A Practical Solution for Perimeter Intrusion Detection

The latest breakthrough in perimeter protection technology

Introduction

Over the past 10-15 years, distributed fiber optic sensing technologies have gained significant awareness and implementation in the field of perimeter security and intrusion detection. The use of singlemode optical fiber and the development of location pin-pointing technologies were the two key factors that contributed to this rapid rise. However, the evolution and practical implementation of new technologies in the field always takes time. Furthermore, it could be challenging for someone less experienced in its implementation to fully understand the complexity of the various options available in the market, as well as the capabilities and limitations of each product. This predicament is compounded by vendors who confuse their customers and often exaggerate capabilities, hide deficiencies and down-play or conceal weaknesses of the technological solutions that they offer.

Another complicating factor is that long–haul perimeter security systems must often work in challenging and noisy environments, where performance on nuisance alarm rate (NAR) always works adversely against performance on the probability of detection (PoD). If PoD is increased, NAR is naturally also increased, which is highly undesirable because it distracts the operator and discredits the aim of alarming. Conversely, the only measure available to reduce high NAR in such technologies would also decrease PoD of the system. Consequently, claims of extreme sensitivities or impressive NAR performance made by vendors of these technologies, without detailing the resultant negative impacts, are misleading. Sometimes these negative impacts are not obvious, they may be subtle, or they may take time to be revealed. This ultimately leads to confusion and disappointment with deliverables of a project and discredits the effectiveness of the technology in the field. Therefore, it is critical to fully understand the various aspects, aims of application, capabilities, limitations, and characteristics of any distributed fiber optic sensing product when evaluating options for a specific application or project.

Fibersonics has over 30 years' of in-house experience in developing various novel perimeter intrusion detection technologies for our customers. In combination with some customers' generous attitude of sharing, with us, their field operational experiences with alternative perimeter security technologies, Fibersonics has been able to overcome many shortcomings and customers' disappointment with their previous perimeter intrusion detection systems by offering them more practical and effective technological solutions.

This Case Study paper provides an example of a real project experience, where some of the scenarios mentioned above were experienced by a customer.

Background

Fibersonics was approached for a large perimeter project that required an effective intrusion detection system. The customer was managing a large facility related to the national security of the country. This was no ordinary customer. They already had over 15 years' experience with distributed fiber optic intrusion detection systems. So, they had more experience on this subject than most customers normally would. Over the 15 years' of experience, they had evaluated and implemented the three major and leading types of distributed, locating fiber optic sensing technologies in the market, namely:

4220 SW 109th Avenue
Beaverton, Oregon, USA, 97005
Tel: +1 (971) 285-4777
www.fibersonics.com

A) Transmissive singlemode interferometers

First-generation locating interferometers (otherwise known as transmissive fiber optic vibration sensing systems) were the pioneering technologies introduced with transmissive distributed capabilities that offered the potential for monitoring very long lengths of cable. While offering unprecedented levels of sensitivity and locating at that time (10-15 years ago), these systems proved to be prone to a high level of nuisance alarming and lack of sensitivity at low frequencies (<300Hz) and high frequencies (>5-10 kHz). This generally resulted in poor detection of tactical intrusion events. In addition, the need for a stable temperature environment for the equipment made it difficult and expensive to operate with consistent and reliable results. Lastly, the systems are very complex and expensive due to the need for active polarization control in the optics housed in the equipment. This resulted in high equipment costs and the need for an expensive temperature controlled rack to house the system. Any loss of control of temperature, or hard physical contact with the cable, will destabilize the polarization of the laser light in these systems, thus rendering the locating part of the system unreliable.

