AI? AI. Oh.
Artificial intelligence comes to security

A PoE Story
Using Power over Ethernet for access control

On the Wings of a Robot
Drones could transform surveillance

SIA TECHNOLOGY Insights

Volume 5, Issue 1
Spring 2017

Welcome

Dear Reader,

In the four years that the Security Industry Association has been publishing *SIA Technology Insights*, each edition has demonstrated how much and how rapidly the security industry is changing.

In this edition, for example, we can read about the security capabilities of drones, the role of artificial intelligence in security, and biometric technologies that include such advanced modalities as voice recognition and gait analysis. Even the articles about more "traditional" aspects of physical security, such as video surveillance, access control and intrusion detection, are vastly different than what would have been written a few years ago and feature analyses of how IT connections, mobility, analytics and comprehensive integration are turning devices into powerful security solutions.

As always, our goal with this publication is to provide security professionals with information that will help them deploy the most effective systems for their enterprise, business, facility or institution. And we hope that people within the industry will find it useful, as well, to learn about new technologies that are outside their field, but could have the potential to complement what they are doing.

Whatever role you're in – whether end user, manufacturer, integrator or anything else – we encourage you to let us know what you think of the publication by contacting the editor, Ron Hawkins, at rhawkins@securityindustry.org. And remember that you can read and share this issue and all previous ones online at www.securityindustry.org/techinsights.

Thank you for reading.

Sincerely,

Denis Hébert
Chairman
Security Industry Association

Don Erickson

Don Erickson
CEO
Security Industry Association

How to Navigate Through the Magazine

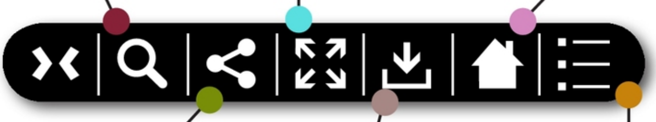
Navigation Bar

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

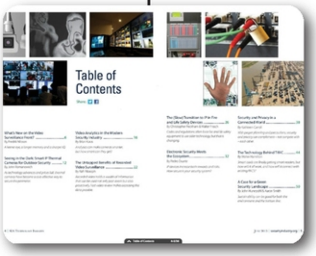
Click the fullscreen button to view page.

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

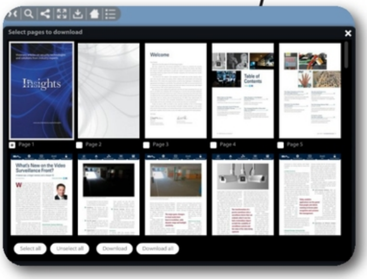
Click the search button to look for keywords.



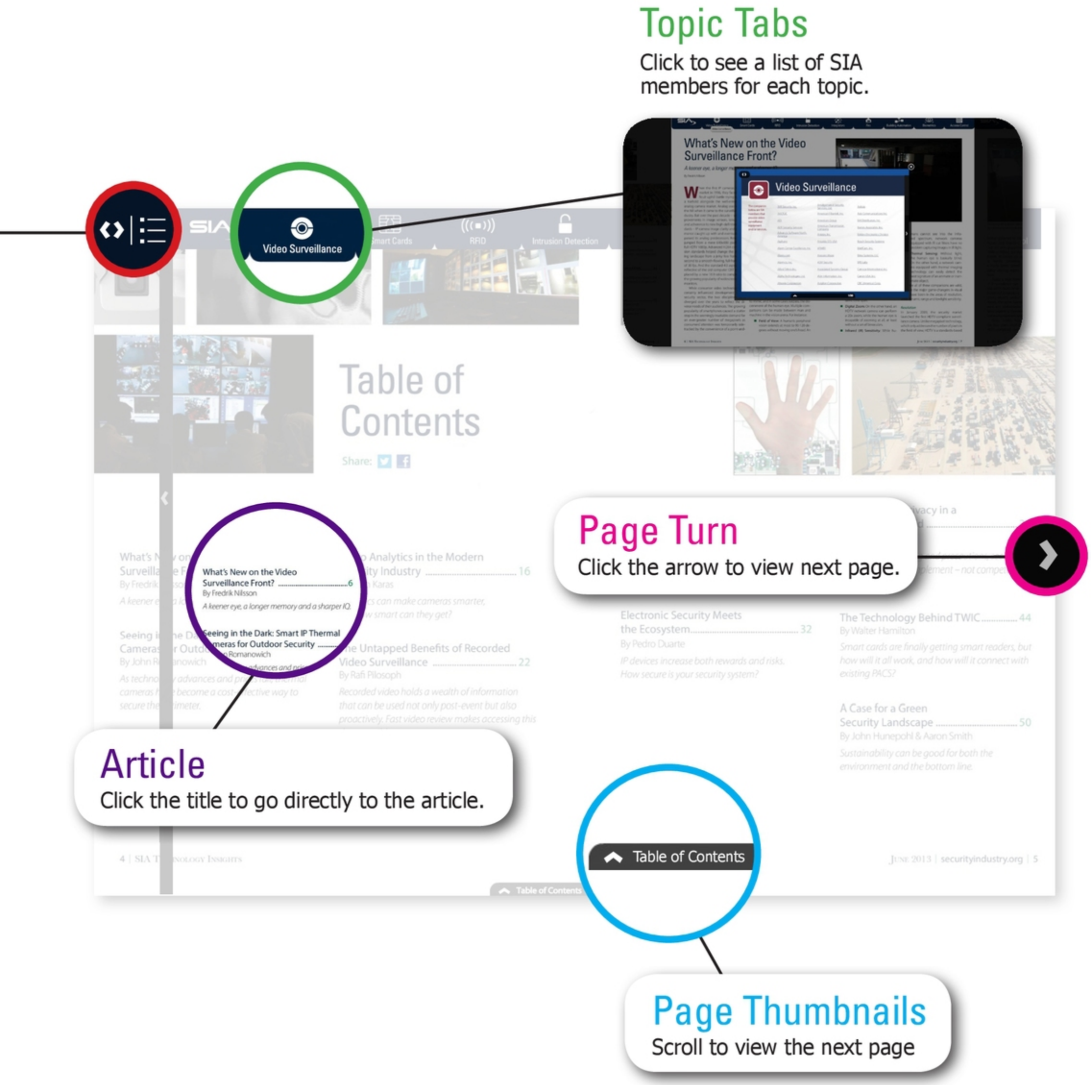
Click the share button to upload content on social networks or to email.



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



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


Video Surveillance
Smart Cards
RFID
Intrusion Detection
Table of Contents
Share:
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
By John Romanowich
Analytics in the Modern Security Industry 16
The Untapped Benefits of Recorded Video Surveillance 22
By Rafi Pilosoph
Electronic Security Meets the Ecosystem 32
By Pedro Duarte
The Technology Behind TWIC 44
By Walter Hamilton
A Case for a Green Security Landscape 50
By John Hunepohl & Aaron Smith
4 | SIA Technology Insights
June 2013 | securityindustry.org | 5

Topic Tabs

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

Page Turn

Click the arrow to view next page.

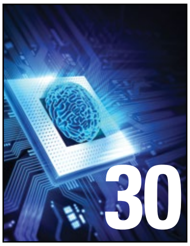
Article

Click the title to go directly to the article.

Page Thumbnails

Scroll to view the next page

Table of Contents



46

56

64

72

80

Interest in and adoption of cloud solutions has slowly started to happen, and it will eventually become the norm rather than the exception, especially as end users become more aware of what flexibility in the cloud means when it comes to physical security.

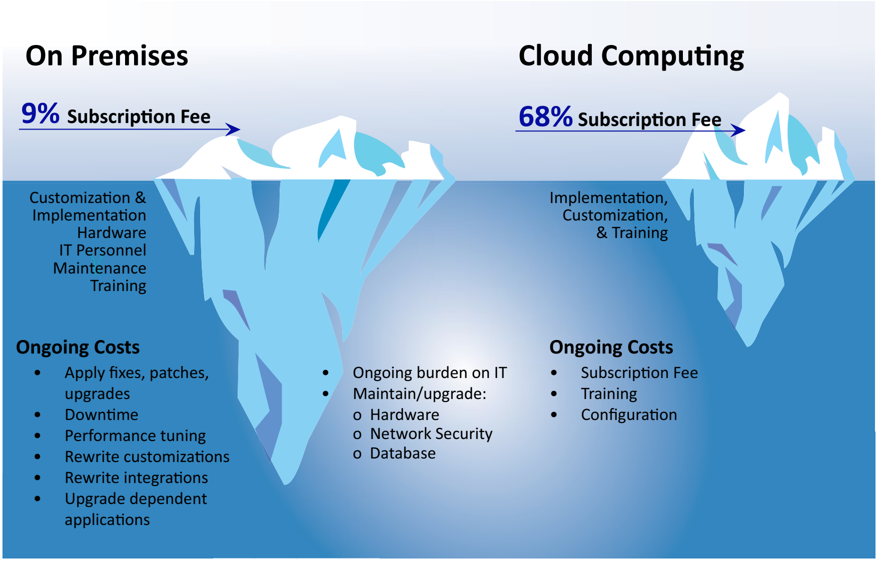
More than Just a Silver Lining

Using the cloud for access control enhances scalability, availability, resiliency, flexibility and security

By Denis Hébert
Feenics

The power of the public cloud has become a catalyst for a dramatic shift in the information systems and security worlds. On-premises solutions no longer exist in many domains, from customer relationship management to expense management to human resources systems to learning management. For example, more than 50 percent of enterprise resource planning installations are now being deployed as cloud-based services.

