Social Spaces
What does Facebook have to do with physical security?

Campus Safety
IP technology can enhance security at colleges and universities

Frictionless Access
Say goodbye to access badges… soon

SIA Technology Insights

Volume 2, Issue 1
Spring 2014

Welcome

Dear Reader,

One of our goals for *SIA Technology Insights* is to provide a look ahead, to give people an idea of what they can expect from security technology in coming years. This edition contains some great examples of that.

- What does Facebook have to do with physical security? Steve Van Till of Brivo Systems tells us in a forward-looking article about social media and security converging in "social spaces."
- Will we ever be able to enter secure areas without first stopping and presenting credentials? Henry Hoyne of Northland Controls describes some possible routes to a "frictionless" future for access control.
- How can technology be used to enhance security in urban environments? Itai Elata of Verint Systems examines the "safe city" model and its potential for making municipalities more secure.

In addition, Bill Bozeman of PSA Security Network offers a broad view of the future of security, and other industry leaders offer articles on fingerprint biometrics, campus security, interlocking doors, video management software, and hardening office building security. If you want to know not only where physical security is today but, also, where it is going, this issue of *SIA Technology Insights* will provide a lot of answers.

We are continuing to work to enhance it and make it an even more vital source of information about electronic physical security. If you have any suggestions, or you would like to propose an article, please contact Ron Hawkins, the editor-in-chief, at rhawkins@securityindustry.org.

Finally, remember that you can view an interactive digital version of *SIA Technology Insights* and download a PDF of the publication at www.securityindustry.org/techinsights.

Thank you for reading.

Sincerely,

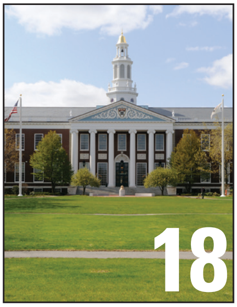
V. John Stroia

Don Erickson

V. John Stroia
Chairman, Board of Directors
Security Industry Association

Don Erickson
CEO
Security Industry Association

Table of Contents



How to Navigate Through the Magazine

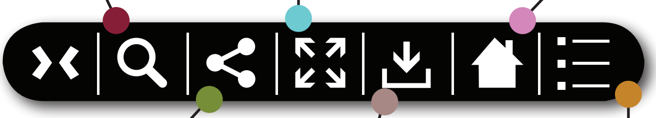
Navigation Bar

Click the arrows button to expand or contract the navigation bar.

Click the search button to look for keywords.

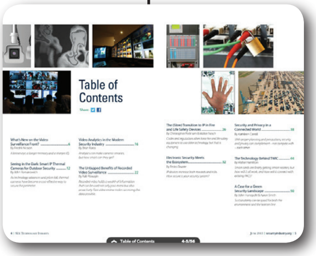
Click the fullscreen button to view page.

Click the home button to go back to the cover of this Magazine.



Click the share button to upload content on social networks or to email.

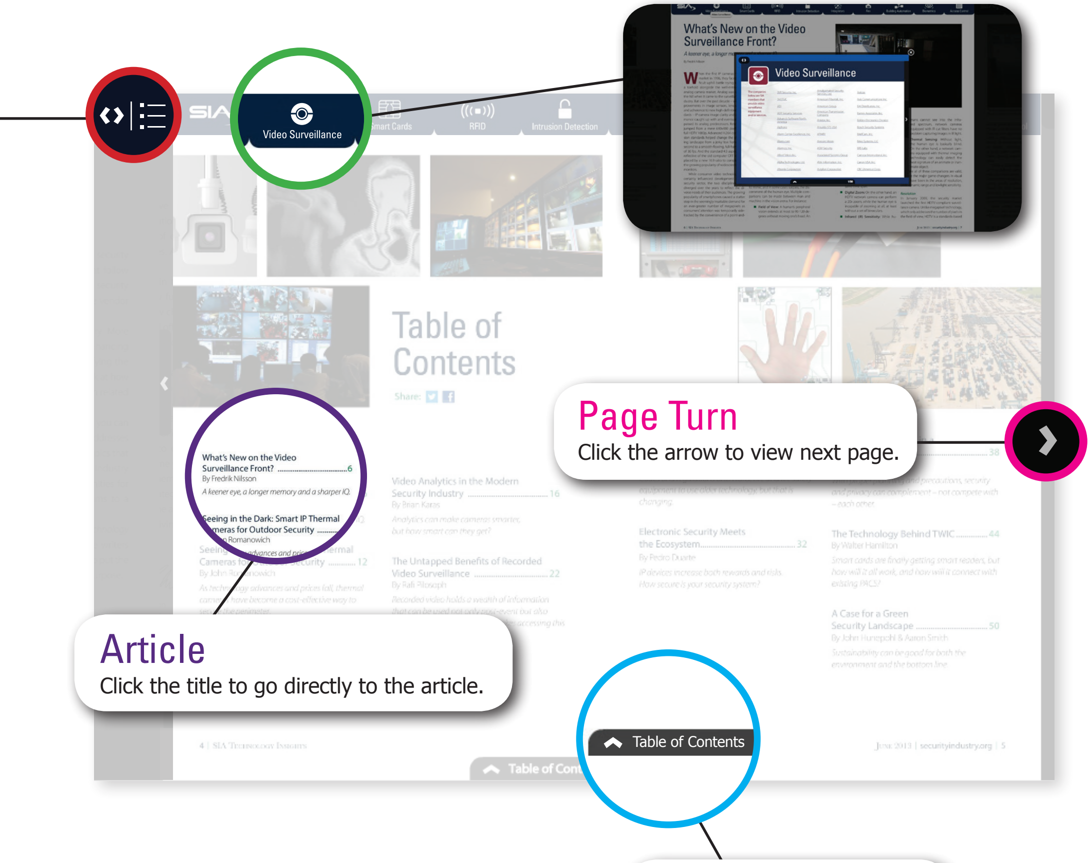
Click the dowload button to save a PDF of the Magazine or selected pages.



Click the bullet button to go to the table of contents.

Topic Tabs

Click to see a list of SIA members for each topic.



What's New on the Video Surveillance Front? 6
By Fredrik Nilsson
A keener eye, a longer memory and a sharper IQ.

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security 12
By John Romanowich
As technology advances and prices fall, thermal cameras have become a cost-effective way to secure the perimeter.

Video Analytics in the Modern Security Industry 16
By Brian Karas
Analytics can make cameras smarter, but how smart can they get?

The Untapped Benefits of Recorded Video Surveillance 22
By Rafi Rikoaph
Recorded video holds a wealth of information that can be used not only post-event but also

Electronic Security Meets the Ecosystem 32
By Pedro Duarte
IP devices increase both rewards and risks. How secure is your security system?

The Technology Behind TWIC 44
By Walter Hamilton
Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?

A Case for a Green Security Landscape 50
By John Hunepohl & Aaron Smith
Sustainability can be good for both the environment and the bottom line.

Page Turn

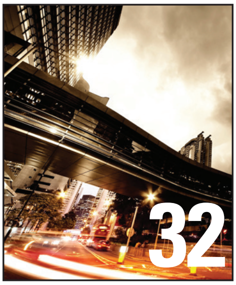
Click the arrow to view next page.

Article

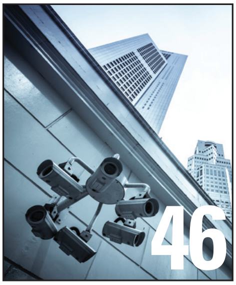
Click the title to go directly to the article.

Page Thumbnails

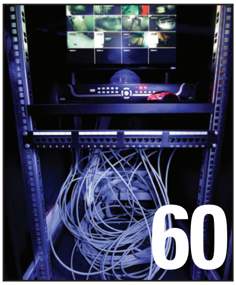
Scroll to view the next page


32

40


46

54


60

What if our buildings knew who we were and why we were there? What if public places could talk about their security concerns? How would that change the practice of security?

Say Hello to Social Spaces

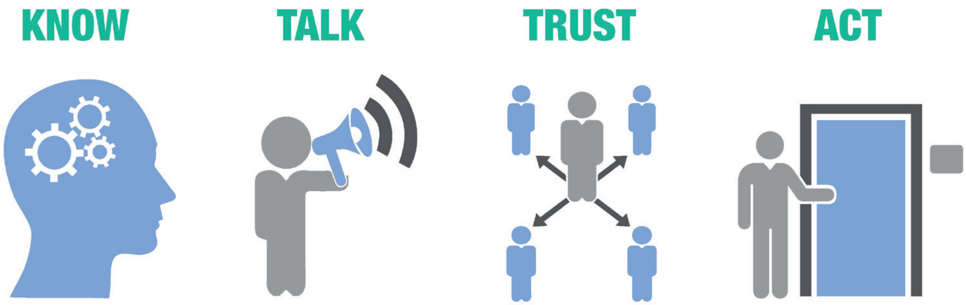
Social applications will transform the security experience

By **Steve Van Till**,
President & CEO
Brivo Systems

Social networks and social applications have become the single hottest growth category for both web and mobile technology. In hindsight, it appears to have been destiny. It's as if the cloud and mobile had a baby, and they called it social networking. It has become not only the biggest growth category for new startups, it also represents the single largest technology IPO in the history of the U.S. stock market. Social applications have literally transformed the way our society uses computing devices, and they now account for the second-largest amount of time spent using mobile devices. Social applications have proven useful in fields as diverse as real estate, navigation, family management, reviews, business networking and news distribution.

And, yet, social applications are almost entirely absent from the world of commercial security. Why is that? Is it just because no one has made the connection?

Outside of the security industry, there is a growing trend called the



"social Internet of things," which is an offshoot of the better-known "Internet of things." It describes physical devices that are connected to social applications so that we can interact with them in the same ways we interact with people. Status updates, texting, group updates, checking in, posting photos, all that, with so-called "social things." A television, for example, may be connected to several social networking accounts and be able to tell people what was watched and when. Refrigerators, meanwhile, are now famously connected to social media and can take part in a dialogue with owners and the purveyors of their favorite products.

If these common consumer "things" can be social, why not the more industrial or commercial products we use to manage our physical infrastructure? What if the physical spaces we manage had the same ability to interact as consumer products when connected to "social devices"? What if our buildings knew who we were and why we were there? What if public places could talk about their security concerns? How would that change the practice of security? How would "social spaces," to define a term, change the management of public places?

Even though the security industry is often late to the party for new technology adoption, it seems inevitable that social applications will find their way into the industry sometime soon. When they do, they have the potential to introduce some of the most sweeping changes we have seen since the introduction of IP technology. A few of the likely outcomes include:

- Enabling a more participatory security process
- Blending the security experience into business processes
- Improving real-time situational awareness
- Creating more intuitive and less obtrusive interactions
- Generating massive data sets about how our spaces are actually used

What Does It Mean to Be a Social Space?

Amid all of the discussions about "social networks" and "social media" and "social applications," one rarely finds a definition of what it means to be social. We know that people are social. Animals certainly appear to be social. But can a building or a physical space be social?

When it comes right down to it, being social is mostly about how something interacts with the rest of the world. For our purposes, we will just say that if something exhibits social behaviors, then it is social. To narrow that down a bit more, in this context, there are four key behaviors that are important for social spaces:

1. They can know who you are
2. They can talk to you
3. They can learn trust
4. They can take action

It's as if the cloud and mobile had a baby, and they called it social networking.

Know

Social spaces will be able to identify and know their inhabitants, visitors, guests, caretakers, administrators and any other people who interact with them. This knowledge is a fundamental building block because social relationships are built on the concept of a stable personal identity over time. This means that social spaces will need a way to identify people uniquely, in a way that does not randomly change, preferably with reference to an external identity provider. Social spaces will also need to understand the attributes and roles that are meaningful in the context of their interactions with us. The way we are greeted, where we are allowed to go, and whatever assistance we receive, for example, will all depend on who we are and why we are there.

Talk

Being social is all about communicating. No communication, no social relationships. Social spaces will communicate with us through social applications, just like our friends and colleagues do today. The more natural this communications is, the better. So instead of having to learn a new application for every place we go, it should be possible to communicate with a social space as if it were a person, using text or voice exchanges. You could ask a social building to let you in, lock the door, or perhaps allow a guest to visit on a particular date, all without having to learn a new application or switch out of the applications you're already using.

Trust

Social relationships are based on trust, and trust is based on familiarity. That is why your dog barks at strangers and not at your friends. A social building wouldn't bark at your friends, either. For social spaces, trust would be built up over time, the same as it is between people or animals. Frameworks to support this type of learned trust are a hot topic in identity research, and automating trust relationships is a thorny problem. That said, automated trust frameworks that operate in public spaces are an important tool for managing the growing number of security concerns we face. The sheer number makes it impossible to manage all of them through explicit rules, as we have in the past. At some point, our things and buildings and spaces will need the ability to operate more like we do, and learning trust is a big part of it. The social graphs embedded in social networks provide a rich data set that can be leveraged for this purpose.

Act

Ultimately, the whole point of creating social spaces is to empower them to take actions based on the ability to know, talk and trust. For example, a social space could remember its past interactions with a person and change its way of dealing with that person as it gets to know him or her better. A social building will know if someone is a friend of someone else and perhaps allow her to enter where a complete stranger would not be permitted without an escort.

It's All About Identity

In order for social spaces to become a reality, they need to be able to identify people and share an identity of their own in return.

Today, we do not really have an agreed upon way in which to assert identity with any universality or uniqueness. The fact is, there are actually too many ways for us to identify ourselves, but they are all bound up in the small world of whichever organization issued us a particular identity token. When we go to work, we use an access card from our employer. When we go to the gym, we use a card from the health club. When we use an automated garage, we have yet another identity based on the fob assigned to our car. This means that we are always identifying ourselves as someone different when we go to different places. And none of these identities has anything to do with the others. No wonder our buildings don't know who we are.

There have been many attempts to find an identity provider that everyone can agree upon, but, so far, none of them has really stuck. The security industry, for example, has many ways of identifying people, but each suffers from a lack of uniqueness and scope. People outside the industry are horrified to hear that proximity cards are not necessarily unique. Smart cards are helping, but the market has been slow to shift to the new technology.