B) Coherent-OTDR, otherwise known as Distributed Acoustic Sensors (DAS)

A new generation of locating distributed interferometer started to emerge about 10 years ago. This technology is a type of 'acoustic' sensor, and is often referred to as a Distributed Acoustic Sensor (DAS). In distributed acoustic sensing, an optical fiber is transformed into an array of thousands of "virtual microphones." Most current DAS methodologies are based on coherent interference of Rayleigh backscattered light. The technology has the high sensitivity of an optical phase interferometer and can determine the position of a 'noise event' very accurately, and that is where it is similar to transmissive interferometers. However, owing to the dependence on Rayleigh backscattered light, these systems are prone to signal fading. Consequently, the sensitivities of these "microphones" fluctuate randomly along the fiber length. As such, specifying the sensitivity of DAS without considering its random nature is incomplete and of limited value.

Furthermore, they have a significantly lower frequency bandwidth, usually up to a maximum range of 1-10kHz, which varies depending on the cable length. This is a useful frequency range for large, gross movements/acoustics, but it is also where nearly all environmental nuisance alarms are generated. For this reason, it is a highly problematic technology for above ground applications, where it generates plenty of nuisance alarms. However, where it performs well is below ground, where it was in fact designed to work. In the ground, there are mostly low frequencies, and the ground absorbs/buffers most of the above ground nuisance signals. However, the cable needs to be installed quite deeply. Otherwise, the system will generate many nuisance alarms. In areas of high background noise, i.e., road crossings, highways, near rail lines, airports, populated areas, etc., it will be susceptible to significant nuisance alarming – it's low-frequency, high-sensitivity is also its Achilles' heel.

There is also another important limitation to understand about DAS systems. They can reach long distances (approaching 50km), they have very good locating resolution down to 1m and have a frequency bandwidth approaching 10kHz – but they cannot achieve all of these important performance capabilities at once. Since DAS systems are based on an OTDR architecture, their location resolution and frequency bandwidth diminishes significantly and rapidly with distance. So, for a 1-2 km cable length system, they may achieve 1m locating resolution and 10kHz frequency bandwidth. However, for a 40-50 km system they can achieve only 20m locating resolution and 1.2kHz frequency bandwidth (which is where the vast majority of environmental and nuisance noise exists).

C) Distributed Fiber Bragg Grating (FBG) sensors

Although Fiber Bragg Grating (FBG) technology has been under development for over 20 years, it is really only in the past 5-10 years where we have seen practical commercial products entering the market. A fiber Bragg grating is a small length of optical fiber that comprises an optical pattern of a parallel series of reflective points that creates a reflection of a particular wavelength of incident light. This structure can be created by intense UV light effectively 'writing' the grating structure into the fiber core. The distance between the reflection points of a fiber Bragg grating is always equal. The optical wavelength that matches exactly the physical distance between the parallel reflection points is reflected by the grating. All other wavelengths are transmitted through the grating without being reflected or dampened. Hence, FBG sensor signals are the narrow spectrum of light that is reflected at each grating. The

wavelength of the individual reflection peak is determined in the interrogator. The interrogator typically contains a relatively broadband light source (enough to cover the full range of wavelengths of all the FBG's in a system) and performs spectral analysis by means of a linear array detector and a spectrometer platform.

As soon as a fiber Bragg grating is subjected to temperature or strain, for example, the distance between the reflection points changes and a different wavelength is reflected. This enables the Bragg wavelength variation to be determined by the interrogator. The values measured by the optical interrogator are the peak wavelengths of the narrow spectrum reflected by the FBG sensor. When strain at the FBG sensor causes the wavelength to change, the interrogator detects a change in the peak wavelength that is proportional to the strain. In a distributed configuration, a large number of fiber gratings are spaced along the length of cable, each at a slightly different wavelength (grating line spacing). The sensitivity to strain change can be extremely high, depending on the capabilities of the interrogator.