This phenomenon is the result of the substantial benefits afforded by cloud-based systems, such as scalability, availability, resiliency, true flexibility and strong security – all of which add up to a lower total cost of ownership. At the same time, this phenomenon has spawned the era of "as-a-service" business models, providing subscription-based alternatives to the traditional capital-intensive approach of business applications. As indicated in the accompanying diagram, the real cost of ownership for on-premises solutions is often not considered.



The security industry is not immune from this trend; in fact, it has been rather intimidated by it. Yet, interest in and adoption of cloud solutions has slowly started to happen, and it will eventually become the norm rather than the exception, especially as end users become more aware of what flexibility in the cloud means when it comes to physical security.

It should be noted that true cloud solutions do not simply mean the virtualization of the standard client/server architecture "parked" in someone else's data center and referring to itself as the cloud. True cloud-based applications are designed from the ground up as a cloud service and are hosted in a proven, secure public cloud infrastructure. This is an important distinction, as the only way to truly leverage the comprehensive benefits of a cloud service is to design for a cloud service from the very beginning.

Scalability

The traditional model of on-premises access control applications has been limited (at times artificially) to door counts or blocks (e.g., 32/64/128/256), labeling versions as lite, enterprise and so on. In most cases, this means greater hardware requirements for running the system, and if globalized for enterprise environments, it requires supplementary hardware to manage regions. For smaller systems, this implies onerous expenses for hardware, which is conceivably over-the-top and does not match the actual need. The more doors added as a system grows, the greater the hardware requirements to manage the data, polling, synchronization, reporting, operating locations and other core functionalities. Either way, organizations find themselves in the computer hardware management business.

Public cloud-based applications alter the scalability landscape. System size – and the ensuing scale required to manage it – becomes a function of subscription count; in other words, it is tied to usage. This elasticity of expense goes up and down easily, transparently and seamlessly. Orders of magnitude become irrelevant, since the cloud absorbs load based on its horizontal scalability and load balancing. When it comes to access control, this means that organizations can increase or reduce the number of doors or users without experiencing delays or bearing unnecessary costs. This on-demand scalability provides added flexibility and greater agility to easily respond to evolving security and business requirements.

True cloud-based applications are designed from the ground up as a cloud service and are hosted in a proven, secure public cloud infrastructure.

Availability

The key to security has always been system uptime. This applies to intrusion, video, fire and access control, and it is accomplished either at the field level with battery backup, or at the host level with costly "hot" systems. Even with this expense, activities related to patching or version control inherently require some downtime, thereby affecting the availability of a host. This does not include power outages, polling device

inconsistencies and other impacts to availability.

Public cloud-based applications bring 99.999 percent availability characteristics, resulting from the capability of the provider to upgrade, patch, change versions and make any other modifications without affecting customers. Accomplished with complete transparency to users, there is no impact on service levels, beyond a client's ability to connect to the Internet.

Public cloud-based applications bring 99.999 percent availability characteristics, resulting from the capability of the provider to upgrade, patch, change versions and make any other modifications without affecting customers.

Resiliency

Though related to availability, the key element to consider when assessing resiliency is the concept of failover caused by an uncontrolled event. Most on-premises applications do not provide for this, as it is cost prohibitive to do so. Resiliency can only be addressed through hot or cold standby, redundant array of independent discs (RAID) technology or other mechanisms, which, if done, are likely implemented in the same location or nearby. This does

not address the problem of a major uncontrolled event such as a flood or earthquake.

Public cloud-based applications can address the resiliency issue by leveraging their design, which is based on geographically-distinct availability zones. Services that cannot be provided in a given geographic location or zone because of a disaster are automatically handled in a different location or zone in a fashion transparent to the user. This redundancy provides the user with an important benefit without requiring additional hardware and expense.

Flexibility

Physical access control systems have traditionally been developed and designed to be somewhat static in their approach (e.g., door definitions, access rights, cardholders, schedules). The databases derived from these attributes and the ensuing events become an integral part of the access control solution, whose purpose is to then systematically create audit logs and reports. That said, the data becomes the property of the access control system. In this scenario, an end user's desire to interact with the data is limited to the functionalities provided by the manufacturer's interface.

This leads to the question, "To whom does the data belong?" If the dataset is created by an end user, for the end user, then it should belong to that end user to work with as they see fit. Open database connectivity (ODBC) connections are too limiting in their capability for true data management and are, therefore, not the method of choice for large datasets in the cloud.

Effective data management is accomplished using real-world tools that empower the data owner to interact fully with the dataset. In today's world of big data, this implies the use of application programming interfaces (APIs). Cloud-based systems designed to use a single API provide this approach, as well as the associated tools needed to interact with the data. A resilient API provides the access control service provider a point for its user interface to work with, as well as all associated services – including communications, database and applications. In addition, such an interface enables the script to have customized requirements for interacting with the data (for example, adding metadata, changing parameters, adding and changing data, creating data-specific reports – all without compromising the integrity of logs and transactions). An API-centric architecture enables the agility to build flexible, fully scalable applications that can be easily connected to other systems inside and outside the enterprise, while being future-proofed to accommodate new technologies.

Security

The idea of housing an access control system on premises to ensure the highest level of security is a thing of the past. The question one should ask today is, "What level of security do we practice internally, and how is the manufacturer ensuring the security of their application?" The likelihood of these questions being answered

favorably is questionable at best. Enterprise security is often a struggle for the best IT departments, primarily because of staffing demands and the expense of keeping systems updated. This is provided that the on-premises system is actually managed by the IT department, rather than the security operations center.

The second part of the question is especially difficult, since most access control manufacturers do not have a robust (if any) methodology for testing the vulnerabilities of their applications. Conversely, cloud service providers depend on the security of their service for business survival. Constant threat monitoring and vulnerability scanning are key to their existence. Therefore, the hardware and resources dedicated to security and data privacy far outweigh those in the majority of businesses today. The resources dedicated to security, compared to a typical organization, are incomparable.

The industry should mandate, as a best practice and built-in specification, continuous vulnerability scanning of all applications and physical access control systems.

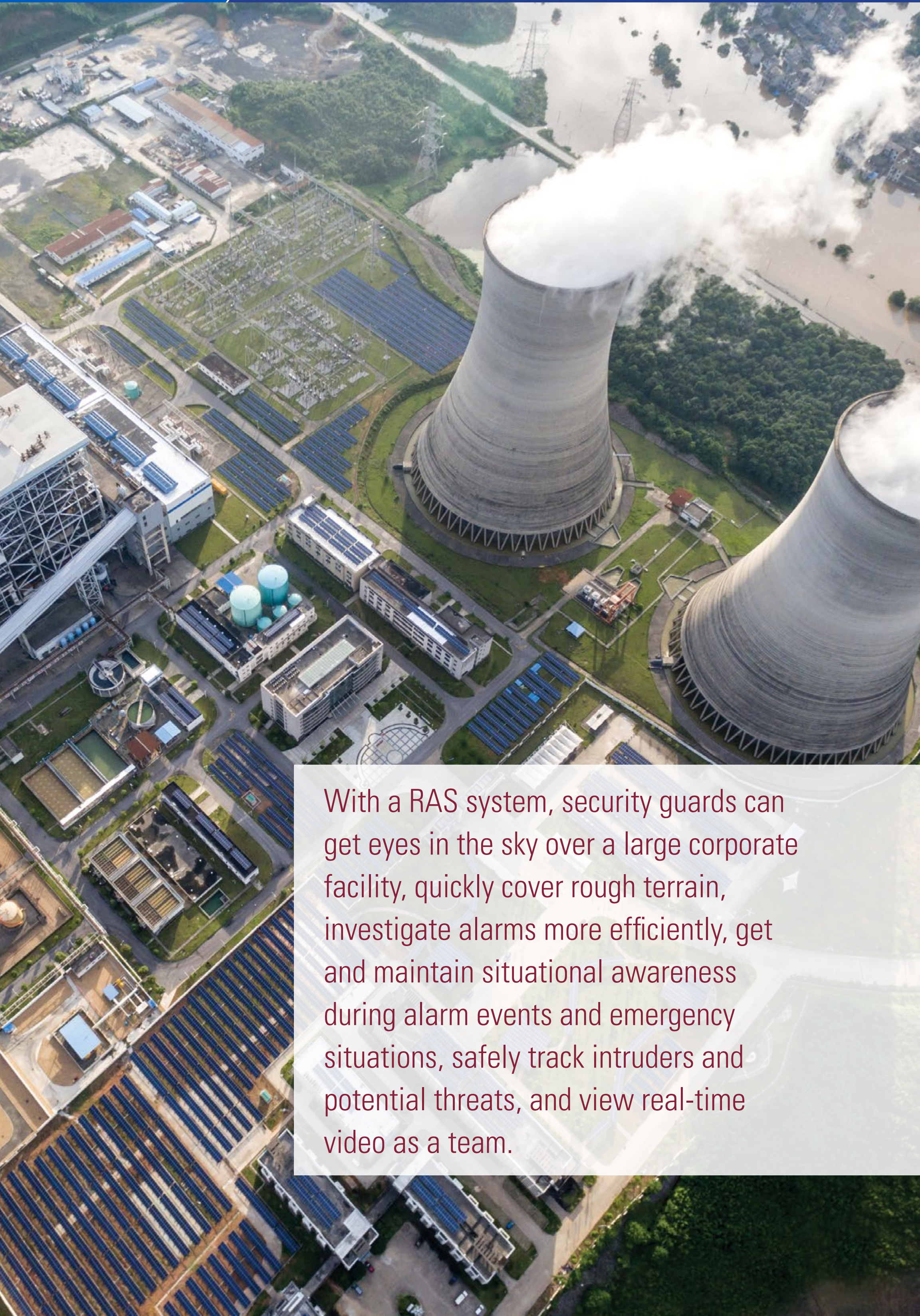
Application security is an area of even greater concern. It has not been a best practice in the physical access control world to consider the potential vulnerability of applications. In fact, very few systems providers would even comply if end users were to make application security a core requirement. Yet, the security industry is responsible for providing the most secure solutions possible. The industry should mandate, as a best practice and built-in specification, continuous vulnerability scanning of all applications and physical access control systems.

