

Performance characteristics for intrusion detection sensors

Editor's Note: Future Fibre Technologies Pty Ltd., (www.fft-usa.com), headquartered in Mulgrave, Australia, has published an excellent report entitled *The Boundaries of Security*, which describes the characteristics of the perimeter protection marketplace, the inevitable trade-offs in performance requirements, and detailed descriptions of a variety of emerging perimeter protection technologies. These two excerpts, reprinted with the kind permission of Future Fibre Technologies, cover the performance trade-offs customers will face, and three specific kinds of fibre optic fence-mounted sensor systems.

.....

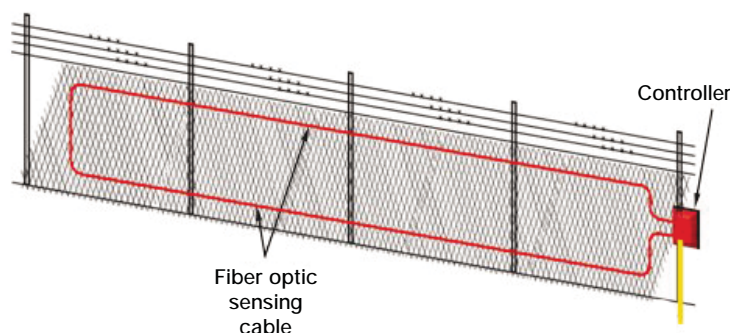
When evaluating any perimeter intrusion detection sensor, there are at least three key performance characteristics to be considered: the probability of detection (POD), the nuisance alarm rate (NAR), and vulnerability to defeat (i.e. typical measures used to defeat or bypass detection by the sensor).

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

The probability of detection provides an indication of a system's ability to detect an intrusion within the protected area. The probability of detection depends not on only 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 percent 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. If a manufacturer were to cite a 99 percent 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 attack has taken place. Generally, false alarms are generated by the hardware or software supporting the detectors. These days, with the advances in electronics, false alarms are becoming increasingly rare.

Vulnerability to defeat is another measure of the effectiveness of sensors

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

Each of these three performance characteristics will vary according to the technology selected and the unique site conditions. Remember, no two sites are ever the same. Also, when comparing POD and NAR rates quoted by manufacturers, the two must be considered together as both are 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, that is, what can really be expected in the field with a real-world installation (this will often be site dependent) and how it matches the customer's expectation. For example, an operator may be willing to tolerate a greater NAR to increase the sensitivity or POD of the system.

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 the multiple CPUs in the centrally installed controllers to run signal fingerprint and pattern recognition type software. This amount and level of processing is typically not available from distributed processing architectures, that is, multiple microprocessor-based sensor controllers installed in the field. The computing required is far more intensive than distributed microprocessors are capable of.

These advanced technologies 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. ■

A primer on fence-mounted sensor systems

Description: Fiber optic sensing systems are relatively new detection technologies, but have a strong following. The 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.

Fiber optic sensors use light travelling 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 provide the 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 one of the newer emerging technologies: Fiber Bragg Gratings.

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 travelling 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 travelling down it change. It is this change in the light that is detected, and if it exceeds a predetermined threshold, 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.

Special Section: Perimeter Protection / Fencing

ZONE-BASED 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 the fiber, and the returned light is compared to determine if there are

up to 6,500 feet are theoretically possible, realistically zones are usually limited to a more manageable 1,000 feet or less.

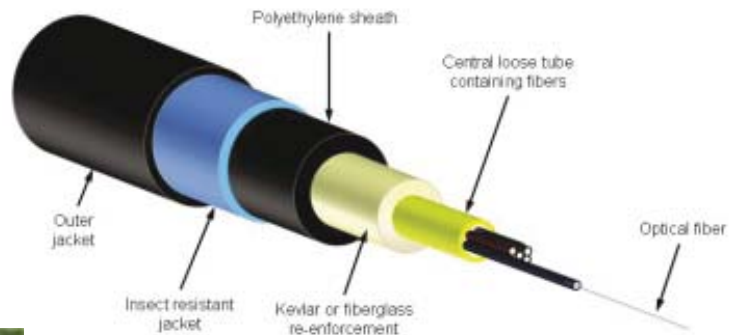
In some systems, the fiber optic sensor cable has to be installed within a conduit to help control environmental conditions such as rain, or with an anemometer to reduce the sensitivity of the system during windy conditions to avoid nuisance alarms being generated by the wind on the fence fabric. Naturally, when the sen-



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

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. While the fiber optic cable itself is immune to EMI, RFI and lightning, the electronics situated in the field are not. For this reason, the latest releases of this detection technology tend to have the controllers housed inside the security center, and fiber only outside the building and on the fence.

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, 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 costs.

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

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

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 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 Microstrain technology which is far more sensitive to situations such as propping ladders against a fence.

INTERFEROMETRIC FIBER OPTIC SENSORS

Operating principle: The newer

The force behind perimeter protection





www.powerfence.com

Intelligent active deterrence and detection 24/7



For more information, contact Gallagher Security USA Inc.
 telephone +1 888 430 0770, facsimile +1 407 302 4955,
 email securityusa@powerfence.com, or visit our website www.powerfence.com

PowerFence™ and Conize systems are manufactured by Gallagher Security Management Systems, a division of the Gallagher Group.

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 single mode 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

effective for perimeter fence lengths of between 1.2 miles and 50 miles 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.

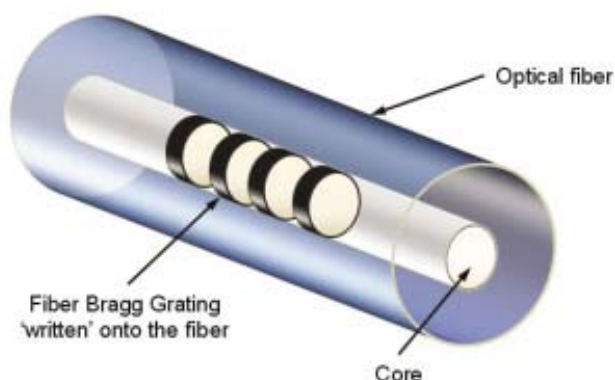
Strengths: Long distance; highly sensitive; low installation costs; intrinsically safe; powerful signal processing; immunity to EMI, RFI and

is moved minutely, these tiny grating spaces change slightly, and so the reflected wavelength changes.

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 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 changed, and therefore provide the location of an event.

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



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 in length, with uniform sensitivity anywhere along the sensor cable. Rather than having hardware-defined zones, this technology allows zones to be easily set in software for improved flexibility and better correlation to fixed perimeter points (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 unaffected 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 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.

Weaknesses: Not connectorized, so requires fusion splicing to join fibers, but there are many telephone contractors capable of doing this.

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

FIBER BRAGG GRATING SENSORS

Operating principle: 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.

The Bragg Grating works by reflecting back a very narrow wavelength or frequency of light travelling through the fiber, allowing all other wavelengths to pass. In its simplest form, it is an optical filter. When the fiber



Threat

Criminals, Terrorists and Vandals

Defense



FFT Secure Zone™

A new, affordable, simple-to-install, zone based fiber-optic intrusion detection system that detects intrusions at the speed of light.
In perimeter security it's the best defense.

Call us toll free at (877) 650-8900

www.fftsecurity.com/SecureZone
Got a QR reader on your cell phone? Scan the code below to visit the product page.