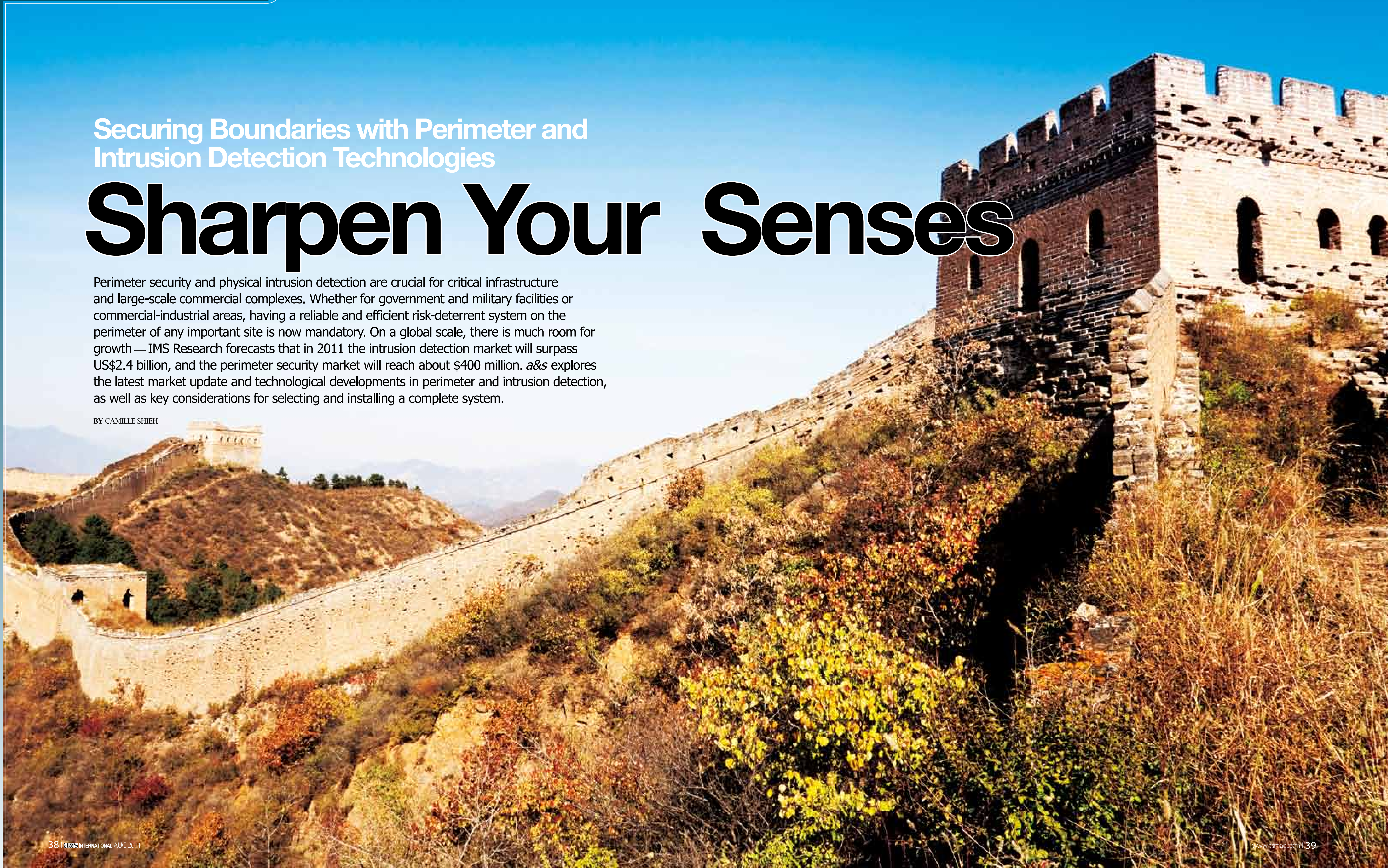


Securing Boundaries with Perimeter and Intrusion Detection Technologies

Sharpen Your Senses

Perimeter security and physical intrusion detection are crucial for critical infrastructure and large-scale commercial complexes. Whether for government and military facilities or commercial-industrial areas, having a reliable and efficient risk-deterrent system on the perimeter of any important site is now mandatory. On a global scale, there is much room for growth — IMS Research forecasts that in 2011 the intrusion detection market will surpass US$2.4 billion, and the perimeter security market will reach about $400 million. *a&s* explores the latest market update and technological developments in perimeter and intrusion detection, as well as key considerations for selecting and installing a complete system.