Summary

Increased scalability, availability, resiliency, flexibility and security are all part of the affordable, realistic benefits of a public cloud infrastructure. Cloud solutions help reduce the initial capital investment by eliminating the need to purchase costly software, while also reducing the staff and training required to maintain the system, leading to an overall decrease in the total cost of ownership. By moving infrastructure to a cloud-based model, organizations can focus resources where they belong: on developing innovative solutions that grow their business. The time and money spent making technology decisions for access control, along with hiring staff to manage and maintain the infrastructure, can be a thing of the past. ■

Back to TOC

Denis Hébert (denis.hebert@feenics.com) is president of Feenics (www.feenics.com) and is chairman of the Security Industry Association Board of Directors.



With a RAS system, security guards can get eyes in the sky over a large corporate facility, quickly cover rough terrain, investigate alarms more efficiently, get and maintain situational awareness during alarm events and emergency situations, safely track intruders and potential threats, and view real-time video as a team.

Up in the Air

Drones powered by artificial intelligence could transform security

By Cary Savas
Nightingale Security

Drones are powerful. They are changing our existence. They are here to stay.

This article examines a drone application with the potential to have an extraordinary impact on the physical security industry. It is called robotic aerial security (RAS).

What Is Robotic Aerial Security?

RAS is sometimes called "drone security," but, in reality, it is much more than that. RAS is a combination of three components – drones, base stations and software – working together to provide autonomous, 24/7 physical security using real-time aerial surveillance cameras and data gathering sensors.

The first component, drones, are specialized, commercial unmanned aerial vehicles (UAVs) designed to carry payloads that are vital to security missions. The drones have one or more sensors, such as for RGB, infrared, thermal, LIDAR and even hazardous materials. New sensors are being developed and deployed, making the drones, and the overall RAS system, more powerful and efficient.

The next component, base stations, provide shelter and recharge the drones. These base stations are much more than just a landing pad. Inside the industrial, weather-proof housing is a charging component and a networked computer to help manage the autonomous operation.

The last and most important component of an autonomous RAS system is the software. Anybody can make a drone (well, lots of people do, at least), but having artificial intelligence software to enable the autonomous operation of a fleet of drones is of paramount importance when deploying a RAS system in a commercial setting. This sophisticated software is a command and communications hub, the brains of the system.

How Will RAS Be Used?

Generally speaking, RAS is deployed in three ways, but the first two are the most common.

Autonomous Rapid Response

Rapid response to an alarm event is a goal of any security organization, but it is often difficult to achieve. This is where RAS can bring significant and measurable benefits. The RAS software is integrated into the existing security system and alarm panels, so it is immediately notified when there is an alarm event. At that point, the RAS system autonomously dispatches a drone to the site of the event and the drone streams live video back to the security team.

In this deployment scenario, RAS is an autonomous rapid response mechanism that is the perfect complement to a system that has multiple alarms and sensors. A RAS system can maximize the value of these alarms and sensors by using them as triggers to autonomously dispatch drones. The benefits of this integration are transformative in terms of how quickly, efficiently and safely

security personnel are able to respond to alarm events.

Alarms go off all the time. And while most alarm activations turn out to be false, each one represents a potential threat that needs to be investigated with a sense of urgency. In large corporate facilities, quickly deploying a guard to an alarm location is challenging, and sometimes a lack of camera coverage prevents security staff from seeing what is going on. That is where a RAS system can deliver value. A drone can deploy autonomously, cover long distances quickly and send a live video stream of a situation to the whole security staff. This provides an unprecedented level of situational awareness – an invaluable asset when confronting a potential threat.

> Having artificial intelligence software to enable the autonomous operation of a fleet of drones is of paramount importance when deploying a RAS system in a commercial setting. This sophisticated software is a command and communications hub, the brains of the system.

Scheduled Autonomous Patrols

Guard patrols are an important part of most security operations and doing it well and cost efficiently can be challenging. But robots are perfectly suited for autonomously patrolling large facilities. With a RAS system, a user can schedule precise patrol missions around a perimeter and throughout a facility and have them repeated at set times, autonomously. He or she can establish several types of missions, specifying the day, time, path, speed, altitude, hover duration, camera/sensor direction and other variables. Once a mission is set and saved, no additional human involvement is required for a RAS system to carry it out. It happens like clockwork. Actually, it is clockwork because the system does not switch off. It is on duty and ready to go 24/7.

One of the ways this is made possible is through redundancy. In military terms, three is two, two is one, and one is none. In short, without redundancy, you have nothing. So an effective RAS deployment will have built-in redundancy. For example, in the event that a drone on patrol is running low on battery power, another drone can autonomously dispatch, relieve the first one and complete the mission. The video feed switches to the replacement drone with no interruption. In the meantime, the first drone has returned to the base station to recharge so it can redeploy when needed.

Manual Surveillance Missions

If there is a major event, such as a fire, oil spill or chemical leak, a user can manually dispatch a drone to any location within the facility. It is during these impromptu, dynamically changing events that personnel most need situational awareness to provide insight into where, how and when to deploy resources. Or, in extreme cases, when to stay away. And while a manual surveillance mission is not an everyday deployment scenario, there are instances when it is an invaluable capability. This is a situation where it is better to have something and not need it than to need it and not have it.

What Is RAS Software?

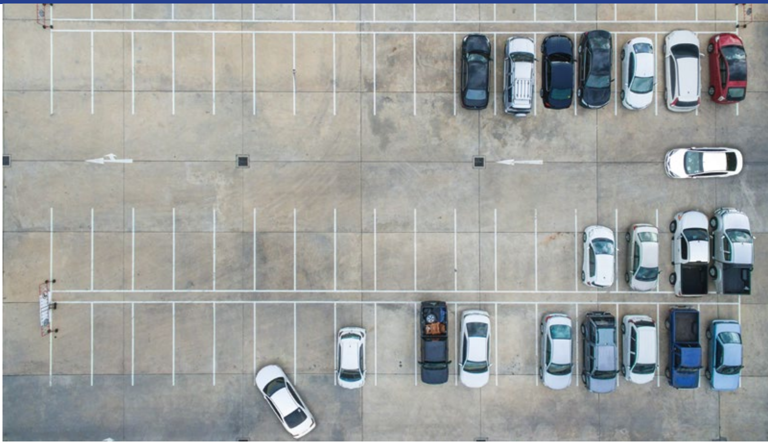
RAS software enables the autonomous operations and the deployment scenarios described above. That said, there are other transformative capabilities powered by software that deserve more attention.

For starters, unlike standard surveillance (piecing together human intelligence, ground-based cameras and witness statements), a RAS system can broadcast everything in real time to everyone on the security staff. It is a communications hub that enables the entire staff to view live video feeds from multiple drones, simultaneously. A guard can watch over his local facility, a regional manager can see locations across multiple states, and a chief security officer can view video feeds from around the world. This new, powerful communications capability will transform how security personnel evaluate and respond to events.

> A drone can deploy autonomously, cover long distances quickly and send a live video stream of a situation to the whole security staff. This provides an unprecedented level of situational awareness.

Another important software-driven capability is the command and control function that the system provides from anywhere in the world. With access to the Internet and the proper user permissions, security staff can configure mission details from anywhere.

Last, but not least, is the artificial intelligence enabled by the RAS software. Drones are powerful data capturing devices, and the RAS software is a powerful data analysis tool. Imagine drones from a RAS system have patrolled a facility over and over for months. These patrols have gathered reams of data about the facility and the AI software has learned what “normal” looks like (where is the path of the perimeter fence, how many cars park in the lot at night, where do delivery trucks go, which areas are off-limits to cars, personnel, etc.). This definition of “normal” allows the system to identify abnormalities and alert staff when something warrants a more detailed



inspection. This is powerful because it makes security personnel more effective. Humans are still (for the time being) better than AI at making complex, real-time decisions, but AI is great at identifying differences in the status quo. One might say that humans, AI and RAS systems are made for each other. As AI software improves, the RAS system will "learn" even more about the facilities being patrolled and become more valuable to the security staff.

Will RAS Affect Manned Security?

Let's look at some market conditions that could lead to RAS systems bringing about fundamental, industry-wide changes.

