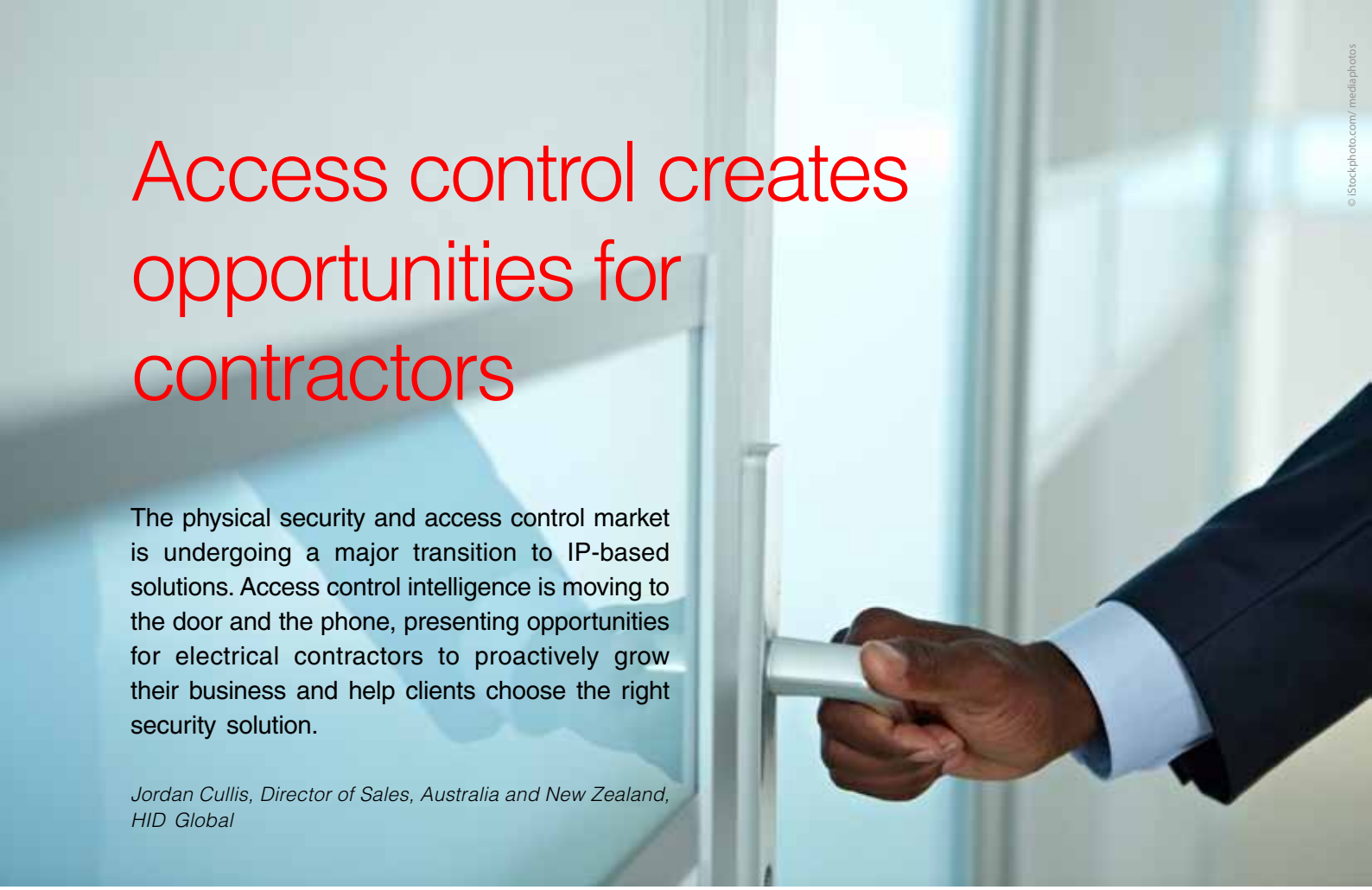
Security and automation

Contents

ebook ECD ELECTRICAL+COMMS+DATA SOLUTIONS
www.ECDsolutions.com.au

Access control creates opportunities for contractors



The physical security and access control market is undergoing a major transition to IP-based solutions. Access control intelligence is moving to the door and the phone, presenting opportunities for electrical contractors to proactively grow their business and help clients choose the right security solution.

Jordan Cullis, Director of Sales, Australia and New Zealand, HID Global

Emerging technologies will deliver ease of operation, simplified expansion and customisation, and the ability to integrate a physical access control system (PACS) with many other solutions sharing the same network. Modern, smart buildings clearly offer many benefits to facility managers, staff and to the enterprise itself, but there are plenty of considerations for people involved in the planning, engineering and physical wiring of the facility as well.