BY CAMILLE SHIEH

Market potential and sales performance for perimeter security and intrusion detection products depend on the region or country's recovery from the recent recession, according to industry experts. Retrofit projects tend to take place in mature markets, while new projects occur in emerging markets. "The increase in demand is almost directly related to a country's GDP growth rate and economic recovery," said Luc Joosens, Detection Product Management Leader for EMEA, UTC Fire & Security. "Countries that have experienced economic recovery in 2010 have demonstrated an increased demand for intrusion detection systems."

The Americas and Asia markets have strong demand for perimeter and intrusion detection products. "The Asian markets have been driven by construction growth, low unemployment, high GDP, a growing middle-class and increased government spending," said Blake Kozak, Market Analyst for IMS Research. "The American intrusion market is forecast to be especially in demand because of the move away from traditional PSTN communications toward GPRS and wireless connectivity."

"The Gulf region is a growth market for us, and we are actively developing our base there," said Stewart Dewar, PM of Senstar. "In terms of emerging markets, India continues to hold opportunity for perimeter intrusion detection system (PIDS) companies as do Mexico, Colombia and Brazil. We have also recently opened an office in Singapore to address this region more aggressively."

Several manufacturers concur with IMS Research's prediction on the perimeter security and intrusion detection markets. "To achieve US$570 million in 2014, the market would need to experience growth more than three times over what was seen from 2009 to 2011," said David Curtiss, Director of Engineering at Smarter Security Systems. "While that type of growth seems aggressive, government programs are placing requirements on critical infrastructure facilities that will need to be fulfilled. Also, there are new video management and analytic technologies now offered to replace or augment existing infrastructure."

Conservative players have

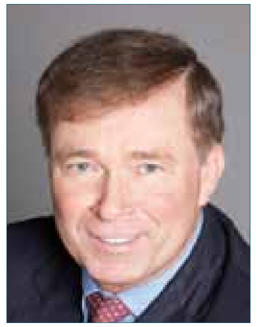
▲ For critical infrastructure, the requirements for intrusion detection are moving toward higher security, meaning better capture performance, signal analysis and communication solutions.

less bullish estimates, although they agree that GDP growth and government programs will drive this market. “The US market, for instance, will turn around over the next couple of years with regulations such as Chemical Facility Anti-Terrorism Standards for the petrochemical industry. The International Ship and Port Facility Security Code in relation to the seaport market is already impacting perimeter security business in Africa and other places,” Dewar said. “The next three years should give the sluggish markets, particularly in Europe, time to rebound and get back on track. In many cases, projects have not been cancelled but rather delayed or pushed off to deal with the economic challenge.”

Others are even more optimistic about potential growth. “The worldwide perimeter security market should reach even more robust levels as new technologies are integrated into comprehensive solutions,” said James Ionson, CEO of Oncam Global. “Open perimeters, such as deserts or waterways, with few, if any, obstacles to access, present new challenges for the industry to address. The spike in piracy at sea and terrorist activity can be expected to result in the need for enhanced security systems for both commercial and luxury travel vessels, as they extend surveillance from a liability focus to also include perimeter security.”