- Contract security guards represent 50 percent of the physical security market, so anything that affects that segment can move the market.
- Security guards have limited performance capabilities. For example, it is difficult for guards to quickly cover terrain at large facilities or remote areas. A rapid response just is not possible at most big facilities. There are also other performance inhibitors, such as sick days, vacation days, holidays, fatigue, human error, malfeasance, etc. But robots do not take holidays. What would they do if they did? Visit the in-laws? Go to the beach?
- High turnover is a systemic and costly challenge facing the security guard market. The annual turnover rate is estimated to be 100 percent, and in some cases, it is as high as 400 percent. As a comparison, the turnover rate for most jobs is 15 percent. The high turnover rate for guards affects staff continuity, performance and the bottom line. In fact, the costs for interviewing, training, and onboarding new employees can range from 30 percent to 400 percent of the replaced employee's salary. This is a painful, recurring expense for security staffing companies.
- The average annual cost for a contract security guard is $52,000 – $25 per hour and 2,080 hours per year. In this equation, the guards get paid $10-15 per hour, so they are not motivated financially. All in all, it

is an expensive situation for end users and an unmotivating job for guards.

Given these market conditions, a RAS system could truly bring about change. With such a system, companies can enhance their existing security posture and reduce the manpower they require. In short, they can do more, and do it more reliably, for less money.

Facilities with large perimeters or remote operations are especially well-suited for a RAS system. This covers many industries, including oil and gas, critical infrastructure, solar farms, power plants, manufacturing, data centers, chemical plants, agriculture, and railyards, among many others. Regardless of the industry, if there is a large perimeter to patrol, a RAS system can do it better, faster and at a lower cost than traditional solutions.

Empowering Security Guards

With a RAS system, security guards can get eyes in the sky over a large corporate facility, quickly cover rough terrain, investigate alarms more efficiently, get and maintain situational awareness during alarm events and emergency situations, safely track intruders and potential threats, and view real-time video as a team. And that's just for starters. As RAS technology improves, so will the capabilities of security guards.

Force Multiplier

When security guards see something suspicious, they call in to the central command and verbally describe the situation. Conversely, a drone from a RAS system that identifies something suspicious broadcasts continuous, real-time video of the situation to the entire security staff. That is much more powerful than a phone call or radio transmission. Now imagine a facility with one security guard at a central command station controlling a RAS system that has three drones. That one guard can patrol and cover the same territory as three guards and do so more capably and at a lower cost.

Superior Mobility

The concept of using human guards for rapid response at a 1,000-acre facility just is not practical. Drones, however, cover difficult terrain better

and faster than human guards. And with performance specifications like 0-60 mph in a little over 4 seconds, a RAS system is an ideal rapid response platform.

Always on Duty

Drones can patrol facilities, perimeters and at-risk areas every hour of every day. They happily work holidays without expecting time-and-a-half.

Large Coverage Area

A drone can cover a linear distance of 5 miles per mission. It is almost impossible for a pan-tilt-zoom camera with good zoom to cover the same distance, even assuming there are no trees, buildings or other obstructions in the way.

Visible Deterrent

Drones can respond to an incident or an alarm event rapidly and serve as a visible deterrent once on scene, without exposing human guards to harm. In addition, simply posting perimeter signs – "Patrolled by Robotic Aerial Security" – can go a long way toward preventing an intrusion.

Cost Effective

Buying, installing, operating and maintaining cameras and sensors for a large perimeter can be expensive. Typical areas of operation for a large corporate facility can range from hundreds of acres to tens of square miles. The costs to outfit a large perimeter with security cameras and sensors can reach millions of dollars, but a RAS system can be deployed for a fraction of that amount.

Easy to Deploy

Buying, owning and maintaining complex hardware and software is a major undertaking. It is a significant capital expenditure that requires regular maintenance and is destined for technological obsolescence in the near future. That is not true for RAS systems, though, because they are available via a subscription model – Robots as a Service (RaaS). Customers do not have to buy, own or maintain anything. A monthly fee and annual contract provides the hardware, software, maintenance and a service agreement. The customer gets hardware and software that is maintained and upgraded as needed by the service provider, and the service provider gets a stable revenue stream.

Humans are still (for the time being) better than AI at making complex, real-time decisions, but AI is great at identifying differences in the status quo.

There are, then, many reasons why robotic aerial security is poised to fundamentally transform the physical security industry. This powerful, new technology offers tangible, immediate benefits for corporate physical security operations, and it is here to stay. ■

Back to TOC

Cary Savas (cary.savas@nightingalesecurity.com) is vice president, marketing, at Nightingale Security (www.nightingalesecurity.com).

By integrating intrusion detection and access control within the video management system, users gain centralized control of security across the enterprise.

Out of Many, One

Integrating components of a security system can vastly improve effectiveness

By Brian Wiser
Bosch Security Systems

When end users call on a security integrator to install or upgrade a system, the basic requirements of the system may already be defined. While these may seem to address all of the needs and wants, the user may be looking at each type of security, as well as communications technology, as a separate entity. Such technology silos can be inefficient to manage, especially for larger organizations, and they lack the ability to provide an overall view of a facility's security.

An integrator should ask a few probing questions to get the user thinking about the system in a new way. Are there areas of the facility that require greater security? Are there manual security processes that could be streamlined? Are there notifications or other technologies that could improve the efficiency of security personnel and the safety of employees? Are there regulations or government mandates that need to be heeded? Understanding how the organization currently works, and how users would like it to work, is key to presenting the best solution.

Because individual security

technologies complement each other to enhance facility control, the best solution often integrates security and communications systems to better mitigate risk and improve the efficiency of personnel operating the system. Whether the solution is for a retail store, school or university, government site, or other commercial or industrial environment, integrated systems increase overall security and reduce complexity for the user.

Choosing an Integration Hub

The key to an integrated solution is technology that can accept alarms from various devices – such as detectors, surveillance cameras and more – and use those alarms to trigger actions that focus the attention of security, office personnel or the central station monitoring the facility.

Some of the latest security control panels and video management systems provide this level of integration and enable customized solutions for the user. Take, for example, a commercial building or industrial site that has integrated intrusion detection, access control and video surveillance. When an employee presents access credentials at the facility entrance, not only does the door unlock, but the intrusion detection system can automatically disarm, and the security operator can be alerted through video displayed from a nearby camera. This helps the operator ensure that no one is tailgating behind the employee.

Video also provides situational awareness when other control panel events occur. If someone tampers with a motion detector, the security control panel can trigger a nearby camera to send a video snapshot via email or text to the facility manager. It can also alert security personnel and trigger a

pan-tilt-zoom camera to focus on the relevant area for further investigation.

If there is a particularly sensitive area in a facility – such as a server room – video, access and intrusion technology can combine to secure the area and can even be used to protect the individual hardware racks inside the room. For example, each server rack can have its own access reader, keypad and camera. This can prevent unauthorized individuals from accessing the equipment and can also restrict authorized people to scheduled days and times, limiting after-hours access to pre-determined times for maintenance and upgrades. Using a keypad and a reader on the racks also enables the use of dual authentication, so the individual must present something he or she has – a credential – along with something he or she knows – a PIN – for even greater security. Adding an IP camera means that any attempt to open the racks by unauthorized individuals will trigger the camera to send a text or email alert with a video snapshot to the facility manager.

Incorporating Intelligent IP Cameras

Cameras equipped with video analytics can also initiate intrusion detection system events when alarms are triggered. Video analytics can be a major asset, as this technology continuously analyzes real-time images to detect suspicious events. It ensures a constant eye on the scene and instantly responds to conditions that require action. This adds an extra layer of protection by providing real-time alerts regarding potential security risks, such as detecting loitering in a parking lot or a perimeter breach after hours. Following are a few of the conditions that video analytics can be programmed to alert on.

> Technology silos can be inefficient to manage, especially for larger organizations, and they lack the ability to provide an overall view of a facility's security.

Line Crossing

Alerts operators if a person crosses a perimeter, whether it is a fence or an invisible line at the edge of an unfenced campus.

Illegal Parking

Alerts operators if a car is parked or idling in an area where it should not be, such as near a loading dock door, in a fire lane, or in another restricted zone. Analytics can also be configured to detect idle objects or objects left behind.

Loitering

Alerts operators if a person enters an area and does not leave after a specified time, while ignoring people who innocently pass through the scene. When programmed for loitering, analytics can alert security personnel that someone may be looking for an opportunity to enter a door when an employee exits or that someone may be vandalizing an area.

Speeding

Alerts operators about vehicles traveling at unsafe speeds in a parking lot. Analytics can filter for speed and size. This enables the system to ignore all movement below a certain speed, but alert the operator when the movement is faster and by an object that is at least the size of a small car.

Color Matching

Alerts operators to the presence of an object that is a particular color, such as a red vehicle that is entering the property or a person wearing a yellow jacket who is in a restricted area. This can be used to notify personnel about the presence of a known security concern.

These are just some of the ways that video analytics can enhance security and safety. And, with an integrated system, an analytic alert can immediately fault a corresponding point on the system's control panel. This prompts the panel to communicate the alarm to the central station or to send video snapshots to the end user.

For example, at a school, a door leading to the playground can automatically unlock when the request-to-exit detector senses a person approaching from inside the building, allowing for easy egress for recess and after-school activities, or in emergency situations. From outside, teachers, aides and other authorized individuals can easily unlock the door with the proper credentials. However, when an unauthorized person attempts to force open the door from the outside, a nearby camera with onboard video analytics that are programmed to alert on loitering, can fault a point on the control panel,

triggering a text or email alert with a video snapshot to be sent to the principal or school resource officer. The notification can also include the IP camera's DNS or IP address, allowing the principal or officer to connect directly to the relevant camera simply by clicking the link.

