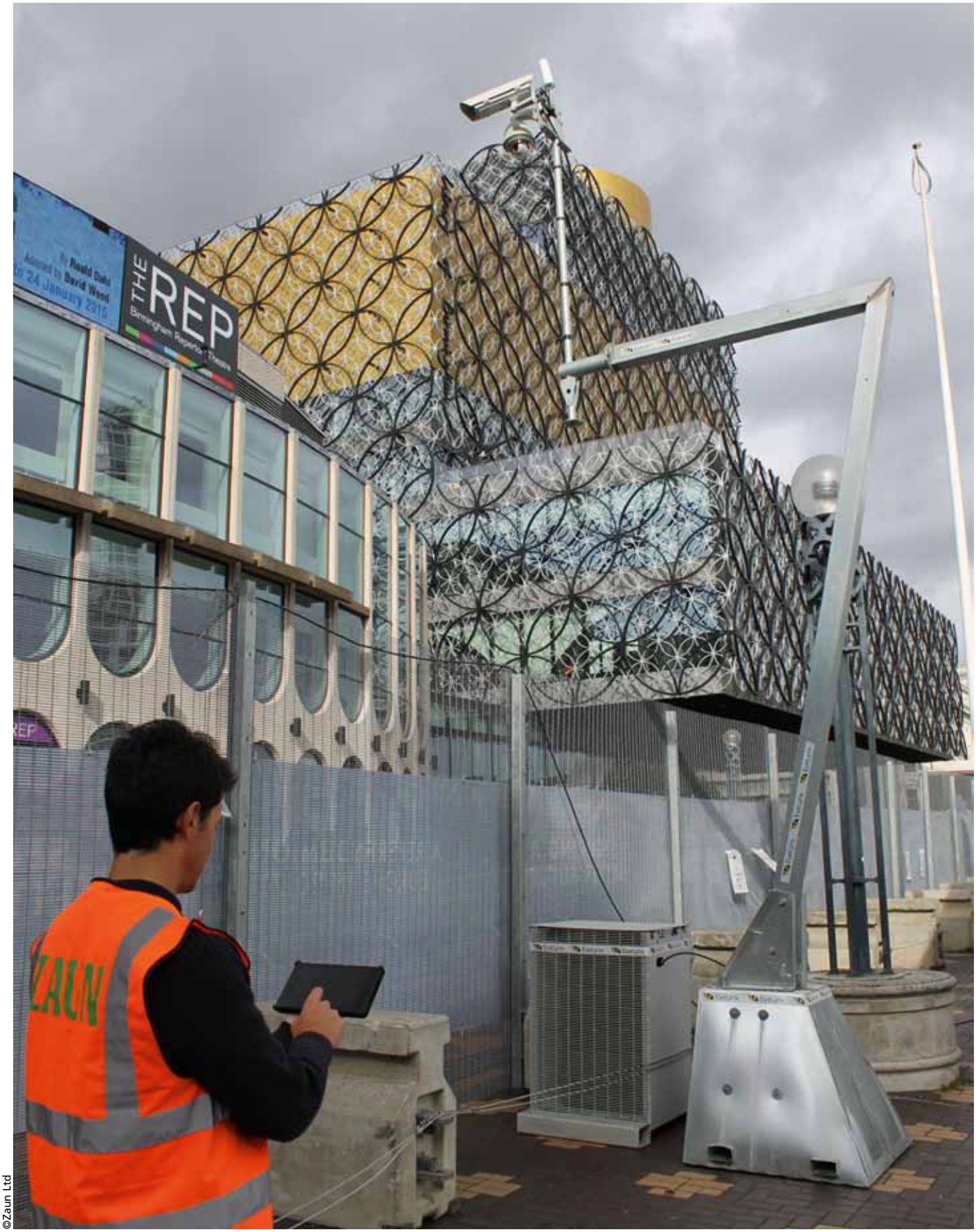
The integration of human, physical and electronic security measures across the CNI is gathering pace, argues **Chris Plimley**, driven by the rapid evolution of the terror threat, technology and user demands

INTEGRATING T



©Zaun Ltd

THE PERIMETER

I watched my wife doing our weekly food shop on her phone from the comfort of a coffee shop the other day and perversely thought how far security integration had come – and how far it may yet go in the next year or two. It's a moot point whether this has been driven by my wife's – and all consumers' – expectation that we should all be able to run our lives from a single personal electronic interface, or by the advancement of technology, or by the ever-evolving terrorist threat and government and legislators' expectations flowing from that.