The federal government has made several stabs at this as well, but the closest thing to a national identity initiative is the National Strategy for Trusted Identities in Cyberspace (NSTIC) program run by the National Institute of Standards and Technology (NIST). As a government initiative, however, it faces many adoption hurdles, especially in the wake of the controversy over the NSA's domestic data collection.

In some sense, though, the public has already voted for its favorite identity providers, and they appear to be the social networking companies. Facebook likely has the largest user base using its credentials to register and log in to third-party websites. Google has been pushing its Google+ credentials for the same purpose. We are even seeing B2B companies like salesforce.com acting as identity providers for enterprise customers.

Against this backdrop, a social space still needs to have its own unique identity in order to interact with social applications on a social network. It is likely they will go in the same direction as the rest of us, using the available commercial identity providers that have become a common way of identifying ourselves online.

Social applications are almost entirely absent from the world of commercial security. Why is that? Is it just because no one has made the connection?

Social Communication Channels

One of the main benefits of having social spaces with social identities on the same network as the user community is that it would enable everyone to communicate with each other using identities and applications that are already part of their daily lives. These communications could be one-on-one, such as a request of or command to a social space, or they could be group messages, with a community of interest being privy to the same stream of information about a particular space or building. They might also be messages about special events, like the arrival of a guest or a change of venue.

We are seeing the emergence of this use of social communication for personal and neighborhood safety in, for example, certain applications that provide integrated messaging and location tools to members of a family. If someone fails to arrive at a location when expected, or goes somewhere he or she should not, geofencing algorithms trigger alerts that allow family members to respond.

Applying crowdsourcing to security is a very powerful way of thinking about how we can increase the benefits of electronic security in general.

Such tools could easily be applied to commercial and public spaces, where the space itself and everyone who uses it are part of the community of concern and are allowed to share relevant information across the social channel.

Security as a Customer Experience

It is probably fair to say that most of our encounters with building security are less than positive. One of my recent security experiences included a long wait in a lobby with a hostile guard who acted like everyone entering "his" building was lying to him about who they were and why they were there. Then there was a long wait while security tried to find the person I was there to see. Even in more hospitable lobbies, the best you will get is usually the stranger treatment involving impersonal processing and a cumbersome sign-in procedure.

The point is, when it is your building, everything about this user experience is turning off your customers. So what should customers expect? A customer experience, that's what.

There was a great line from a *Mad Men* episode in which Roger Sterling, an advertising executive, reminded a colleague, "The client should never experience a negative emotion while in your presence." That should also be true for people – customers – any time they are in a secured space.

A truly social space could be set up to know in advance who will be visiting. With that information, the guest could be welcomed by name upon arrival, rather than being treated like a stranger and handed a clipboard. By using a mobile credential or pass sent in advance, registration and badging could be as simple as scanning the invitation. The social space would then use a preferred social network to tell the hosts that their visitor has arrived. This would transform an impersonal security interaction into a welcoming customer experience.

Crowdsourced Security

Social spaces give rise to the possibility of what might be called "social security" – if the term were not already in use – or "crowdsourced security." Crowdsourcing is the practice of obtaining services from a large group of people who are part of an online community, rather than a traditional employee responsible for that function. Applying this concept to security is a very powerful way of thinking about how we can increase the benefits of electronic security, in general.

Consider the usual model for intelligence collection and protection of a building. It is having one or more dedicated guards or other security personnel watching computer screens and cameras. This is an expensive process, and there is no way that a small group of people can ever hope to be as observant as a large group. And many companies, small businesses in particular, cannot afford to have dedicated security departments. But every company has an employee base that could be plugged into a social network group that receives alerts or images about possible issues.

Awareness is readily generated through crowdsourcing, and many of us are already using such crowdsourcing without knowing it by that name. It has become commonplace to look at online (crowdsourced) reviews of restaurants, hotels, vacation spots, mechanics and many other commercial services. This same socially sourced model fits with the trust level that might be associated with any particular individual entering a public space. Think of it as a personal review of every person who might be entering your building.

Forewarned is forearmed, and more awareness is always better.

When Is It Coming?

Social spaces are not exactly here yet, but many pieces of the puzzle are coming together:

- The use of mobile phones as an identity platform
- Wearable computing devices that interact with their environment
- The proliferation of application programming interfaces (API) for cloud-based social platforms
- The relative ease of stitching services together to form a social fabric around "things"
- The emergence of social applications that include interactions with inanimate objects like cars, refrigerators and other connected home appliances
- The growing acceptance of social applications in the business world

Like many other technologies, social computing will move into security slowly at first, then it will become pervasive, and, finally, it will leave us wondering how we ever did without it. ■

Back to TOC

Steve Van Till is president and CEO of Brivo Systems (www.brivo.com) and vice-chairman of the SIA Board of Directors Executive Committee. He can be reached at steve.vantill@brivo.com.

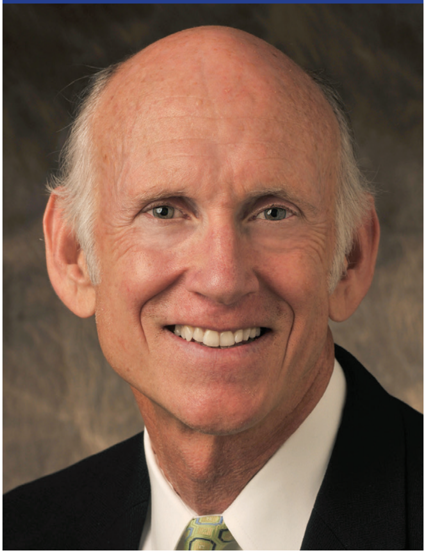
Global recognition and acceptance of security technology will provide more opportunities than our community has ever witnessed.

VISION
Lorem ipsum dolor sit amet, tation prompta pro cu, duo luptatum vulputate ex, quo quot vivendum reprimique an. Id reque doming everti usu, eu detracto iudicabit pro. At meis harum complectitur nam. Ad graeci numquam est, docendi adversarium ea est, vis ut mandamus liberavisse. Veniam facilis lobortis ut mea, sea ne malis aeque malorum.
Primis epicurei assueverit cu ius, vis noster erroribus ne, sit et meliore lucilius. Vis malorum meliore eu, mei cu ornat.

What Is in Store for the Physical Security Community?

New technologies will open up great opportunities for the industry

By **Bill Bozeman**,
President & CEO
PSA Security Network



Let's begin by defining the physical security community. If you are a security technology user, designer, software or hardware supplier, integrator, trade reporter or distributor, you are part of this community.

As security morphs into a service that affects a vast number of the inhabitants of the planet, everything changes. Large corporations and top flight talent are now attracted to the security space. The days of security being perceived as a cottage industry are gone. It is now a big business that many, but certainly not all, security professionals are prepared for. Some security veterans will prosper; others will have difficulty adapting and will perish.

C-level executives no longer delegate security to a retired street cop and hope for the best. Security has become very high-profile, and the new visibility of security professionals affects the security community much more than most of the industry's leaders realize.

Understanding the corporate security budgeting process and where

security fits into a specific company's strategic plan is paramount if the plan is to grow an organization's value with security-minded corporations.

Cyber security rules the security budget roost today and will continue to do so for the foreseeable future. How significantly this will affect budgets in the physical security space remains to be seen, but it is difficult to see any scenario in which traditional physical security is viewed as more important than cyber security in the C-suite.

C-level executives no longer delegate security to a retired street cop and hope for the best.

The recent data breach at Target is just the tip of the iceberg. Houston, we have a problem, and it is one that has the attention of the world's most brilliant cyber criminals. For the elite cyber crooks, our problem is their opportunity, and they are all about exploiting it for an economic windfall.

Cyber crime is now more profitable than the illicit drug trade and physical crime, and what we are experiencing is just the beginning. Those in the know regard cyber crime as the biggest threat that security professionals face, and government officials predict that cyber crime will be a bigger problem for the security of our country and the security of corporate America than traditional terrorism.

Criminal cyber rings control massive botnets capable of hijacking online financial accounts. New cyber security companies will flourish as the need to more securely encrypt communications and disrupt the use of those botnets increases. With cyber security dominating the security budgets of corporate America, startups in that field will be better positioned than traditional security providers with regard to getting financing.

The cyber security meltdown has not gone unnoticed by the accounting industry, which has developed a reporting process known as SSAE 16 that provides a professional opinion as to the effectiveness of corporate cyber controls. Security professionals can expect more standards, requirements and certifications specific to cyber security as regulators crack down on organizations that have lax cyber standards or no standards at all.

> Houston, we have a problem, and it is one that has the attention of the world's most brilliant cyber criminals.

Thus far, we have not seen much notable crossover or many formal partnerships between traditional physical security businesses and cyber security providers, and such alliances appear to be unlikely in the immediate future. Cyber security companies have not been acquiring physical security companies in an effort to provide the whole security package, something that many students of the industry had predicted would happen. Industry experts have also been incorrect in their predictions that network integrators would acquire principal security integrators. While we have seen some of this type of consolidation, it has been very limited.

New developments and cost reductions in storage will open a host of opportunities for security directors, integrators and manufacturers. With the cost of local storage dropping like a rock and remote cloud-based accessibility becoming an affordable and deployable reality, new applications and opportunities are now available.

Network-attached storage (NAS) devices are particularly interesting, as they offer more cost-effective solutions than storage area network (SAN) devices, and they are also easier for integrators to configure and end users to maintain. Solutions that are easier to deploy and maintain and are also more cost-effective have historically been exceptionally well received by the cost-conscious security community.

SD cards also provide a cost-effective solution for low to middle-end applications. Video surveillance providers can now offer cameras with dual 256k cards, providing adequate storage for many retail applications. The larger SD storage capabilities integrated with embedded intelligence open up a new world of powerful, flexible and cost-effective offerings.

Video analytics may provide the most exciting opportunity of all. The unrealistic hype of the recent past has

cast a cloud of doubt over the analytics niche. However, successful retail and industrial deployments have the smart money taking a very close look at the latest developments. Successful and cost-effective implementation of analytics will boost overall video surveillance acceptance more than any other individual variable. The larger security software and hardware developers are either working independently on video analytics solutions or partnering with analytics specialists to ensure that they do not miss out on this opportunity.

Security biometrics offerings seem to have been around since before the Rolling Stones. Unfortunately for biometrics investors, none of the technologies has caught on nearly as well as the Stones. Biometric companies have come and gone with little to show for their efforts and investments. This will change as new developments in iris recognition provide accuracy in a noninvasive manner. Facial recognition and fingerprint offerings also continue to improve, and the cost of deploying these technologies continues to drop. As with analytics, many deep-pocketed developers continue to work to refine facial recognition and fingerprint devices, and both technologies will find a market niche as price performance improves and deployments become more common. Several companies are utilizing new advanced algorithms to improve accuracy, decrease deployment difficulty and reduce the up-front cost of facial recognition solutions.

Another positive is that security integrators are finally embracing biometrics and more frequently offering biometric options to end users. Equally important is that the end user community is requesting biometric solutions.

Privacy concerns, as expressed by the American Civil Liberties Union (ACLU) and others, have the potential to slow the mass deployment of facial recognition. To address this issue, the National Telecommunications and Information Administration is working on a voluntary industry code for the use of facial recognition technology. The code will be reviewed by the White House, which has an initiative to enact baseline consumer privacy legislation.

Mobile security applications have the potential to disrupt the traditional security market more than any of the other technologies mentioned in this article.

The concern with facial recognition is not about the technology itself, but, rather, whether a person has the right to control his or her biometric data and how and who can use that data. The ACLU has been closely monitoring the subject.

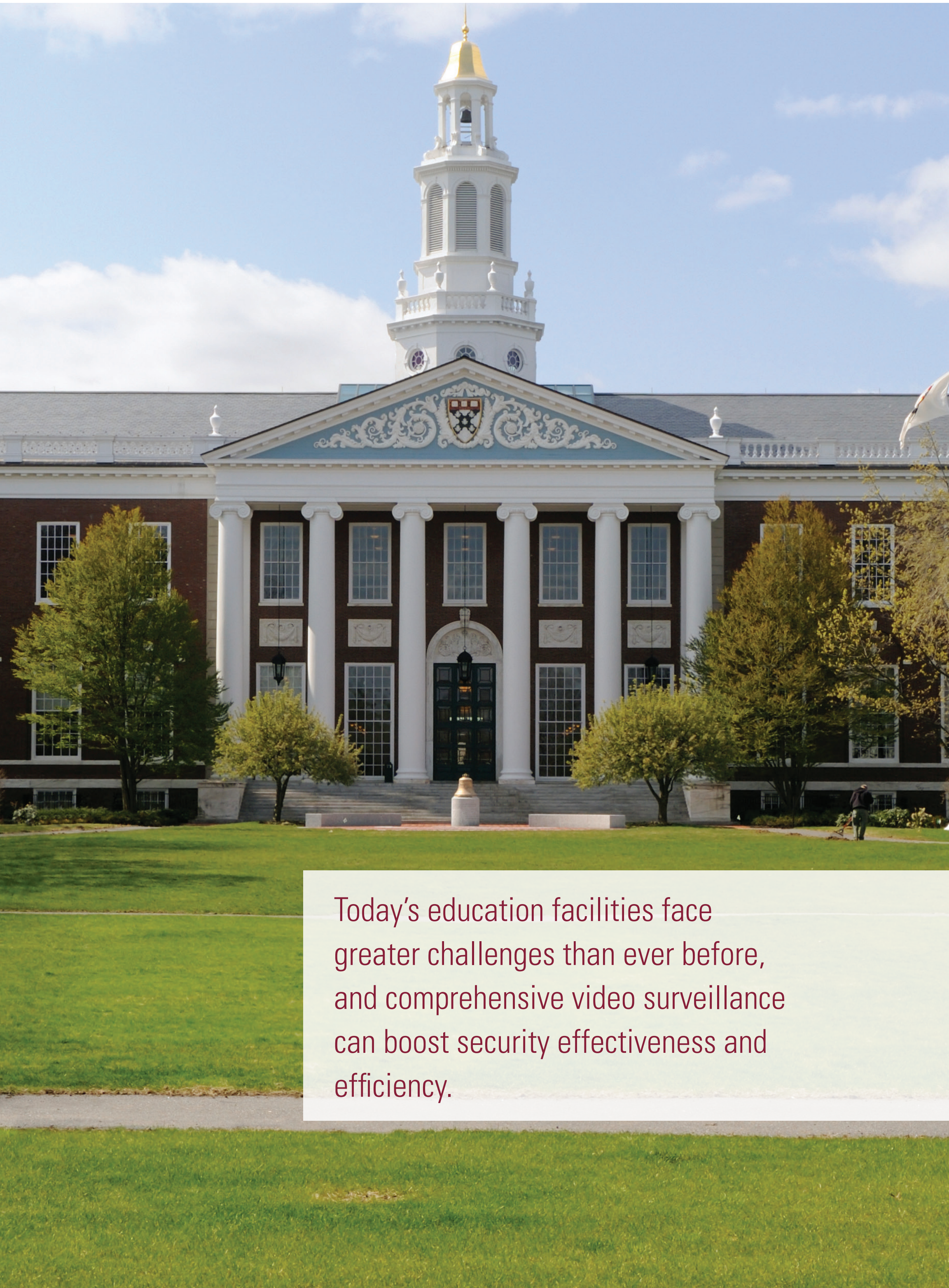
No summary of the future of physical security would be complete without a discussion of mobile applications. All niches in the physical security space have embraced mobile, including video surveillance, access control and alarm point monitoring. New mobile features seem to pop up daily, making security technology that previously was utilized only by security directors much more accessible and affordable to the masses. Mobile applications will change the face of physical security, providing a huge upside for those who embrace the opportunity.

