

Perimeter security ... expanded dramatically in recent years

Joe Citizen, if asked to describe the concept of perimeter security, would probably sketch a verbal picture of a fence or wall erected to keep people from gaining illegal access to a facility. For high risk environments such as maximum security prisons, he'd most likely add a second layer of walling or fencing, probably electrified.

He'd be right in that perimeter security essentially encompasses the first layer of a security system, very often in the form of a physical barrier.

However, the field of perimeter security has expanded dramatically in recent years, to the point where it now comprises elements such as fibre optics, buried detection systems, microwave barriers, infrared beams and fence-mounted microphonic cable systems, most of which would mean little to the average South African who just wants to live and work in safety.

Always a challenge to secure high risk sites such as prisons and national key points, these must surely pale by comparison with the challenge of securing South Africa's 5 000km of land borders, which Nhlanhla Ngidi, the Scorpions' head of crime analysis, describes as "porous".

Speaking at a conference on border control in Africa in June this year, Mr Ngidi said organised crime, already "pervasive", was likely to increase in South Africa as the 2010 Soccer World Cup approached.

Noting how vulnerable South Africa was already as a result of it having 72 official ports of entry, he said its porous problem was being exacerbated by numerous unofficial entry points and under-resourced policing capabilities. He warned further that terrorist groups were reportedly preparing for the event, hence the critical need for a comprehensive border security strategy.

Security Focus spoke to some experts about how they would go about securing South Africa's perimeters if it was up to them, and what the trends are in terms of more regular applications.

SECURING SOUTH AFRICA'S PERIMETERS Nemtek specialises in domestic, industrial and overseas prisons installations. Securing South Africa's borders would be the most extreme of cases, says Nemtek's technical director Sean Hurly, who believes the solution would lie in a combination of technologies. These would include physical barriers, electric fencing, video and buried detection cables. "The effectiveness of such a system would depend on system integration/networking, limited distances per



Ingrid Olivier
Special correspondent

zone, and operator response," he explains. "Distances per zone would have to be limited to be meaningful, and all systems would have to be networked into a system using appropriate protocols that could be policed within a certain time frame. Assuming one zone per kilometre, the system would comprise about 2 500 two-zone energizers and 79 Linux-based Sage controllers, each with 32 energizers attached to them. The Sage platforms support most TCP/IP protocols, so the system could be monitored and controlled by any number of remote locations.

"This, in my opinion, would be the technically correct solution. Practically speaking, however, one would have to find ways around challenges such as the requirement for rapid human response after an incident, and the additional costs of bandwidth via satellite and power reticulation."

Brendon Cowley is the sales director of C3 Shared Services which specialises in the design and implementation of high-end perimeter security solutions and military grade intrusion detection systems. It is also the only distributor in sub-Saharan Africa for iomage intelligent video appliances and Opgal thermal cameras.

In a country wracked by crime, he says perimeter security has to be the first line of defence for any property. As far as he's

concerned, the ultimate perimeter solution, whether for the country's borders, or homes and businesses, is a combination of intelligent video analytics and thermal cameras.

"This will give you a number of benefits: extremely low false alarm rate; a 99 per cent probability of detection even in no light conditions and last, but not least, it is easy to install and maintain with iomage intelligent video analytics, which are DSP-based, fully-embedded stand-alone units."

Using today's technology, and with a bottomless pit of finances, South Africa's borders could be made vastly more secure, believes Brian Gibbens, owner of Gem International, which specialises in gate and palisade manufacture and electric fence installations.

Although he feels that most criminal activity in the country comes from within, he nevertheless sees enormous room for improving the security of South Africa's borders. The logical physical element of any system separating two countries from one another would have to be electric fencing, in his opinion. "It would require more than one fence in order to effectively counter vandalism. Power sources to feed the set-up would have to be extremely elaborate, as would monitoring, which would also have to be sectionalised into manageable sections."

