



## **Meeting the Growing Demand for Integrated, Intelligent Security Systems**

*By: Jean-Marc Zola, Vice President of Fire and Security Strategy, TAC*

Helping the world's businesses keep their buildings, employees and customers safe and secure is a fast growing multibillion-dollar industry. Topping the list of building and property owners' security concerns are employee theft, property crime, information security and burglary.

To protect against these and other threats, and increase their business value at the same time, companies worldwide will spend \$73 billion on security in 2008, according to The Fredonia Group. And IMS Research predicts the security market will experience 55% growth during the next five years.

A whopping 40% of revenue currently earned in the security market comes from the sale of integrated security systems. Other big revenue makers are CCTV systems with 19% and access control systems with 14% of the revenue, according to Security Distribution and Marketing magazine. Integrated systems are earning the lion's share of the revenue because of how they help to reduce costs, simplify usage and greatly improve the overall security of businesses' and property owners' physical and logical assets.

In addition to these advantages, integrated, intelligent security systems enable businesses to broaden their security objectives and expand them to help meet their overall core business goals. Key to achieving these metrics are three important benefits of integration:

- A single user interface into all building systems
- The ability to manage all facilities and remote sites from a single computer or a variety of devices anytime, anywhere
- The ability to add intelligence to security systems and link them to business management systems to address P&L issues and more

### **Single Security Interface**

The "state-of-the-art" expression in security management is evolving quickly. Once seen as a set of separate processes, procedures and equipment aimed at guarding facilities or databases against unauthorized entry or use, security is now viewed as all encompassing and more software-centric than hardware-centric. For example, pin numbers and ID badges are being replaced by intelligent ID systems that use finger prints, hand prints, eye scans, facial recognition or radio frequency identification (RFID) technology to identify people and verify their level of access to facilities or information.

As they add intelligence to their security subsystems, forward-looking businesses are integrating those systems with their building management systems (BMS) and ultimately their IT and business management systems. Optimum integration enables companies to exploit that intelligence for security-related purposes and to add value to their businesses' bottom lines as the technology and familiarity with its capability matures.



Here in 2007, we are only at the very beginning of the security integration evolution. Today, most buildings contain a hodgepodge of proprietary security networks and 24x7 monitoring systems that help security officials and systems authorize or deny access to facilities or information. These buildings also contain networks and systems that control and maintain elevator banks, energy use, fire safety, HVAC and lighting. Often times these networks are overseen by multiple control environments.

Businesses interested in evolving all of these networks into an environment that offers both business value and security management without limits are installing new integrated security systems. Integrated management systems can be installed when constructing new buildings or as an overlay to existing proprietary networks. An ultimate goal is to link all of a building's systems and networks to a single Internet Protocol (IP)-based network.

IP enables all of the networks connected to the integrated security system to be networked together and controlled by a single control environment. An IP-based control environment provides security officials with additional flexibility, programmability and capability. They can access the system and manipulate it, and the networks connected to it, using a single computer, or from multiple IP-based devices or Web pages on- or off-site when such flexibility is desired.

A single security system control environment also reduces complexity, which in and of itself increases security overall. For example, the key security systems in use today are intrusion detection, access control and video surveillance. If each of these systems are purchased and administered separately, training and administration can be a burden to a company or building/property owner. This is because intrusion alarms occur on one system, access badges are administered in a stand-alone database and intelligent digital video technology runs on dedicated computer equipment. Each system requires its own oversight, service, maintenance, administration and training.

By integrating separate systems under a flexible BMS, building owners realize a lower upfront investment and in the process, gain a considerably more powerful security solution. Installation of new capabilities, and training to use those capabilities, occur on a single system. Training in this environment is much less challenging than trying to train security officers on each new system or upgrade that is added to the security mix. Security managers will feel less apprehension about adding new elements to that mix, because they will be integrated to the single security system interface and require less training and expense to be put into use as a result.

When it comes to actual use of these networks, security officials can enhance security by exploiting the ability of all of a building's networks to work together and share data and information. Sensing trouble of some sort, security officials, or systems themselves can trigger door locks, light up or darken an area, capture video, take control of cameras to



get a better view of what's taking place, increase video resolution or frame rates, halt elevators or enact other building controls to heighten security and gather more information for immediate and future use.

For example, many businesses are installing video analytics software, which examines a video camera's field of view for suspicious patterns of movement such as falling, fence climbing, lurking and trip-lines. It also helps security managers focus on trouble spots by configuring video equipment to alert security managers and only display video if a specific event or alarm occurs.

Staff can then control pan-tilt-zoom cameras or search for video clips stored on digital video recorders. When an alarm is triggered by the BMS, it can command the appropriate DVRs to switch from monitor mode to record mode and display video from a linked camera at the location, map the alarm location and send an e-mail to the administrator all at the same time.

