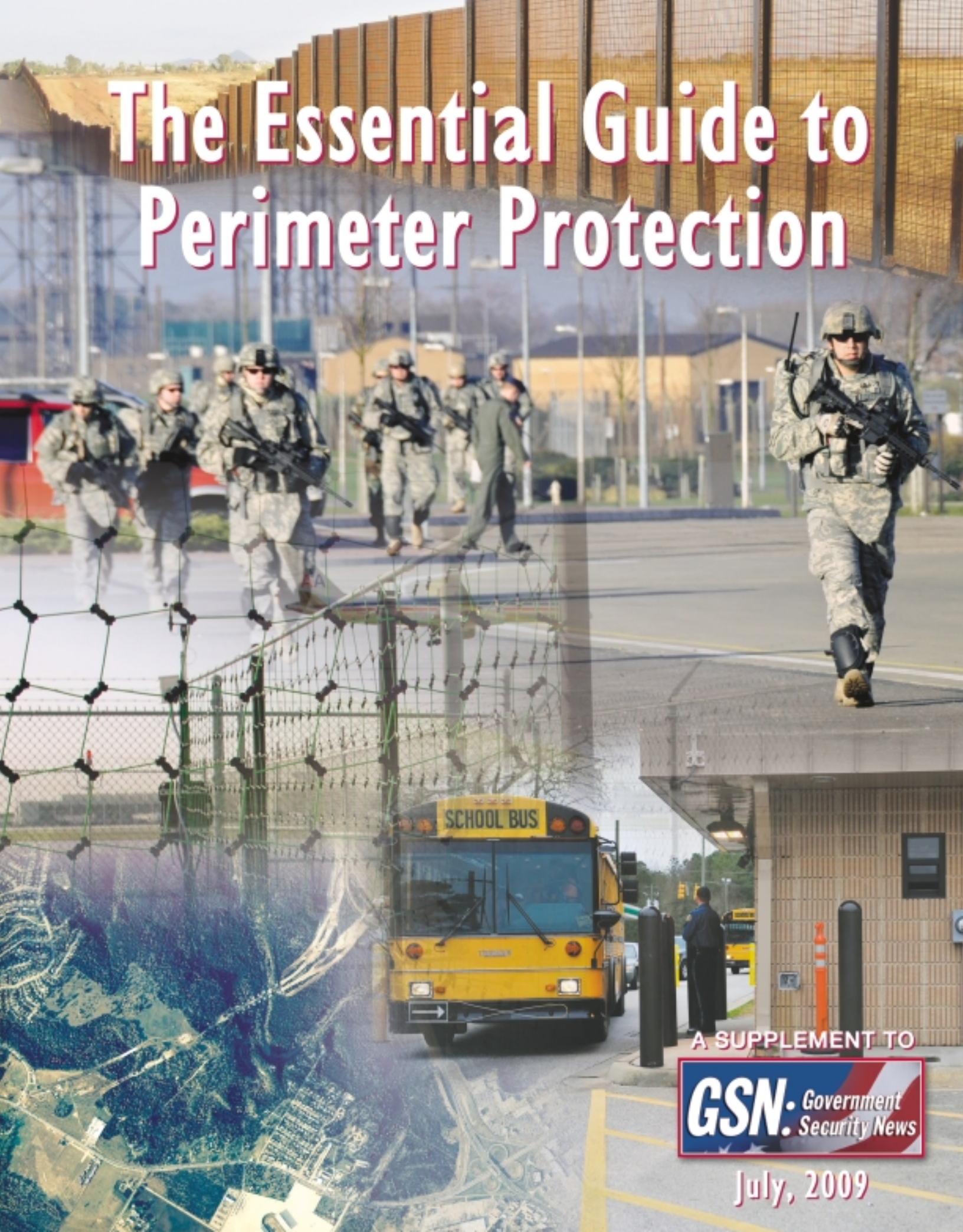
The Essential Guide to Perimeter Protection



A SUPPLEMENT TO

GSN: Government Security News

July, 2009

Why does Birmingham Water Works Board trust Gallagher PowerFence™ to secure its sites?

PowerFence™ Trophy FT is a flexible, scalable and IT network friendly perimeter security system. It has the scope to meet whatever perimeter security requirements you may have and more. For Birmingham Water Works Board (BWWB), PowerFence™ Trophy FT delivers by...

- Providing a deter and detect solution 24/7, fulfilling BWWB's duty of care
- Satsifying the Board and local authorities that it would meet stringent legal health and safety criteria
- Being integratable with other security systems e.g. access control and imaging
- Providing centralized management and fence zone monitoring of multiple distributed sites.

Need to know more? Contact Gallagher Security USA Inc
Phone +1 407 302 4055 Fax +1 407 302 4955
Email securityusa@powerfence.com
www.powerfence.com

POWERFENCE™

The ONLY Complete Range of K2–K12 All Electric Barriers and Bollards.

*Future*WEDGE™ 2400

The all electric bolt down 2400 series has a plate height of 24 inches in the armed position and can stop and immobilize a vehicle up to 10,000 lb. traveling @ 30 m.p.h. (K2/PU40). Single entrances up to 16 feet wide can be secured with simple "plug and activate" installation.

*Future*WEDGE™ 3100

The all electric 3100 series can be bolt down or installed with a shallow foundation, depending on the crash rating required. It has a plate height of 31 inches in the armed position and is rated to stop and immobilize a vehicle up to 15,000 lb. @ 40 m.p.h. (K8/M40). Single entrances up to 16 feet can be secured.

*Future*WEDGE™ 3600

This is a maximum security (K12) all electric, shallow foundation barrier, with an armed height of 36 inches. The 3600 series features a flush mount design and can secure single entrances up to 20 feet wide. It has rapid deployment (1.5 seconds) with much higher duty cycles than hydraulic units.

Complete Range of Bollards

SecureUSA has the only complete range of all electric and manual retractable, super shallow foundation fixed and removable bollards, with K2-K12 crash ratings. We have a staff of design engineers that develop custom bollard solutions, incorporating aesthetically pleasing finishes that blend with streetscapes.

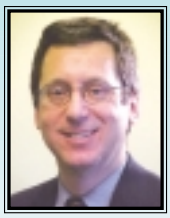
SecureGREEN Go GREEN

GREEN Perimeter Defense Technologies

SecureUSA® Inc.

Defense Solutions You Can Trust

Contact Us Today at 888.222.4559 or go to www.SecureUSA.net



A message from Jacob Goodwin, *GSN's* Editor-in-Chief

Perhaps you remember the era of, "We don't need no stinkin' badges." Perhaps you've fumed quietly (or maybe not so quietly) at a guard gate, waiting your turn to flash a photo ID so you could enter some high-rise office building, wondering if you'll miss your appointment.

After all, carping about perimeter protection is as easy as complaining about the weather.

But just ask a frontline U.S. Marine in the southern Afghanistan province of Helmand how important it is to protect the perimeter, and you'll soon learn that it can mean the difference between life and death.

And that's true whether that perimeter is a forward observation post, the meandering southwest border, a crucial piece of the national infrastructure, or even your own back yard on a moonless night.

In *GSN's* special section, you'll find examples of state-of-the-art perimeter protection methods -- from cyber-defense to systems that employ radar to video surveillance systems that learn while they watch to the latest in physical fences.

Enjoy!