One of the most obvious benefits of IP-based access control is the ability to move intelligence to the door for streamlined system monitoring, management and reporting via standard web browsers. In such a system an individual door will have onboard ethernet connectivity, and a smart lock that can engage with smart cards, tags or NFC-enabled mobile phones. This will present a new opportunity for an electrical contractor, as every door in a security-controlled area of the facility will now require connection to a power source and be wired to the local area network (LAN).

Traditionally, up to sixteen wires are needed to connect a door to the physical access ecosystem. With an IP-enabled door, this can be reduced to one CAT 5/6 cable, so the facility will save overheads on wiring and, with a quicker install time, the contractor will be able to provide a more competitive quote.

IP-based solutions are also scalable and can quickly be expanded or adapted as the need demands. Adding switches can quickly multiply the number of end points in a system from ten up to thousands. Some solutions are power-over-ethernet (PoE), which can eliminate additional overheads for the facility involved. Since PoE is scalable as well, power consumption can be minimised and the facility can reduce its carbon footprint.

Unlike traditional systems, IP-based access control solutions can also conduct constant 'health checks', immediately notifying the user when a problem is identified. End users can maximise their investment by upgrading to the latest hardware technologies while using their existing IP infrastructure.

Intelligent wireless locksets are the first step to untethered connectivity in the networked access control environment, and these devices will become more prevalent as lower-cost, energy-efficient models are introduced to the market. Meanwhile, the use of NFC-enabled phone handsets is also on the rise for mobile access control, which will enable users to carry credentials on phones that fit into the existing network environment.

The most basic approach for mobile phone access is to replicate existing card-based access control principles: the phone communicates identity information to a reader, which passes it to the existing access control system. Based on a predefined set of access rights, the access control system makes the decision to unlock the door. This model provides a safer and more convenient way to provision, monitor and modify credential security parameters, temporarily issue credentials as needed and cancel credentials when they are lost or stolen.

As more and more organisations embrace the advantages of IP connectivity for access control, the concept will evolve further to wireless connections, including locksets as well as NFC-enabled handsets. As mentioned, these will initially emulate the ID cards

and tags that we all know and use today. Ultimately, NFC-enabled mobile solutions will leverage the phone's own network connection and the cloud to move access control intelligence and decision-making all the way to the palm of one's hand. Instead of carrying a card or tag, each user will be able to push an app on their enabled mobile phone to advise the facility that they are 'in the house'. The mobile device will then send a message via the network or even the private cloud to the locked door verifying the person's credentials, unlocking the door when access is granted. In essence, the mobile device will become the key, processor and rules engine for the physical access ecosystem.

Despite the benefits of IP-based access control, until recently security concerns have blunted its adoption. These concerns are rapidly waning as the industry realises that IP-based access control actually improves security. Integrating video surveillance with access control, for instance, offers a more comprehensive view. For example, as well as IP security cameras watching all critical areas of a facility, the central server will be able to record all access to the building by staff and visitors. When the security system enables all of the various subsystems - from video management and access control to video analytics, intrusion devices and all associated IP-based edge devices - situational awareness is significantly enhanced because all information can be immediately combined and correlated.

Furthermore, with an integrated security network, all levels of physical security and access can be managed through a single user interface, which significantly streamlines the task of securing a premise. This host system can be used to monitor a site remotely so, in effect, a new facility can be set up on the other side of the country, with the host site communicating with the new hardware over the WAN.

Parameters can be set for physical control, as well as activating alarms, sensors and security cameras within the same ecosystem. For example, if a cleaner needs to access certain parts of the facility - such as the lunch room, corridors and common areas - then those parameters can be set by the central security management servers. If an unauthorised person tries to access the boardroom or admin office, permission will be denied and security cameras alerted, sending a message straight to the controlling PC or even mobile phone of the security officer in charge.

Parameters can also be set to provide safety to staff - locking doors at certain times when potentially harmful activity is taking place in a manufacturing plant for example, or on a mine site to block access to areas where blasting is about to begin.

IP-based access control is here and growing in adoption. It delivers valuable benefits including simplifying operation, expansion and customisation, while enabling a PACS to be integrated with many other solutions on the same network. By moving intelligence to the door, it also streamlines system monitoring, management and reporting. Ultimately, the concept of networked access control will continue to extend with the ongoing adoption of NFC-enabled smartphones. Solutions for smartphones will in turn continue to develop, with enhanced access control intelligence and decision-making, which will enable the electronic security of far more doors than ever before.

another ebook from
www.ecdsolutions.com.au

published by
WESTWICK-FARROW MEDIA

Driving the Building Information Modelling revolution

Andrew Chew and Meredith Riley, Corrs Chambers Westgarth

A technological revolution is changing the way large projects are being built and managed in Asia, Europe and North America. Governments and private owners are turning to Building Information Modelling (BIM) to deliver projects at a lower cost as well as operate them more profitably. Australia has been slow to adopt BIM, but can we afford lagging behind yet another innovation frontier?