Mobile command and control of the system via apps for smartphones or tablets also keeps users connected even when they are not onsite.

Integrating Audio

Integrating security technology with a public address system can also provide added protection of sensitive areas. Requiring dual authentication to enter an area and combining that technology with video analytics and automated audio announcements maximizes security for high-risk locations. For example, the system can alert security personnel if unauthorized individuals attempt to touch high-value assets, while also triggering a pre-recorded audio announcement to notify the individuals that their actions are being monitored.

Audio integration is also beneficial for initiating pre-recorded messages based on security events. For example, activating an emergency pull station or pressing a wireless panic button can automatically trigger a public address system to play emergency instructions through a loudspeaker, while also contacting facility personnel with a different message through two-way radios.

Controlling Integrated Systems

By integrating intrusion detection and access control within the video management system, users gain centralized control of security across the enterprise. This increases efficiency for the operator and simplifies management of the system, which is often a key selling point for the security or facility manager who is constantly challenged to accomplish more and address more risks with a limited budget. End users want their systems to be as simple to use as possible with one interface for monitoring and controlling devices.

Mobile command and control of the system via apps for smartphones or tablets also keeps users connected even when they are not onsite. Within the same app used to arm or disarm an intrusion system or area or control doors, users can also view live video from IP cameras integrated with the system.

Adding Services

Combining these security technologies with video monitoring services enables the central monitoring station to intervene immediately when a potential security risk is identified, providing a powerful deterrent that may prevent damage and theft. For example, once an intrusion alarm is transmitted to the central monitoring station and verified through video images, the operator can take immediate action with audio intervention using a nearby camera that is equipped with a loudspeaker. If intruders are warned that they are on camera and that the local authorities have been contacted, they may flee the area before doing any damage.

Bringing It All Together

There are many possibilities with integrated systems. This requires integrators to expand their skillsets with greater knowledge of security software. It also requires proficiency in the ways that technologies can be integrated to create customized

solutions. The examples described above demonstrate how products that work seamlessly together can increase facility security, protect sensitive areas, and make systems easier to manage.

While standards like ONVIF have helped to make integration easier for some technologies and have provided integrators with more options, a system that involves intrusion and access control from one manufacturer, cameras from another, a video management system from a third, and a public address system from a fourth, puts the integrator in the middle. If part of the integration does not work properly, the integrator may have to troubleshoot with multiple manufacturers to fix the issue, which can require additional time and energy and add expense to the project. Or the integration may not include all of the available features of the individual technology components. It is important to fully research integration claims to ensure the solution will fit what the end user requires.

In some instances, using multiple manufacturers may be required by the user or specifier, or there may be an existing video, access control, intrusion or public address system already in place. If this is the case, partnerships that exist between some manufacturers may help to ensure a smoother integration.

In situations such as new buildings or renovations, where the integrator has a choice of technologies, selecting systems from a single vendor that has designed the products to work together can help to speed and simplify installation. This approach also ensures that updates or software changes will not affect the integration, as the manufacturer will have tested for that prior to release. In the end, selecting technology from a single vendor can reduce total system costs for both the integrator and the end user.

> Combining these security technologies with video monitoring services enables the central monitoring station to intervene immediately when a potential security risk is identified.

Overall, using integrated systems can help integrators provide end users with solutions that meet their needs in ways they may not have known were possible. With knowledge of the capabilities of integrated systems and the skills to implement them, integrators can become strategic advisors and trusted partners. ■ **Back to TOC**

Brian Wiser (brian.wiser@us.bosch.com) is president of sales – North America for Bosch Security Systems (www.boschsecurity.us).

AI is going to have a major impact, starting from the nascent but growing field of computer vision.

The Real Benefits of Artificial Intelligence

'Computer vision' powered by AI could radically change video surveillance

By David Monk
Umbo CV

When people think of artificial intelligence (AI), they tend to think of either Skynet – a dark, malicious entity – or C-3PO – a bumbling though harmless droid. But both images misunderstand the concept of AI and what it means to the world. Simply put, AI is going to have a major impact, starting from the nascent but growing field of computer vision.

AI's Computing Origins

Scientists have been working on artificial intelligence since the 1950s, when it was mostly based on the concept of "symbolic artificial intelligence." This framework assumed that many aspects of intelligence could be achieved through the manipulation of symbols. Despite considerable success, symbolic artificial intelligence ultimately fell short, especially in the field of computer vision.

A new AI approach then emerged – statistical AI and convolutional neural networks, which use millions of data points to make a computer "program itself." These networks are "trained," meaning they are fed some data to process, then tweaks are made to the network and it is retested. This cycle continues until the resulting algorithm is highly performant.

Neural network-based technologies are already making their presence felt. In 2016, Google's AlphaGo gained a lot of publicity by defeating one of the top Go players in the world in a five-game match. AlphaGo determines its moves by using a neural network. Facebook uses a neural network to identify and suggest tags for people in uploaded photographs. Its DeepFace network is trained on a dataset of 4 million facial images belonging to more than 4,000 people.

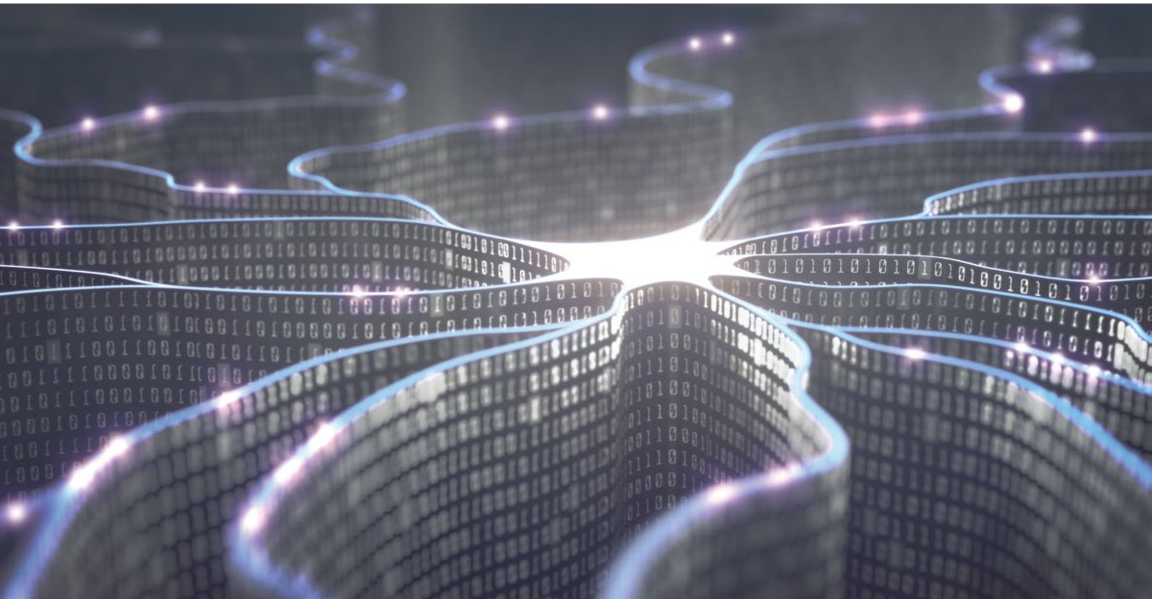
Video security without video analytics is only as effective as the people doing the monitoring.

These new technologies have unlocked new uses and behaviors that would have been impossible or impractical for a programmer or team of programmers to create. Computer vision is at the forefront of these new uses.

Computer Vision

AI applications that use deep learning applied to images and video are referred to as "computer vision." A recent *TechCrunch* article by Colin O'Donnel named computer vision's video-as-a-sensor technology as the most important of the emergent technologies that are changing societies.

Video security without video analytics is only as effective as the people doing the monitoring. A human operator has to maintain a high level of concentration, while also dividing that attention to monitor feeds on multiple screens. Even when operators are trained, research has found that the error rate is high. Humans are simply



not that good at monitoring for rare events across multiple video streams.

While one study done at a prison in 1972 found an 85-97 percent detection rate of conspicuous events such as running and climbing walls, the prison scenes did not show much movement in the video footage; the subjects were standing still. A follow-up study in 1973 with moving figures in the footage found the range of detection rates expanding to 35-100 percent.

> This enables thousands of hours of recorded video to be scanned within a matter of seconds, compared to the hours or days of manual review required by traditional human monitoring.

Increasing the number of monitors that surveillance operators have to observe decreases their performance. In the 1973 study, the perfect rate was achieved only once and only when a single display was observed at a time. A study in Britain found that a detection rate of 85 percent with one screen dropped to 45 percent when nine screens had to be monitored. But, at the same time, having one display does not necessarily translate to consistently high performance.

Another study in Britain in 2003 that looked for incidents of theft in an industrial setting – which is a much more complex scene than a prison – reported a detection rate of only 25 percent.

The State of the Technology

For enterprises, critical infrastructure, higher education, and government entities deploying more than 1,000 security cameras in a distributed environment, human monitoring misses security events, and traditional rules-based systems record many false positives. Both are significant liabilities. Large organizations can record millions of hours of video each month that need to be monitored live and then reviewed forensically to find events of interest. Unfortunately, those poor results from the studies mentioned above have not seen any significant industry-wide improvement in the past few decades.