GSN. Government Security News

Main Number: (212) 344-0759
Fax: (646) 336-3960
www.gsnmagazine.com

EDITOR-IN-CHIEF:
Jacob Goodwin
(212) 344-0759 x2003
jgoodwin@gsnmagazine.com

ART DIRECTOR:
Mark Kaplan
(212) 344-0759 x2005
mkaplan@gsnmagazine.com

SENIOR EDITOR:
Louis Chunovic
(212) 344-0759 x2007
lchunovic@gsnmagazine.com

PRODUCTION MANAGER:
Mike McCabe
(212) 344-0759 x2009
mmccabe@gsnmagazine.com

RESEARCH ASSOCIATE:
Laura de la Torre

PUBLISHER:
Edward Tyler
(212) 344-0759 x2001
etyler@gsnmagazine.com

ADVERTISING SALES

Vice President Sales:
Michael J. Madsen
(212) 344-0759 x 2004
mmadsen@gsnmagazine.com

Managing Partner:
Adrian Courtenay
(212) 344-0759 x 2002
acourtenay@gsnmagazine.com

Vice President Sales:
Michael Stack
(847) 367-7120
mstack@gsnmagazine.com

GSN International All Digital:
Craig Renfro
(972) 416-9782
crenfro@gsnmagazine.com

GSN International All Digital:
John Keiser
(214) 206-1154
jkeiser@gsnmagazine.com

New England e-media Reg. Mgr.:
JoAnne Lifavi
(917) 559-7821
jlifavi@gsnmagazine.com

SALES SUPPORT MANAGER:
Anne Tyler
(631) 275-0264
anne@gsnmagazine.com

REPRINTS MANAGER:
JoAnne Lifavi
(917) 559-7821
jlifavi@gsnmagazine.com

LIST MANAGER:
Edith Roman
Postal: **Kevin Collopy**
845-731-2684
kevin.collopy@edithroman.com
E-mail: **Maggy Pizzuto**
845-731-3844
maggy.pizzuto@epostdirect.com

CIRCULATION DIRECTOR:
Hilde Stein Sprung
(516) 695-9859
hstein@gsnmagazine.com

WORLD BUSINESS MEDIA, LLC
Edward Tyler, President

Adrian Courtenay, Chairman
(212) 344-0759 x2002
acourtenay@gsnmagazine.com

GSN: Government Security News (ISSN 1548-940X and UPS 022-945) is published monthly except semi-monthly in February (13 times per year) by World Business Media, LLC, 233 Spring Street, 3rd floor, New York, NY 10013. Telephone: (212) 344-0759. Periodicals postage paid at New York, NY and additional mailing offices. POSTMASTER: Send address changes to *GSN: Government Security News,* Subscription Department, P. O. Box 316 Congers, NY 10920-0316. For government decision makers and business executives involved with security products, systems and services. The *GSN* Web site is: http://www.gsnmagazine.com.

TABLE OF CONTENTS

MaxStop™ Maximum Delay and Denial Welded Wire Barriers

- No other barrier contains more dependably or protects high-risk properties and equipment more thoroughly than MAXSTOP™.
- Climb and cut resistant, Welded Wire Mesh MAXSTOP™ Barriers provide enhanced security and are installed as stand alone systems.
- Welded Wire Mesh MAXSTOP™ provides a durable and attractive alternative to chain link.
- Welded Wire Mesh MAXSTOP™ is precision welded with computer-controlled welding equipment. Mesh size is true. Panels are flat and accurate.
- All MAXSTOP™ welded mesh materials is manufactured and produced in the United States, distributed worldwide.

MAXSTOP™ by C.E. Shepherd Company L.P. provides welded wire barrier fence ensuring effective public security and safety.

MaxStop™

MAXSTOP™ IS THE SECURITY FENCE DIVISION OF:
C.E. SHEPHERD COMPANY L.P.
WITH OVER 50 YEARS OF MANUFACTURING EXPERTISE

MADE IN AMERICA

HUBZone





MAXSTOP™ APPLICATIONS INCLUDE

- Border Security
- Ports
- Correctional Facilities
- Chemical Plants
- Power Generation and Electrical Substations
- Military Battlefield Command Centers
- Nuclear Facilities
- Airport Perimeters

TO FIND OUT MORE ABOUT OUR SECURITY FENCE PRODUCTS
CONTACT MAXSTOP™ TODAY
AT 800.324.6733

2221 CANADA DRY ST. • HOUSTON, TEXAS 77023 USA • 800.324.6733 OR 713-924-4300 • FAX 713.928.2324 • MAXSTOP.COM

Improving perimeter protection through night vision and video analytics


By Willem Ryan and Dr. Bob Banerjee

Video surveillance systems are advancing at a rapid pace, and many of these developments are ideal for helping public and private sector security directors and customs and border personnel protect their perimeters. These innovations revolve around capturing high-quality video in difficult lighting conditions and alerting security personnel to potential risks before they occur.

Night vision is critical for surveillance of perimeters, as these areas are often unlit or have only widely dispersed, high-intensity lamps that create overexposed "hotspots" against a backdrop of darkness in surveillance images. Adequate illumination is essential to acquiring images that allow security personnel to monitor an area, observe activity at the location, and identify specific actions, objects or people.

An alternative to adding visible lighting to a perimeter is to use infrared sensitive day / night cameras combined with infrared illuminators. Active-infrared illumination is light that lays in the wavelength region of 700 to 1,000 nanometers (nm). Its wavelength is just beyond the visible region of 400 to 700nm, making it invisible to the human eye.

Available options for adding infrared illumination are cameras offering integrated infrared or standalone infrared illuminators placed near existing cameras. These devices produce nighttime surveillance video that more closely resembles the crisp, monochrome images captured during daylight hours. With either option, security personnel should look for illuminators that eliminate hotspots and underexposure by lighting both the foreground and background of an entire scene. More advanced than conventional illuminators, these products allow for improved situational awareness 24 hours a day.

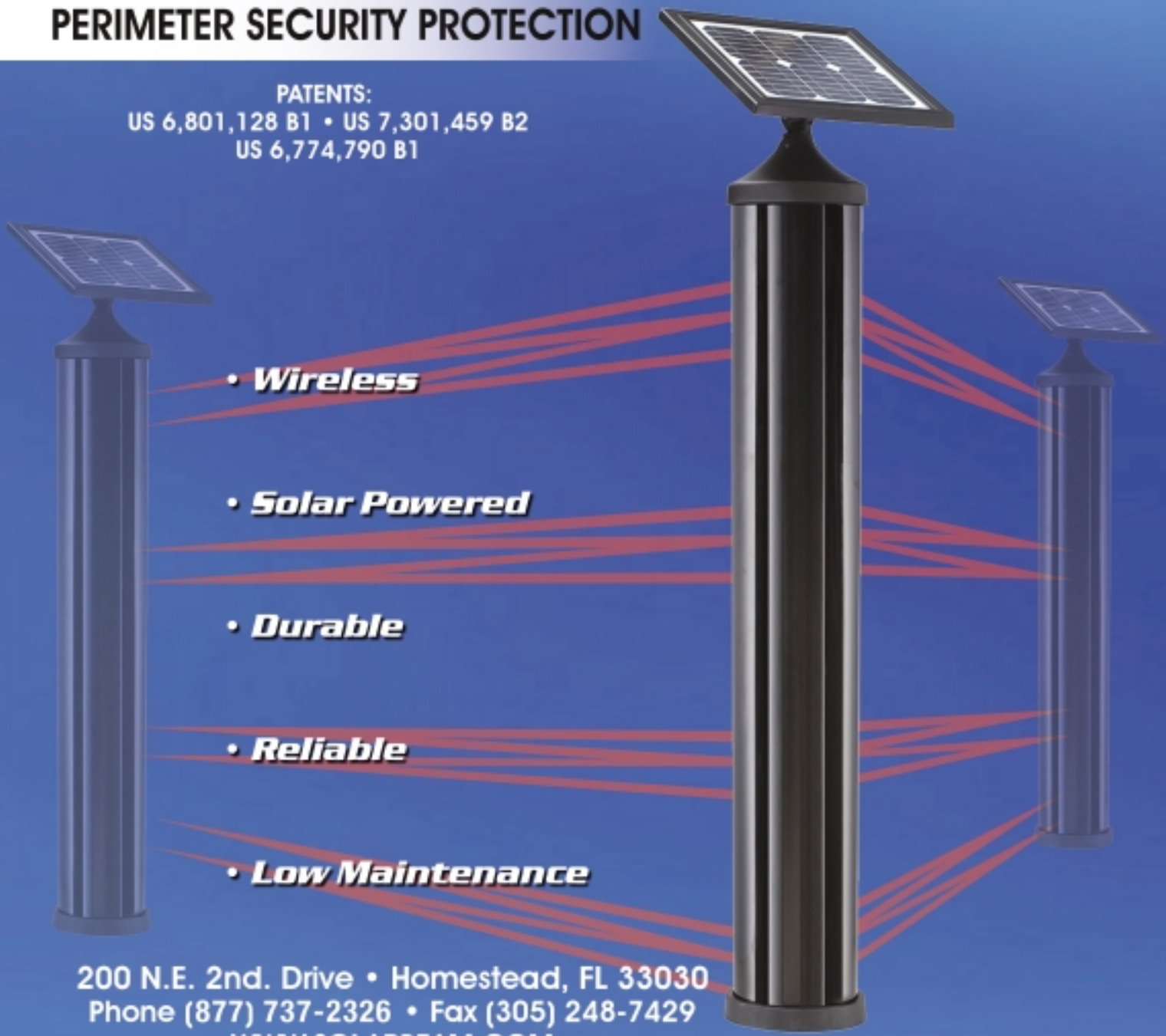
Since infrared illumination produces clearer nighttime images that are more evenly illuminated, 24 / 7 event detection through video content analytics (VCA) is possible. There are often too many video streams along a perimeter for security personnel to monitor effectively, and VCA is an important assistive technology that can help focus the operator's attention to possible risks. However, VCA does not function well in low-light, as the technology processes the graininess of these images as movement. Since VCA looks for motion as a trigger for behavior detection, the technology will produce continuous false alarms in low-light conditions. Using infrared illumination to enable nighttime detection with VCA can add an extra layer of protection when darkness could otherwise provide a protective cover

Solarbeam
SECURITY ™

GO GREEN!
GO SOLARBEAM™!