Effectively, distributed FBG systems contain a large array of FBG sensors spaced along the length of the cable being monitored. Consequently, the proprietary cable is special and relatively costly. The interrogator must measure and analyze the wavelength and the wavelength change of every single FBG in the array. For a long cable application, say of 2km and up, this could amount to thousands of FBG sensors. Consequently, the amount of time needed to monitor the spectral properties of each FBG can be considerable. For this reason, FBG systems tend to have a low-frequency bandwidth and slow response time. Depending on the number of FBG sensors and the high complexity of the equipment needed to monitor them, FBG systems can be very costly. Collecting, transmitting, analyzing and managing such a large amount of sensor data is also very challenging and often limits the performance of these systems for long-haul applications.

Based on what they had learned from the experience of working with these older technologies described above, the customer had explicit system specifications and performance requirements for the system, namely:

- The system must be all optical fiber, with no conducting or electrical elements outdoors.
- The system must operate on a 3m high weld-mesh fence, with Concertina wire on top, with 100% coverage of the entire barrier fabric and structure.
- Detection rate for climbing was specified at ≥90%, aided and unaided.
- Detection rate for single cuts of the fence fabric was specified at ≥80%.
- The system must perform with a NAR of <1 nuisance alarm per km per day.
- Location accuracy for a detected intrusion must be ≤20m.
- The system must be resilient to defeat by having redundancy and one-cut, cable cut immunity (the system must continue to detect normally after the cable is cut once).
- For the testing and validation of the system, the equipment had to operate normally in field conditions, utilizing only a temporary air-conditioned construction container. Power was to be provided by a generator.
- The system had to maintain uniform performance regardless of weather or environmental noise conditions.
- The system had to continue operating through massive simultaneous disturbance of the fence across 6-8 fence panels. The system should not be incapacitated by such activity.
- The system must have a fast response time from the onset of an intrusion event.
- The system must interface with external CCTV VMS with low latency.

We were surprised and puzzled by some of these requirements and what we considered to be relatively low PoD for climbing and cutting detection. The customer explained to us that these requirements came about through their earlier experience of working with the systems previously mentioned across several of their sites. Some of the problems and issues that they had experienced are summarized in the following table.

Previous Problems Experienced by the Customer	Product Technology Used	Description/Comments
Vulnerability to Catastrophic Failure in 2-Channel Systems	• DAS	To bring costs down, the vendor proposed a 2-channel interrogator solution to the customer. However, hardware failure later led to both channels of the system being down, thereby losing all monitoring capability for the site during equipment down-time. Had the customer implemented 2 single-channel systems, any hardware failure in one system would still allow partial monitoring of the perimeter by the second system. This was a lesson on the benefits of true redundancy.
Dead-Time During Switching Function of 2-Channel Systems	• DAS	Vendor failed to explain honestly to the customer that the 2-channel interrogator actually utilized an optical switch internally in order to 'share' the one laser to both channels. As a result, the system has a dead-time during the switching function. In addition, while one channel is being monitored, the second channel is completely dead. This dead-time can be in the order of many seconds for a long cable length system. This problem would not exist if the customer would implement two single-channel systems.
The Requirement for Strict Temperature Control in the Equipment Room	• First-Gen Transmissive Interferometer	Vendor imposed very strict temperature control requirements for the equipment room. This was not possible in a standard rack housed inside an air-conditioned room. Therefore, the customer had to place all the equipment in costly air-conditioned racks. Then, condensation and water-run off became problems that had to be catered for.
Vulnerability to Incapacitation by Polarization Instability	• First-Gen Transmissive Interferometer	If the equipment experienced temperature changes outside the vendor specifications, the polarization of the laser light in the equipment became unstable. The vendor specification requirement was ±5°C. As a result of the polarization instability, the system was not able to locate disturbances with any reasonable accuracy, effectively incapacitating the system until the polarization of the laser light was brought back to a stable condition. This process could take several minutes. The same polarization instability occurred in the system if the outdoor cable experienced rapid temperature changes or large physical disturbance. In fact, this vulnerability creates a method for an intruder to defeat the system.