BIM has been identified by governments globally as a better way to construct and operate projects over their life cycle. BIM discards the old way of building design where upfront architectural work is often done with little input from other project participants such as engineers, contractors and facilities managers.

Instead, BIM brings together all parties and connects them into a virtual 'design' forum to review the simulated structure, share information and raise issues. All the design and construct elements (including electrical and mechanical services, data and other communication systems, civil infrastructure, structural and architectural elements) are integrated into the model along with spatial relationships, quantities surveys and operational elements.

The resulting model becomes a shared resource that supports decision-making through the entire building life cycle, including construction and facility operation. For professionals involved in a project, BIM enables a virtual information model to be handed from the design team (architects, surveyors, engineers, etc) to the main contractor and subcontractors and then on to the owner/operator. Each professional adds their own data to the single, shared model.

This improves coordination among the various stakeholders (whether they are designers, contractors, fabricators) and allows for scheduling or design clashes to be detected early. It also reduces information losses that can occur when a new team takes 'ownership' of the project, and means fewer costly misunderstandings between the design and the construction participants, and the facilities managers.

Where does Australia stand?

Australia is lagging behind other developed nations in adopting BIM. While Building Smart launched the Building Information Modelling Initiative last year, it is still trying to get off the ground in any meaningful way with federal government budget constraints a key inhibitor.

By comparison, the US government is already using BIM in its delivery of projects and intends to further expand the role

of BIM to support the asset management of the facilities with the overall purpose to leverage facility data through the facility life cycle. Similarly, it is now government policy in the UK, Singapore and South Korea to use BIM on government projects.

More collaborative contracting structures such as Integrated Project Delivery are emerging in the US whereas other governments are being more cautious and using BIM protocols.

Using BIM protocols does require care and consideration. BIM protocols can be considered a collateral contract and thus modify the legal regime as set out under the main contract. In addition, the parties' acts pursuant to the BIM protocol could give rise to various legal causes of actions such as estoppels, misrepresentation or misleading and deceptive conduct in the event of a dispute.

Regardless, both approaches are designed to encourage more collaborative working and more appropriate risk sharing under the contractual documentation required for the greater use of BIMs. It is the higher degree of risk sharing that encourages parties to work in a BIM environment. Australia's apathy toward BIM means our major projects are missing out on technological advances that other developed nations have already embraced. Is this something that Australia can afford?

BIM: present and future

BIM is evolving rapidly. The current practical use of BIM is to provide a 3D virtual walkthrough of a project as it is built. In the future, BIM will expand to include a fourth dimension (time - construction sequencing), and fifth (cost information) and sixth (facility management) dimensions.

Each additional dimension integrates more information about a project, giving insight into cost-saving opportunities and how the asset can be managed most efficiently. Ultimately, the BIM model will contain all the technical information relevant to the asset's operation, and building sensors will allow the model to evaluate energy efficiency, monitor a building's life cycle costs and optimise its cost efficiency.

Will the real leader please stand up?

So, who should be taking the lead on BIM in Australia? In other countries, governments have been driving the implementation of BIM in projects. However, in Australia, there appears to be a stalemate between principals and contractors.

Principals who see BIM as part of risk acceptance and allocation in the delivery of projects believe contractors should be responsible for investing in it. Other, more forward thinking owners are taking the lead on BIM use by having a different approach to project delivery risk allocation - one that fosters investing in technology and collaboration between assets owners, design consultants, contractors and facility management operators.

A detailed paper on the state of the use of BIMs and legal and commercial considerations has been published in the International Construction Law Review July 2013 edition.

Corrs Chambers Westgarth
www.corrs.com.au

another ebook from
www.ecdsolutions.com.au

published by
WESTWICK-FARROW MEDIA

A holistic approach to security

*Michael Brookes**

Security is at the forefront of many an executives' minds, and to compound the issues the industry is undergoing a transformation - or what the industry pundits term as convergence. This article discusses the challenges presented by the convergence of physical security and IT and the benefits of a holistic approach.

What is meant by convergence? A quick Google search will give you a plethora of explanations, one of which fits the security convergence topic quite well:

"A coming together from different directions, especially a uniting or merging of groups or tendencies that were originally opposed or very different."

There is now a need to think of security as an integral component of risk management, as a business imperative, not just a 'have to have', or a sunk cost. This means that business owners need to think laterally about the investment in security; how can the investment be leveraged in other areas such as employee benefits or occupational health and safety improvements. Businesses need to think about ownership and accountability - where before there were silos, now there needs to be a holistic approach.