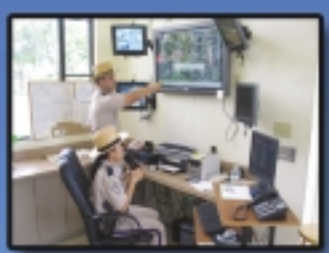
WIRELESS SOLAR POWERED PERIMETER SECURITY PROTECTION

PATENTS:
US 6,801,128 B1 • US 7,301,459 B2
US 6,774,790 B1



- Wireless
- Solar Powered
- Durable
- Reliable
- Low Maintenance

200 N.E. 2nd. Drive • Homestead, FL 33030
Phone (877) 737-2326 • Fax (305) 248-7429
WWW.SOLARBEAM.COM

for would-be intruders.

VCA can be configured to detect a number of behaviors that would indicate a person is about to or attempting to cross a perimeter. One of the most common uses of VCA at a perimeter is the tripwire function. With tripwire, the technology is programmed to set an invisible line, often along a fence or the coast of a waterway. When the camera detects that a person or object, such as a boat, crosses that line, it will issue an alarm and bring up video of the scene on the operator's screen. If the site does not have security personnel monitoring video at all times, the system can also trigger an intrusion control or access control system to alarm, thereby sending an alert to the alarm company monitoring the site.

Loitering is another behavior that is important to detect at perimeters. VCA can be configured to issue an alert if a person or vehicle enters an area and does not leave that area after a specified time, while ignoring those that innocently pass through the scene. When programmed for loitering, the technology serves as an early warning system to alert security personnel that someone may be looking for an opportunity to enter the facility. With advanced warning, security personnel can send a patrol to the area before the person actually breaches the perimeter.

By tracking the way objects behave, these behavior-based sensors are able to distinguish between small animals, people and vehicles, thus reducing the chance of a false alarm and providing greater perimeter protection. This capability is an immense improvement over more traditional motion detection, which struggles with accurate detection in outdoor applications.

Video content analysis technology combined with active infrared illumination results in effective and automated video surveillance day and night. With this technology in place, security personnel are better equipped to watch over and secure their entire perimeters in even the darkest conditions. ■

Willem Ryan is a product marketing manager for Bosch Security Systems, responsible for the company's line of active-infrared cameras and illuminators. He can be reached at: willem.ryan@us.bosch.com

Dr. Bob Banerjee is the product marketing manager for IP video products at Bosch Security Systems, including the company's video content analysis technology. He can be reached at: bob.banerjee@us.bosch.com

Pipeline perimeter security: Advance warning

By Tim Arion

Over 250,000 miles of pipelines in the United States move crude oil and processed fuel to refineries, regional storage facilities, and distribution networks, throughout the country. To date our network of pipelines has remained relatively secure, since much of the pipeline network is underground. As the risk of terrorism increases, and uncertainties in the U.S. economy continue, a snapshot look at Third World problems with pipeline security may provide us with advanced warning as we continue to "harden" our systems in the interest of national security.

Since a large portion of the U.S. pipeline system is underground, pipeline security today seems more focused on flow rate monitoring technology designed to detect leaks in the pipeline between termination points. At above ground termination points the security trend seems to be implementation of advanced intrusion detection systems that mix a combination of fiberoptic sensing cables, IR sensors, microwave, wireless, motion sensing technology, wireless Ethernet, CCTV and other technologies that are designed to provide some sort of security alarm to an operator located at a central monitoring station that may not even be in the same state. However, Third World pipelines have much of their infrastructure above ground; pipelines run through very remote and rugged country; there is considerably less security; and the entire systems are very susceptible to terrorism, vandalism and pilfering.

For the most part, Third World oil refineries are reasonably well protected. Perimeter fences are the norm and, in many cases, a double fence is in place as an added level of security. Various sensor systems are in-place and, by and large, an oil refinery in the Third World is viewed as a difficult target.

Pipelines, on the other hand, provide an attractive target in the Third World. Typically pipelines run through very unpopulated areas with easy access from a road system; the pipeline is run above ground; availability of electricity and communication is spotty at best; and distances between termination points can be in excess of 60 kilometers. A terrorist, or a group intent on pilfering for resale on the black market, find the pipeline to be a very "soft" target.

Pipelines in the Third World can be classified into two groups: (a) a pipeline that carries crude (black) oil from oil well collection stations to a refinery and; (b) a pipeline that carries refined product in the form of gasoline, diesel, or other "end use" product from a refinery to a distribution point.

Rarely do "black oil" pipelines suffer damage. Although occasionally a terrorist, or disgruntled local populace will blow up a black oil pipeline, the negative environmental impact on the immediate area might make a political statement, but there is no economic benefit from this type of destruction. The target of choice is the pipeline that carries refined product. This pipeline proves to be the most profitable for both the terrorist, or a pilfering network. As examples, Nigeria, Venezuela, Colombia, Ecuador and Mexico have all been subjected to attacks on pipelines carrying refined product. It is not unusual to uncover very well orchestrated attacks on a pipeline by groups who surreptitiously identify a pipeline that runs within a reasonable distance of a road; spend the time required to covertly dig a trench from an innocuous shack beside the road to a pipeline; bury a four-inch hose leading from the shack to the pipeline; and then tap into the pipeline leaving a shutoff valve in place for periodic "milking" of the refined product for sale on the black market. During the night, it would not be uncommon for an 18-wheel tanker truck to appear by the side of the road; filled (milked) with refined product from the pipeline; and be gone within an hour. Assuming this "attack" takes place 30-40 kilometers from the nearest monitoring station, the whole process is over long before a security response team can arrive to investigate why there was a drop in pipeline pressure.

Ultimately, proceeds from the sale of the tanker full of refined product can then be used to fund additional terrorist activities, revolutionary activities, or gang related activities. A recent study indicates that one Latin American country loses close to eight percent of its annual GDP to "milking."

In conclusion, superb technology exists in the marketplace to identify pipeline security breaches. However, as part of response planning, a systems approach should be included in any response plan that elicits coordinated responses by oil company security personnel and local law enforcement. ■

Tim Arion is president/CEO of EMX Inc. in Melbourne, FL. He has extensive global security / surveillance experience, having worked for *Fortune 200* companies such as Texas Instruments and Emerson Electric.

Deter, Detect and Delay vital assets with solutions by the industry leader in innovative fence design.

Payne Fence Products delivers revolutionary anti-cut, anti-climb barrier systems, including solutions proven on the U.S southern border, detention and prison facilities, and sensitive industrial and governmental sites.

The Guardian Fence System® by Payne presents a formidable barrier using security mesh panels, making it the solution of choice for creating high security perimeter lines and partitions fully integrated with intrusion detection, communications and surveillance equipment.

Call us, and let us show you how our Solid Solutions can meet your security needs.

SOLID SECURITY SOLUTIONS

PAYNE
FENCE PRODUCTS

SOLID SOLUTIONS

Payne Fence Products, LLC is A Member Of The Betafence Group BETAFENCE

guardian@payneFENCE.com • 972.878.7000 • www.GuardianFenceSystem.com

Rapid deployment intrusion detectors

By Eugene Gerstein

In today's world, the term “perimeter security” has taken on many, often confusing shapes. Players from the IT world, looking to capitalize on the convergence hype, are using this term to describe a means to secure a network, while traditional security industry players look at it from a physical standpoint – perimeter means either a solid means of protecting an area, such as bollards, fences, etc, or perimeter intrusion detection systems. PIDS come in many flavors – buried cable, fence mounted cable, tensioned cable, acoustic (microphonic) cable, magnetic cable, seismic, infrared, radar and microwave, which would be the focus of this article.