Lack of Sensitivity to Cutting of Fence	• FBG	The customer site has 3m high weld-mesh panels for the fence. The weld-mesh is embedded in concrete at the bottom (footing) of the panel in order to make lifting of the panel fabric impossible without cutting the fence fabric. Therefore, the most likely scenario for intrusion for this type of fence construction is for an intruder to cut the fence near the bottom corners of the panels in order to create an opening large enough to lift the loosened fabric and crawl through. However, the bottom corners of the panels are positions on the panels that are physically furthest away from the fiber optic sensing cable attached to the fence panel. Consequently, a major focus of the customer testing was on cutting along the bottom (foot) of the fence panels. The customer found that the FBG system had lower sensitivity to cutting of the fence fabric at the foot of the panel, so they set a much lower PoD (≥80%) for the cutting tests. Of course, this is an undesirable compromise on system performance and effectiveness.
Vulnerability to Nuisance Noise Signals	• First-Gen Transmissive Interferometer • DAS • FBG	The customer is located in a densely populated geographic region near the sea. Their sites experience occasional strong winds and frequent heavy rain. In addition, there is considerable 'traffic' noise along certain parts of the sites. In order to satisfy the detection requirements of the customer, the vendors all configured their systems to be as sensitive as possible, with the consequence that nuisance alarming to wind and rain was very high. Some days, the systems reported thousands of nuisance alarms.
Vulnerability to Incapacitation by Large Distributed Force	• DAS	At one site, the customer was alerted that 8 panels of their perimeter fence had been accidentally knocked down by a speeding truck that had smashed into the fence. The customer was shocked by this news, as the DAS system never reported any alarms. Somehow, the fiber optic cable had remained intact, so not even a "fiber break" alarm was created in order to warn of this occurrence. Concerned about this incident, the customer tested the system by placing 8 people, each at 8 adjacent panels, and instructed them to start hitting the fence simultaneously very hard with rubber mallets. To their surprise, they found that the system was overwhelmed by the very large signals and did not alarm.
Lack of Sensitivity During Periods of High Environmental Noise	• First-Gen Transmissive Interferometer • DAS	After using these vendor products for a number of years, the customer noticed that NAR performance had improved considerably in the most recent 2 years. The vendor explained that the impressive performance improvement was due to new NAR mitigation algorithms developed and perfected by the vendor for these 2 systems. Testing of simulated intrusion attempts by the customer showed that PoD was within the system requirements, so there was no

		apparent need for concern. However, at some later time, an intruder was apprehended at one site. An investigation into the incident found that the intruder had scaled the fence in order to enter the site and the system had not alarmed. Needless to say, the customer was surprised by this and proceeded to conduct a thorough re-evaluation of the system. During planned testing, the system performed within specifications. However, the operator of the site started to do their own random testing of the system over an extended period of time. To their surprise, they found a repeatable pattern of when the system would not alarm at all during simulated intrusion tests. They found that the system would not alarm when the random tests were conducted during windy or raining conditions. The customer was alerted of this finding and they insisted on a thorough explanation and understanding from the vendor on why this was happening. The vendor was not very cooperative, as though they had some fact to conceal. After persistence by the customer, they eventually found that the new NAR mitigation algorithms implemented by the vendor basically looked for periods of high environmental noise and subsequently reduced the system sensitivity in order to artificially reduce the NAR. The critical problem with this approach was that the sensitivity was turned down so low that even real intrusions were not detected! This is how the intruder managed to scale the fence and not be detected – he scaled the fence during a windy day.
Lack of Sensitivity During Periods of High Background Noise	• DAS	As mentioned earlier, the low-frequency, high-sensitivity of DAS systems is also their Achilles' heel. We have found, along with this particular customer, that some DAS systems cannot operate well with high background noise conditions or environments. They effectively lose sensitivity when overwhelmed by noise. Some of the explanation for this is specific to DAS technology and some of the explanation may also be due to the NAR mitigation approach mentioned in the previous point. We have found that one easy way to defeat a DAS system is to place a small and noisy generator near the cable. This often renders the system unable to detect real events.
Vulnerability to Incapacitation by Large Data Transfer	• FBG	As detailed earlier, long-haul FBG systems can contain a very complex array of thousands of FBG sensors placed along the length of cable being monitored. At one site, this customer implemented an FBG system with over 3,000 individual FBG sensors distributed along a long cable length. The customer found that during periods of strong wind or heavy rain, thousands of events were being detected by

