, the system sensitivity being set too high, or an unrealistic expectation of the capabilities of the selected system.

If you are planning to use Wi-Fi as the communications medium, then customers need to be aware this requires high levels of expertise to both deploy and maintain – especially if CCTVs are involved, so it is important that customers budget an adequate amount for ongoing main-

tenance to accommodate the environmental or local changes (weather, nearby wireless users etc.) that can interfere with and degrade the performance and bandwidth of the system.

In addition to selecting the right technology, you need to look closely at the system integrator, as most system commissioning issues generally revolve around a lack of technical skills with the integrator. As the newer generation of intrusion detection systems and cameras are now computer based, far greater IT skills are required to conduct installation and service activities.

A perimeter intrusion detection system that fails to meet the customers' expectations will invariably create an unhappy customer, increased commissioning costs for the integrator, and may render the job or project unprofitable. It is critical that the customer expectations, test procedures and test results are clarified, agreed to, and signed off in advance of work beginning so there are no false or unrealistic expectations of the completed installation.

THE COSTS

The true cost of a perimeter intrusion detection system is often very easy to underestimate. Manufacturers often quote just the cost per metre for the system, and this figure is typically 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 and maintenance.

Suppliers tend to downplay or understate the actual installation and commissioning costs involved, often citing best case scenarios when comparing costs to their competitors. It is important to always use a realistic 'total installed price' as the basis for comparing system costs. The low up-front purchase price of the perimeter intrusion detection system hardware can be far outweighed by the high costs associated with providing the power and communications infrastructure. It is not uncommon for these infrastructure and installation costs to be four to five times the cost of the actual PIDS hardware.

Regardless of the system selected, the need for adequate warning and a response mechanism for an unwanted intrusion is essential. It is not sufficient to simply know that a breach of the perimeter has occurred.

Perimeter security is all about the deterrence, detection, assessment and delaying of the intrusion for a response to be initiated. Every application is unique in the type of facility to be protected, operating environment, perimeter fence construction, intrusion and security history, and perception of threats. The protection of the perimeters of these individual facilities also needs to be tailored to suit the unique requirements of the site. Site layouts, sensitive areas, facility buildings, the surrounding environment, activity in and surrounding the site, local weather conditions and topography are all factors to be considered when planning a perimeter intrusion detection system. These all influence the detection technologies selected and subsequent overall system performance. Often the final intrusion detection solution will consist of several different but complementary technologies to form 'layers of protection'.

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

- 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 available and what is covered?
- What will be the response times if I have a problem?

Physical Security Integration Management – larger organizations tend to have multiple security systems (e.g. access control, perimeter intrusion detection, CCTV, video analytics etc), typically sourced from various vendors – each with their own unique security management systems. The cost of a PSIM system is very high, but it may solve these disparate system issues. Conversely, the risks are that the PSIM does not fully integrate with all of the functions of the individual security systems leaving the customer with a less than ideal solution. From an integrators perspective, PSIM systems are not simple plug and play solutions. The commissioning and managing PSIM systems can be very time consuming, leading to cost overruns and eroding any profit for the project away.

Almost any sensor manufacturer can quote and offer a 99.99% POD under ideal conditions, that is, a large target and sensor sensitivity set to maximum. Of course, at max-

imum sensitivity, both the confidence level and the NAR may be totally unacceptable. If a manufacturer were to cite a 99% POD figure, they would need to furnish very extensive test data to verify their claims! The 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 and storms, and not by an actual intruder. The newer intrusion detection systems categorize 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 event has taken place. Generally, false alarms are generated by the hardware or software supporting the detectors. Today, 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 interrelated and to some extent can be traded off against each other. Anyone can quote a high POD by increasing the sensor sensitivity, and conversely, a low NAR by decreasing the sensitivity. It is important to understand what the simultaneous POD and NAR figures will be, in other words, what can really be expected in the field with a real-world installation (this will almost always be site dependent) and how it matches the customer expectation. For example, a customer may be willing to tolerate a greater NAR to increase the sensitivity or POD of the system.

Signal discrimination and the way sensor information are analyzed have undergone major developments and advances in recent years. This is only possible because of the large amount of multi-parameter sensing information that can be collected by the newer and much smarter technologies, such as interferometric fiber optic sensors, and the processing power available from multiple CPUs in centrally installed controllers which can run signal finger-print and pattern recognition type software. This 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 the capability of these distributed microprocessors. These advances in technology were originally designed for military applications but have made their way into the security arena where they are capable of clearly discriminating between ‘real’ events and background clutter. This capability 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 minimizes the effects of wind, rain, storms, aircraft, traffic and lightning while maintaining the required high levels of sensitivity and intrusion detection. You also need to look at what and how much hardware you are installing in the field. While each component of the hardware may have an individual reliability or Mean Time Between Failure (MTBF) figure of say 10,000 hours, when you combine many pieces of hardware in a ‘system’, the ‘system’ MTBF will be significantly less due to the high component count and the many points of failure. Conversely, if you select a system with a ‘head end unit’ or with all of the electronics in a single location for improved reliability, then you need to ensure that there is sufficient redundancy built in to minimize the chance of a system failure.

CALCULATING THE QUALITY OF PERFORMANCE OF A PERIMETER INTRUSION DETECTION SYSTEM

Alec Owen
International Client Manager
Future Fibre Technologies Pty Ltd

Calculating a realistic probability of detection (POD) or determining a measurement of actual detection performance for Perimeter Intrusion Detection Systems (PIDS) is not quite as simple as many people believe. You need to understand the highly interactive and closely coupled relationship that exists between the detection of intrusions and unwanted nuisance alarms. This article offers one method to calculate a systems comparative performance taking this relationship into account.