Mobile will open up a new stream of business revenue for service providers, storage specialists and associated supporting video surveillance providers. Mobile security applications have the potential to disrupt the traditional security market more than any of the other technologies mentioned in this article.

To say that the future of security is bright is an understatement. Global recognition and acceptance of security technology will provide more opportunities than our community has ever witnessed. This same recognition and acceptance will also bring new investment and new competition to the security marketplace. New investment and new competition indicates a healthy environment, and, for this, we should all be grateful. ■

Back to TOC

Bill Bozeman is president and CEO of PSA Security Network (www.psasecurity.com). He can be reached at bill@psasecurity.com.



Today's education facilities face greater challenges than ever before, and comprehensive video surveillance can boost security effectiveness and efficiency.

Making Campuses Safer with Innovative IP Technologies

Networked systems mean more information, more collaboration and more security

By **Kim Loy**,
Vice President
DVTEL

The range of security challenges facing large campuses is a study in extremes. Security has to act quickly during busy times when a campus is teeming with students and also be responsive on weekends when parking lots are deserted. It must be able to protect urban environments as well as wide-open spaces. It has to be fast in an emergency situation when seconds matter and also dependably keep watch over long, slow periods at night and on weekends.

Security systems have to provide protection in an open environment to control multiple risks, and the systems must be unobtrusive and in the background of a welcoming and productive educational institution. Campuses are open yet restrictive, uncontrolled yet protected. Security systems have to collect information from the far corners of a large campus, and they must provide that information to security officers and administrators wherever they go.

Security solutions in campus environments serve as force multipliers for campus police. The systems have

to be easy to operate. Surveillance solutions must help to ensure the safety of students, faculty and staff and protect valuable assets. Security technology provides extra eyes and ears – and information – to manage campus operations. Today's education facilities face greater challenges than ever before, and comprehensive video surveillance can boost security effectiveness and efficiency.

Simplified operation is a requirement across the board in education environments. For campus police, operating the video surveillance system should not be a high-tech challenge. System interfaces should be simple and intuitive enough to enable even a casual or infrequent user to get information in a timely fashion. In the K-12 vertical, for example, systems are often used by school principals and office administrators, in addition to school resource officers, so a simple user interface is critical.

Security solutions in campus environments serve as force multipliers for campus police.

Dependable, Scalable Systems

IP technology has become the solution of choice in campus environments. More than a replacement for analog video systems, intelligent IP surveillance solutions enable organizations to leverage a variety of communications, video and data to enhance security and prevent criminal activity. The increase in data collection from various networked sources enables campuses to streamline investigations, improve protection of critical assets and optimize business efficiencies.

Campuses need dependable, scalable surveillance systems that are user-friendly and can be easily integrated with future security management systems. An IP video network and a powerful video management system (VMS) provide live monitoring and incident review, and can even serve as a crime deterrent.

Educational institutions already have robust information networks that can be leveraged by IP video surveillance to configure systems that are cost-effective. Existing Ethernet cabling and even fiber optic networks that reach across long distances can simplify connectivity for video and security systems and also make it easier to tie those systems into other campus functions. As a consequence, campuses at all levels, from universities to K-12 school districts, benefit greatly from effective surveillance systems.

> More than a replacement for analog video systems, intelligent IP surveillance solutions enable organizations to leverage a variety of communications, video and data to enhance security and prevent criminal activity.

New camera capabilities are also contributing to better video surveillance systems in campus settings. Higher-resolution cameras, such as megapixel and HD cameras, make it possible to cover larger areas, such as parking lots, with fewer cameras (and a less expensive system). Higher resolution is also valuable when one needs to examine the details in an image, such as the cash denomination

Case Study:

North Carolina State University

North Carolina State University, located in Raleigh, N.C., has approximately 35,000 students, 8,000 faculty and staff and 500 buildings. It sits on more than 2,000 acres and is home to a nuclear reactor and sensitive biological and animal material handling sites.

"N.C. State is the size of a small town," said Scott McInturf, the school's director of security applications and technologies (SAT). "Our job is to provide the technology to efficiently and effectively protect all these assets in an urban environment with a dynamic population comprising more than 60,000 people on any given day."

Faced with the need to upgrade its security system because of increasing risks, N.C. State spent a year evaluating network video management systems (VMS). Key selection criteria included scalability, ability to utilize and sit atop the existing campus network, and potential for integration with future networked systems. An enterprise-class network VMS was chosen. It manages more than 650 cameras, provides a user-friendly interface, and easily partitions to allow each individual department access to only its video data.

The surveillance program is unique in that one department, SAT, manages the servers, storage and administration while offering each campus department the opportunity to purchase and integrate the cameras they need. When buildings are added or a department expresses security concerns, SAT, working with the university police, serves as a security consultant, outlining the standards and criteria that new users need to address. All parties agree on a security template for the building(s), and the project integrator supplies the project management and technical support.

With the help of its advanced video management and IP surveillance camera network, N.C. State can address today's complex security requirements. As the university's system expands in size and capability, it can continue to convert complex video data into productive, valuable and manageable information.

in a transaction at the campus bookstore or the face of someone who enters a parking lot.

Greater, Faster, More Effective Security

College campuses and K-12 institutions across the country are implementing IP-based systems that collect raw data from multiple areas – classrooms, dorm common areas, perimeters and special event sites – and turn it into actionable information. Real-time notifications of crimes in progress can provide officials with the opportunity to improve, and even automate, decision-making. This results in greater, faster and more effective security, lower costs and enhanced productivity. Security systems can reduce crime rates, as well as provide evidentiary footage of crimes when they occur. Use of video analytics can boost manpower efficiency. Rather than requiring an operator to constantly watch a video screen, the system can detect specified events and create a real-time alarm to get the attention of campus police officers. An alarm could be based on a camera programmed to detect when a person or vehicle enters a restricted area or crosses a "virtual tripwire," for example.

IP technology also drives collaboration. When campus law enforcement, public safety officials and first responders take an integrated approach to security, they are able to share information in real time and build a proactive approach to keeping people safe. Collaboration increases the ability of officials to address incidents quickly and to share critical security data easily. Open systems architecture contributes to effective integration of systems required for collaboration.

A reality in the campus environment is that most systems are not monitored at all times. Rather than sitting at a desk watching a video screen, safety officers are more likely to be patrolling the campus, responding to an incident or otherwise engaged. Because most systems are not consistently monitored, successful investigations depend on the preservation of clear video evidence of an incident. Large campuses, especially at the college and university level, require video to provide views of remote locations and collect critical forensic evidence during an incident.

There is also increased interest in mobile applications in campus

environments. With smartphones now able to act as video cameras, new systems can incorporate video from phones into the VMS. In a university setting, campus police can use their smartphones to record, analyze, review and export video from any location. These systems operate over WiFi, 3G/4G and LTE networks, and they provide security teams with more mobility than ever before, complementing existing surveillance networks and reaching places traditional cameras cannot.

> When campus law enforcement, public safety officials and first responders take an integrated approach to security, they are able to share information in real time and build a proactive approach to keeping people safe.

In addition to collecting video from mobile platforms, IP video systems can deliver video to mobile devices, such as smartphones or tablets being carried by police officers as they move about the campus. This is another way that systems are making campus officers more efficient.

Strong Technology Platforms

Integrators and resellers are looking for strong technology platforms and support networks to serve customers. Manufacturers now provide robust training options specific to the education market, offer support around the globe, and even help generate leads for new business. Ideally, integrators and manufacturers should act as partners with the common goal of establishing trust with the end user. At the same time, integrators can rely on manufacturers to play a valuable support role to help them assess and respond to customer expectations. Customer satisfaction depends on the best efforts of everyone involved in a system sale.

In the education vertical, the end user is often well versed in networking and related technologies, which makes it all the more important that resellers have the technological capabilities and qualified personnel to serve this sophisticated customer. The customer, however, may lack basic familiarity with the design of effective security and surveillance systems. He or she may not be familiar with issues such as camera placement, how to deal with varied lighting, etc. That is where the dealer can add value, but he or she also needs to have networking knowledge to build credibility and rapport with the customer. Savvy manufacturers provide their channel partners with the resources required.

More than in other verticals, campus systems often involve multiple stakeholders. Involved parties obviously include the security and

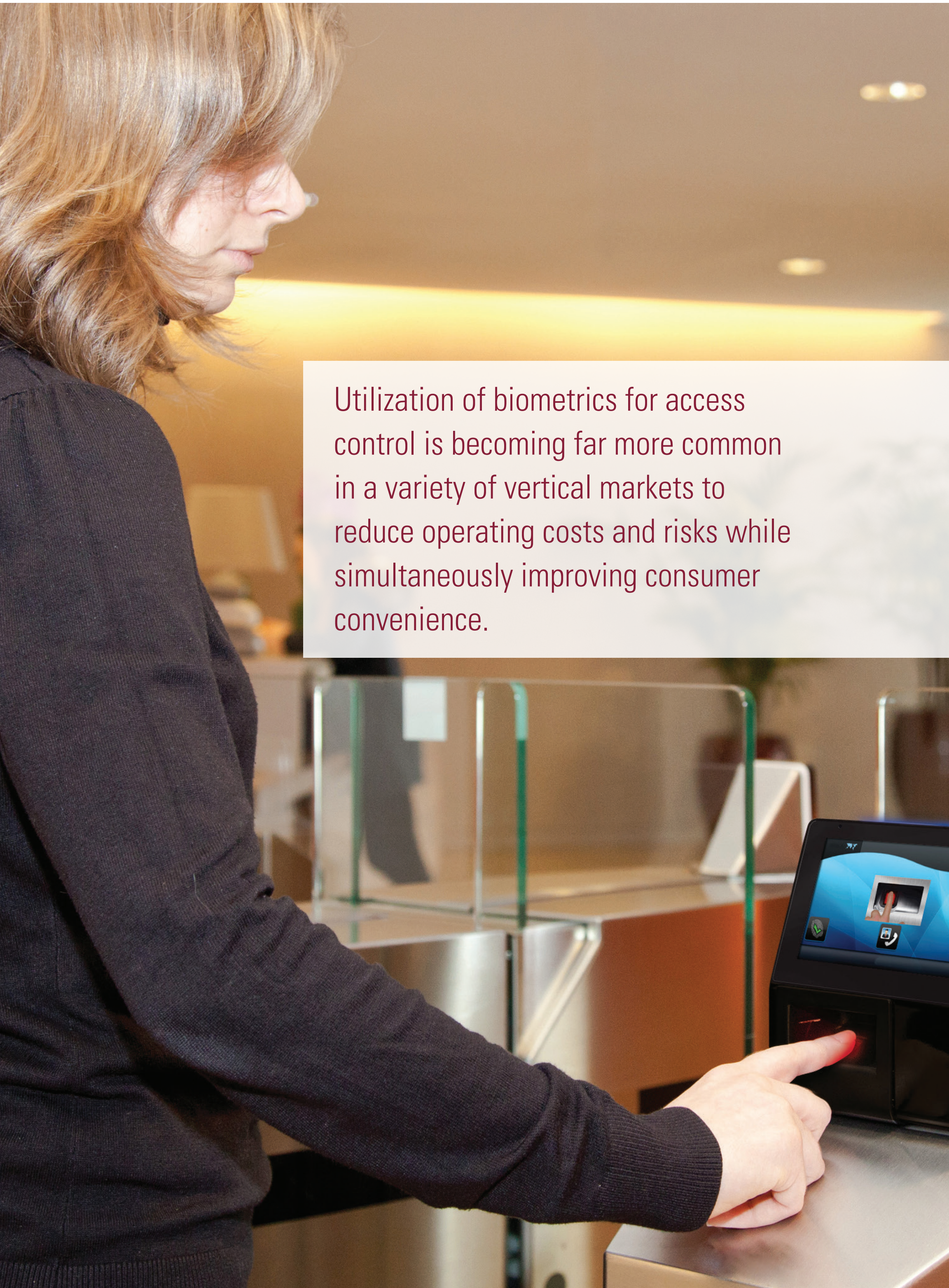
IT departments, but they might also include physical plant representatives, as well as procurement, accounting and administrative personnel. An IP video system offers new ways to demonstrate return on investment. Having more parties at the table opens up these discussions.