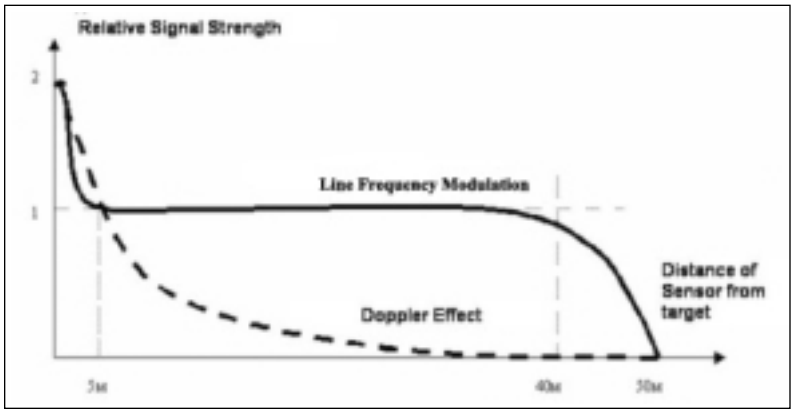
Traditionally, PIDS are divided into two categories – bi-static (transmitter / receiver) and monostatic (transceiver) sensors.

Bi-static sensors come in various flavors, with detection zones ranging from 30 feet in the traditional type, to 2,500 feet in some of the modern millimeter wave systems, creating long and narrow zones. This transmitter / receiver style of detection, gives you an ability to establish a kind of “invisible fence,” where the detection field serves to identify human and / or vehicular intrusion. Intruders create a sort of a “void” in a detection zone – that void is analyzed by the system, through the use of complex algorithms, which compare this void to a matrix, populated with parameters equalling various human “shapes.”

Monostatic sensors are also known as volumetric, named for their mass sensing ability. Traditionally, these devices were being used to protect enclosed spaces, such as rooftops, garbage dumps, etc. Modern applications are a lot more diverse, with an ability to protect individual objects, such as vehicles, aircraft, etc. Since these objects have a constant mass, the sensor begins its detection process only when that mass changes, which would be the case during an intrusion. If the parameters of the object causing the change in mass, match those of a human, an alarm is created. Usually, these sensors are based on the Doppler effect, which has a drawback – objects moving at speed across the detection zone or directly towards the detector may go undetected. This problem is solved with detectors using Line Frequency Modulation (LFM), which constantly probes segments of the zone, thus eliminating the aforementioned concern.

Important type of sensors, based on classic transmitter / receiver series, are mobile rapid deployment intrusion detection systems. Restricted primarily to military and law enforcement use in the past. Today, they are used in a wide variety of applications, anywhere from aircraft and cargo protection, to concert crowd control. These sensors employ the same principles of operation as their stationary counterparts, but do so in a lighter, more compact, fashion. They are often deployed with the use of tripods, long lasting batteries and wireless alarm transmission. Another type of rapid deployment systems, is based on seismic sensors. They feature exceptional battery life (one to five years, depending on the manufacturer), an ability to form a wireless mesh network for reliable delivery of alarm signals. There are multiple accessories available, such as breakwire and magnetometric (ferromagnetic) sensors, allowing, for example, the detection of armed humans within a protected perimeter.

Over the years, an unfortunate trend has shaped itself – a large number of professionals became distrustful of microwave sensors. Some of the problems were reliability, difficult calibration procedures, complex service re-quirements and most of all, the dreaded false alarms. While the technology is still conceptually the same (since science has its limits and a breakthrough discovery has yet to be made), many steps were taken by some of the industry players to address these issues. With the ever increasing demand for perimeter protection, it is safe to say, things have changed. Some detectors now have the ability to adapt to changing terrain conditions, consume less power, handle uneven ground, immunity to electromagnetic interference (EMI); the list goes on and on. The sensors are more robust, easier to install and use, false alarms are lower then ever, and most of all, prices have gone down significantly – microwave intrusion has finally become affordable. ■



Eugene Gerstein is a retired Israeli Defense Forces special reconnaissance squad officer and former narcotics officer. He is the managing director for STR Inc., a manufacturer of outdoor microwave intrusion detectors.


OPTEX
The World Leader
in Sensors
for 30 Years
30
OPTEX
NO WIRES, NO HASSLES.
FINALLY.
Introducing The New WIRELESS READY, BATTERY OPERATED
PHOTOELECTRIC DETECTOR From the World Leader in Outdoor Protection.
The new AX-TFR battery operated photoelectric detector is a revolution in the perimeter security industry. Available in 100 ft. (AX-100TFR) and 200 ft. (AX-200TFR) models, the detector offers a significant cost saving alternative to a traditional hardwired system.
The versatility of the AX-TFR series allows for it to not only be installed where power is not available, but also allows for it to be easily moved to a different location if necessary. No Trenching, No Wires, No Hassles. The new AX-100TFR and AX-200TFR from OPTEX.
AX-TFR SERIES
The newest addition to the OPTEX family of outdoor detectors.
Visit www.optexamerica.com or call 800-966-7839 for more information.

Protecting our government from cyber thieves requires layers of defense

By Jon Ramsey

Having a dead bolt lock on your front door at home is good, but is it enough to keep intruders out? Because intruders may not be deterred by a single lock, a well-protected home has sturdy doors, deadbolt locks on every door, a loud dog, security bars on the windows and a home security system with motion sensors that will alert the police should the alarm sound.

Whether it's the military, public safety agencies, elected officials' offices or some other government agency, protecting the government's computer networks against intruders requires many layers of defense – just like your home. The more layers you implement, the more likely it is that a thief will move on to a less-protected environment.

THREE LAYERING TECHNIQUES

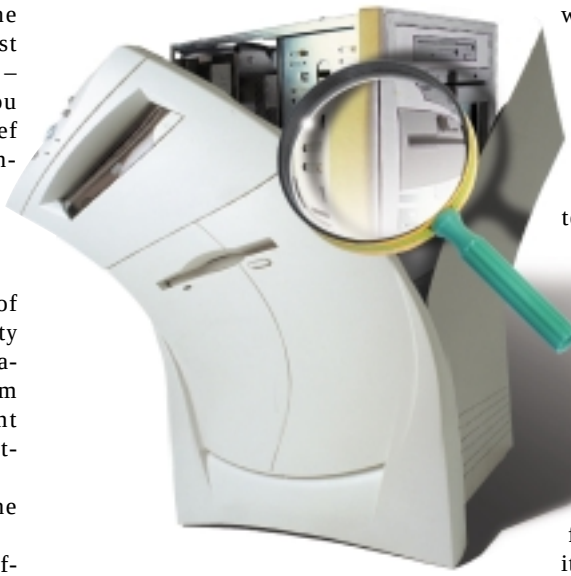
There are three primary methods of defensive layering in information security recommended by SecureWorks, an Atlanta-based information security services firm that provides protection for government entities, as well as other corporate networks:

- layering different technologies in the same area of the IT infrastructure;
- layering similar technologies across different vantage points within the infrastructure; and
- layering a highly capable and trained human organization on top of all of the security technologies in a 24/7/365 scheme.

LAYERING DIFFERENT TECHNOLOGIES IN THE SAME AREA

The most common mistake agencies and organizations make is to assume that a firewall alone can defend their network perimeter. Firewalls block certain types of traffic that are inherently unsafe and allow other types of traffic that are deemed safe. Unfortunately, hackers disguise attacks to appear safe - using the safe paths (such as Port 80) to infect networks and obtain confidential data. While no organization should go without a firewall, this alone will not block many of the new attacks launched today.

The perfect complement to the firewall, the Intrusion Prevention System (IPS), is not designed to block wide categories of traffic, like a firewall. Instead, the IPS is tuned to find and stop very specific attacks such as overwriting one single buffer in a certain memory segment of a specific application. These two technologies work in different ways to secure the perimeter of your network.



