THROWING THE NET WIDER TO PROTECT THE CORE

Steve Bailes *reveals that while the ability to construct more and more impregnable physical fence lines is important, comprehensive security is best achieved by the clever integration of all technologies*

The day after the recent Intersec show closed, samples of our fencing systems were 'attacked' in the presence of potential clients and accreditors in the region where there is a stated requirement for fencing to meet the highest of security standards.

The current highest standard in fencing is Security Rating 5 (SR5) as tested by the Buildings Research Establishment (BRE). LPS 1175 certification was introduced by the Loss Prevention Certification Board (LPCB) at the BRE in the mid-nineties.

The LPCB works closely with UK Government security agencies, police services, risk consultants and architects to determine the standards for fire and security products and services and independently tests and certifies fencing systems to LPS 1175 SRs.

An SR5 fence must resist a serious attempt at forced entry with top-end battery power cutting tools used by fire and rescue teams including a 750W reciprocating saw with specialist blades and 18V circular saws, jigsaws and disc grinders, axes, a hooligan bar, 1.5kg lump hammer and 500mm long bolt cutters.

TECHNOLOGY IN ACCESS CONTROL IS ADVANCING AT A STAGGERING PACE

To be certified to SR5, the system must resist breach for more than 10 minutes by testers from BRE mounting a sustained attack armed with this astonishing arsenal. But perhaps there is a better way of securing the most critical and sensitive assets than going on adding more and more layers of steel mesh to perimeter fences to gain higher and higher SRs.

It feels to me like a case of 'throwing the kitchen sink' at security. I argued this more considered approach at a short talk at the UK Security Expo (UKSec) late last year as a part of the building and facilities management conference there. My basic premise was that site operators need to weigh many factors in order to determine the appropriate and proportionate physical, electronic and human security measures to put in place.

First are the threats posed to their building or facility; second, the chances of those being realised; third, if they are, the costs to the organisation or enterprise – both monetary and potential downtime – diversion of focus and reputational damage. And, of course, what investment they are prepared to make in mitigating against those threats and risks.

I still believe the old 'onion skin' principle to security can't be beaten – with successive layers of deterrent and defence for an intruder to overcome at a deeper and more robust level the nearer they get to the most critical and sensitive assets.

JEWEL IN THE CROWN

The crown jewels are a perfect example of this. They are displayed behind bombproof glass under the watchful eye of armed guards and more than 100 hidden CCTV cameras. The Jewel House itself is a vault within barracks at the Tower of London, protected by the 22-strong Tower Guard, on detachment from the British Army, and the 38 resident Yeomen Warders, who are ex-military too. And heaven only knows how many fences, gates, barriers, blockers, cameras and other high-tech wizardry are employed around the perimeter of The Tower.

But few secure sites have the equivalent of the Crown Jewels to protect – or the budgets that such security costs! Nor is it necessary. I believe there is a better way of securing the most critical and sensitive assets than going on adding more and more layers of steel mesh to perimeter fences to gain higher and higher SRs. And another conversation at UKSec pointed the way to this potentially more appropriate and proportionate approach – adding PIDs to a simpler perimeter security fence.

This is consistent with the onion skin principle and acknowledges that most security managers will muster a human response to any genuine threat rather than leave people acting suspiciously at or outside the perimeter for 10 minutes trying to break in. So, doubling up electronic PIDs on a physical barrier that both deters and defends seems a better use of resources. This, I believe, is where specifiers must go in the future. Buying time against the threats is the key goal.

Successive onion skin 'rings' of protection – integrating physical, electronic and human security measures – is the way to protect our sites of critical national infrastructure. And we need to think outside the box, literally. With radar detecting threats up to hundreds of metres away, this now enables us to look beyond the perimeter, at the perimeter and within the perimeter.

Within the perimeter, technology in access control is advancing at a staggering pace. A few years ago, it was felt sufficient to block unwanted access with old-school metal keys or basic swipe cards. Now, IP-based security systems can monitor and record in HD signals, warnings and alerts from a multiplicity of sensors and systems anywhere on site and send responses back in real time.

This is what is driving the rapid adoption of biometric systems linked to access control, a trend that prompted the Centre for Protection of National Infrastructure in the UK to issue a guidance document more than three years ago.

Day by day, all of us – whether employees, construction workers, tourists or shoppers – face an increasing array of 'bodily measurements' to uniquely identify us, from fingerprints or palm scanning to retinal scans and voice pattern and face recognition. Whether it's trying to access your bank account or mobile phone, start the engine on your vehicle or gain entry to secure assets, both physical and electronic, at work – it's likely you will be biometrically checked in the next 24 hours. So, it is in the seamless integration of physical, electronic and human systems – and the ability to cross-check and challenge in real time – that we are creating the most protective multi-layered cordons around the most secure of sites.