Greater Challenges than Ever

Today's education facilities face greater challenges than ever before, with the threat of violence looming large. Following tragedies like the shootings at Virginia Tech and Sandy Hook Elementary School, officials are seeking to enhance security. They must prepare for the worst, while still maintaining a welcoming environment in which students are comfortable and happy. In addition to the possibility of active shooter scenarios, educational institutions also must deal with a wide range of everyday threats and challenges. An effective video surveillance system can be a valuable tool in any type of incident. ■

Back to TOC

Kim Loy is vice president, global marketing, and chief product officer at DVTEL (www.dvtel.com). She can be reached at kloy@dvtel.com. ✉



Utilization of biometrics for access control is becoming far more common in a variety of vertical markets to reduce operating costs and risks while simultaneously improving consumer convenience.

Fingerprint Biometrics for Secure Access Control

Moving beyond passwords and tokens can enhance security while decreasing costs

By **Consuelo Bangs**,
Senior Program Manager
MorphoTrak

Why is biometric technology still considered an innovation and not a standard part of everyday life?

Fingerprint technology continues to have a mystical aura, its use seemingly relegated to access of highly classified information (logical access) or, more commonly, restricted, secure or high-value areas (physical access).

Yet, despite this perception among the general public, utilization of biometrics for access control is, in fact, becoming far more common in a variety of vertical markets to reduce operating costs and risks while simultaneously improving consumer convenience. From time and attendance systems in the workplace to biometric controls on sophisticated machinery to sports/health club facility access, biometric sensors provide security and convenience in an ever-increasing spectrum of applications.

Two-Factor Authentication for Added Security

Access control systems are designed to make facilities more secure by letting authorized people in

– to entire networks, to facilities, or to defined areas within those networks or facilities – while keeping unauthorized people out.

It has become clear that tokens or passwords alone are inherently unsecure and do not provide a sufficiently strong barrier to keep out a determined intruder. Tokens can be lost, stolen or damaged; passwords can be guessed or otherwise discovered.

> It has become clear that tokens or passwords alone are inherently unsecure and do not provide a sufficiently strong barrier to keep out a determined intruder.

Systems that use an ID card for access control must ensure that they allow entry of the credential *owner*, not simply the credential holder. To verify the owner of the credential, an additional factor of authentication must be provided for access to be granted. One type of authentication pairs a password with an ID card. This is referred to as two-factor authentication – something you have and something you know. For those situations where the rightful cardholder must be unequivocally linked to the card, adding a biometric is the best solution. The biometric template, an encrypted mathematical representation of the card owner's finger, is stored on the card. The card owner's live finger must match this template. Two-factor authentication that includes a biometric provides assurance that the person seeking access is the card owner and is authorized to enter the building.

What about organizations that require employees to wear badges? They often use the ID card/badge for easy visual identification of who has the right to be in a given area and use biometrics only for entry. This makes it fast and easy for authorized individuals to go through a turnstile or door. A biometric sensor is touched, the person is identified, and he or she walks through. The process takes less than a second, as opposed to the longer process of first presenting a card, then touching the biometric sensor.

Biometrics Encoded in Cards for Added Security

Because many industries already require their employees to wear a badge, ID cards are the ideal medium in which to encode fingerprints.

Adding biometrics to a smart card – with embedded chips that already carry identity information – protects the card owner by creating a secure environment in which access is only allowed to authorized individuals, and safeguards against card swapping and card theft, deterring criminal activity.

The card owner's fingerprint template, the encrypted mathematical representation, is easily stored on a smart card. The advantage of this approach is that the template resides only on the card, not in a central database. This prevents exposure of the template to cyber hacking attempts, and encryption enhances the protection of personal information.

Card technology ranges from magnetic strip and proximity cards with little or no security requirements to cards with contact and contactless microchips. The magnetic strip and proximity cards only hold a very small amount of information, and data on these cards is unprotected. There are standards for cards encoded with personal information. Standards-based card technologies include several branded contactless cards, the Transportation Worker Identification Credential (TWIC), the federal government’s Personal Identity Verification (PIV) card, and the U.S. Department of Defense’s Common Access Card (CAC). The standards define methods and requirements to protect access to the personally identifiable information written to the chips on the cards.

> Systems that use an ID card for access control must ensure that they allow entry of the credential *owner*, not simply the credential holder.

Another Alternative: Fingerprints Alone

Access control systems today are capable of taking advantage of the combined technologies of biometrics and identification cards. In a workplace that issues magnetic strip or proximity cards, biometric authentication can be added to ensure that the card holder is the card owner. This can be accomplished by installing a biometric device at the door. An individual’s biometric template is created and stored on the device in an encrypted database, and his or her live finger is compared to that template. This is termed a “one-to-many” match for identification. In workplace environments that issue smart cards with a microchip, a biometric terminal with an embedded smart card reader is installed at the door. The card owner touches the card to the biometric terminal, the biometric template is read from the card, the card owner touches the

biometric sensor, and the terminal performs the match. This is termed a "one-to-one" match.

The most cost-effective biometric access control systems have the flexibility to be implemented in a way that suits a given company's operations best. The security benefits of biometric authentication for access include:

- Identity cards can be faked while fingerprints cannot
- Identity cards can be lost; fingerprints cannot
- Passwords can be forgotten, guessed or passed on to someone else; fingerprints cannot
- Identity cards can be lost or forgotten; fingerprints cannot

The economic benefits of biometric authentication for access include:

- Elimination of the cost of cards
- Elimination of the cost of managing and issuing cards
- Elimination of the cost of printing cards

Biometric Access Control Increases Security and Saves Money

Drawbacks to traditional access control without a biometric include ID swapping or "buddy punching" – a person clocking in an absent co-worker – staffing for manual badge checks, security breaches related to unauthorized access to secure areas, and frequent card replacement. A biometric access control system overcomes these problems and provides numerous efficiency improvements.

The use of biometrics, either alone or as part of two-factor authentication, can save money by:

- Reducing frequent card or key replacement
- Reducing password changes
- Reducing theft and losses
- Reducing or eliminating monitored ingress/egress checkpoints
- Reducing queuing while clocking in to begin a work shift

Conversely, non-biometric security measures may be vulnerable to breaches. If a non-biometric ID card is lost, it remains active (and can be misused) until it is reported. Intruders can circumvent manned guard stations.

Choosing a Biometric Technology

Enrollment (initial capture of fingerprints) can be difficult for some people, such as children, the elderly and those who work in certain industries that cause excessive wear on the fingers, such as textiles and mining. If you can't enroll, then you can't match, and the system will be a failure. Strong fingerprint algorithms and sensor technology ensure maximum enrollment. The biometric algorithms and sensors must be sensitive (accurate) enough that they do not deny access to authorized people (false rejection), while simultaneously not allowing access of unauthorized people (false acceptance). Consequently, the selection of biometric technology is important.

> Implementing access control measures at a facility demands a careful balancing of convenience and security.

There are two types of biometric sensors: capacitive and optical, each of which has different features. While capacitive sensors are smaller and, as a result, can be integrated into smaller devices such as mobile phones, they also require more frequent cleaning (because residue left on the surface can affect image quality), and their silicon coating can be damaged or scratched, reducing the sensor's effective lifespan. Optical sensors have a larger scanning area, which captures more surface area on the finger, thus providing higher accuracy. They are scratch resistant, and they tend to have a longer lifespan.

Biometric sensors on consumer products, such as the Touch ID on the iPhone 5s, typically use solid-state capacitive sensor technology. Capacitive sensors use electric current to sense and capture the fingerprint. Biometric devices that are used to grant access to secure facilities, however, typically use an optical sensor, which uses one or more light sources to illuminate and capture the fingerprint.

Optical sensors that are equipped with "liveness detection" are able to detect fake fingers, whereas capacitive sensors are not. (This is one reason why the Touch ID was hacked within days of the newest iPhone's release.)

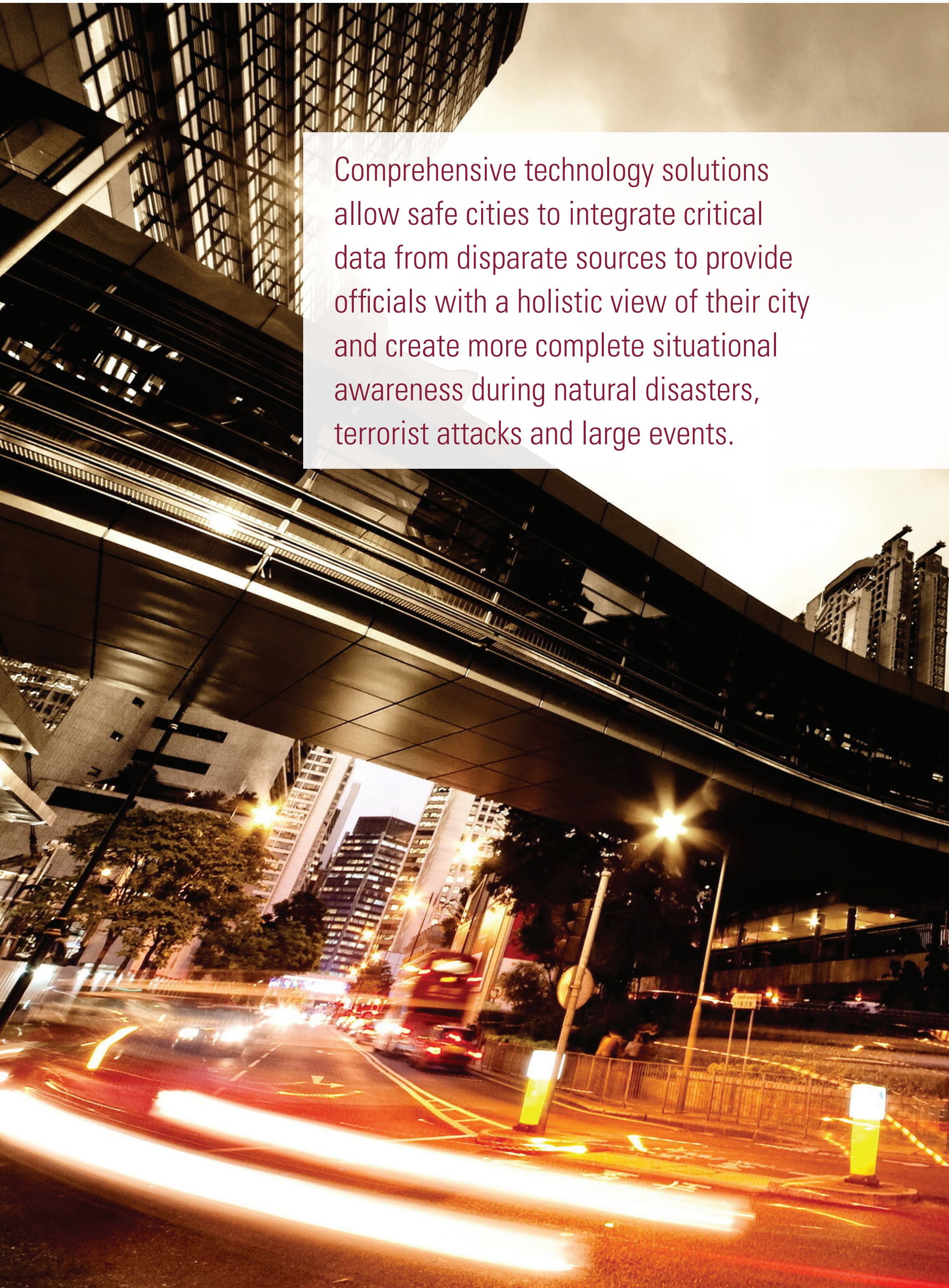
Implementing access control measures at a facility demands a careful balancing of convenience and security. Administrators at higher security facilities may decide to accept more potential false rejections if it means reducing possible false acceptances.

Conclusion

Using biometrics for access control enhances employee safety by keeping a facility secure from intruders. Whether using finger-only or finger paired with ID cards, biometrics are an effective technology for reducing operating costs while increasing security and ensuring that identified, authorized individuals receive and deliver services and perform work for which they are paid.

Back to TOC

Consuelo Bangs is senior program manager at MorphoTrak (www.morphotrak.com). She can be reached at consuelo.bangs@morpho.com.



Comprehensive technology solutions allow safe cities to integrate critical data from disparate sources to provide officials with a holistic view of their city and create more complete situational awareness during natural disasters, terrorist attacks and large events.

Technology-Enabled Collaboration Builds Safe Cities

Better management of more information can enhance the protection of people and property

By **Itai Elata**,
Senior Vice President
Verint Systems

Worldwide, the population is exploding, with experts projecting that it may exceed 10 billion by the year 2050. Included in this growth is a move from suburban to urban areas, filling cities to the limit and forcing municipalities to invest in ways to boost efficiency and improve the quality of life for residents. In the United States alone, it is expected that 90 percent of people will live in cities by the middle of the century. With large and complex infrastructures serving millions of people, today's municipalities are vulnerable to threats driven by overcrowding, criminal activity and natural disasters. As a result, there is a growing trend toward deploying citywide public safety and security solutions to better protect people, property and assets.

According to a 2012 Homeland Security Research Corporation report, annual investments in homeland security and public safety products and services increased from $48 billion in 2011 to $51 billion in 2012, and they are projected to grow to $81 billion by 2020.

The question becomes how should municipal agencies work together to best use technology to effectively and efficiently address the enormous security challenges they are facing?

Not only are cities growing, but information gathering has expanded as well. Municipal governments and agencies have more data than ever before, and it is critical that cities leverage technology systems that help users distill the most timely and relevant information from "big data." The actionable intelligence that such solutions provide positions these organizations for more informed and effective decision making.

Collaborating for a Safe City

Many municipalities are taking a "safe city" approach to secure assets, prevent disorder and enhance the safety of citizens and visitors. The safe city concept integrates security-relevant information from various sources, such as video surveillance, sophisticated analytics, citizen reporting platforms and even social media, on a consolidated IT platform to provide full situational awareness to key stakeholders, including law enforcement, public safety and intelligence agencies. Taking a comprehensive approach to city security, collaboration between government agencies, corporate enterprises and citizens is central to the success of a safe city project.

What technologies are enabling the level of collaboration required to effectively protect a city's people and assets? At the core, IP technology has become the solution of choice for rapidly growing cities. More than just a replacement for analog video systems, intelligent IP surveillance solutions enable organizations to leverage data from a wide variety of communications, video and data sources to enhance security and prevent criminal

activity. IP technology also drives collaboration. When law enforcement agencies, public safety officials and private entities take an integrated approach, they are able to share information in real time across various platforms. This approach enables officials to address incidents and emergencies immediately, instead of waiting for updates from other departments.