LAYERING SIMILAR TECHNOLOGIES ACROSS DIFFERENT VANTAGE POINTS

To protect the government's critical infrastructure, its four primary layers must be secured: the perimeter, the internal network, the external and internal servers and the desktop. Contrary to popular belief, a secure perimeter does not secure the entire infrastructure because attacks don't always enter from the outside. There are multiple ways to get into a network besides the front door. Encrypted Web browsing is increasingly being used to sneak attacks in through perimeter security devices and ultimately into the internal network. A textbook example of layering security by vantage point is to introduce strong anti-virus (AV) defense in the mail server and the IPS on the perimeter, while also implementing strong desktop AV for each individual user. These solutions reinforce each other by catching different types of viruses – introduced in different ways into your network. Intrusion prevention should also be layered at multiple vantage points with Network Intrusion Prevention at the perimeter and Host Intrusion Prevention for internal servers. Internal servers are vulnerable to deliberate insider attacks and also to careless employees who bring infected laptops into the network from home. Both of these types of attacks can be caught only at the host and won't be stopped by perimeter defenses.

LAYERING A 24/7 HUMAN ORGANIZATION ON TOP OF TECHNOLOGY

No matter how sophisticated security technologies become, many attacks are first detected and stopped by well-trained, highly certified security analysts. Organizations have the option of developing their own team or taking advantage of a partner who is monitoring their security environment 24/7. It may not be cost-effective for an agency to staff around the clock and it is difficult to add "security" to a long list of responsibilities for internal resources. Most experts recommend outsourcing – or at least supplementing – the security analyst role with a dedicated external team. These teams are focused exclusively on researching new vulnerabilities and exploits, monitoring many clients to detect emerging attack patterns by industry or geography, and using sophisticated correlation and visualization technologies to quickly respond to security events from across your network. ■

Jon Ramsey is chief technology officer at SecureWorks. For more information, visit SecureWorks at:
info@secureworks.com

Effective security fencing

By John Payne

Keep them out, and better yet, keep them from even considering trying to get in. And if they try, make them take enough time for you to respond. A simple enough concept, and in industries dealing specifically with security, these thoughts are reflected in the three Ds: Deter, Detect and Delay.

Terrorist plots against high-risk targets – such as government facilities, power plants, and transportation nodes – underscore the importance of perimeter control to prevent or mitigate unauthorized parties from breaching the perimeter of a wide range of facilities, particularly critical infrastructure and military facilities.

THE THREE Ds

Whether a fence, gate, or partition, a security barrier must achieve security's three Ds:

Deter: Preventing an attack from occurring, or diverting it to a more appealing target, is the most effective perimeter security tool, and for effective deterrence, size matters. The fence must eliminate attack by presenting a formidable-looking obstacle that discourages attempts to penetrate or circumvent the barrier.

Detect: Should someone attempt to breach the barrier – over it, through it or below it – knowing that an attack is occurring in real-time is critical for mitigation and response. The physical security barrier should be considered a fully integrated component that works in concert with an overall site security plan and includes intrusion detection, surveillance and lighting.

Delay: A tall and heavy barrier – such as anti-climb, anti-cut security mesh fencing – will hinder penetration attempts and increase the probability of detection and response by security personnel or law enforcement. With respect to anti-cutting resistance, the weight, the type and the general design of the barrier material all impact delay time. Some materials may be heavy, but can be relatively easy to disassemble, such as many offerings of chain link material.

SECURITY MESH PANEL FENCING

Fencing constructed with anti-cut, anti-climb security mesh panels have gained popularity in the U.S. – after years of being the standard in Europe and other parts of the world – because they incorporate small openings that prevent a would-be intruder from effectively gaining a hand or foot hold with which to climb. Small mesh openings also resist cutting tools – and the substantial thickness of most mesh resists all but the most substantial breaching equipment. Typically installed using 4 x 8 foot sheets or panels, mesh is available in a variety of styles, including welded wire, expanded metal and woven wire.

Field tests have demonstrated the strength of security mesh panels against cutting attacks. When common breach tools were applied, the mesh demonstrated a substantial delay in penetration; in some cases, entirely resisting the creation of a useable gap. Conversely, a standard six-foot chain link fence can be cut entirely, from top to bottom, in a mere 20 seconds, using a simple set of hand-held wire cutters.

Recent developments in the construction of security mesh panel fencing allow the seamless integration of surveillance, intrusion detection cabling, lighting, and even communications. The result is an anti-cut, anti-climb mesh "smart fence" that offers not merely a barrier, but the framework upon which to build a "system of systems" within the overall site security plan reflecting all three Ds. This smart fence can be created without the added expense of trenching, and intrusion detection cabling is protected from weather, vandalism and tampering because it is contained within the horizontal rails within the overall fence framework. This type of integration is uncommon in chain link, ornamental, and palisade-style fencing.

This same development in fence technology also enables easy and affordable retrofitting of chain link fencing without removing the existing posts. The result is a more secure barrier at a cost that is lower than a complete replacement of the existing posts.

TAKING THE NEXT STEP

Once the threat to a facility is defined and barrier types analyzed and ranked, the next step often involves consultation with a firm experienced in designing security barriers. Qualified fence manufacturers are capable of engineering a solution to fit a facility's requirements while assisting in the development of a barrier specification that adheres to performance standards specific to any applicable geographic, environmental and security regulations.

Performance standards are critical. Ultimately, a facility's security is measured against the ability to meet or exceed performance standards and protect the asset (e.g., U.S. Department of Homeland Security's Chemical Facility Anti-Terrorism Standards [CFATS] regulations). Security standards for barriers are only one of many considerations, but appropriate fencing is critical – the success or failure of a site's overall security plan often begins or ends at the perimeter line. ■

John Payne is president and CEO of Payne Fence Products, LLC, a member of the Betafence group of companies. He can be reached at:
Security@payneFENCE.com

When security matters, speed counts

By Dick Loos

We've all had to remove our shoes, watches and almost everything else to get through airport security when traveling. What about the airport operations areas outside of the terminal, where even large international airport facilities offer minimal perimeter security?

Most of the airport operations areas (AOA) feature imposing barbed-wire fences and some number of access gates which are controlled using card readers, keypads, fingerprint recognition, etc. Airport security procedures mandate that once an authorized vehicle enters or exits the AOA, the driver is to wait until the gate is completely closed before continuing. Although the security personnel try to enforce this procedure and most of the users comply, there are a few that do not and that might jeopardize the safety of passengers.

Today's gate operators are mechanical, utilizing chain, hydraulics, cable or gear systems. Mechanical operators are prone to failure over time and require periodic service. The speed of these operators varies from one to two feet per second. A typical entrance is 20 feet, which means that it takes 10 to 20 seconds to open and then another 10 to 20 seconds to close. Add another five seconds to drive through and you have a worst-case scenario of 45 seconds to enter or exit. This time becomes crucial when there are emergencies requiring additional security and ambulance services.

This very potential vulnerability prompted us to patent and develop a new gate operator that is fast and reliable. Called VMAG (Velocity Magnetic) this new high-speed magnetic gate operating system moves slide gates up to six feet per second and uses no mechanical drive components. Russell Timmerman, our lead engineer of product development, designed the VMAG to be significantly faster than traditional gate operators.

Timmerman says the revolutionary VMAG technology conquers the inherent weaknesses in other existing slide gate systems and is competitively priced compared to other higher end industrial gate operators.

We see VMAG developing not only around airports but at various security-priority locations, such as nuclear power plants, chemical companies and depots, petroleum reserve sites, military bases and embassies around the world.

The VMAG has no moving drive mechanisms. It uses two linear induction motors; similar to the technology found on high-speed roller coasters, whose motors are entirely magnetic, resulting in reliability and fast but smooth rides. John and Jeff Wood of VMAG got the idea from watching the high-speed roller coasters during a trip to a theme park 10 years ago and obtained a U.S. patent for use on gates and portals.

The VMAG has no gearboxes, hydraulic hoses, cables or roller chains, which can become maintenance issues over time, thereby compromising reliability. The linear induction motor is constructed using only magnetic coupling, which provides a smoother operational process. Another plus is that it can be adapted to existing gates of any weight and length. The VMAG motor simply adjusts itself to the existing gate automatically, according to engineer Timmerman.

For that extra security measure not standard in other gate operators, a positive locking feature secures the VMAG gate whether it is in the open or closed position. There is no way to force this gate open.