He continues: "Most electronic devices are pretty basic in that the end result is the closing or opening of a relay or solid state contact to drive a device which can be utilised for whatever purpose required."

Project co-ordinator of Botech, Frank Grobler, is another advocate of combination systems to secure South Africa's perimeter. "An underground optic fibre pressure sensor system coupled to a long-range CCTV system with cameras at key locations would be ideal," he suggests. "The optic fibre pressure sensors would be linked to guardhouses stationed at nodes along the borders. In the event of unauthorised entry into the border terrain, alarms would be triggered at the guard houses. We're looking at an essentially detection-based system since deploying physical guards would be more effective in terms of neutralising intruders."

"No matter what security system is in place, it can be breached by the persistent, the determined and the desperate," says Perimeter Security managing director Mike Rumble. "Noisy alarms and electric fencing are just not enough to stop people or save lives. In the event of a breach of any security measures that may be in place, or of a threat coming too close for comfort, the ability to receive effective warnings (intelligence) in time is essential. Forewarned is forearmed, and when intruders don't know that you know they are there, you automatically have the upper-hand," is his contention.

That's why he's so keen on wireless, battery-operated, easy to set up and operate technology such as the RoboGuard system, utilised as an early warning alert system in a host of different environments from households, farms, plots, golf courses, residential estates and business parks to industrial estates, and, potentially South Africa's perimeter.

"Fences, trenches and even land mines won't stop the most desperate people: high-voltage fencing is impractical, while large and difficult terrain is very challenging to monitor effectively and full-time," he says.

"Fortunately people (including criminals), tend to be predictable. There are obvious entry points, paths and weak spots in areas that must be passed through to get to their goal and specific high-risk areas that need to be monitored.

"RoboGuards can be set up to cover an entire perimeter area over large distances and will send a signal to a handheld wireless receiver which will activate a warning signal, a siren, lights or send an SMS. It can also be wired into an existing alarm system as an extra zone. In the event of a breach, appropriate action can be taken, and taken in time. The intruders will probably never figure out how they were detected."

With regard to beefing up South Africa's perimeter, Mr Rumble suggests placing RoboGuards strategically around and along known and identified weak points. "SMS signals could then be sent to a control centre that would be able to send in appropriate forces based on area-specific intelligence and respond to specific incidents rather than have costly and inefficient patrols or other measures. RoboGuards would work when other perimeter security measures such as fences are breached."

LAND, AIR AND SEA BORDERS

"The ultimate solution with regard to monitoring South Africa's extensive borders and providing quick and effective intelligence on crime in general, would be unmanned air vehicles (UAVs or Flying Robots)," suggests Mr Rumble.

"UAVs are available right now, and can be launched within minutes by a single person from vehicles, or even by hand. They are small, super-efficient and near-silent; they fly intelligently in all situations and conditions, provide extensive detailed and accurate real-time information; can get to, find and track perpetrators even if they are moving at high speed for prolonged periods of time and they can land themselves."

He continues: "UAVs would be able to pick up on any suspicious movement any time, night or day, and cover huge areas very effectively and efficiently. Information is the foundation of crime prevention and response to security breaches. Perpetrators would never know how they had been caught and it should stay that way: the operation should be completely secret and as if the arrests were pure chance."

ANY OTHER DEMANDING SITE

Just as one would secure the country's borders using a combination of technology, so one would apply the same solution to other, demanding sites, say the specialists.

"The greater the mix, the greater the effectiveness of the overall system," is Mr Hurly's stance. "What is often neglected is the response of system operators in the event of alarms. Some software integration companies have addressed this issue by recording or detailing operator response to an event, which results in a very professional solution."

What has evolved, particularly overseas, is the integration of any number of systems such as CCTV (closed circuit television), access control, perimeter fencing and fire, into a single system, he says. This ensures the accountability of all equipment suppliers, as well as the operator. He's also seeing a very strong trend towards using embedded Linux as an operating system, owing to its unparalleled stability in networked applications.