AI-driven computer vision technologies are entering the video security industry to help humans better perform security-related tasks. Accurate pixel-level human detection and object-of-interest detection in combination with configurable in-scene video region of interest allows for autonomous monitoring. When combined with capable video management systems (VMS), live notifications mean that security managers can be aware of situations as they happen. This same level of accuracy in computer vision can forensically find events of interest by scanning meta tags. This enables thousands of hours of recorded video to be scanned within a matter of seconds, compared to the hours or days of manual review required by traditional human monitoring.

Does this mean that computer vision autonomous algorithms will replace humans? A better way to

view this technological shift in video security is to say that AI is making today's security personnel much more efficient, resulting in:

- Reduced loss of life
- Faster identification of critical behavioral events and the parties involved
- More informed first responders
- Reduced waste of resources resulting from false alarms

The promise of computer vision-enhanced video security is tempered by the complexity of the task, though. Traditional intelligent video systems (IVS) that purport to do this work are based on motion detection and external sensors mounted at key points along a perimeter. This means they will be triggered by nearly any kind of movement. The result is an immense amount of false alarms being activated, and personnel eventually just ignoring them.

Traditional IVS's are unable to progress beyond simple motion detection for a good reason: The act of recognizing a person is subject to millions of edge cases that have to be accommodated by the algorithms.

A security camera has to deal with a lot of issues. It is sitting outside exposed to the elements, such as rain, wind, snow, sun and more. Each of these can wreak havoc on human counting or identification algorithms. Each camera keeps seeing a scene that its software regards as unique. Even something as simple as putting up Christmas lights can cause many artificial intelligence and computer vision algorithms to trigger false alerts every time the lights turn on or off. Before long, the sheer number of alerts would overwhelm users and reduce the effectiveness of the system.

There are countless variations on this issue. For example, what happens if the wind moves the camera's perspective a little bit? Now everything has a different look, which could cause many false alarms. The algorithm needs to be retrained to acknowledge the new "normal" scene.

The key obstacles that IVS developers face are both technical and psychological. Computer vision algorithms must be flexible enough to deal with variable situations. And it is more than just having the most accurate tracking possible. There must be a middle ground. A super-accurate algorithm is pointless if it registers too many false positives.

The solution that industry leaders are taking is to create customized models trained on custom hardware with proprietary data captured from real-world situations. There are a plethora of open-source AI software products and online services available to developers, many of them backed by major tech companies.

Despite their prestigious backers, though, these off-the-shelf models still face the same issues as traditional IVS solutions. Only custom models specifically geared toward surveillance video footage created out of custom data – collected from real-world locations with real-world errors – will be able to move along the learning curve quickly enough.

Predictions for Computer Vision

As AI-powered deep learning techniques improve, behavioral analytics will identify suspicious activity and send specific notifications to surveillance operators in real time. Human trespassing and behavioral notifications require the algorithm to identify a human out of a group of non-human objects. Additional techniques and data will be able to identify characteristics about a specific person or group of people.

> As AI-powered deep learning techniques improve, behavioral analytics will identify suspicious activity and send specific notifications to surveillance operators in real time.

Some problems already have potential solutions. For example, trials are underway that focus on detecting people who are wearing masks, helmets or any other headwear that obscures their face, something that human surveillance operators are trained to look for. Fight detection, meanwhile, is a specific set of clearly defined behaviors that is already addressable with today's computer vision recognition algorithms.

In the far future, there are other behaviors that human surveillance operators watch for that will offer greater challenges for computer vision. Behaviors that have to take into account the time development factor are especially thorny. Algorithms today look at each frame of video individually, which is why they are suited for identifying human shapes. But behaviors that take time for an observer's "intuition" to develop, such as robberies, accidents and theft (which is particularly difficult because it is a concealed act) offer different challenges as algorithms need to learn how to recognize significant changes in frames over periods of time.

The AI technological paradigm shift is imminent, as a list of recent milestones indicates:

- The volume of "big data" being collected and made available is increasing exponentially, generating demand for rapid deep neural network processing chip technology advancement.
- Enterprise-level cloud computing adoption is exceeding 70 percent.
- The number of AI researchers is at an all-time high, marked by a 300 percent increase in Ph.D. and Ph.D. candidate papers published globally in just the past year.
- More than 550 startups using AI as a core part of their products raised $5 billion in funding in 2016.

There are certainly challenges ahead, but the AI field is advancing at an exponential rate. What is possible today represents a huge leap forward in the field and offers great promise for AI-driven computer vision technologies that will contribute to the safety and security of people in years to come. ■ **Back to TOC**

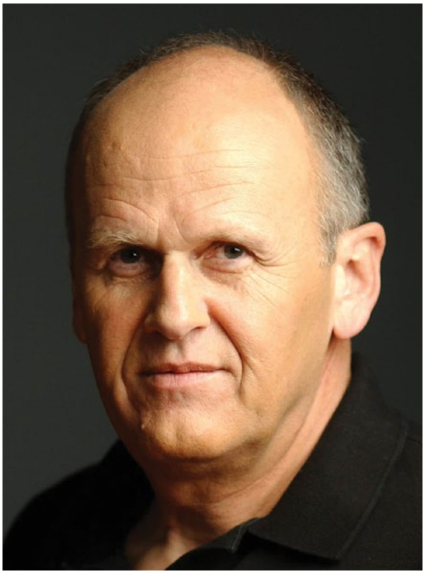
David Monk (david.monk@umbocv.com) is eastern regional USA senior account manager for Umbo CV (www.umbocv.com).

Security analysts, researchers and developers are coming to the conclusion that a strong, unified, multi-tiered biometric security solution is the next step in public and private protection.

Walk this Way, Talk this Way

Combining gait analysis, voice recognition and other biometric identifiers provides a fraud-resistant security solution

By Maj. Gen. (ret.) Aharon Zeevi Farkash
FST Biometrics



According to the statistics, terror attacks are continuing to climb as political climates heat up and radicals look for security weaknesses they can exploit to further their messages globally. The list of cities that have fallen victim to major attacks keeps growing: Tel Aviv, Istanbul, Nice, Brussels, Quebec City, Orlando, and more.

So what can be done to stem the tide of global terror? The answer begins with better intelligence.

The ultimate goal of intelligence would seem to be finding the one source of information – the one informer or spy – who could provide all the answers needed. But this is a fallacy. In the world of intelligence, the best way to get answers is by gathering information from multiple locations, an ecosystem of sensors that combine to provide a clear picture of a situation that security personnel can assess to prevent terror attacks.

This ecosystem can include a vast array of sources: signal intelligence, cyber intelligence, visual intelligence (from satellites, surveillance balloons and drones), special forces, human intelligence, interrogations and others. Any of these sources alone would do little good; but when combined, they provide a clear picture of the security landscape.

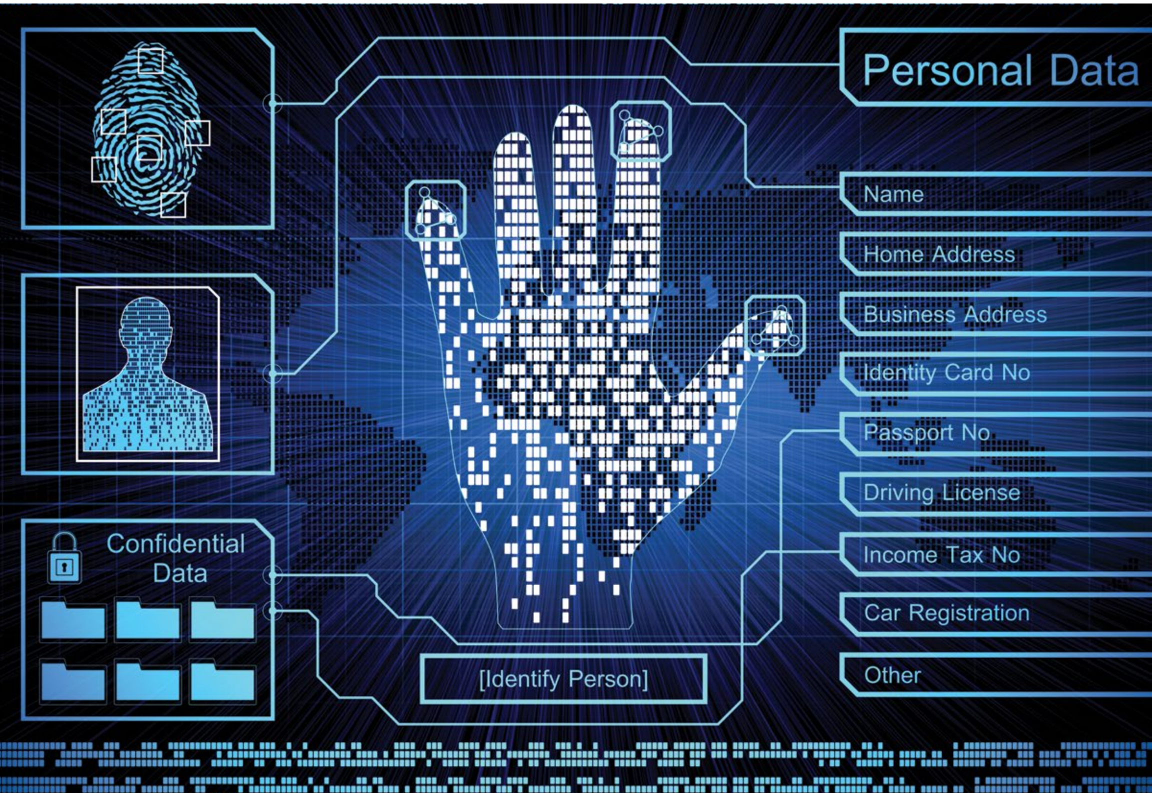
> The best way to get answers is by gathering information from multiple locations, an ecosystem of sensors that combine to provide a clear picture of a situation that security personnel can assess to prevent terror attacks.