When it comes to installation, no concrete pad is required. The drive motors and reaction plates mount directly to the gate. There is also no programming. The VMAG will automatically program itself on startup and is compatible with all access control devices.

Other planned enhancements include the ability to tie into a network, phone system or other type of remote communication where an operator can go online to monitor or change gate operations.

VMAG is currently in use at the San Antonio International Airport and has cycled through more than 170,000 times with no equipment problems relating to this heavy usage.

Much has changed in airport security over the years, including vast improvements in passenger check-in and boarding. We believe passengers should be equally safe, while sitting inside a plane, waiting on taxiways before take-off or inside the terminal. ■

Dick Loos is president of VMAG.

Networked laser-enabled perimeter protection

by Geoffrey Anderson

The Department of Homeland Security, through the Critical Infrastructure Partnership Advisory Council, is responsible for implementation of government standards and congressional acts, such as the Chemical Facility Anti-Terrorism Standard and the Marine Transportation Security Act, which define an overall National Infrastructure Protection Plan to ensure the continuity of the nation's critical infrastructure and key resources.

The goal of compliance with these standards and acts is achieved through the deployment of resources including video surveillance, infrared detectors, and a variety of other sensor technologies. The web of electronic and physical security is designed to protect the nation's security, public health and safety, economic vitality, and way of life, around the clock. Nevertheless, every security solution has its vulnerabilities and the ability to remain ahead of a potential intruder is critical. Thus, the development of stricter regulations and stringent penalties has forced more and more facilities to upgrade to or implement new design solutions to increase measures for providing the required security.

Whether your facility is an electric power plant, nuclear reactor, communications grid, water treatment facility or other utility or service vital to the public at large, upgrading your video surveillance system with laser-enabled detectors is a major step toward maintaining

situational awareness and a heightened level of first defense.

Optex, Inc. recently introduced the Redwall (RLS-3060), an innovative laser-enabled scan detector which can detect a moving object's size, speed and distance with high reliability. Once the sensor has detected the location of intrusion in the covered area, the information is communicated in less than 1/100 of a millisecond to a PTZ (Pan/Tilt/Zoom) camera and network video recorder. Unlike passive infrared, the laser technology can see through dense fog and heavy rain and is immune to daily heating and cooling of the surface areas in the field of view. A single RLS-3060 laser detector is capable of detecting 180 degrees of area, significantly improving the coverage for perimeter intrusion detection. Applications for laser-enabled perimeter protection include border protection, government offices, schools and any facility or campus. Laser perimeter security provides immediate coverage without the need for expensive investment in trenching, wires and tedious testing and setup, not to mention continuous weekly calibration for other sensor-based systems. Laser sensors will speed up compliance and reduce overall security costs.

"We have seen our clients combining traditional and non-traditional sensors with CCTV systems in order to adapt to the new standards," said Jason Beardsley, VP sales & marketing, Optex, Inc. "The condition of perimeter protection is rapidly changing, and the acts and standards implemented by the DHS have created new requirements for designing integrated electronic and physical security systems."

Optex recently teamed up with JVC video security to integrate the laser sensor capability into the JVC IP network video recorders and IP PTZ network cameras, using the Redwall laser sensor to provide instant automatic notification of a perimeter breach. When an intrusion is detected by the Redwall laser, split second decisions need to be made. Often times the PTZ camera is on patrol covering a wide area and chances are it would miss the intruder until the facility was actually breached.This is where laser timing provides that near instantaneous information of the exact location of the perimeter breach and directs the PTZ camera to the breach.

The JVC VN-V686WPBU IP PTZ network camera has lightning fast reaction time with the ability to spin to the intrusion point at 400 degrees per second and then lock onto the target with the built-in video analytics intelligent auto tracking. If the camera had to wait for the analysis commands from the system controller, it would surely lose tracking of many types of intrusion. JVC's intelligent auto tracking in the camera provides near instantaneous response to the intruder's movement and trajectory, allowing the security system operator to implement the intrusion response while the camera stays with the intruder automatically.

Laser technology gives more precise and reliable alarm activity. Advances in IP network cameras and network video recorders also provide faster response time with intelligence built into the camera providing continuous intruder information after acquisition by auto tracking. Today's laser technology from Optex is capable of providing a full 3D overlay on a given perimeter: roof-to-ground and fence to wall, for any application with unlimited boundaries. Using JVC IP-based CCTV equipment integrated with laser sensor technology is the optimal development safeguarding every facility to the standards of the DHS and certainly provides an added level of automatic split second decision making which is essential in securing critical infrastructure. ■

Geoffrey Anderson is the manager, marketing and brand strategy with JVC.

CBRN false positives & perimeter protection

By Greg Eiler

Whether it is a military base perimeter, a lobby inside a Class A office building or the four corners of a school campus, these are all perimeters that need protection from an airborne CBRN release, whether accidental or a targeted terrorist attack. Without reliable detection, an automated response and real-time data acquisition, those inside the perimeter could fall victim to the same chlorine style attacks of World War I.

How important is reliability? Critical! If you are unable to rely on the equipment deployed, you are at a supreme disadvantage. In the case of detection technology, false positives create false alarms; false alarms initially create panic, then nuisance, then ultimately, the alarm is ignored or removed from service. Money, time, effort and true protection wasted – possibly life as well. Case in point – the TSA just removed over 100 explosive detection devices from 37 U.S. airports because the detection information was false all too often, thus creating a failed sense of security and long lines at the gates, not to mention customer complaints.

So how does one overcome the issue of false positives and false negatives? In the case of a San Francisco start-up company, it comes down to the approach taken to cure the problem. Many detectors have been taken from a laboratory environment or developed to meet a predetermined specification. The shortcomings to those approaches include equipment that may not function properly in an operational environment, or often the specification challenged the engineering process as a result of being too broad, lofty or extremely difficult if not impossible to attain thus yielding a less than expected outcome once manufactured.

Preserving human life is what most CBRN detectors are deployed to protect. Certainly assets are important, and the mission is also important, but life is what we value most. To properly protect the humans inside the perimeter, reliable technology must placed on or outside the perimeter to answer these goals.

Building Protection Systems, Inc. (BPSI) was founded to engineer and manufacture the best of breed detectors to assist in the war on terror post 9/11. BPSI began with a focus on following the instruction of various programs and white papers in order to build detectors based on a given specification, yet we kept running up against the same problems other manufacturers were; a detector with acceptable laboratory performance but less than adequate field performance and false positive indications from environmental interferences. When discussing this challenge with others in the same business, many of the rationalizations were that something within the various specifications was at the root of the problem. Others just advised that their detector was the best on the market and the closest offering to the specification at hand.

When quantifying the performance of the various devices available, a common thread became apparent: the modus operandi was to engineer and build a detector; yet when the detector was utilized in actual field conditions with marginal operational results, the next step was to rationalize the overall functionality and performance of the device through exceptions to the given specification. In the case of detection, the downside to this was the unacceptable rates of false positive indications, slower than desired speed to detection or even a lack of proper identification.

Over the past five years, Building Protection Systems, Inc. (BPSI) has worked with an "out of the box" engineering methodology when developing our next generation detectors referred to as the Sentry One family of products. With this direction, BPSI has figured out how to eliminate many of the issues plaguing the detection industry with some of them being: false positive / false negative indications, time to accurate detection and identification, as well as the need for costly maintenance and reliable operation for years in the absence of any human intervention, just to name a few. "What was the most impressive thing about this operation was they weren't prepared to go to market until they were professionally satisfied that it was a fail-safe system. All you need are one or two false positives and you can forget about marketing their product. They did it right, rather than doing it quick," said former Homeland Security Secretary Tom Ridge during an interview in early June 2009. ■

Greg Eiler is the president and CEO of Building Protection Systems, Inc. He can be reached at:
geiler@BPSIglobal.com

Zoomier.

With our 36x zoom, PoE, and progressive scan CCD imaging, JVC's VN-V686 IP camera is the ultimate security blanket.

The JVC VN-V686 PTZ Dome IP camera helps you see closer and clearer than ever before—**with the industry's only IEEE 802.3af Power over Ethernet (PoE), optical 36x zoom** and progressive output CCD imaging. Our imaging engine delivers dual JPEG and MPEG smooth-motion streams at 30 frames per second, plus you can easily lock onto and track targets with our new Intelligent Auto Tracking. Both our exterior weatherproof and interior units feature a hot-swappable camera head for easy maintenance and are backed by JVC's hassle-free, 3-year warranty. No wonder we won the New Product Showcase Award from the Security Industry Association (SIA)!