VARIOUS TECHNOLOGIES

In the end there are various technologies available for perimeter security, each with its own set of pros and cons, says Mr Hurly.

ELECTRIC FENCING

"The main advantage of electric fencing is that next to a detection system, it is a strong deterrent," he says. "It is also the only one of the applications that will actually stop someone or slow down the attack. If an electric fence is properly installed and kept clean of vegetation, it offers a low level of unwanted alarms. It is also very cost-effective. On the down side, though, it cannot cope with vegetation and is also relative easy to tamper with, which means the level of security offered is lower than other techniques."

FENCE MOUNTED PROTECTION

On fence-mounted protection, Mr Hurly says this can be achieved with microphonic cabling, vibration sensors, taught wires, fibre optic cables, torsion/tilt measuring systems, or leaky coax systems which measure the disturbance in an electro-magnetic field when someone is near the fence.

"Fence-mounted protection was notorious for creating unwanted alarms in the past," he points out, though he adds that the problem has all but been resolved with the use of the newer, vibration-based systems. "I would go so far as to say that the better fence-mounted protection systems provide a higher level of security than the average electric fence today. The newer systems have little problem with vegetation or wind load and are able to detect a whole variety of attacks, including climbing with or without the use of a ladder, cutting, ramming and grinding.

"One disadvantage is that the system is not able to see the difference between children playing and accidentally hitting the fence and an intruder really climbing the fence. Another limitation is that the detection is limited to the fence itself, so there is no protection against bridging or tunnelling."

UNDERGROUND DETECTION

When it comes to sophistication, Mr Hurly has no hesitation in recommending underground or buried detection. "This forms an invisible line in the terrain that will be able to detect an intruder crossing," he explains. "Various technologies are employed in this solution, ranging from vibration/seismic sensors to leaky coax and even fibre optics. Buried systems offer complete protection against bridging (as long as an intruder doesn't know where the system is positioned) and tunnelling. Another advantage is that it is aesthetically pleasing – when it is installed, it doesn't create the feeling of living in a fortress, or jail. Ironically, this can be a disadvantage as well since some form of fence or boundary would need to deter would-be intruders and slow down attempts to break in."

ACTIVE AND PASSIVE SYSTEMS

A proponent of passive, as well as active infrared systems, Mr Hurly is nevertheless aware of the shortcomings of the technology. "In short, the main disadvantage of passive IR is that it is very prone to false alarms. With active IR, the chances of false alarms are a lot less but it offers only limited protection against break-ins since it can be fairly easily bypassed by creeping under or over the beams. A solution to this is radar, which can basically be divided into two systems, namely TX/RX units, which are similar to active infrared, and transducers that work on the Doppler Effect."

SECURITY FOCUS

INTELLIGENT VIDEO

Moving on to video content analysis (VCA), he says it is vastly different from the video motion systems of the past. "VCA analyses camera images and looks for signs of intruders. It can skeletonise a moving object and measure its shape, size, speed and direction, as well as trigger an alarm based on this information. There are systems in place that will even automatically detect if a person drops a bag and walks away, or if someone is walking in the opposite direction to the rest of the crowd."

Video motion systems, on the other hand, only detect pixel changes and then alarm correspondingly, he notes.

"It's no longer enough to rely on electric fencing, CCTV cameras or patrols, says Mr Cowley, who promotes the use of intelligent video. "It watches over areas that are too dangerous for security guards to patrol; it enables you to monitor extensive areas and detect not just short range movements such as would be picked up by an infrared motion detector, but true behaviour scenarios. It's also able to differentiate between people and small animals, shadows and other objects which drastically reduces the number of false alarms – in most cases by 99 per cent."