Design of a security solution to address these issues requires a balancing act between safety and service, duty of care and regulatory compliance. No longer is security viewed as the sole responsibility of the security manager; it now warrants a more integrated approach incorporating more contemporary functions of planning, management and people-focused services. Security, along with safety and emergency management, should be a key consideration during the initial planning process to ensure that workflows are seamlessly integrated with technology to deliver the most cost-effective outcomes for the facility. It is important to work with organisations capable of delivering comprehensive and best-of-breed security solutions. This provides the benefits of accountability, risk mitigation and knowledge transfer not typically available from a multivendor approach.

From a technology perspective this has certain implications; where once it was common practice to purchase security systems based on their individual functionality - access control, CCTV, intrusion detection, perimeter detection, fire detection etc - without too much concern about their level of interoperability, there is now more of a need than ever to have these systems sharing data and integrating with the organisation's standard operating procedures. The widespread adoption of internet protocol (IP) is helping deliver these outcome-based security solutions, both from an implementation standpoint where there is more of a 'plug and play' environment that often utilises the corporate network and from a process standpoint where backup, restoration and data storage now falls in line with IT practices. This convergence with IT can also simplify the installation process by removing the need to put in place disparate systems that each require their own dedicated infrastructure, instead taking advantage of the enterprise network, consolidating hardware and utilising open systems protocols to provide interoperability between systems.

This move towards security convergence is delivering some real benefits such as improved operational efficiencies, better risk

management and reduced costs, and the investment is slowly becoming shared across the business as technologies such as number plate recognition and crowd monitoring are being used to enhance the customer experience.

- Centralised monitoring and control provides an enterprise view of the facility, simplifying incident management and reducing response times.
- Event-based automated workflows reduce the need for manual intervention, freeing up valuable resources.
- Early detection and notification of events enables the appropriate response to be taken in a time of crisis.
- Automated incident response enables fast restoration of normal business operations.
- Reduced capital costs are achieved through a converged ICT infrastructure resulting in lower hardware and cabling requirements.
- An open, futureproof system through the use of IP networking.
- Early identification of customers enables a personalised customer experience.

Prior to the onslaught of convergence, our technical experts also fell into their respective silos; network specialists, server specialists, application specialists, security installers, security guards, and the list goes on … Convergence means we need to revisit this traditional approach - we are now looking for technical experts with well-rounded experience that can demonstrate an appreciation of all aspects of security and how they impact the business. This requirement is recognised by our educational institutions with qualifications such as BSc Internetworking & Security Degree; Bachelor of Security Analysis being on offer. This, however, presents its own set of challenges.

Firstly, there is a time lag between school-leavers attending university and being employable. This means that we may need to upskill the workforce we currently have or look to engage specialist organisations capable of providing the broad range of skills required; many of the traditional physical security organisations have developed these skills as part of the rapid growth opportunities in their industry.

Then there is the remuneration debate. Again, our two ends of the security spectrum have historically had very disparate working conditions and pay structures. How does a company retain all the required skill sets and at the same time maintain equitable conditions for all involved. Creating a culture in which physical security and IT personnel work well together can be difficult; these staff often have different perspectives, priorities and reporting relationships. This factor alone suggests that a culture of corporate security management needs to be driven from the highest levels within the organisation, ideally with visibility and representation at board level.

For the individuals involved in, or looking to get involved in, the security industry, it is an exciting time. There are opportunities aplenty on the employment scene; there are new skills to learn and some large projects in the wind. The traditional physical security organisations have broadened their horizons and now look to include IT-skilled people when doing their recruitment; conversely, IT organisations are including what were traditionally physical security solutions such as IP CCTV in their portfolio.

All in all, there are clear benefits to be derived from an active, strategic approach to corporate security management and the implementation of a converged security infrastructure. Organisations can take a holistic view towards risk management and compliance while reaping the rewards of systems that have lower costs of administration and support. Those seeking to embark on such a strategy need to be clear on the outcomes expected and ensure that buy-in is gained at all levels; these strategies need to be closely aligned with business objectives and not be viewed as simply a security project. A phased approach should be taken and appropriate time allocated to the process. Key objectives should be set to measure the benefits of each stage as it is rolled out.

Security convergence is here, with all of its challenges and benefits as we have seen with other technologies like voice over IP (VoIP). How we reap the rewards both organisationally and individually is up to us.

Michael Brookes is the Regional Leader of Marketing and Strategic Development for Honeywell Building Solutions in Australia and New Zealand. In this role, Brookes spends time analysing customers' critical business requirements to ensure that Honeywell's products and services are aligned to customer needs. In his 10 years at Honeywell, Brookes has covered a broad range of industries such as healthcare, industrial plants, airports, correctional and government facilities, and stadiums, where he has seen the application of integrated security solutions deliver demonstrable results to business. He has written a number of published thought leadership articles on security and has presented at various trade shows and conferences.

another ebook from
www.ecdsolutions.com.au

published by
WESTWICK-FARROW MEDIA