V.NETWORKS

Take a closer look at JVC's VN-V686 IP cameras by visiting www.jvc.com/pro

www.jvc.com/pro

JVC®

The Perfect Experience

Blast-mitigating window systems

By Tom Mifflin

One of the final lines for perimeter protection is the building façade itself. High-performance window systems engineered to meet current requirements will protect the most valued asset -- the building occupants – by reducing the amount of hazardous flying glass and debris, thereby lowering the possibility for serious injury and / or death.

Two essential documents guiding blast mitigation in the planning, design, construction and modernization of U.S. facilities are the Department of Defense's Unified Facilities Criteria (UFC) for "Minimum Antiterrorism Standards for Buildings," and the General Services Administration's Inter-Agency Security Committee's "Security Design Criteria for New Federal Office Buildings or Major Modernizations."

Both the DoD and GSA often refresh their publications to reflect increased knowledge, new technologies and innovative materials. Identifying and understanding the most up-to-date standards is critical to ensure accurate specifications that comply with the facility's intended level of protection.

Once the protection level is prescribed, an appropriate response for the window system can be defined. As extreme pressures released by an explosive mass impinge on a building's exterior walls, the elements of the window or curtainwall assembly, must work together with the building structure to withstand the blast load and dissipate its energy. Instead of the historical design practice of specifying thick windows with rigid frames, modern blast-mitigating assemblies are intended to be flexible, and absorb blast energy.

By design, the glass is the weakest component within a blast-mitigating window system. Depending on the criteria, the surrounding components' purpose is to ensure that when the glass breaks, it is retained in the frame, and that fragments exiting the frame fall harmlessly within a specified distance.

DoD UFC 4-010-01 indicates a clear preference for blast hazard mitigating window and skylight systems that incorporate laminated glass. It states, "Window retrofit products that rely on fragment retention film, fragment retention as a part of a retrofit system, or blast curtain systems generally have higher life cycle costs than laminated glass window, due to their shorter design lives and due to operation and maintenance issues."

During a blast event, laminated glass can take the brunt of the blast force. The framing connections, glass bites (the depth of glass captured by the frame), and glazing materials work together keeping the lites in their frames. The mullions and sashes adequately deflect to handle the system's changing shape. And ultimately, reducing the energy imparted to the building structure itself.

Exterior blast loads must be transferred and dissipated through every intervening component between the glass and the building foundation. Window and curtainwall anchorage systems play a key role. Here again, flexibility is key. Too many anchors will add too much stiffness to the system, as well as unnecessary time and cost to the installation schedule. Three-way adjustable anchors are preferred for unitized window systems. They accommodate variation in substrates, allow for several types of curtainwall-to-building fasteners, and are capable of transferring high loads. Contributing to ease-of-installation, they can be adjusted without the use of special tools or complicated hoisting and lifting systems.

Early coordination between manufacturer, blast consultants, glazing contractors, other building trades, and designers is crucial to ensure proper anchorage and installation. Any modification to the substrate, glass type, size, rigidity, configurations or required energy absorption through deflection will significantly alter the performance of an integrated system.

Exterior sun shades and interior light shelves also should be assessed as integral components of the window system. Features like these are increasingly desired for solar control in green building designs. Energy-efficient glass options and recycled aluminum content in framing systems are other items frequently requested on green buildings. All of these elements should be carefully evaluated to assess the structural integrity and overall performance.

Computer modeling and analysis allows the building team to verify its designs and account for multi-hazard mitigation, such as seismic, high wind or thermal performance needs. Rather than expensive trial-and-error experimentation in the laboratory, in the shop or in the field, computer modeling cost-effectively verifies performance, while minimizing opportunity for delay or mishap during fabrication and installation. ■

Tom Mifflin serves as government / military market manager for Wausau Window and Wall Systems. He can be reached at: **tmifflin@wausauwindow.com**

Become more informed, more competitive, and more profitable.

IN A NEW YORK MINUTE.

Security with an emphasis on now. The all-new Public Security & Safety Expo at ISC East, a one-of-a-kind event offering government, law enforcement, and campus security officials the opportunity to see the latest technology and solutions for securing homeland, municipalities and infrastructure. You'll have the opportunity to forge relationships with new vendors and educate them in an intimate setting on current projects, specs, and issues.

You'll find a broad look at all public security sectors, including:
Law Enforcement • Urban/Border Protection • Campus Safety • Transportation Security

SECURE YOUR PLACE. REGISTER FOR FREE AT: **WWW.ISCEAST.COM/GSN**

Your registration also gives you full access to ISC East, where you'll find:

- Access Control
- Alarms & Monitoring
- Biometrics
- Fire Control
- Remote Monitoring
- Systems Integration
- Video Surveillance
- Wireless Applications
- and more...

SPONSORED BY: SIA

THE OFFICIAL PUBLICATION: GSN

ENDORSED BY: CASIA

CORPORATE PARTNERS: AXIS, DSC, HID, Honeywell, Infinova, NAVCO, PELCO, ovi

CODE: AD1

New perimeter security solution secures vital Birmingham Water Works

By Tom LaRose

The Birmingham Water Works Board (BWWB) in Alabama is committed to providing the highest quality water and service to their customers and service area.

As a concerned corporate citizen, the BWWB is responsive to the needs of the entire community and strives to maintain, preserve and conserve the region's precious water resources in order to ensure adequate water quality and supply for future generations.

The number one priority of BWWB is to provide the highest quality water possible for its customers' health, welfare and enjoyment. The company uses the latest technology in water treatment and consistently meets and exceeds state and federal standards for safety and quality.

The BWWB has four water treatment facilities – Carson, Putnam, Shades Mountain and Western Filter Plants. Combined, these filter plants deliver an average of 100 million gallons of water a day to customers in five counties.

In today's world of anti-terrorism initiatives, multiple regulatory requirements and increasing health concerns, several industries, especially water utilities, must implement a tremendous number of system upgrades. The BWWB is no exception and has initiated a 10-year Capital Improvement Plan to battle these and other issues. This includes ensuring that when faced with an emergency, water supply is not compromised.

THE CHALLENGE

The U.S. Environmental Protection Agency (EPA) enforces clean water and safe drinking water laws that the BWWB, as well as other water utilities across the U.S., must comply with. After 9/11, the EPA ordered all large water systems to do a vulnerability assessment. Each water works had to identify the most critical activity it must be able to sustain if under attack. This involved determining where critical assets were vulnerable to physical destruction of infrastructure (e.g., pumps, dams and filter plants) and also contamination at any stage of the water treatment process.

As a result of that assessment certain recommendations were made to harden critical sites, i.e., raw water intake stations, inline pump stations and filter plants.

One of the recommendations included upgrading physical perimeter security at critical sites, which originally consisted of chain link fence at a few locations. The perimeter security system upgrade had to meet a number of criteria. It had to:

- Provide a deter-and-detect solution 24 hours a day, seven days a week, fulfilling the BWWB's duty of care;
- Satisfy the Board and local authorities that it would meet stringent legal, health and safety criteria;
- Be integratable with other security systems, e.g., access control and CCTV/DVR; and
- Provide centralized management and fence zone monitoring of multiple distributed sites.

THE SOLUTION

After investigating a number of options, the decision was made to install the PowerFence Trophy FT perimeter security system from Gallagher Security Management Systems, at eight critical sites over a period of five years.

PowerFence systems are non-lethal electric fence systems designed to both deter would-be intruders and detect attack. They have been proven over more than 20 years and installed on a wide variety of sites, including defense and critical infrastructure.

Terry Oden, security director at BWWB, with over 40 years of field experience in security and risk assessment, recalls, "Through prior experience with physical protection, I knew that Gallagher PowerFence technology had been approved by government agencies for use in some highly classified locations. It had an excellent reputation."

Terry adds, "The team at Gallagher were willing to work with us to customize a solution to meet our requirements, for example, installing the fence on rough terrain. It required some very creative thinking."

Terry was also able to use the Gallagher Code of Practice to help overcome local ordinances against electric fencing. The Gallagher Code of Practice and Minimum Installation Standards meet and exceed the requirements of all national and international standards regarding safety and the application of electric fence systems.