Luc Joosens, Detection Product Management Leader for EMEA, UTC Fire & Security

Stewart Dewar, PM of Senstar


James Ionson, CEO of Oncam Global

SPICING UP OLD FENCES

Perimeter security and intrusion detection products are more complex and powerful than ever. End-user behavior has also shifted from using individual products to combining various detectors and sensors for holistic protection. “As a result of the fact that basic detection technology has been getting better and more advanced, the coverage of different risks is currently much better than some years ago,” said Juergen Grasmehr, Global Portfolio Manager Intrusion and Perimeter Systems, Siemens Building Technologies. “It is now possible to cover almost any kind of areas or objects, such as fences, walls, ground, water, air, building roofs and building facades. Together with other technologies like video surveillance, it is now possible to have very high detection quality combined with an automatic, sophisticated verification thanks to automatic camera tracking, zooming, object classification, visualization in overview maps and the like.”

DIFFERENT TYPES OF INTRUSION DETECTION

- For fence climbing detection: microphonic cable, active IR (AIR) beams
- For detection of entry in open spaces: AIR beams, outdoor microwave, outdoor motion detection, video surveillance
- For abandoned object detection: VCA
- For detection of penetration of roofs and walls: microphonic cable
- For forced opening of shielded spaces detection (for instances water tanks, vaults, gun cabinets): Seismic sensors
- For detection of the opening of doors/windows: contacts, shock sensors
- For window glass breaking detection: acoustic glass-break sensors
- For detection of entry in a room: motion sensors and video surveillance

Source: UTC Fire & Security

One way to provide greater security at critical infrastructure sites is to combine multiple security technologies. “Indoor detection systems can be expanded with perimeter protection for advanced warning, while multiple technologies can be combined in the perimeter protection, such as fence and active IR; fence and microwave; motion and video surveillance; or combinations of these,” Joosens said. “Improved anti-masking technology reports sabotage attempts to the security system, and finally the increased use of video surveillance cameras with higher image quality and longer range provides better security at key sites.”

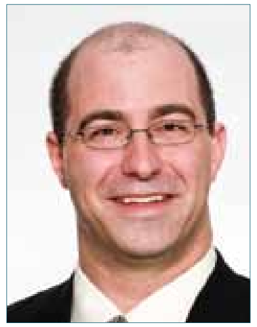
IR with microwave, quad pyro elements, multicurtain laser and 3-D detection based on time-of-flight technology are some examples of basic detection technology becoming more advanced, Grasmehr said. "Also, detector information can be delivered faster and more precisely with current technology. For instance, placing a number of alarms in a specific zone from different detectors can increase or decrease the real alarm probability."

For outdoor detectors, the increased development quality, as well as manufacturing quality of electronics and mechanics, is manifested in affordable high-end products such as laser scanners, radar detectors, high-end fiber optical detection systems or piezo dynamic sensors, Grasmehr said. "New sensor systems are more flexible, and in some it is possible to run and combine multiple, complex detection algorithms on one detector at the same time. For instance, a laser scanner is able to detect small object in one area and large object in another area." Dual motion sensing technologies — such as double passive infrared (PIR) or PIR with microwave — are also gaining popularity, as combinations are capable of achieving higher false alarm immunity, Joosens said.

"Using the latest K-band dual technology, this kind of sensor verifies the PIR signals with the microwave signal prior to any alarm decision and is less likely to trigger false alarms as K-band microwaves do not penetrate walls and glass as easily," explained Tony Makosinski, External and Security Industry Liaison, Honeywell Security. "Therefore, faster and more reliable detection is achieved, and false alarms and associated intervention costs are reduced. As this technology becomes more developed, it is increasingly taken up by the rest of the industry."

Tony Makosinski, External and Security Industry Liaison, Honeywell Security

Jason Burger, Sales and Marketing Manager, Navtech Radar



Dennis Petricoin, VP of Product Management for Intrusion Detection, Bosch Security Systems

For fences, cable sensors deploying fiber optics and coax are prevalent today, said Curtiss. "For fences with detectors, PIR detectors offer superior performance when complemented with a perimeter security system in areas such as gates, roads or any location that may require trenching."