Data Collection from Multiple Sources

With innumerable strategically located sensors, such as video cameras, access control devices, citizen reporting platforms, video analytics and weather detection equipment, cities can collect and analyze information faster and manage and respond to situations more efficiently, often before an emergency escalates.

The additional information that municipalities have – from crowdsourcing applications, video analytics and social media – can be used to streamline investigations, improve the protection of critical assets, prevent disorder and optimize business efficiencies. Timely and accurate sharing of all of this information is vital during disasters and emergencies. It can make the difference between a successful response and a failed one.

There is a growing trend toward deploying citywide public safety and security solutions to better protect people, property and assets.

Today's social media platforms, including Facebook, Twitter and LinkedIn, have changed the way the world communicates, making individuals important news sources. While social media can improve communication, it is only helpful in an emergency situation if it is properly coordinated and deployed. City officials must cooperate with private institutions and individual citizens to leverage social media networks in a positive way during a crisis.

Making Sense of All of the Information

With all of this information available from different sources, municipal agencies need a quick and easy way to share and analyze data to improve response times and keep citizens safe. Time is of the essence in emergency situations, so finding a way to weed through the abundance of information and pinpoint useful intelligence in real time is imperative. To accurately assess risk and identify threats to the public, municipalities need information management systems that can leverage the available material quickly.

Comprehensive technology solutions, such as video management software, surveillance analytics, physical security information management (PSIM) platforms, and audio recording and analytics solutions allow safe cities to integrate critical data from disparate sources to provide officials with a holistic view of their city and create more complete situational awareness during natural disasters, terrorist attacks and large events. For example, cities now have the ability to track a suspect from a stadium to a subway station, onto the train and to a park across town. In some cities, officials may even be able to gain access to video from private surveillance networks, such as retail and corporate facilities or even residential properties. This type of integration allows officials to respond

Case Study:

Surat, India

A "safe city" is a concept focused on providing a more secure municipality for residents, businesses, officials, first responders and tourists. As more residents flock to cities to embrace urban living, the task of providing a safe environment is both paramount and daunting. Surat, India, knows the challenges and pain points of a burgeoning population. In one of the first security projects of its kind in the region, Surat is embracing the safe city concept to provide a new level of situational awareness, paving the way for a more secure and connected municipality.

In Surat, the safe city concept is being spearheaded by the Gujarat state government. The project is an ongoing collaboration between multiple stakeholders and technology providers. Serving a population of approximately 4.4 million people in an area that encompasses nearly 126 square miles, Surat officials decided to invest in the safe city project to ensure the security of the area, while continuing to make it an attractive locale for businesses. In addition to its large population, the city has a high concentration of key industries, including diamonds (some 92 percent of the world's diamonds are cut and polished in Surat), textiles, engineering, and oil and gas.

Phase one of the project consisted of the specification and installation of more than 100 video surveillance cameras, which are used to monitor major traffic areas along critical entry and exit points in and around the city. Upcoming phases call for extending the video coverage in the city and increasing the number to events as they unfold, no matter where they occur.

Surveillance Analytics

With access to so much security video and data, municipalities can benefit from utilizing surveillance analytics solutions that generate actionable intelligence for faster, more effective responses. Integrated analytic applications can automatically pinpoint potential breaches, disorder and significant events, and can send alerts, whether from video sources or other sensors, to the appropriate people, departments and agencies. With this intelligent software, city officials can, for example, detect suspicious vehicles causing traffic obstacles or entering restricted areas, monitor crowds, and identify suspicious objects. Designed to address the specific safety and security requirements of towns and cities, surveillance analytics provide

of surveillance locations to more than 5,000.

A new central command center that includes a 280-foot video wall is used to monitor, aggregate and analyze multiple surveillance feeds. The solution includes citywide mapping and graphing capability and the ability to monitor and assess fire alarms and water levels. Evacuation and disaster recovery plans are also part of the project.

The surveillance system is managed by an enterprise-class video management solution and a physical security information management (PSIM) system, which includes video viewing and distribution, system health monitoring, and investigation management. The PSIM platform ties multiple subsystems together into a manageable solution that provides key parameters, alerts and other resources to enable operators to react more quickly. For command and control centers like the one in Surat, PSIM helps to reduce operational and planning costs while streamlining responses in an easy-to-use-and-interpret interface. Whether receiving feeds from across the street or from miles away, multiple users can view events, alerts and video, then assess the next steps.

> For command and control centers like the one in Surat, PSIM helps to reduce operational and planning costs while streamlining responses in an easy-to-use-and-interpret interface.

Integrating video surveillance into the local command and control center with PSIM software allows first responders in any city to have keen situational awareness that informs quick and effective responses.

the information needed to deter and manage potential threats.

Situation Intelligence

Today's PSIM solutions generate situational awareness from a variety of security, safety and facility management systems, including access control, intrusion, radar, border control and HVAC systems, as well as various other communications systems and public and private databases. PSIM solutions enable operators situated in different locations to share and analyze information to identify and respond to situations quickly and effectively. Facilitating system management across multiple agencies, PSIM solutions boost collaboration across the municipality and enhance situational awareness for faster emergency response. Together, municipal organizations can analyze the data gathered to address emerging security needs, enable regulatory compliance and enhance overall security operations.

Taking a comprehensive approach to city security, collaboration between government agencies, corporate enterprises and citizens is central to the success of a safe city project.

Audio Recording and Analytics

Advanced digital multimedia recording, retrieval and quality assurance solutions can also play a key role in ensuring public safety by enhancing the performance of emergency personnel and control room operations. Using these audio recording and analytics solutions, city officials can capture audio, video, text, telematics, maps and other data across a range of communications channels for improved performance, incident reconstruction, liability management and enhanced overall safety.

The combination of these advanced solutions simplifies management of enterprise systems and significantly improves situational awareness, emergency management and operational efficiency. Better still, citizens moving into municipal areas feel safer, encouraging new growth throughout the city.

Cyber Security a Priority

The growth in information technology across all sectors of society has presented a new challenge for homeland security. In fact, there are estimates that the average American is exposed to three times more information every day than in the 1980s. The shift toward social media as the primary mode of communication has resulted in new security challenges that can be difficult to manage. City officials must embrace new solutions to address a range of cyber threats, the most common of which is hacking. What makes this even more difficult is that these threats can come from large organizations or individuals on private networks at home.

Law enforcement and government agencies can use cyber intelligence solutions to intercept, monitor and analyze communications to uncover leads and neutralize terrorism and crime. These agencies can also share intercepted communications and intelligence with others in a collaborative effort to connect the dots in national and global investigations.

Another significant challenge that local agencies face is determining how to securely manage the vast amounts of data being shared across complex communications networks to effectively detect, investigate and neutralize criminal and terrorist threats. Designed to quickly make sense of complex scenarios, communications and cyber intelligence solutions readily handle vast amounts of data from a wide variety of sources and provide the tools needed to integrate and analyze information from multiple sources. More efficient collaboration between various agencies generates better evidence and enables more efficient and productive investigations.

> Timely and accurate sharing of all of this information is vital during disasters and emergencies. It can make the difference between a successful response and a failed one.

Collaborating to Protect People, Property and Assets

Comprehensive technology solutions, such as IP-based surveillance systems, video management software, intelligent analytics and PSIM software, combined with more advanced mobile video surveillance solutions will provide city officials with easier and more timely access to surveillance video and will help link data from disparate sources to create the most comprehensive picture of an event. The end result is greater situational awareness and better protection of citizens. By integrating surveillance, sophisticated data collection and analytics in the intelligence world, municipalities can identify threats earlier than ever before – or, at the very least, they can respond to and resolve incidents more quickly than would have otherwise been possible. More and more cities around the world are rolling out safe city initiatives in an effort to meet a range of modern challenges, from evolving communications media to homeland security concerns, and to enhance the safety of citizens and protect critical infrastructure, property and assets. ■

Back to TOC

Itai Elata is senior vice president, homeland security practice, video and situation intelligence solutions, at Verint Systems (www.verint.com). He can be reached at itai.elata@verint.com. ✉

Limiting access to some areas to certain personnel at specified times is the primary consideration in access control. To do this, a facility may incorporate some types of security hardware or control systems that require special interactions.

Integrating Card Access with Interlocking Door Controls

While there may be implementation challenges, interlocks can greatly enhance portal security

By **Bryan Sanderford**,
National Sales Manager
Dortronics Systems

Card access systems can be used with door interlock controls for enhanced security and, sometimes, for environmental cleanrooms. The focus here is on security, although most of the concepts can be applied to cleanroom interlocks.

Door Interlock Applications

An interlock application is a set of doors – two or more – set up so that a person enters the first door while the next door is closed and cannot pass through the next one until the first has closed. Casinos, for example, frequently utilize mantraps with card access to secure money counting areas. Many systems use an automated interlock control, with the card access system providing the request-for-access input on a valid card read. If the related doors are secure, the relay outputs of the interlock unlock the appropriate door following the access control relay for a time-delayed relock. These applications use both maglocks and strikes on each door. In the case of a power failure with maglocks deactivated, the doors remain locked by the strikes and are unlocked manually by key as needed.

One casino uses a card access system not to unlock the door, but, instead, to trigger an indicator light and sounder on the guard console, signaling an authorized request-for-access and switching a video monitor to view the door. The security guard then views the person by CCTV monitor before initiating door access from the console. Activation of the associated door release button triggers a request-for-access to the interlock controller, which unlocks the door only if the related doors are secure.

Armored car depots utilize a complex system of interlocks operated in conjunction with a card access system and a security guard at a console to control vehicles and personnel moving into, out of and within a facility. Truck bays are controlled with interlocks to limit access to the loading docks and segregate drivers from the inside personnel. Only the money enters the secure depot from the dock.

Credit card manufacturers and encoders are required to have some of the most sophisticated interlock controls available. The physical security specifications for these facilities incorporate card access plus pedestrian and vehicle interlocks similar to armored car depots. However, these systems also limit access in given areas to certain personnel and do not allow people from other groups into those areas at the same time. People counters and anti-tailgate controls are incorporated into these facilities as well. The security specifications for these facilities are very stringent and differ by credit card brand. As a result, the security system must be designed to the most secure conditions of each.

Military bases have recently installed automated gate controls as a result of budget cutbacks. These projects allow for reductions in manned presence and the ability to control entry and exit from a remote location.

Military bases have recently installed automated gate controls as a result of budget cutbacks. These projects allow for reductions in manned presence and the ability to control entry and exit from a remote location. One system uses card access controls, arm gates with truck barriers, and sliding fence gates. The interlock system allows only one vehicle to enter or exit at a time. LED traffic lights advise personnel when their credentials are accepted and when the vehicle trap is cleared for passage. CCTV and remote overrides allow for high volume and extra secure operations.

High security interlocks are installed at sensitive compartmented information facilities (SCIF), such as encrypted transmission facilities. These incorporate card access, CCTV, EMF

shielding and special doors and frames with inflating gasket seals. Some also require custom timing functions and sequenced operations. Since these projects incorporate unique features, the access control system is frequently mated with a door interlock control.

Door interlocks and card access are being used in courthouses and police stations to control access into judges' chambers and prisoner holding areas. The detention areas may also include a sally port interlock with card readers to bring prisoners into the jail. Prison facilities have unique requirements, and contractors that specialize in these types of projects often use card access with special interlock controls made for these types of buildings.

Card access controls with door interlocks are frequently used for cleanroom applications, including electronics manufacturing and biomedical laboratories. For contamination control, sensitive areas may require the security of doors with card readers and interlock controls with automated door openers.

> Except in government facilities, life safety codes and the local building inspector have the final say on the types of locking devices that may be used.

Interfacing with Special Security Devices

Limiting access to some areas to certain personnel at specified times is the primary consideration in access control. To do this, a facility may incorporate some types of security hardware or control systems that require special interactions.

When a card access system is used with a door interlock controller, the lock control relay of the access control should be used as a request-for-access input of the interlock. When a card is validated, the lock relay is activated for a preset time or until the door is opened. If the related doors are secure, the interlock will unlock the door following the request-for-access input. Multiple requests-for-access should be held pending while the first door is accessed. This can result in false

audit trail entries or lock some users out if anti-pass back is in use. Some access control software is able to track the door opening and disregard the valid card read, but, if this is not possible, one may want to use an additional output of the interlock to disable the card reader while the door is inhibited. Similarly, the card access request-to-exit device can also be inhibited to eliminate pending door access requests.

All card access systems require a door status input, as does the programmable logic controller (PLC) interlock controller, and both systems cannot share the same door switch contact. There are two ways around this: either use two door position switches or use a DPDT switch to isolate the two system circuits. To save wiring, it may be easier to "mirror" the door switch through a PLC relay output for the access control system.

Life Safety Considerations

Except in government facilities, life safety codes and the local building inspector have the final say on the types of locking devices that may be used. One project with card access and interlocks was allowed to have locks on controlled doors only if they also used a National Fire Protection Association (NFPA)-compliant delayed egress control. The doors were secured and released through the interlock controller, but an exit was always allowed by the delayed egress system to override the card-controlled interlock. While many "smart" door control systems could have performed the emergency egress function, the codes required an NFPA control for this operation.

Most door interlock systems incorporate one or more emergency unlock options. These may be necessary to reach an incapacitated person inside a locked area or, more commonly, in the event of a door switch failure or a door closer that does not fully close the door. If the door status switch does not report the door as being fully closed, then the controller will not unlock any related door. When failsafe locking hardware is used, the lock power supply system can be tied into the fire alarm.

Small mantrap systems may use strategically located emergency door release stations to trigger the FAR interface of the power supply. Larger interlock systems will incorporate multiple emergency release stations to unlock just the related doors in the area. Another option is to disable the door interlock feature but not actually unlock any locked doors, allowing the card access system to continue to limit access but also allowing multiple door openings. This can be a feature of the PLC interlock program. Emergency release stations may be similar to the fire alarm pull – they may be any color but red – or a push-pull button with or without the key reset. Sometimes, momentary push buttons are used to trigger an emergency unlock, and a single reset button is used to return the operation to normal. Indicator lights and/or sounders are effective in communicating the system status to facility personnel.