Key benefits of the PowerFence Trophy FT system for BWWB are its scalability, network compatibility, integration possibilities, system architecture and ability to implement electronic access control and intruder alarms.

The operations team at BWWB have found the PowerFence Trophy FT system very easy to operate. Terry adds, "The operating system is highly compatible with our other security systems. The quality, flexibility and dependability of the Gallagher technology meets all our expectations."

The Birmingham Water Works Board is satisfied that by installing the PowerFence Trophy FT perimeter security system, it has successfully secured its critical sites in line with the anti-terrorism and risk management objective; that is, providing safe water facilities for employees, the surrounding community and the environment. ■

Tom LaRose is the Gallagher Security Management Systems business development manager (North & South America). For more information, visit: **www.powerfence.com**

ADVERTISER'S INDEX

Leaky coaxial cable sensors: The past, present and future of this covert technology

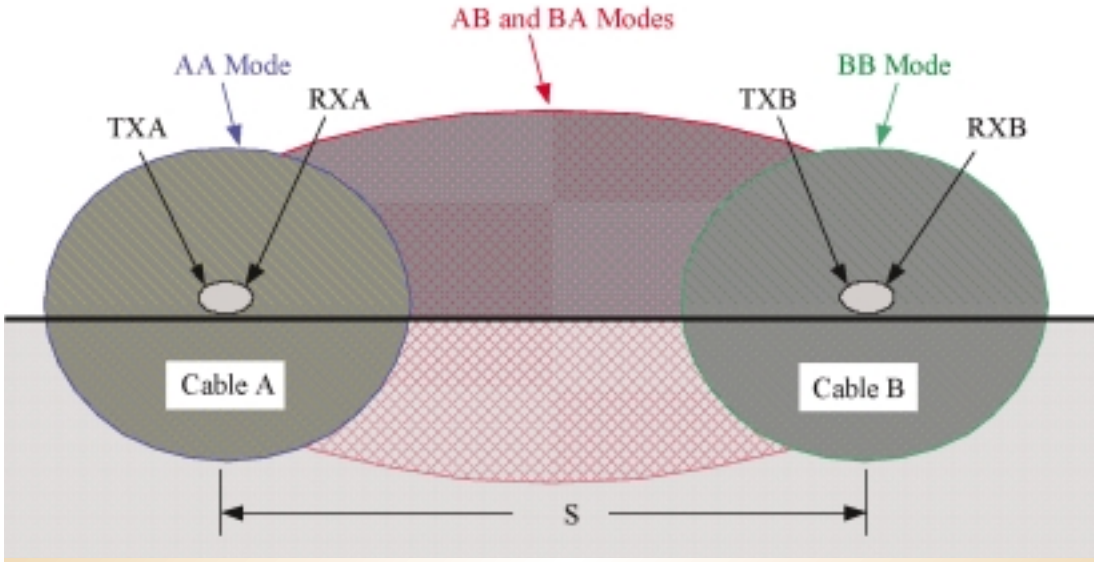
by Dr. Keith Harman

BACKGROUND

Leaky coaxial cable sensors have been used in outdoor perimeter security for more than 30 years. They are a guided radar technology and completely covert buried cable sensor that can go around corners and up and down hills. Such products are relatively immune to environmental conditions and can operate in the presence of vegetation. The invisible detection fields are very difficult to locate and evade. For over 30 years, this technology evolved from GUIDAR, a very expensive ranging product with coarse location accuracy, to a number of distributed CW (continuous wave) "block" type sensors, such as Sentrax and Perimitrax. These CW sensors were lower in cost, with zones being defined by the length of the sensor cables and addressed long perimeters by networking multiple processors with power and data over the cables. The fact that the same cables were used for sensing, power and data networking, allowed these closed loop networks to be inherently secure and reliable. This technology further evolved into OmniTrax, a true ranging radar with a one to three meter accuracy. OmniTrax can also be networked to include secure power and data networking over the cables to protect very large perimeters.

UNDER DEVELOPMENT

Recently the OmniTrax technology has been enhanced to address the rapidly deployable market through the use of "Quad Processing," whereby two cables are laid on the surface around the protected resource. Quad Processing overcomes the noise created by minute cable motion which has restricted all leaky cable sensors to buried applications. This makes "through the woods" applications possible where it is not possible using most other outdoor perimeter security sensors. This development was done in collaboration with the U.S. Air Force. With enough interest, Senstar can turn this application into a commercial product.



Quad Signal Processing

THE BASIC CONCEPT OF QUAD PROCESSING

Signals are simultaneously transmitted and received on Cables A and B. Proprietary coding techniques are used so that responses to each transmission can be independently measured. This effectively allows the processor four independent views of the detection zone (AA, AB, BA and BB). In the rapidly deployable product, the AA and BB modes are used to detect and discriminate against cable motion while the AB and BA modes are used to detect and locate intruders.

THE FUTURE

Looking forward, the same Quad Processing can be used to create an enhanced buried cable sensor that is covert, terrain-following, with pinpoint target location. In addition, it can provide the direction and speed of the crossing, target classification and extremely well contained detection fields. The classification routine can differentiate between small animals, humans and vehicles and in some cases, the type of vehicle.

COVERT DETECTION ON LONG PERIMETERS

The covert terrain-following features of OmniTrax with the enhanced capabilities of Quad Processing can be used to greatly improve the security for long perimeters, including airports and borders. These ultra-high-performing sensors can be used as a covert "trip line" to detect, locate and to some extent, identify targets that should be tracked and assessed using wide area radar or VMD. This eliminates the problem of detecting and tracking all moving animals or objects over larger tracks of land and allows assessment tools to focus on the intruders of interest. It also helps overcome the line of sight restrictions on these technologies. ■

Dr. Keith Harman is vice president of engineering for Senstar Corporation.

One vendor's challenge

by Maury Shepherd

The Department of Homeland Security's Secure Border Initiative (SBI) plan requires a complex interplay of intelligence, infrastructure and human capital to achieve its goal of operational control of all U.S. borders. Even deployment of a single infrastructure component – fencing, for example – demands a vast supply of product, produced to rigorous standards and delivered on an unyielding schedule.

The end result – a seamless, unbroken barrier – demonstrated the tremendous teamwork and coordination required to achieve it.

C.E. Shepherd Company supplied installation-ready, welded wire mesh perimeter protection panels at the distribution point. Panels were produced to U.S Army Corps of Engineer's specifications, which included exact wire gauge and mesh spacing, with no margin of error. This required a commitment to large scale production quantities with little or no down-time.

While C.E. Shepherd Company is a large manufacturer of engineered wire mesh, the delivery requirements for this project required a new level of performance. This required two specially designed machines, running at full 24 / 7 production mode for eight months. The immense demand was not simply on the company's own internal infrastructure, but on the suppliers and transportation partners as well. Close cooperation with the primary government contractor and coordinator of multiple installation contractors was essential. C.E. Shepherd Company experienced the equivalent of an eight-month sprint relay, completed simultaneously with necessary repairs, parts replacement and set-up changes.

To complicate the challenge, nature threw a curve when Hurricane Ike came ashore just miles from the production facility, rendering both plants and administrative offices powerless for a full two weeks. What Ike stopped had to be brought to an immediate and full re-start with no ramp-up. Once again, the production team, suppliers and transporters stepped up to meet the challenge.

The result? One hundred and forty-one miles of welded wire mesh perimeter fence manufactured in eight months, on time, and engineered to exact SBI specifications.

By meeting the exacting volume, time and technical standard requirements of this job, C.E. Shepherd Company can point to miles and miles of product and appreciate not just its contribution and a challenge well met, but the comprehensive effort required by many to secure our country's borders. ■

Maury Shepherd is executive vice president of C. E. Shepherd Company.

Do You See What We See?

Mobile Surveillance System

Telephonics' ThreatSTALKER™ Mobile Surveillance System integrates Ground Surveillance Radar, a long-range EO/IR sensor package, and a laser range designator into a common operating picture that is networkable to multiple platforms.

With an extensive library of multiple plug-and-play sensors, the system is completely customizable to fit your requirements – from Chem/Bio to unattended ground sensors.

Preferred supplier to U.S. Customs and Border Protection and currently in production.

NOW ...
You *Can* See What We See.

For further information
contact us at 631-549-6158

35321

TELEPHONICS®
A Griffon Company
www.telephonics.com