Many advances in the areas of sensors, encryption and intelligent video tied to access control have certainly been made as a direct result of requirements published by the US Department of Homeland Security. Meanwhile, the UK's Centre for the Protection of National Infrastructure (CPNI) held its first manufacturers' training day a few months ago on a new Cyber Assurance of Physical Security Systems standard. CPNI's advice covers physical, personnel and cyber security and information assurance and how best to integrate these physical, human and electronic elements to maximum effect.

Rapid technological development and the increased adoption of internet-based services throughout business and society as a whole have also led to an increased expectation of, and capability for, unified systems. The security market therefore demands more joined-up physical security technology; as a result, the integration of security fencing and lighting, access control, PIDs and intruder alarms, CCTV and video analytics, as well as guard patrols and security control rooms, is now commonplace.

In the search for greater security control, enhanced employee safety and operational cost savings, some businesses have taken it further by integrating fire-fighting systems, building services controls such as lighting, air conditioning and lifts, and even business information systems and HR records. In such cases, the various facets work directly together to improve overall management of a facility and make it considerably simpler and more efficient. But this has been possible only through the development of systems and software that are capable of administering and simplifying the operator's task of running multiple functions from a single portal and with the advent of more standardised and open protocols and standards.

But, I'm running ahead of myself. And for all of the fantastic fancy stuff that is now possible, we need to get back to basics and do only what is necessary and cost-effective. This involves asking the time-honoured basic security questions: what asset base are we trying to protect – physical, human, intellectual and even reputational; what risks do or might they face, such as damage, theft or sabotage; and who or what might pose these risks and how might they carry out their threats? Only when we match the particular threat on the particular asset with the particular risk can we design the most effective mitigation solution – and then integrate pre-existing security measures with new ones to make it all work in tandem.

A good example of best practice is a UK electricity supplier that used its acquisition of two additional delivery licences as a catalyst for a fundamental review and improvement of its total security solution. Here, "integration" took place not just of different security elements and systems, but also of existing measures with new ones across more than 600 sites – all monitored, analysed and controlled remotely from one central Alarm Receiving Centre (ARC).

A central ARC is vital in the event of a security breach or emergency, as head office must be certain who is present and that only authorised personnel can gain access. Someone at HQ needs to know the moment the perimeter is threatened or compromised, even at the smallest substation, or if anyone is in a place they shouldn't be. If an alarm is triggered, video can automatically be sent to mobile phones, PDAs, laptops or other devices so that security can decide how best to respond. Integrated video and alarms systems can help immediately target security breaches so that any 24-hour onsite patrol can react quickly and prevent property loss, or worse. Access control systems can also be programmed to lock certain areas of the facility to confine any search for the perpetrator.

Knowledge of who is where is just as necessary from a safety point of view as a security one. If an accident occurs or there are fatalities, it is essential the company knows how many and who was on site through a "persons on board" report. This can be available automatically by taking the data from the access control system integrated into gates, barriers and turnstiles on the perimeter, providing a report for emergency services to tally against.

It is hardly a new technology, but often a fire alarm is the first system to activate. In a modern integrated system this can alert a control room and, if necessary, escalate the warning automatically to the emergency services, letting them know who is on site before they arrive and even any special medical needs. CCTV can also be used to see if people are trapped or areas are potentially dangerous before emergency services arrive and thus avoid putting their lives at risk.