Further, he points out that security guards' inability to be everywhere at once means that breaches or damage are often only discovered after the cause and when the criminals have already fled. "With automatic intelligent video monitoring, security officers are tipped off rather than having to discover events for themselves during scheduled patrols," he says. "Thanks to intelligent video and its ability to automatically detect intruders, security guards only need to view and respond to actual alarm events rather than watch hours of motionless video. Studies have shown that after 22 minutes, control room operators miss 95 per cent of scene activity. This technology, combined with the use of thermal cameras, means the perimeter is equally secure day and night."

ROBOGUARD

"For flexibility and ease of set-up," Mr Rumble says, "the RoboGuard system has proven successful in a range of applications. Essentially the system comprises any number of wireless, battery-operated RoboGuards that can be programmed into multiple hand-held wireless battery-operated receivers, able to receive and interpret early warning signals of breaches in a number of ways. They are stand-alone, easily mounted on walls, trees or poles, controlled from the receivers and require no attention at all."

Another advantage of this technology, he continues, is that it has remote activation devices to arm and disarm the system. "This means that when you arrive on site and disarm the system, it will tell you if there has been an activation via an audible sound or flashing light. You'll then know to check the area out before proceeding."

CASE HISTORY 1

Xanadu Eco-Park, a R2,1 billion residential development situated between Pretoria and Sandton in Gauteng, is one of C3 Shared Services' largest and most recent successes. Surrounded by indigenous bush and with an informal settlement on one side, its perimeter is approximately eight kilometres in length.

In all, the estate consists of 680 residential stands and sites for approximately 200 townhouses, 196 lifestyle village units for the over 50s, and assisted living units with frail care. Forty-five per cent of the land has been earmarked for use as an eco park, which will see the creation of additional lakes, islands and walkways in the future.

What was needed to ensure both residents' safety and the retention of the eco-friendly nature of the estate, was a system that would function equally well day and night, with no additional lighting required; a system that would alert control room operators to any breach of the perimeter and inform them of where the intrusion was located, explains Mr Cowley.

Prior to C3 Shared Services being called in, he says traditional methods of security such as electric fencing, CCD high speed dome cameras and solar power had been utilised – but with little success. "These methods proved inadequate as evidenced by the occasional breaches of the perimeter. Intruders also tampered with the electric fencing in their attempts to gain access to the estate. The high speed dome cameras were inoperable at night due to inadequate lighting, which meant that security personnel had to physically locate the cause of each and every alarm."

C3 Shared Services' answer was a combination of two military grade technologies: thermal imaging cameras (OPGAL) and intelligent video (ioimage). The perimeter security system can now detect intruders in pitch darkness at distances of up to 350 metres. This, in turn, enables control room operators to make correct and speedy decisions in terms of alerting designated armed response teams to areas where intrusions are detected.

CASE HISTORY 2

Botech's Frank Grobler spends his work days overseeing installations of electronic security, surveillance, perimeter security and alarm

systems. He and his team recently did an installation on warehousing premises in a rural area that were regularly subjected to break-ins and theft. Because of the location of the site, he says remote monitoring was a must, especially since it had no on-site guarding services at the time. "The solution we provided was an infrared beam network around the perimeter of the warehouse, integrated with the alarm system so that alerts could be sent to the owner via his cellphone in case of intrusion. This, coupled with remote log-in to the CCTV system inside the facility, helped eliminate false alarms and enabled the client to immediately contact the relevant security officers to investigate disturbances."

CASE HISTORY 3

Another of Mr Grobler's recent cases was a retail client whose preventative measures comprised electric fencing and razor-wire along with a 24-hour guarding service but no alarm system. "Crime in his area wasn't a big problem at that stage, but he believed that prevention was better than cure, hence his decision to upgrade his security," says Mr Grobler. Since the area requiring security was fairly large, it was decided to install a motion detection system on the fence and link it to an internal alarm system that could send alerts to the relevant security officials and the owner in the event of any threats.