Detecting every intrusion on your perimeter is the primary expectation of any PIDS system, but equally important is the confidence that your security staff have in the system not only capturing and reporting all legitimate intrusions, but just as important is not reporting nuisance alarms. Too many false or nuisance alarms will seriously erode confidence in the system, often to the stage where all alarms – real or not – are simply ignored by security staff. When this happens, your actual quality of performance in detecting an intruder in this scenario suddenly becomes 0% – regardless of what figures your vendor quotes for the equipment. So the question is how do you measure and quantify this quality of performance?

Almost any vendor can claim 100% detection of intrusions, but because of the high sensitivity settings typically used to achieve this figure during testing, a corresponding increase in nuisance alarms may render the system completely unusable from the customer's perspective. We need to measure both detection and nuisance alarm figures simultaneously in order to get a realistic Quality of Performance (QOP) or a measurement of relative system performance. This same methodology can be applied for the comparison of different manufacturers and technologies.

With a relatively small number of tests (in the order of 100s) being carried out on a site over a short period of time as part of the commissioning and acceptance procedure to determine the QOP and level of confidence, one method to use is as follows:

$$\text{Detection Rate} = \frac{\text{number of detects (or hits)}}{\text{number of tests}}$$

This can be testing by cutting, climbing, or spreading the fence fabric etc.

$$\%\text{Confidence} = \frac{\text{number of hits}}{\text{number of alarms received}} \times 100$$

The aim of this confidence figure is to factor in the effects of unknown, false, nuisance, or environmental alarms. In other words, how confident your guard will be that each alarm he receives is a real intrusion event.

$$\Rightarrow \text{Quality of Performance} = \text{Detection Rate} \times \%\text{Confidence}$$

Example1: As part of the commissioning of a PIDS system if, for example, we do a series of 30 climb tests on the fence and detect 29 out of the 30 climbs, giving us a Detection Rate of 29/30 or 0.966, and we also received one nuisance alarm during the tests also giving us 29 hits but with a total of 30 (true and false) actual alarms received = 96.6% confidence.

The Quality or Performance (QOP) would be:

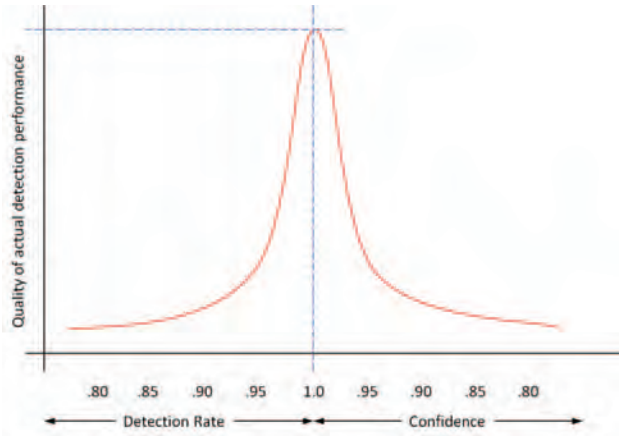
$$\left(\frac{\text{number of detects (29)}}{\text{number of tests (30)}}\right) \times \left(\frac{\text{number of detects (29)}}{\text{number of alarms received (30)}} \times 100\right)$$

$$= 0.966 \times 96.6$$

= 93.3% QOP with a 96.6% confidence

If we recorded the same detection rate but with no nuisance alarms during this test, then the result would be:

$0.966 \times 100 = 96.6\%$ QOP with 100%confidence



Example 2: If we then increased the sensitivity during the test in order to improve the detection rate, we may expect an increase in nuisance alarms. If we get a detection rate of 30/30 or 1.0, but a confidence of say, 30/35 = 85.7% (5 nuisance alarms) then the QOP would be 85.7% with an 85.7% confidence.

Example 3: Conversely, if we reduced the sensitivity to have fewer nuisance alarms, we may miss actual intrusion events. So for example a detection rate of 27/30 or 0.9, but a confidence of 27/27 or 100% would yield a QOP of 90% with 100% confidence.

As we go either side of the optimal detection/nuisance alarm settings, the QOP or detection performance falls off significantly. Always set the system up to achieve this optimal figure with any installation – ideally it would be 100% – but there are many external and site specific factors that can influence this figure, such as fence type, fence quality, weather extremes, etc. No two sites are ever the same and in addition to site specific and environmental factors, the detection rate may also be affected by the skill and knowledge of the intruder and their ability to defeat the system.

BIBLIOGRAPHY

Garcia, ML 2008. *The Design and Evaluation of Physical Protection Systems*, 2nd edn, Butterworth-Heinemann, Burlington, MA.

Mahmoud, SS & Katsifolis, J 2009. "Elimination of rain-induced nuisance alarms in distributed fiber optic perimeter intrusion detection systems," in *Fiber Optic Sensors and Applications VI (Proceedings Volume)*: SPIE Vol. 7316, proceedings of SPIE Defense Security and Sensing Conference, Orlando, USA, April 2009.

Naval Command, Control and Ocean Surveillance, In-Service Engineering, East Coast Division (NISE East) 1997. *Perimeter Security Sensor Technologies Handbook*.

Tarr, S & Leach, G 1998. "The dependence of detection system performance on fence construction and detector location," Proceedings of the Annual IEEE International Carnahan Conference on Security Technology, pp. 196–200.

Udd, E (ed.) 1991. *Fiber Optic Sensors*, John Wiley & Sons, Inc., New York, NY.

www.fftsecurity.com