> Since the locking door hardware on new construction may be specified and supplied by a contractor other than the security integrator, one must verify that the hardware will function with the access control and interlock equipment as required.

Specifying the Interlock Design

The design of a card-controlled interlock system is specified in the door schedule with notations on the floor plan and a door matrix indicating the door relationships. A simple interlock operation can be described as "if door-1 is unsecure, then lock and inhibit door-2 and door-3." If the required operation is complex, a more detailed description of the interlock operation is required.

Both the card access system and the interlock controller must be compatible with the door hardware specified. Since the locking door hardware on new construction may be specified and supplied by a contractor other than the security integrator, one must verify that the hardware will function with the access control and interlock equipment as required. The voltage and power needed for the electrified hardware that will be controlled by the security system should also be checked.

Conclusion

Card access interlocks for security or cleanroom portals can represent a challenge. For both applications, which involve the integration of card readers, interlock controls, electric door hardware, status indicators, remote consoles, alarms, and process controllers, the challenges center on the compatibility of power requirements and the connectivity of shared controlled devices.

Finally, the system design must adhere to all applicable local and national building codes, as well as any special environmental requirements that apply to cleanroom projects. ■

Back to TOC

Bryan Sanderford is national sales manager for Dortronics Systems (www.dortronics.com). He can be reached at bryan@dortronics.com.

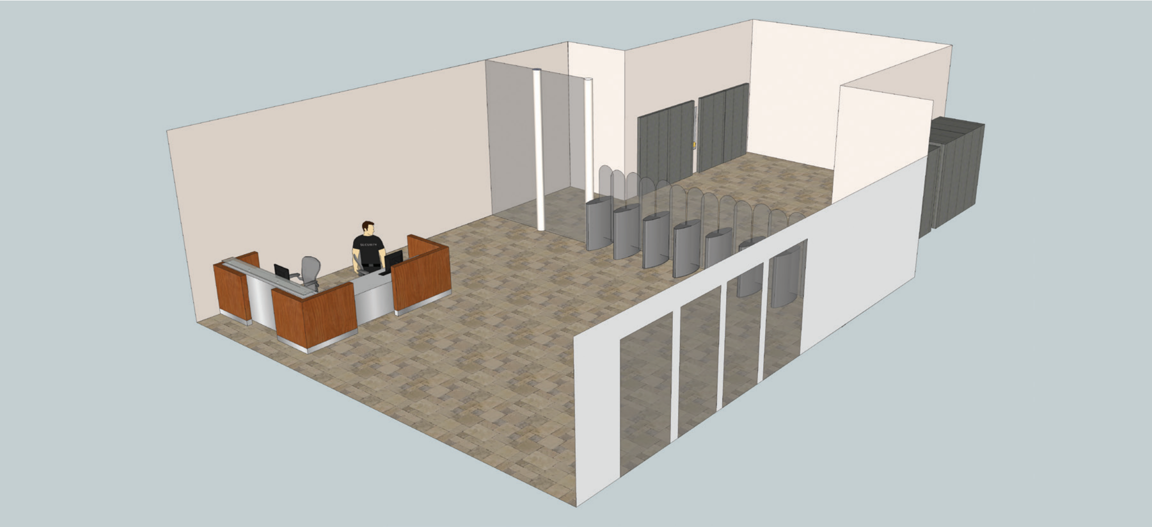
We are seeing an entire high-rise office building becoming far more secure than in times past, with layers of security within.

More Security, From Bottom to Top

Buildings are increasing entrance controls on the main floor and upstairs

By **Tracie Thomas**,
Marketing Manager
Boon Edam

Since the terrorist attacks of 9/11, the demand for physical security products to control entrances (turnstiles, security revolving doors and mantrap portals) has continued to grow across many verticals. Installations of turnstiles and security doors have increased in both single and multi-tenant "Class A" office buildings – the most prestigious buildings with the most features and amenities – and corporate and government offices and campuses. There have also been increased installations in recent years at universities, infrastructure facilities (e.g., utilities, gas/oil), data centers and airports (with federal support of security staffing being reduced). Finally, with the recent active shooter incidents in K-12 schools, movie theaters and shopping malls, there are new verticals that are searching for security technology. So just about everywhere, building owners are gravitating toward physical security solutions.



Lobbies with turnstiles offer a moderate level of security and require some degree of supervision.

Emerging Trend in Class A Office Buildings

In the past three years, there has been a shift in monitoring and tracking technology combined with physical security installations in Class A office buildings. When you think of a Class A office building, whether single or multi-tenant, do you envision a lobby with security guards or a receptionist desk and optical turnstiles to allow access to the elevators? If so, then you are describing what has been the status quo since optical turnstiles entered the marketplace in the 1990s. And this is still the most common solution for Class A office buildings. But here is what we are starting to see:

- The *level of security* is increasing on the ground floor. This means that higher security capabilities are being requested than what is typically provided by optical turnstiles.
- Physical security solutions are being installed in upper levels of the building, in addition to the ground floor.

Overall, we are seeing an entire high-rise office building becoming far more secure than in times past, with layers of security within. To use a term from the data center industry, Class A office buildings are "hardening the core."

> When we talk about the level of security, we are talking about the ability to control physical passage by users in and out of a secured area.

What is 'Level of Security?'

When we talk about the level of security, we are talking about the ability to control physical passage by users in and out of a secured area. We break this ability down into three levels based on the ability to detect, deter, delay and prevent crime as follows.

Low – Monitoring or Controlling Traffic

This is just "keeping honest people honest." Upon authorization, users are forced to be deliberate and, in some cases, are slowed by a physical barrier, such as a waist-high turnstile or a gate. This situation requires supervision at all times because the purely physical operation of the barriers can be defeated by either jumping, climbing, tailgating or piggybacking. The benefits of a low level of security are primarily very high throughput and crowd control, such as at a museum, stadium, mass transit system, etc. The role of supervision is to prevent or quickly respond to attempts to defeat the barriers.

> As the level of security increases, the amount of supervision required decreases, which offers a financial benefit in addition to the operational one.

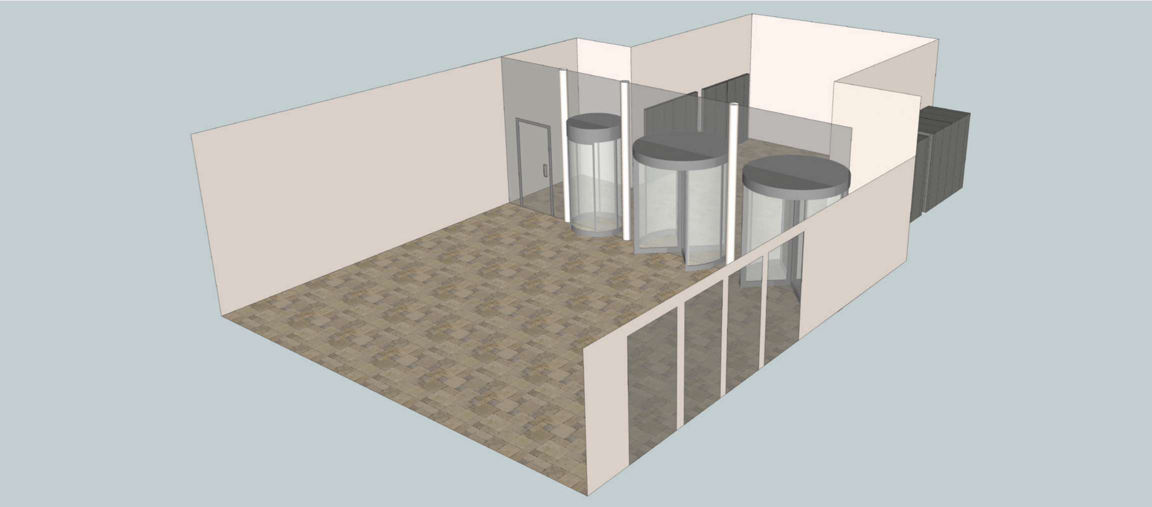
Medium – Tailgating/Piggybacking Detection

This involves a high level of detection, a physical deterrent, and a moderate level of physical prevention. A turnstile, typically an optical turnstile, has sensors installed that will sound an alarm when tailgating occurs. This level of security allows for supervision to be at a further distance and may require fewer supervisors. However, it should be clear how the supervisor would respond when tailgating occurs. Is anyone else notified to confront the tailgater? Do cameras zoom in to identify the users in the area?

High – Tailgating/Piggybacking Prevention

This provides for a very high level of detection discrimination and a very high level of physical prevention. The design and operation of the equipment makes tailgating or piggybacking extremely difficult or, even, impossible. Examples of such products are security revolving doors and security mantrap portals. No supervision is needed, but cameras are almost always used for monitoring in case of suspicious loitering nearby.

Thus, we have three levels of security: monitoring traffic, detecting tailgating and preventing tailgating. As the level of security increases, the amount of supervision required decreases, which offers a financial benefit in addition to the operational one. In addition, this also mitigates physical violence opportunities, enhances loss prevention, and provides superior evidence collection capabilities.



Lobbies with security revolving doors and/or mantrap portals require no supervision.

Increasing Security in the Lobby

Let's take a look at what is happening in the lobby areas of Class A office buildings. We are seeing a shift from low and medium levels of security, such as mechanical and optical turnstiles that require supervision, to the highest level of security provided by security revolving doors, which do not require any supervision. Visitors can be greeted and provided with a pass at the "front" of the building, then proceed through the revolving door, while employees can enter other sides of the building via security revolving doors without any supervision. What is the payoff for doing this? High crime deterrence on all sides of the building and in the lobby. Trends indicate that downtown areas that are targeted for socio-economic revitalization enjoy the greatest benefits, including:

- No tailgating or piggybacking
- Ability to know who is in the building at all times, improving mustering capabilities and loss prevention.
- Smaller staff needed to supervise and respond
- Energy savings from reduced air infiltration

How about throughput? Security revolving doors allow up to 24 people per minute in each direction simultaneously or up to 48 people per minute in both directions combined. Optical turnstiles with barriers hover at around 30-36 people per minute in both directions combined. When undertaking throughput analysis, it is vital to estimate peak throughput needs for shift changes and the building occupancy capacity in order to ensure the installation of the appropriate number of doors.

What about cost? A security revolving door provides for two lanes of simultaneous traffic in and out. To accomplish the same throughput with optical turnstiles, it would require two optical turnstile lanes (either three or four cabinets). The cost of having two optical turnstiles installed is about equal to having a single security revolving door. However, if security staff is reduced or reallocated, that provides an additional ROI with the deployment of security revolving doors. With optical turnstiles, the need for supervision is constant.

How about the need to train thousands of employees on how to use the security revolving door? The same training protocol and learning curve applies to a security revolving door as to an optical turnstile, and in most cases, it is even simpler. While the operation of a security revolving door is more sophisticated than an optical turnstile, employees and visitors can be trained on proper use very quickly. For a new building or renovation, employees can be trained via staff meetings with video demonstrations and discussion. On opening day, volunteer "ambassadors" can stand by to assist if needed.

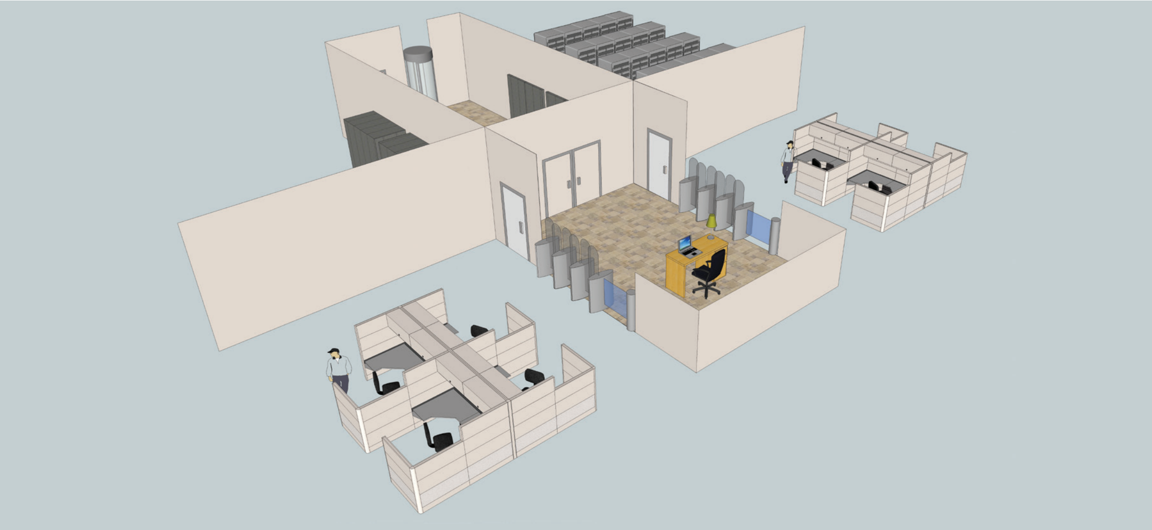
Full-height turnstiles, revolving doors and mantrap portals are being installed right outside the elevator banks on certain floors to prevent access by unauthorized personnel.

What about a fire alarm situation? The door wings of a security revolving door automatically unlock during a fire alarm and will either freely rotate or collapse to create an opening. Local codes also require egress doors within 10 feet of the revolving doors to comply with National Fire Protection Association (NFPA) requirements. These adjacent egress doors are typically alarmed and are set for delayed access, if allowed.