		the system and the data was being transmitted to the alarm management software of the customer. The sudden onslaught of thousands of alarms being communicated to the alarm management system basically overwhelmed the system while it attempted to process each message. The end result was a 'hung' system.

Having a good understanding of the background issues, problems and challenges faced by the customer in the past was helpful and useful for developing an effective implementation plan for the customer. After a thorough process of communicating and working with the customer, a system design and a test plan was conceived and implemented. The following sections briefly summarize the validation test results.

Fibersonics' new generation Long Ranger™ Intrusion Detection System

Fibersonics has a unique Distributed Vibration Sensor (DVS) system that is practical and effective in the detection of attempted intrusions along a perimeter due to its unique ability to detect, locate and classify vibrations caused by physical activity along the entire length of the perimeter, in real-time. The patented Long Ranger™ DVS technology is based on a proprietary hybrid transmissive interferometer. One of the key novelties of this system is that it utilizes two completely different and independent interferometers in a type of differential-sensor configuration. This results in higher sensitivity and a type of built-in redundancy and self-check capability for the system. It also offers the critical advantages of having little or no polarization instability and perfectly uniform performance over the entire length of cable, regardless of cable length.

In comparison with other competing technologies, Long Ranger™ is distinguished by the following main operational capabilities:

1. It operates over an extremely broad frequency range (3Hz to 500kHz) and is the world's first and only distributed ultrasonic detector. As a result, it can detect and locate many difficult or complex types of signals, directly and much earlier than other cable-based systems.
2. It is effective at discriminating different patterns of interferences and environmental noises from potentially dangerous operational events/threats. A significant part of this unique capability is that the system can detect intrusion signals that have useful frequency content that does not overlap with the frequency band of background and environmental noise. Therefore, by reducing nuisance alarms, the system alarms for events of true concern with an increased degree of confidence. Subsequently, this allows for automatic response mechanisms with a practical degree of responsibility.

The Long Ranger™ system utilizes the fact that light waves propagating in a fiber optic cable are extremely sensitive to any movement, vibration and acoustic-type noise that may be generated in its nearby environment. These disturbances create microscopic stresses or vibrations in the surrounding barrier structure (fence), and are mechanically coupled into the attached fiber optic sensing cable. These forces on the cable, in turn, generate highly-sensitive optical phase changes within the fibers. The amount of optical phase change is determined by the strength of the disturbance. Amplitude (strength) and frequencies, as well as several other parameters, are detected. Proprietary software is used to interpret and classify these changes in order to determine if the signal is a true event or standard ambient/environmental conditions. When a security/safety event is detected, an appropriate alarm is triggered and then transmitted to the mapping software (graphical user interface).

Many companies with distributed fiber optic sensing products claim to have developed databases of event "signatures" that they detect and classify alarms from. We believe this is unreliable and practically impossible to achieve, since so many uncontrolled factors impact on the characteristics of a signal (ie., barrier type, barrier material, barrier condition and how it changes over time, cable design, cable attachment, temperature, distance of disturbance from cable, soil type and rock/moisture content for buried systems, etc.). So, signatures can easily be different from site to site.

Fibersonics has developed a different approach to event classification. Our proprietary Unified Algorithms (UA) are a structured, layered approach to event classification and alarming, consisting of algorithms that look at staged data sequentially, applying user-defined parameters and algorithms that maximize the PoD while minimizing the NAR. We are having great success with this approach.