In this environment, every event is recorded and analysed, both in real time and for training, learning and prosecution purposes after the event.

One of the most significant events is entry through building access points. The swipe of a card, the print of a thumb or even the scan of a retina can trigger a cascade of recording and monitoring systems, allowing security operatives to track personnel while on site.

We are even now seeing a growth in the use of trusted identities with smart cards, mobile devices, wearables, embedded chips and other smart devices, especially in industries with a focus on regulatory compliance, such as government, finance and healthcare.

This cash handling centre adopts a number of methods of securing its perimeter

Picture credit: Zaun Group

This will accelerate the move from legacy systems to NFC, Bluetooth Low Energy and advanced smart card technology.

The clever combination of physical and high-tech electronic measures is the key. Our installations have typically involved a Critical National Infrastructure ArmaWeave Plus fencing system on the outer perimeter. We have also employed hostile vehicle mitigation measures to avert against vehicle-borne attacks.

The way we now use CCTV cameras again demonstrates technological progress. Originally it was largely employed as a deterrent on the premise that 'Big Brother' watching was historically sufficient to discourage people from misbehaving.

SUCCESSIVE RINGS OF PROTECTION IS THE BEST WAY TO PROTECT CRITICAL INFRASTRUCTURE

It evolved into a forensic tool, collecting evidence after a crime had occurred to identify what had gone on and potentially catch and prosecute the perpetrator.

But as CCTV has become more easily integrated with monitoring devices, alarm systems and access control devices, it is gaining momentum as an interdictive security measure: helping security personnel to identify and interrupt security breaches as they're occurring, or even before they take place. I can see the ongoing prevalence of drone technology being used in the future as well as fixed cameras.

Already, intelligent video algorithms, such as sophisticated motion detection, can identify unusual walking patterns and alert a security guard to watch a screen to which the video is fed. Object-recognition algorithms can identify someone that is loitering suspiciously in a vulnerable area, or even a bag or other suspicious object that is left somewhere it shouldn't be. Again, the system can alert a monitoring guard so that appropriate action can be taken. CCTV bridged to intrusion alarms, physical security patrols and access control systems complete the total integrated security package. And in the most advanced cases, access control systems, or 'credentials technologies', are employing biometrics to restrict access both to physical areas and to intellectual property.

FLEXIBLE FRIENDS

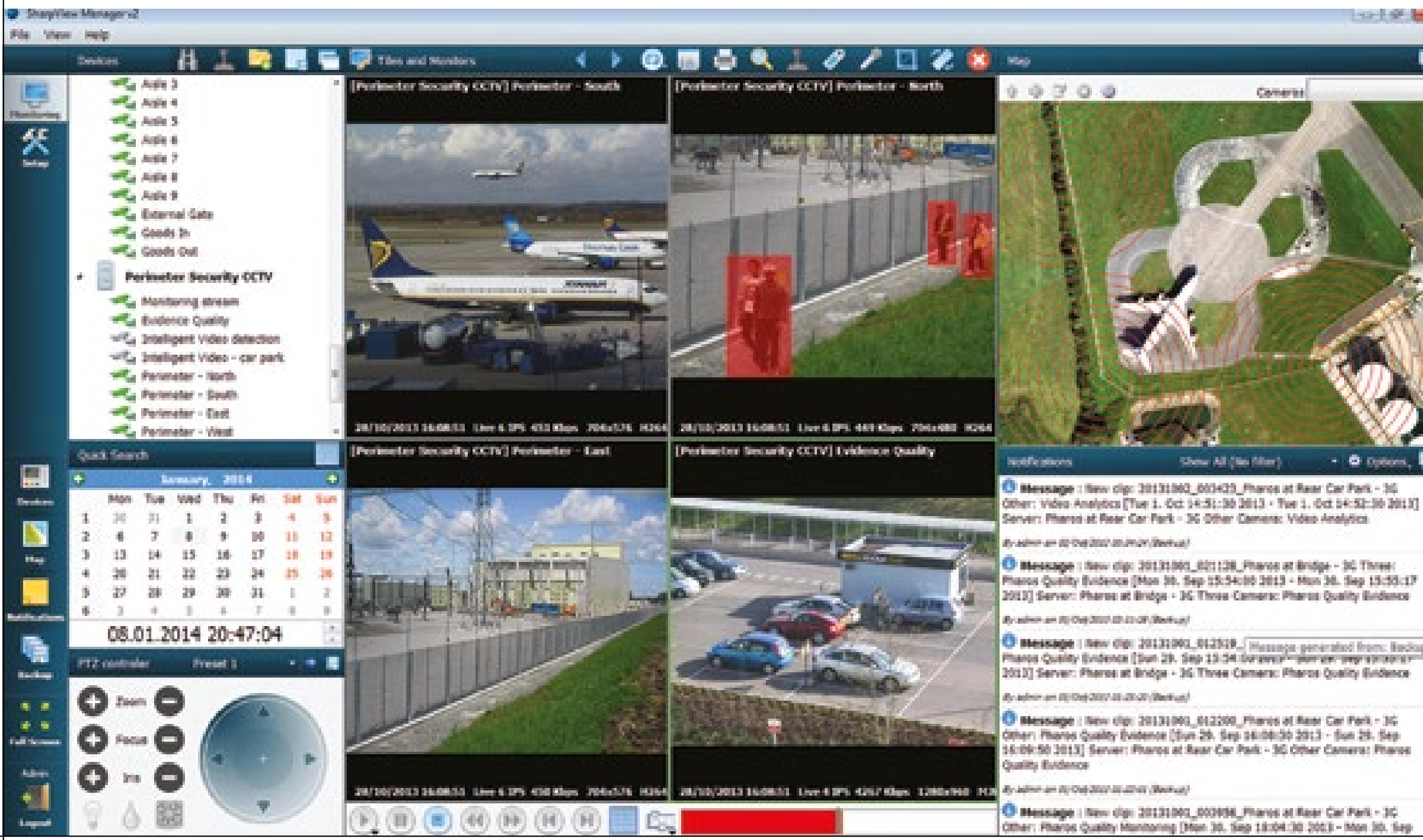
These systems use fingerprint, facial, voice or iris recognition to authorise a user, sometimes combined with another form of identification such as a proximity card or PIN, to make the system more flexible.