Introducing Physical Security Upstairs

For several decades, installations of doors and turnstiles have been primarily on the ground floors of buildings. Once users were granted access to the elevators, they could access any floor. This is changing, especially in multi-tenant buildings, but also in single-tenant facilities. Full-height turnstiles, revolving doors and mantrap portals are being installed right outside the elevator banks on certain floors to prevent access by unauthorized personnel. A few reasons for this are:

- To protect highly sensitive information housed on certain floors
- To protect all employees, especially executives, from crime and solicitors
- To offer employee-only access to certain floors in leased buildings that are shared by multiple companies; this is often the case when the building owner or manager is reluctant to place physical security in



Some long-term tenants in high-rise buildings are adding optical turnstiles and gates near the elevators on upper floors, along with a receptionist, to manage visitors.

the lobby (for cost, aesthetic or space reasons) but is willing to accommodate long-term tenants on certain floors

- To provide a simpler solution than having elevator access cards, visitor passes or keys for certain floors, and to address challenges created by the difficulty of monitoring stairwells

These upstairs installations typically prevent unauthorized entry onto the entire floor or part of the floor. We will take a look at a few scenarios and explain some of the reasons why certain solutions were selected.

One company wanted its employees and visitors to check in with a reception desk before being allowed to enter the secure work area. Because the area would be supervised, they chose optical turnstiles, as well as an ADA-compliant gate to allow for passage of wheelchairs or large packages. The driving factors for deploying this solution were aesthetics and feel. Optical turnstiles with waist-high glass tend to provide a more open, unobtrusive and welcoming environment.

Another company installed security mantrap portals on the fifth floor of a building that they completely owned and occupied to protect sensitive data. Now, only certain employees can enter this floor by swiping a badge to open the first door. Overhead sensors and high-tech cameras scan the portal with near-infrared to create a 3D image and confirm that the employee seeking access is alone. This is a two-tier authorization verification design, and the employee must confirm his or her identity with an iris scan before the second door opens. The small number of employees on this floor justifies the slower operation of the portal (about five to eight people per minute).

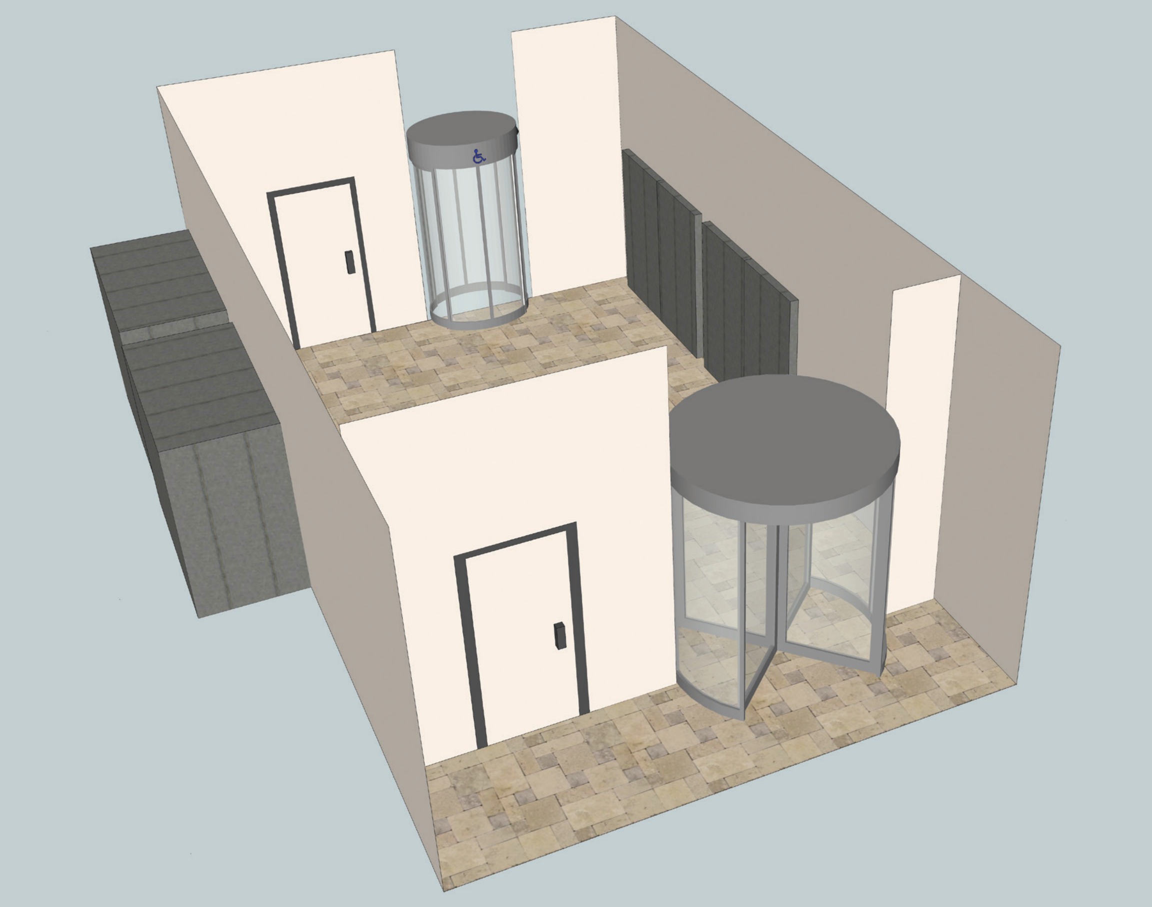
Since a mantrap portal can operate without supervision, there is no need for a receptionist or guard, so the initial investment is recouped in about a year.

Deploying high security solutions that do not sacrifice throughput, safety or comfort is becoming more and more common. The ability to accomplish this while enhancing fire mustering capabilities, loss prevention and violence risk mitigation is driving the trend. Tenants and owners alike are also recognizing the financial benefits of being able to reduce manning. Improving and complementing human capabilities with new technologies, and providing an ROI justification for a higher upfront investment, will continue to encourage conversions to more secure entrances. ■

Back to TOC

Tracie Thomas is marketing manager for Boon Edam (www.boonedam.us). She can be reached at tracie.thomas@boonedam.us. ✉

Some companies are starting to install security revolving doors and mantrap portals near the elevators on upper floors to protect employees or restrict access to sensitive data.



No badge hanging around your neck, no digging in your bag for ID, no presenting credentials to a reader or stopping in front of a camera. Just walk into a controlled space without having to do anything special.

Frictionless Access Control: A Look over the Horizon

New uses of biometric and RFID technologies could make access badges obsolete

By **Henry Hoyne**,
Vice President
Northland Controls

The Holy Grail for the global security director is to know who is in the building, and to be assured that they belong there. Thus, the nascent drive toward "frictionless access" is seemingly counter-intuitive. The idea is to permit access to an area without interfering with the user's experience, to make it as natural – as "frictionless" – as possible. No badge hanging around your neck, no digging in your bag for ID, no presenting credentials to a reader or stopping in front of a camera. Just walk into a controlled space without having to do anything special.

There is an employee recruitment competition at many organizations that comes down to, "My environment is more conducive to your lifestyle than theirs, so you should work here instead of there." Lanyards, badges and readers have increasingly entered these organizations' cross-hairs. These "stinking badges" get in the way of a free-thinking, free-flowing and collaborative work environment, critics say. The director who wants to know who is in the building and if they

belong there is now being asked to get rid of high-friction badge presentation processes as soon as possible.

Current thinking around frictionless access includes:

- Long-range biometrics. The door is secured, but I can see you coming and will unsecure it before you get to it.
- Short-range radio frequency technology. The door is secured, but I can sense your valid RF device and unsecure the door fast enough for you not to know it.
- Security by exception. Full-time tracking of a wearable device. The door is unsecured until a non-compliant person is sensed, at which time it is automatically secured. The wearable device uses a combination of biometric and RF technology.

> These "stinking badges" get in the way of a free-thinking, free-flowing and collaborative work environment, critics say.

Long-Range Biometrics

The most common current approach to long-range biometrics involves facial recognition technology. The simplest deployments use off-the-shelf video cameras with software analytics to reference persons entering the field of view against a database. This works reasonably well at locations with a limited number of people entering and exiting the facility. However, as the population for a given facility or environment goes up, the technology cannot keep up with the required throughput.

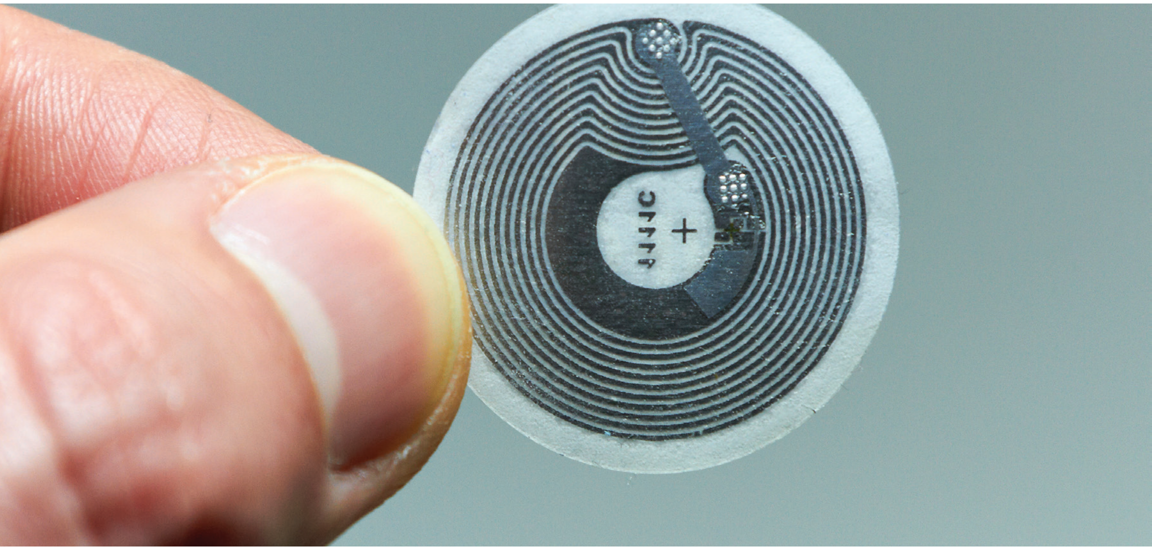
If only 25 people need access to

a facility, the technology can easily handle this load with a 100 percent success rate. As the number of people goes up to, say, 1,000, though, a success rate even as high as 92 percent becomes unacceptable, since 80 people will either be incorrectly allowed access or incorrectly denied access. In addition, the "friction" created by those failures will create backups, affecting many more people.

More sophisticated technologies use 3D facial modeling. These tend to be significantly more expensive, larger and, potentially, more error-prone. However, extensive research and development is continuing on improving this technology. Considerable work is still needed, though, to achieve the accuracy, reliability and miniaturization needed for it to be truly effective in high-volume throughput applications.

For high security areas, facial

As the sophistication of antennas increases and the correlation with mapping software improves, RFID tags may play an important role in the evolution of frictionless access.



recognition "who-you-are" technology could be enhanced with voice recognition "what-you-know" codes. Since such areas tend to have relatively low throughput, dual authentication at the entrance would be fairly expedient, though not completely frictionless.

Short-Range Radio Frequency Technology

Short-range RF technology is able to identify a person or device carrying either a passive or active RF transmitter. These transmitters can be the size of a quarter or a typical ID badge. When the person or device is in range of a receiver antenna, the system can validate the authorization related to the tag and grant access.

RFID tags have been shown to work well under constrained conditions. However, to increase the accuracy of a system, many more antennas are needed. The antennas usually are only 4x4 inches and can be unobtrusively placed, but the positioning and quantity needed to make the system effective can become a maintenance and support issue. Without a wide enough distribution of antennas, it is difficult to determine if a tag is coming or going, whether it is on the other side of a wall, and which access point in a corridor full of access points is the appropriate one to unlock. Nonetheless, as the sophistication of antennas increases and the correlation with mapping software improves, RFID tags may play an important role in the evolution of frictionless access.

In addition, as smart phones have become ubiquitous, they may simplify the process by transmitting RF signals themselves and making separate tags unnecessary.

Security by Exception

Security by exception combines features of RF technology and biometrics. A smart device would be RF-enabled and would have a real-time view of a biometric feature such as an iris, finger or voice print. An enormous amount of data would be generated, and the system would be able to create a map of every single person in a building, which floor they are on, and what secured areas they are near.

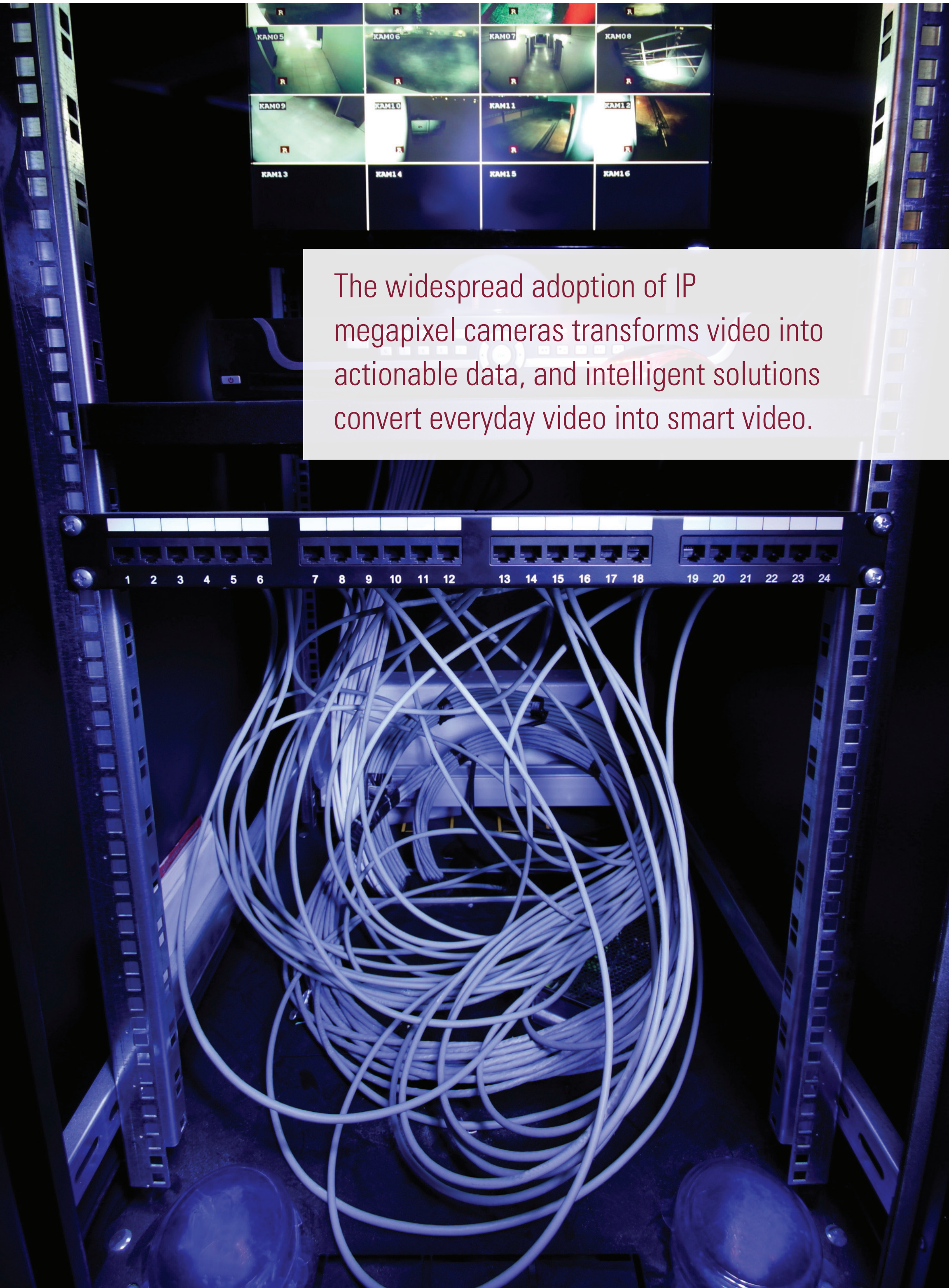
This would go beyond the security director's dream of knowing who is in the building and being assured that they belong there to also include information about each person's exact location. Since, in most commercial and industrial settings, people know where they belong and are simply moving around to perform their responsibilities, a majority of controlled access points could simply be unlocked at all times. When the system senses a person who is not authorized for a particular area approaching an access point, it could send a warning and immediately secure the door.