Deploying the Long Ranger™ system provides reliable perimeter security for up to 50 km through a single fiber optic cable, detecting and locating within 10 meters over the entire perimeter. Daisy-chaining additional controllers provides unlimited reach. Up to seven different levels of actual physical sensitivity can be achieved through the cable configuration, thus optimizing system performance for different media requirements, including chain link fence, weld-mesh fence, solid-wall or buried cable. Furthermore, one-cut, cable cut immunity is available in redundant configurations.

Customer Experience with Fibersonics' Long Ranger Intrusion Detection System

The Long Ranger™ system was installed and commissioned on a section of perimeter security fencing at the customer site. The system was installed for the purpose of testing and evaluating the performance of the Long Ranger™ system for its detection capabilities and its nuisance alarm rate.

For the system test, Fibersonics deployed 2 single-channel Long Ranger™ APUs in a redundant configuration that also provides one-cut, cable cut immunity. One APU was configured to monitor the weld-mesh fence and the second APU was configured to monitor the Concertina wire on the top of the fence.

The customer organized and conducted intrusion detection tests over a 2-day period, in order to evaluate the performance of the system. A detailed and thorough test plan was prepared and followed. The results were formally recorded by the customer.

Immediately following the 2-day PoD tests, the system was left to operate unmanned for 15 days in order to determine the vulnerability of the system to background and environmental noise levels. The system parameters and configuration were left identical to the 2-day PoD tests and were not allowed to be changed for this monitoring period. Remote access to the system was blocked.

Results of the Tests:

Test Conducted	Results of Test	Description/Comments
Detection Rate for Scaling the fence unaided	>96%	A small person was instructed to scale the fence in as careful and quiet a manner as possible.
Detection Rate for Scaling a fence post unaided	>95%	A small person was instructed to scale a fence post in as careful and quiet a manner as possible.
Detection Rate for Scaling the fence aided by hooks	>99%	A small person was instructed to scale the fence using the aid of metal hooks.
Detection Rate for Scaling the fence by ladder	>99%	A small person was instructed to scale the fence using the aid of a ladder. Detection most often occurred when the ladder was placed

		"normally" on the fence or Concertina/barb wire.
Detection Rate for Scaling a fence post by ladder	>95%	A small person was instructed to scale a fence post using the aid of a ladder. Detection most often occurred when the ladder was placed "normally" on the fence or Concertina/barb wire.
Detection Rate for Cutting the fence fabric	100%	A person was instructed to carefully cut a single wire of the weld-mesh fence fabric. Contact of the wire cutter on the fence fabric was avoided before and after the cut took place. This was a major focus of the testing by the customer, for reasons explained earlier. As a result, the customer cut the fence panels over 500 times! The cutting was conducted at various positions on the panels, but largely focused on the bottom sections and corners.
Detection Rate for Cutting of the cable tie used to attach cable to the fence	100%	A person was instructed to carefully cut off a cable tie holding the cable to the fence. Direct contact of the cutters with the fence was avoided.
Detection Rate for Cutting the fence fabric with loose cable attachment	100%	All the cable ties holding the cable onto a panel were first removed. Cable ties on the panel before and after the test panel were left in place. The cable was left dangling in the air, avoiding direct contact with the fence fabric. A person was instructed to carefully cut a single wire of the weld-mesh fence fabric at the middle and bottom of the panel. Contact of the wire cutter on the fence fabric was avoided before and after the cut took place.
Detection Rate for Cutting Concertina/barb wire on top of fence	100%	A person was instructed to carefully cut a single wire of the Concertina/bard wire on top of the fence panel. Contact of the wire cutter on the Concertina/bard wire was avoided before and after the cut took place.
Detection Rate for Cutting cable tie used to attach cable to Concertina/barb wire on top of fence	100%	A person was instructed to carefully cut off a cable tie holding the cable to the Concertina/bard wire on top of the fence panel. Direct contact of the cutters with the Concertina/bard wire was avoided.
Detection Rate for Cutting Concertina/barb wire with loose cable attachment	100%	All the cable ties holding the cable onto the Concertina/bard wire on top of the fence panel were first removed. Cable ties on the panel before and after the test panel were left in place. The cable was left dangling in the air, avoiding direct contact with the Concertina/bard wire and fence. A person was instructed to carefully cut a wire of the Concertina/bard wire on top of the fence panel. Contact of the wire cutter on the Concertina/bard wire was avoided before and after the cut took place.
Detection Rate for Massive simultaneous disturbance to 8 fence panels	100%	Eight people, at 8 adjacent panels, with rubber mallets were instructed to simultaneously hit a fence panel as hard as possible for a continuous amount of time. The system was unaffected by this massive activity and continued to operate normally. Alarms were generated with the locations of the people.