The highest levels of military intelligence fuse all of this information together in real time and determine actionable intelligence for end users, namely, special forces and similar units.

This leaves us with a clear, sound approach to proactive intelligence and security, one that involves the fusion of sensors, stories and information. This is a powerful thing in the intelligence world. Real-time data fusion is what allows agencies to approach security with a preventive philosophy that helps to prevent hostile events from occurring.

Global Megatrends and the Need for Convenient Security

There are two global megatrends that greatly affect the way in which we approach security. First is the growing



need to prevent terrorism. Second is the increase in urbanization with the rise of megacities during the past several years. As a result of these two trends, proactive security has become a necessary part of our reality.

How can we protect ourselves – physically and technologically – from these real threats to our safety? Security analysts, researchers and developers are coming to the conclusion that a strong, unified, multi-tiered biometric security solution is the next step in public and private protection.

But can developers create a technology that is accurate, private and convenient enough that people do not feel like they are living in a police state? In fact, the technology for such a solution is closer than one might think.

Can developers create a technology that is accurate, private and convenient enough that people do not feel like they are living in a police state? In fact, the technology for such a solution is closer than one might think.

Why High-Level Security Is Not Enough

Alongside the security issues stands another challenge: a fast-paced, instant gratification generation that demands efficiency and convenience, as well as security. It is not enough to just have a solid security system in place. People want to feel unwavering protection, and they also want it to be instantaneous, seamless and easy. Imagine having to stand in a long line of shoppers because the identity verification software is slow. It is unlikely that consumers would tolerate such delays.

Many people are willing to forgo safety for convenience, adopting an attitude of, "I know it's safer to do it that way, but I just can't be bothered." More often than not, for example, people would rather compromise the data on their phones by not using a PIN than give up slightly faster access to their Facebook app. Society would quickly dismiss a security system that takes too much time, is cumbersome, or is inconvenient to use.

A hack-resistant, flexible, full suit of armor that is also fast and easy to use? Are we demanding too much from technology? Maybe, but with the right minds set to the task, security system developers are rising to the challenge, and they may have come up with a solution.

Biometrics for Proactive Security

There are clear needs that must be addressed to meet the following demands:

- A solution that provides a high level of security, while not making people feel that they live in a police state

- A solution that is convenient for users and does not interrupt their pace of life

Biometric technology provides a solution. Biometrics allow us to quickly and securely identify individuals before they even enter a building. This can prevent many security breaches.

However, the question then becomes, what is the strongest, most effective and most convenient approach to preventive biometric security? The lessons from intelligence gathering apply to biometrics as well: what we need is fusion.

Any sensor on its own – facial recognition, fingerprints, iris recognition, voice recognition – cannot provide the accuracy, speed or aesthetics needed for strong security that is also convenient.

The strongest, most convenient and most secure forms of biometric technology employ a fusion of technologies to provide speed and accuracy, as well as simplicity, to the end user.

The most secure and convenient biometric identity verification technologies must leverage the power of fusion. For example, fusing face recognition and body behavior analytics, including height, gait and other characteristics, is very accurate and does not require a user to stop for identification. This fusion of sensors allows a user to understand a person's identity in real time, with a high degree of accuracy and speed.

Single Mode Biometrics and Fraud Concerns

Biometrics are a powerful way to provide identity verification, and the range of biometric security options is vast and growing. Currently, the public can make use of fingerprint scanners, iris scanners, facial recognition, and

gait analysis tools. Other technologies that are still in the research stage include ear scanners, speech pattern recorders, and heartbeat data monitors. Even typing style is being studied for possible future use.

On the surface, these may seem like sure-fire security and identity protectors – after all, how can someone possibly fake these intrinsic biological components? Yet, any technology, when it stands on its own, can be susceptible to fraud.

Identity theft is no longer just for cyber criminals who go online, steal credentials, and rack up bills on somebody else's credit card. In fact, the term "identity theft" is taking on a more real definition than ever before. It is now being perpetrated at a biological level, with biometric factors being duplicated and stolen in new, almost surreal ways.

Fingerprints

Hackers are notorious for lifting fingerprints off of doorknobs, drinking glasses, receipts, and other publicly accessible items/areas. What's even more disturbing than this is the recent discovery that a high-resolution image is all a talented criminal needs to create a duplicate of a person's fingerprints.

Fingerprints can be duplicated using materials as rudimentary as Play-Doh or ink from a printer. Photocopies, printed circuit boards, silicone and rubber cement have also all been implicated in fingerprint copying. A simple piece of masking tape can even pick up a fingerprint for replication. Technology itself seems to be against the fingerprint scanner – a seemingly harmless glove has been developed, crafted to help smartphone users fight the cold by grafting the user's fingerprints onto the glove.

Eye Scans

Faking an eye scan is easier than it looks. Using a high-resolution image, developers can make contact lenses that duplicate the shape and pattern of a person's eyes. And these lenses are completely unnoticeable. A security guard will not be able to see that anything is amiss if a person walks in with this fraudulent eyewear.

Biometric Fusion: Ultimate Security, Ultimate Convenience

Fusion is not a new concept; it encompasses the idea that "the whole is greater than the sum of its parts." The idea of biometric fusion is to combine the strengths of different technologies so that each one complements – and compensates for the shortcomings of – the other. In addition, fusion adds complexity to the identification, making biometric fusion almost impervious to fraud.

One of the most advanced biometric fusions available today includes facial recognition and body behavior analytics. What makes this combination so strong?

> The strongest, most convenient and most secure forms of biometric technology employ a fusion of technologies to provide speed and accuracy, as well as simplicity, to the end user.

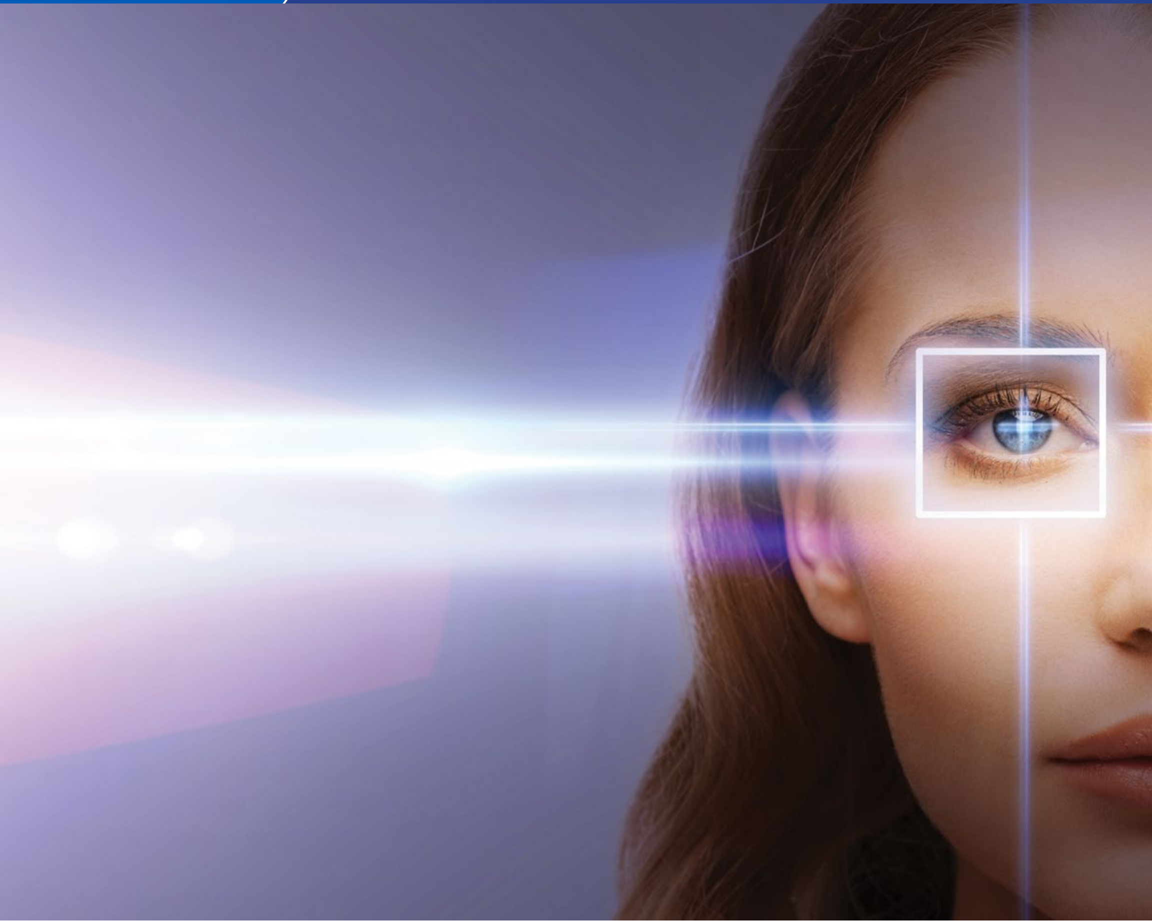
First, gait and body behavior biometrics, while newer to the market, are making a big impact because of their efficacy. Each person has a unique combination of movements. In fact, gait is probably one of the hardest biometric signatures to replicate. Even the most advanced robotics have not been able to successfully duplicate the movements and nuances of a human body. This makes gait and body behavior some of the strongest biometric guards available today.