Buried fiber-optic systems appear to be taking the lead versus radio frequency/leaky coaxial types of sensors in underground detection due to their immunity to water, lighting and soil conditions, said David Smith, CEO of Optellios. "Although fiber optic technology is not new, the prevalence of its use in security deployments is on the rise compared to strain gauge, microphonic and shaker systems, because it is easy to install." Fiber requires no electronics on the fence, no additional power and is immune to lightning and radio interference. It has sufficient bandwidth to handle video and access control communication.

Detection technologies initially developed for military applications, such as radar detection, are more common in civil security projects, Grasmehr added. "The radar system could detect and track a person from a considerable distance before he or she is even near the fence or up to the fence line, and continues to track once the person has entered the fenced perimeter," said Jason Burger, Sales and Marketing Manager, Navtech Radar. "Radar does not require light or good weather to function, and would work in all light and weather conditions."

"Some airports are using radar arrays that are configured to detect movement in both the X and Y axes. This data is then combined to produce a 3-D display of the target," Curtiss said.

SOFTWARE POWERS

PSIM and mapping software are coming into the spotlight with more offerings from established leaders and startups, especially for critical sites operating with multiple security systems. "The ability to integrate the many disparate security devices and locations within an organization into a common operating platform that enables efficient assessment and response from a command and control center as well as field personnel is highly desirable," Curtiss said. For entry-level security management, alarm integration modules enable fast deployment interfaces to other security subsystems, using dry contacts for handshaking, Dewar said.

To facilitate integration between PIDS sensors and a security management system (SMS), it requires several things from the PIDS vendor. "First, a well thought-out software architecture — one that provides sensor management tools that can be used at the same time the PIDS software is exchanging information with the SMS, and one that allows the SMS to do a query for the current status of all sensors," Dewar said. "By having this capability, after a power-up or restart, the SMS can quickly be synchronized to the state of the perimeter system. Second, a comprehensive SDK is required that clearly documents the protocol by which alarm and status information is exchanged and that provides a high-fidelity simulator so all sensor events can be simulated in software to test the eventual integration."

The addition of video surveillance and VCA maximizes the effectiveness of a perimeter or intrusion detection system, which can both be managed through central management software. Video verification is carried out by PIR that triggers a camera and sends snapshots or a compressed video clip via the control panel to the monitoring station or directly to the end user for verification of the alarm, Joosens explained. "Both wired video verification systems as well as wireless video verifications systems exist, but as the distribution of the images is handled by the control panel, the systems are typically proprietary to the control panel manufacturer and interoperable with other intrusion systems. There are major differences in the various systems on the market in terms of the type of image sent, the image quality and the transmission time."

"Video verification and analytics is a necessary combination that end users need to implement if they can. Let the PIDS detect the intruder and let the video provide the video surveillance to determine the appropriate response," Smith said.

Video surveillance solutions that interrogate and verify potential threats enhance the effectiveness and efficiency of perimeter security systems, Ionson said. "They enable timely and measured responses while dramatically reducing costly false alarms. Using 360-degree imaging, with its total situational awareness, to trigger a colocated PTZ camera to quickly zoom in on a suspicious event increases both the speed and accuracy of threat verification."

"Video verification and analytics are a highly-recommended combination that can be used alongside perimeter security and intrusion detection."

WHAT'S NEXT?

Choosing the right perimeter security and intrusion detection products depends on the site that they are supposed to protect. There is no one solution for all perimeter security applications and each application should be approached with this knowledge, Dewar said. "While specific challenges from site to site still exist, the introduction of standards across the board has led to significant advancements in the reliability of physical intrusion systems," Makosinski said.

When considering critical infrastructure, the requirements for intrusion detection are moving toward higher security, meaning better capture performance, better signal analysis and better communication solutions, with multiple paths and better integration into other subsystems, said Dennis Petricoin, VP of Product Management for Intrusion Detection, Bosch Security Systems. "We continue to see integration and flexibility as a key part of the industry's future."

Selecting suitable products that satisfy end user requirements is only part of the equation. The second part of this feature explores key considerations system integrators should pay attention to during and after installing a perimeter and intrusion detection system. a&s