Nuisance Alarms for fence during the 2-day testing period	0	No nuisance alarms were detected for the 2-day testing period.
Nuisance Alarms for fence during the 15-day monitoring period	9	A total of 9 Nuisance Alarms were logged during the 15-day monitoring period.
Nuisance Alarms for Concertina wire during the 2-day testing period	0	No nuisance alarms were detected for the 2-day testing period.
Nuisance Alarms for Concertina wire during the 15-day monitoring period	5	A total of 5 Nuisance Alarms were logged during the 15-day monitoring period.

Conclusions

As stated earlier, it is critical to fully understand the various aspects, aims, capabilities, limitations and characteristics of any distributed fiber optic sensing product when evaluating options for a specific application or project. Fortunately, using a prudent and methodical approach, it is possible to successfully implement a practical and effective system and maintain it in a good operational state for many years. This Case Study illustrates one such scenario with a real customer and project. Via methodical planning and stringent validation, the customer found the Fibersonics Long Ranger™ Distributed Vibration Sensor (DVS) system to be a cost-effective, high-performance solution for the protection of long perimeters and other infrastructure.

About Fibersonics Inc.

Fibersonics Inc. is a recognized world leader in perimeter, pipeline and data security solutions. Fibersonics manufactures reliable, high-performance fiber-optic intrusion detection solutions for a wide variety of markets. One of its key missions is to develop and commercialize novel distributed fiber optic sensing products and solutions for security and safety applications. Fibersonics has highly experienced management and technical leadership. Its Founder, Edward Tapanes, is a serial entrepreneur with 30 years' track record in development and commercialization of fiber optic sensing technologies. He is a pioneer and patents holder in this field.

Advantages of the Long Ranger™ DVS System for Perimeter Intrusion Detection

- The longest range of real-time precision monitoring capability in the world with a single APU using single fiber-optic cable up to 50 km; daisy-chaining controllers provides unlimited reach
- Unparalleled PoD and NAR performance utilizing Fibersonics' proprietary Unified Algorithms for signal analysis and discrimination
- One-cut, cable cut immunity is available in redundant configurations
- Very high sensitivity; the system can be used with a variety of singlemode fiber cable and with protective conduit
- Uniform characteristics along the entire cable length, regardless of length, provides consistent performance over long distances
- Flexibility in configuration and actual physical sensitivity of the cable for an unlimited number of customized zones
- Capable of pinpointing intrusion over the entire length of a perimeter to within 10 m, with unlimited zones
- 3RU, 19-inch, rack-mount, alarm processing unit (APU) reduces costs and electronics footprint in control room
- Hardware based on dedicated programmable microprocessor and DSP chips
- Permits true remote control of monitoring system and integration with third-party alarm management systems
- Immune to electromagnetic or radio frequency interference (EMI/RFI)
- No energy requirement in the field reduces infrastructure and maintenance costs
- Optical self-calibration occurs continuously; requiring almost no maintenance
- Minimal communications bandwidth required; can operate on modern TCP/IP networks of any speed
- Robust with low energy consumption – APU produces nominal heat, eliminating the need for air-conditioned racks
- Field upgradeable firmware ensures equipment software can be brought up to the latest version on the spot, even over TCP/IP