Integration also enables different groups within a company to access and use the security system and its satellite networks for their own purposes. It is important to remember that while a single interface can provide several people with access to the system, the interface does not provide everyone with the same access or control of everything controlled by the system. In fact, facilities and information can be blocked or opened up to any given individual, or groups of individuals, at a moment's notice. Security is enhanced because all the actions of people using or administering the integrated security system are logged by the system's central database. It is much more difficult and resource intensive to keep track of, manage use of, and control access to, multiple proprietary systems.

Data and information sharing made possible by a single security interface enables security managers to change security modes or levels in an instant or step-up data collection activity by specific systems. This type of building intelligence truly builds business value within the organization. Information sharing also promotes occupant safety because it helps security managers more quickly and clearly identify problems and react to alarms. For example, muster reporting can be used to help security managers make faster decisions on whether or not to order an evacuation of a building. And improved cross-system communication enhances overall reporting and promotes a better understanding of overall facility, or multiple facility operations among security personnel and company employees.

### **Multi-facility Security Management**

The benefits that an integrated security system provides to a single building can also be migrated to multiple locations owned and operated by a business, regardless of the number of facilities or their geographical location. Once connected to the centralized site via an IP connection, each security system or network at branch office locations can be



controlled, monitored and managed by the same computer/interface used to control security at the main site.

In addition to reduced CapEx and OpEx, companies gain another important benefit from linking branch offices to the centralized integrated security system. Employees moving from one location to another are familiar with the security processes and procedures because they are the same at every site. For example, a person from the U.S. going to do business in an office that is overseas or across town, the state or the country will not have to take time to learn the security procedures or be issued a new badge or pin number at the foreign office.

Also, because all facilities are connected to a centralized control center, security changes made in one office can be made to all of a company's offices in an instant. Businesses can implement heightened security measures rapidly in areas where there is a threat, be it local, regional or all around the world at any time of day or night. For example, if a security officer in London perceives a threat to company offices in an area of the world where offices are closed for the evening, he or she can make the adjustment to those facilities from London.

In addition to managing multiple locations via a single computer, security managers can manage their integrated security systems from a variety of devices, anytime, anywhere. Web pages, PDAs, cell phones or pagers can each be enabled to give a security manager access to the system should remote management be necessary or desired. If an evacuation is necessary, security managers can evacuate a building and still have control over the systems on-site.

### **ROI on Core Business**

When businesses choose to link their integrated security system and subsystems to their BMS and their business systems, they are able to realize an ROI on security and on their core business. This is because data collected from a company's security systems can be combined with data in its BMS and business systems in ways that can have a direct impact on the company's P&L.

For example, retailers could use this approach as an anti-theft measure. A company with multiple retail outlets across the U.S. could use it to ensure that items returned by customers are being rung up as returns and returned to stock, instead of being stolen by employees taking the returns. Using its security system's video cameras in conjunction with its business systems, the retailer could determine when articles are being returned and stolen to pinpoint the employees involved in the thefts.

Another vertical market that could use video cameras deployed for security purposes to improve business value is mass transit. For example, a transit authority could use its security cameras to manage the flow of people in its subway stations. Cameras used in



conjunction with video analytics software and other intelligence capabilities could be used to count the number of people waiting at different times of the day. Transit officials could use this data to optimize the train schedule and reduce the number of people waiting at peak times, thus reducing the security risk in its stations. Reduced crowding also would likely have a positive impact on revenue and profitability because people would feel more comfortable using the transit system.

### **Summary**

For building owners and property managers, as well as the companies, tenants and customers that are involved in whatever business is taking place, the addition of an integrated and intelligent security system offers numerous advantages. It provides for reduced installation and operating costs because it eliminates component redundancy and allows customers to streamline operations. Intelligence and integration reduce training and empowers system operators by allowing them to perform their duties more efficiently.

Enhanced safety, security and comfort for building occupants or customers also can have a direct and positive impact on productivity and business value. This is especially true when security systems and the BMS are linked to business systems. Fully integrated, intelligent security systems help support the security goals of building owners and tenants, and they help companies achieve their overall business goals.

### **TAC Security**

TAC provides superior security and automation solutions in a wide range of applications, including commercial offices, industrial/manufacturing sites, retail stores, supermarkets, hospitals, sports arenas, banks, schools, all of which are located in buildings of all types and sizes.

TAC is a leading provider of building automation solutions based on Open Systems for Building IT®. TAC's mission is to provide added value through building environment services for indoor climate, security and use of energy, delivered with advanced technology to end users and property owners throughout the world. With over 80 years of experience in the HVAC, building automation and security arenas, TAC employs more than 5,000 people worldwide, with partners and branches in 80 countries. TAC's parent company, Schneider Electric, is the world leader in automation and electricity management, with 92,000 employees worldwide and operations in 130 countries.