Limit the number of entrances and exits to a site through the perimeter and secure them more effectively with speed gates, ANPR and appropriate turnstiles to allow the effective flow of authorised personnel onto site.

The balance between maintaining this flow and locking out unauthorised people is a tricky one to strike, as would-be intruders have become increasingly adept at 'tailgating' to get through security barriers and doorways. In this instance, it may be necessary to introduce airlock-type control 'sterile zones' to lock down high-security areas more securely.

This is where biometrics may come into their own, offering the ability to identify personnel uniquely, with an 'unlock code' that only that individual inherently possesses. Biometrics are even being incorporated into advanced CCTV-based face-tracking systems to identify unique facial traits. But just make sure that you don't get wowed by the sci-fi and forget the basic know-how of time-honoured security principles ●

Steve Bailes is business development manager at the Zaun Group, the integrated perimeter protection and event overlay systems provider, securing prisons, water, gas, oil, electricity and nuclear sites and temporary events in the UK, mainland Europe and the Middle East



Message : New clip: 20131001_003423_Pharos at Rear Car Park - 3G Other: Video Analytics [Tue 1. Oct 14:51:30 2013 - Tue 1. Oct 14:52:30 2013] Server: Pharos at Rear Car Park - 3G Other Camera: Video Analytics

By admin on 02/Oct/2013 [illegible] (Backup)

Message : New clip: 20131001_021128_Pharos at Bridge - 3G Three: Pharos Quality Evidence [Mon 30. Sep 15:54:00 2013 - Mon 30. Sep 15:55:17 2013] Server: Pharos at Bridge - 3G Three Camera: Pharos Quality Evidence

By admin on 01/Oct/2013 [illegible] (Backup)

Message : New clip: 20131001_012519_ Message generated from: Backu Pharos Quality Evidence [Sun 29. Sep 13:34 [illegible] 2013] Server: Pharos at Bridge - 3G Three Camera: Pharos Quality Evidence

By admin on 01/Oct/2013 [illegible] (Backup)

Message : New clip: 20131001_012200_Pharos at Rear Car Park - 3G Other: Pharos Quality Evidence [Sun 29. Sep 16:08:30 2013 - Sun 29. Sep 16:09:50 2013] Server: Pharos at Rear Car Park - 3G Other Camera: Pharos Quality Evidence

By admin on 01/Oct/2013 [illegible] (Backup)

Message : New clip: 20131001_003858_Pharos at Rear Car Park - 3G Other: Pharos Quality Monitoring [Mon 30. Sep 18:04:30 2013 - Mon 30. Sep

Systems like EyeLynx SharpView can be adopted to monitor perimeters

Picture credit: Zaun Group