Thus, rather than constantly granting access to people who belong, the system will manage access by exception, locking the door when someone should not be there. This will be further reinforced through social engineering. A locked door will suddenly inconvenience a number of people who will immediately become aware that something is amiss, that someone in their midst does not belong. This sudden friction will be unacceptable to staff who have become accustomed to the new paradigm. They will put extraordinary pressure on people who breach areas where they do not belong and discourage them from causing such problems again. They will also put pressure on the security and IT departments that provide and support this new ecosystem. The reliability and accuracy of the system will be paramount.

> Rather than constantly granting access to people who belong, the system will manage access by exception, locking the door when someone should not be there.

Individual aspects of the technology needed to make security by exception work exist today. Progress will be made to integrate the technologies and make them faster, smaller and more reliable. As smart devices and "big data" have disrupted how we live our lives today, security by exception will dramatically alter the access control landscape and our awareness of who is in and around secure areas. ■ **Back to TOC**

Henry Hoyne is vice president of professional services for Northland Controls (www.northlandcontrols.com). He can be reached at hhoyne@northlandcontrols.com. ✉



The widespread adoption of IP megapixel cameras transforms video into actionable data, and intelligent solutions convert everyday video into smart video.

Harnessing the Increasing Power of Video

New functionalities and greater ease of use enhance the value of video in both security and non-security applications

By **Mike Scirica**,
President
WavestoreUSA

Video surveillance data is more valuable than ever. The use of video is moving far beyond cost-oriented security applications and toward use in revenue-producing business functions, such as optimizing staff sizes, providing customer service training and analyzing buying patterns. The widespread adoption of IP megapixel cameras transforms video into actionable data, and intelligent solutions convert everyday video into smart video.

The impact of these new applications on video management software (VMS) and video recording systems is dramatic. A demand for more detailed image quality increases requirements for robust video management solutions to manage and sort rich data streams. Today, the role of VMS and recording solutions is to help the user take advantage of the video they are capturing.

In today's crowded VMS market, users and systems integrators need to be savvy regarding which solutions work for a specific market application. This article looks at what features

users are demanding and how integrators can best meet those needs by deploying platforms with new functionalities.

Intuitive Options

Consumer electronics have set the standard for ease of use. Getting a new smartphone up and running is a simple process, thanks to the intuitive operations built into the device.

Now this trend is crossing over into the physical security video surveillance arena, and similar intuitive interfaces are available with today's VMS solutions. In recent years, the industry has moved forward with building solutions (even beyond VMS) that are intuitive, user-friendly, open and scalable. In a world in which security personnel are being asked to do more with less, ease of use is key to intelligent security operations.

The use of 360-degree cameras takes it a step further, reducing the total number of cameras required (each 360-degree device replaces up to eight standard cameras), improving aesthetics, reducing system complexity and simplifying documentation of incidents.

A Broader View

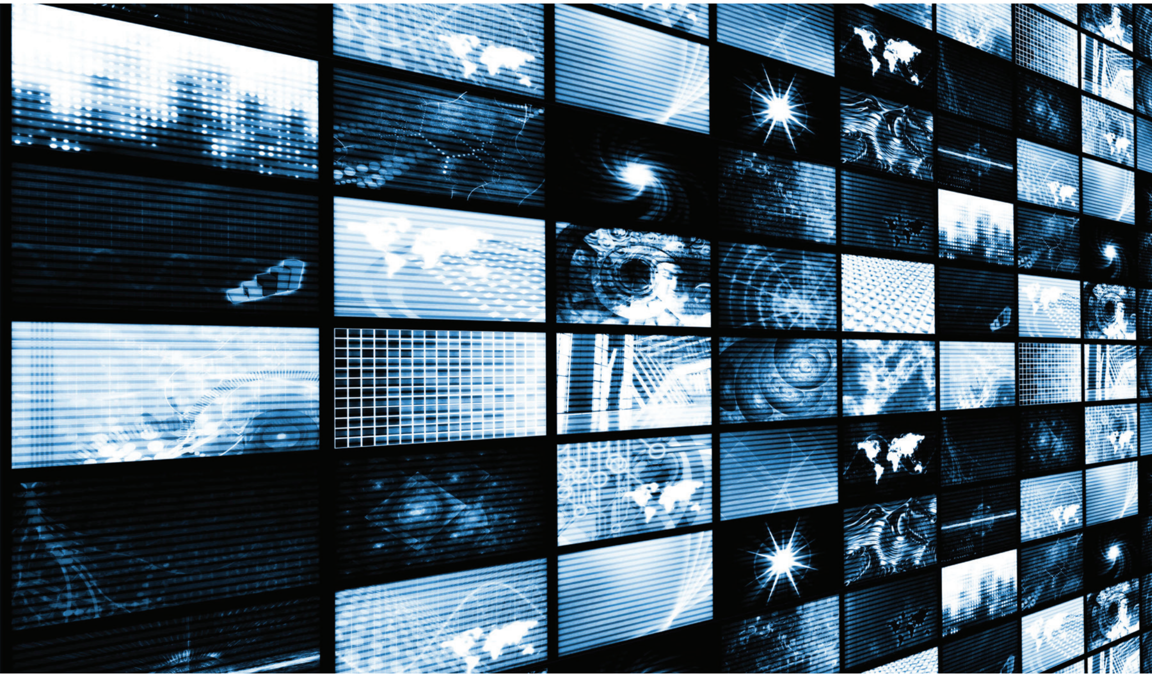
Support of high-definition (HD) video cameras increases coverage and enables better detection and resolution of security issues. The use of 360-degree cameras takes it a step further, reducing the total number of cameras required (each 360-degree device replaces up to eight standard cameras), improving aesthetics, reducing system complexity and simplifying documentation of incidents.

Being able to manage a workforce, a network or a physical technology platform from a remote location is no longer a preference, it is a requirement.

The adoption of fisheye and 360-degree cameras continues to increase as users find new levels of value in the deployment of such edge devices for wide-area surveillance. According to a recent report from IHS, the worldwide market for video surveillance equipment is expected to expand by more than 12 percent this year, to $15.9 billion, up from $14.1 billion in 2013. IHS notes that growth in the video surveillance market will be led by strong demand for fixed-dome and 180/360-degree network camera products.

With the growing demand for hemispheric cameras, there is an increasing need for unique software capabilities to take full advantage of these devices. Fisheye or hemispheric cameras are optimized with the use of a VMS or network video recorder (NVR) with

Continued on page 66



Case Study:

Burlington Coat Factory

Burlington Coat Factory sought to upgrade its video surveillance capabilities to address shrinkage in stores and to provide a video platform for marketing, operations and safety. The existing video equipment, which was 10 to 15 years old, was unreliable and subject to frequent downtime.

This was one of several significant measures that the company employed to address shortage issues in stores. It also upgraded its electronic article surveillance (EAS) systems, implemented new detection systems and expanded in-store burglar alarms.

A compressed time frame required installation over five months at 159 locations across the entire company footprint, from Puerto Rico to Alaska. Old equipment had to remain in place until the new technology was fully functional, and existing equipment had to be removed carefully because the company planned to use it at other locations.

A New IP System

The cameras selected included 360-degree fisheye cameras and fixed mini domes. The 360-degree cameras cover large areas and allow the use of fewer cameras. At each register area, 360-degree low-profile domes are installed no higher than 10 feet from the floor, uniformly for visual appeal, to achieve the best

image quality. Each retail aisle has a 360-degree dome camera installed slightly higher to provide a broader view. One 360-degree camera can view an area that previously required eight cameras.

A wide dynamic range dome provides complete coverage at the entrance of each store. Select stores also have 360-degree cameras outside the main entrance or at the corner of the building to monitor the parking lot, as well as cameras at the back of the building to cover the dock or employee entrance.

With its new VMS platform, Burlington Coat Factory is able to operate and use its video surveillance system in a more effective way, which allows the company to focus on generating more revenue.

The VMS platform includes a built-in dewarping feature to allow the company to create dewarped images from the 360-degree fisheye cameras. New images can be dewarped on the fly, and dewarped images appear as separate camera feeds in the VMS and provide evidentiary support.

The VMS platform is based on a robust Linux-based OS featuring simple operation to enable the end user to view live video, play back video, dewarp images and create clips from a single interface. The open standards platform enables user-friendly remote video viewing, which is operated easily even by inexperienced users with minimal training.

A wireless interface enables remote viewing at workstations located at store entrances. The network allows for remote access by regional and corporate loss prevention teams and select staff members. Store operations and design teams can also access camera feeds. Modularity makes it easy to relocate and expand the system to adapt to the changing retail landscape.

With its new VMS platform, Burlington Coat Factory is able to operate and use its video surveillance system in a more effective way, which allows the company to focus on generating more revenue.

Quantifiable Results

The new surveillance equipment has helped Burlington Coat Factory decrease its shrinkage, in some cases, by more than 90 percent. In several instances, the video images enabled loss prevention staff to see the details of thefts and the perpetrators with perfect clarity, leaving no doubt of criminal intent.

Continued from page 63

built-in dewarping capabilities, which, put simply, allows the user to view images without distortion. This feature simultaneously displays multiple dewarped images from a single hemispheric camera stream, while a virtual pan-tilt-zoom (PTZ) function allows operators to view enlarged portions of the total image. The software receives and stores only the original 360-degree stream, which is very bandwidth and storage efficient, while ensuring video can be presented and verified in a court of law. When played back via the client, the operator can display multiple dewarped images, regardless of whether the virtual views were created previously.

Remote Access

The video surveillance market moves rapidly, and so do user expectations and requirements. Being able to manage a workforce, a network or a physical technology platform from a remote location is no longer a preference, it is a requirement. VMS platforms, video recorders and storage appliances have to offer remote management options to help users keep up with their own fast-moving internal initiatives. For integrators, the ability to tap into a system remotely to troubleshoot issues limits the need for travel and allows the user to receive quick resolution of any problems.

Centralized management of systems is key to scaling. VMS platforms must offer extensive remote capabilities, such as configuration of server/recorders, cameras, and accessories; management tools; supervision of system health; and software upgrades. Cloud storage of incidents (small video clips, high priority alarms) provides additional backup to high-resolution recording on the premises.

Get Current, Stay Current

The emergence of IP-based systems drives the need for training. Resellers with a strong level of IT expertise will benefit from streamlined deployment and troubleshooting. Those without internal IT support will have to invest in hiring personnel who have experience with IP technologies or participate in training programs to enhance their skill sets.

> As more vendors incorporate industry specifications and standards, end users and integrators are provided with more technology options and flexibility than were previously possible.

The rapid evolution of technology means that integrators must move quickly up the learning curve. As new technologies are released, it is critical that manufacturers stay in constant communication and provide robust education and training options. These offerings are paramount to both parties' success and to effective implementations of security solutions.

IT-friendly architecture provides options for budget-conscious users who rely on IT infrastructure. When systems integrators can deliver IT expertise coupled with physical security, a user experiences the best of both worlds. Integrators can then demonstrate ideal camera placement while maximizing existing infrastructure to reduce deployment and management costs.

'Open' for Business

Since the launch of open standards organizations, the security market has been focused on standards-based systems. As more vendors incorporate industry specifications and standards, end users and integrators are provided with more technology options and flexibility than were previously possible.

By specifying standards-based VMS and video storage platforms, integrators can offer end users a broad range of options so they can find the hardware that works best for them.

Overall, open architecture hardware and software designs support a wide range of cameras and encoders, and also support analog and network cameras to allow the integrator to build a best-in-class solution to meet the specific needs of the client.

Looking Beyond Security

Users demand that VMS systems easily integrate with both security and non-security functions, such as video analytics, point-of-sale and business management. By choosing a system that is built on open architecture, integrators can deliver VMS platforms that will be able to work with other systems as business and security needs grow.

There are many opportunities to combine new devices with existing technology to ensure investment protection. And as new innovations, such as video analytics and physical security information management (PSIM) systems, become proven in real-world applications, integrators familiar with the benefits of unifying systems will be able to better respond to customer needs. ■

Back to TOC

Mike Scirica is president of WavestoreUSA (www.wavestoreusa.com). He can be reached at mscirica@wavestoreusa.com. ✉

securityindustry.org/techinsights

Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700