INNOVATION

With regard to innovation in the field of perimeter security, Mr Grobler highlights microwave-based detection systems. These work on a volumetric movement detection pattern analysis to give the user an idea of the size of the intruding threat. They are most effective in open range areas such as borders and spaces between fencing and the buildings on the site, he says.

He's also a fan of PIR (passive infra red) or laser-based systems, which are used for short-to medium-range detection. Although he says they are not as effective as the microwave-based systems, they do offer a more cost-effective solution for the detection of intruders.

As far as physical security is concerned, he favours recent technologies such as Starwall™ (a South African manufactured product) which is being implemented both locally and overseas. "When implemented in a layered security solution, this type of innovation can greatly increase the general security level of a site," Mr Grobler says. "And let's not forget the good old electric fence, which is still effective as a deterrent to would-be intruders."

MAJOR CHALLENGES

As with all sectors in the electronic industry, there are regulations set out by authorities such

as PSIRA (Private Security Industry Regulating Authority) pertaining to installations and equipment. Yet, quality and the enforcement of standards are ongoing bugbears for its role players.

Sean Hurly says there is a lack of enforcement with regard to both the suitability of the equipment and its correct installation. "The maintenance of installed systems also leaves much to be desired," he adds.

He's therefore impatiently awaiting the finalisation of a standard for the installation of electric fencing equipment in South Africa. It's a long-awaited, joint effort by the electric fencing industry and the SABS (South African Bureau of Standards) technical committee, which will on implementation, govern physical installations and equipment quality.

"Unfortunately, the current lack of enforceable standards has resulted in many problems," Mr Hurly says. "The SABS no longer has the facilities to do compliance testing on electric fencing products. Some of the local test facilities test part of the compliance but not all, and often make mistakes due to the esoteric nature of the equipment. Claims are made by

manufacturers that cannot be substantiated and the findings of some local tests have been found to be incorrect."

Brian Gibbens voices his concerns, too. "There is little, if any control, in the market place right now when it comes to who installs electric fencing. It seems to be a free-for-all business." The need to differentiate his company from the "boot slammers" (as fly-by-nights are referred to in KwaZulu-Natal) has motivated him to issue letters of compliance to customers, although he points out that there are no hard and fast rules from SABS, only guide lines at this point.

"I have watched this industry grow in leaps and bounds over the last 25 years," he says. "Now more than ever it needs to be controlled, not by greedy business people but by professional, technical people who understand the importance of correct installation."

Another pressing challenge, according to Mr Grobler, is to find people with appropriate skills. Although there are a number of certifications available, he says it's not easy to find employees with hands-on experience in installations and a variety of security systems.

Then there's the challenge of convincing people that the technology will provide the requisite solutions, ventures Mr Cowley. "They are usually sceptical about the performance of the technology although once it's proved itself on site, they buy into it."

Lastly, cost is a problem. "Anything security-related is viewed as a grudge purchase," Mr Cowley says, adding that people would rather go for the cheaper security solutions.

IN SHORT ...

Any well-rounded security system needs to include perimeter security, says Mr Grobler. "Just having an alarm system or just having physical preventative measures does not guarantee the safety of your premises. Using the layered security approach means that you cover all your bases in terms of safeguarding your property. The first of these bases is perimeter security and if the appropriate combination of systems and measures is installed and implemented, you will get the peace of mind that comes from knowing that your human and material assets are protected by a well-rounded security system." ■

SA'S LARGEST DISTRIBUTOR OF QUALITY CCTV & ACCESS CONTROL EQUIPMENT



- Cameras
- IP Solutions
- Video Transmission
- Dome Systems
- Hardware
- Digital Recording
- Access Control

NORBAIN - The pick of the bunch

(Jhb) 011 887 1546 (Dbn) 031 569 1200
(CT) 021 551 5841 (PE) 041 373 0395

Circle 9 on reader enquiry coupon.

NORBAIN

www.norbain.co.za