In short, the greater the integration, the better able everyone is to build more effective security plans and architectures, respond more quickly and appropriately to security threats and breaches and ultimately protect people and property better than ever. The more technology advances, the more intelligent the systems per se become. Specifiers now just as often include high-tech perimeter intrusion detection (PID) systems in tenders as they do the classic low-tech solution of electric fencing. Gone are the days when PIDs were simply mounted on a fence. Now threats can be monitored, analysed and recorded in real time so that, for instance, the same person approaching the perimeter at three different points on three separate occasions can be identified, marked as a threat and

Integrating IP surveillance and intrusion detection systems into the perimeter allows them to be better used as interdictive security measures

potentially apprehended without ever even touching the fence line.

The manner in which CCTV cameras are now used also demonstrates that technological progress. Originally surveillance was largely employed as a deterrent on the premise that "Big Brother" watching was sufficient to discourage people from misbehaving. It has, however, evolved into a forensic tool, allowing security personnel to collect 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 particular screen to which the video is fed. Object-recognition algorithms can identify someone who 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. In the most advanced cases, access control systems, or "credentials technologies", are also employing biometrics to restrict access both to physical areas and to intellectual property. 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. The most exotic of these may still be a few years down the road; nevertheless, wholesale integration of such commercial security systems is all but inevitable.

Case Study

NBA integrated with electronics for Conservative Party conference, UK

The National Barrier Asset (NBA) was established in 2004 to give UK police forces the capability to deploy temporary security barriers to protect high profile locations or temporary events, such as political conferences, from vehicle-borne attacks. The size of the NBA was tripled in 2008 and expanded again four years later to meet growing demand.

The Home Office owns the NBA, while Sussex Police acts as the lead force for a framework agreement involving all police forces and all government departments, agencies and public bodies. It includes a stock of TATA Bi-Steel products and Zaun security fencing which has been deployed at the G8 Summit in Northern Ireland in 2012, the Nato Conference in South Wales in September 2014, and for the first time overseas at the Nuclear Security Summit in The Hague in March 2013. It is also rolled out each year for the UK's major party political conference season. In the autumn of 2014, Zaun used the Conservative Party conference as an opportunity to demonstrate the possibilities offered by integrating CCTV with the fencing.

Electronic security developer and manufacturer EyeLynx, which is now part of the Zaun group, used its SharpView solution and integrated i-LIDS-approved video analytics with Pharos Rapid Deployment CCTV on the fencing. They created a rapid deployment CCTV tower with embedded cabling and an integrated power cabinet in the post base to enable quick and easy on-site deployment without the need for heavy machinery. The whole setup was completely wire free, with no external connections required. With Harper Chalice PIDs now integrated too, Zaun has a total perimeter security solution specifically designed for temporary events.

The company deployed two such towers – each with a full HD1080p PTZ camera and adjoining wide-view slave cameras – throughout the four days of the Conservative Party conference at the ICC in Birmingham in September 2014, helping to demonstrate how to reduce further the number of officers needed to police events of this nature.

Only the master unit needs a SIM card, which provides remote connectivity over wireless 3G or 4G to beam video intelligence to a workstation or mobile device into which anyone authorised can dial to view live footage, or rewind and replay from any of the cameras. Pharos records HD1080p video 24/7, and whenever a PID is activated or a potential intruder approaches too close to the fence, the system sends a snapshot alert to the control centre for visual verification – or even to assigned personal mobile devices, such as the police chief or nearest constable to the breach.

West Midlands Police hailed the integration of the most advanced electronics and top-end CCTV as an add-on to the existing physical perimeter security provided by the NBA as a great success. They said not only did it enable them to reduce the number of police needed to secure the event, and therefore the cost, but also it helped better cover specific strategic positions on the perimeter.

©Zaun Ltd

Chris Plimley is sales manager for high security products at Zaun Limited, a British manufacturer of high security event overlay and perimeter protection systems with regional offices in France and Dubai.