Combining body behavior with facial recognition creates an extremely strong PAD (presentation attack detection) that is nearly impossible to crack. The likelihood of a fraudster being able to replicate a person's face, while showing liveliness, and also copying exactly that person's body characteristics, including height, gait, and specific behaviors, is vanishingly small.

It is not hard to see how a fused solution can help prevent fraud. Copying a fingerprint may be easy enough, but how successful would a criminal be at spoofing a system that scans a user's face and gait? This is nearly impossible.

The Solution to a Growing Problem

By combining the strengths of multiple biometric markers – by building a complex fusion – we create a system that is stronger and more resilient than any one of the components could ever be by itself.



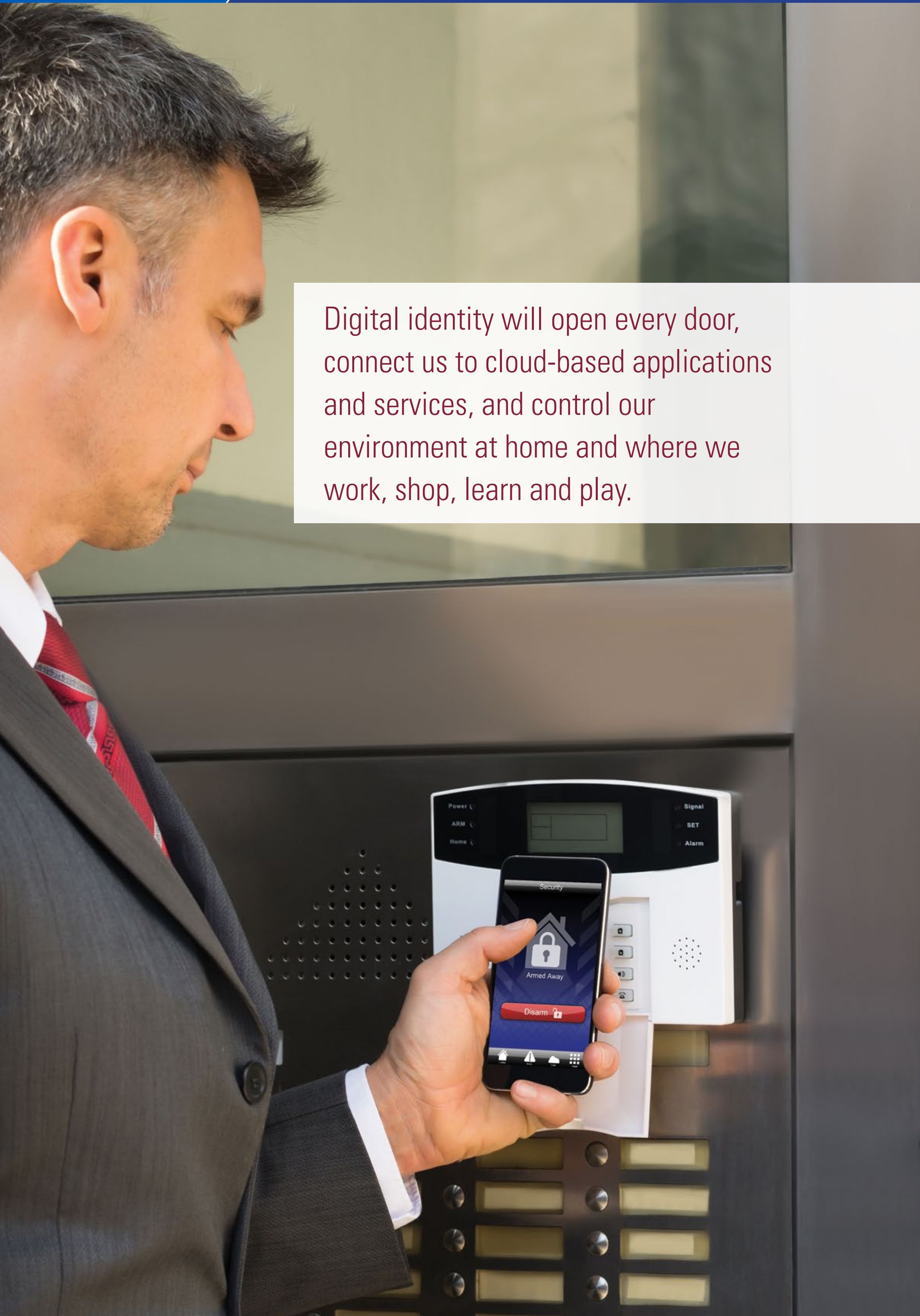
And all of this is done without causing a negative impact on time and convenience.

While some solutions include multimodal biometrics (combining fingerprints and a PIN, for example), forward-looking industries are starting to adopt biometric fusion technologies to secure facilities, improve operational efficiencies, and provide better, more catered experiences to users. The revolutionary benefits of biometric fusion will soon be seen everywhere – from personal devices like smartphones, laptops, and banking apps, to public areas such as stadiums, hospitals, airports and universities.

All of these systems give us a clear picture of how combining multiple biometrics can combat threats. Even the best hacker would be hard-pressed to duplicate a person's face, gait, movements and voice. Fusion takes strength in numbers to a whole new level, and keeps attackers at bay. ■

Back to TOC

Maj. Gen. (ret.) Aharon Zeevi Farkash (farkash@fstbm.com) is founder and president of FST Biometrics (www.fstbm.com) and was head of the Israeli Defense Forces Directorate of Military Intelligence from 2002 to 2006.



Digital identity will open every door, connect us to cloud-based applications and services, and control our environment at home and where we work, shop, learn and play.

A Matter of Trust

New digital identity technologies will increase security, functionality and convenience in many areas

By Stefan Widing
HID Global

A shift in the use of identity technology is leading to increased adoption of mobile devices and the latest smart card technology, a greater emphasis and reliance on the cloud, and a radical new way of thinking about trust in smart environments and the Internet of Things (IoT).

Initiated more than a decade ago with the move to smart cards that carry digital identities on microprocessor chips, this shift in thinking has precipitated the move from legacy systems to near-field communication (NFC), Bluetooth low energy (BLE) and advanced smart card technology to meet the evolving needs of governments and organizations worldwide.

Moving forward, organizations will use a broader range of smart devices than ever before, extending beyond cards to mobile phones and wearables, while enabling users to do much more than simply open doors in an increasingly connected world. This will directly affect how customers view and use trusted identities on both mobile devices and smart cards for more activities and in more connected environments.

Trusted access and other physical and online interactions will become more personal, contextual and valuable, as everything comes together through unified, more fraud-resistant, end-to-end identity and access management systems.

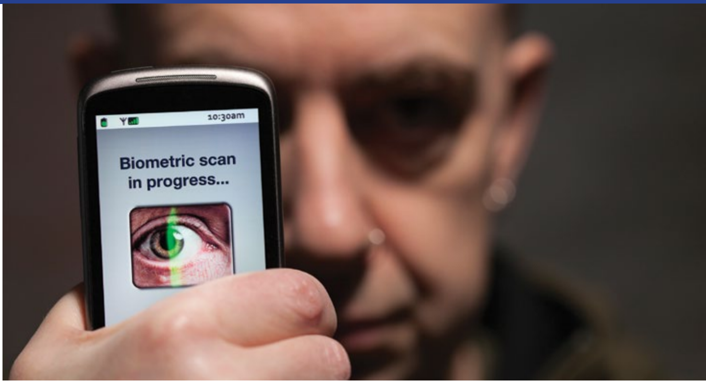
Today's shift in the use of trusted identities affects businesses, institutions and other organizations in many ways, including improving the user experience as these identities are embedded more deeply in everyday activities. It will also yield better ways to establish, create, use and manage secure credentials, while creating new options to deploy hybrid on-premises and cloud solutions for access control – and to tie people, assets and processes to the Internet of Trusted Things (IoTT).

Trust will become increasingly important, along with a focus on biometrics for conveniently and reliably associating digital identities exclusively with the true identity of the person claiming to own them.

Improving the User Experience

The consumerization of security will lead to heightened demand for using phones, wearables or smart cards to open doors and log in to cloud resources, not to mention enabling personalized on-demand printing of documents and consuming many other building services in the connected office.

Trusted identities that integrate security, privacy and convenience will provide a new level of assurance to these applications and transactions, while making secure access more personalized to the individual.



Outdated security policies and procedures will be replaced by better ways to use digital identities that are trusted and work easily with cards, mobile devices and/or biometrics, and users will have more control over how they access and interact with their work environment, and how they discover, purchase and enjoy commercial services and experiences.

The industry will also look toward complete identity relationship management that considers the need to grant access based on the context or circumstances for risk-appropriate authentication across trusted identities assigned to people, devices, data and things in smart environments. This will pave the way for the virtual equivalent of a personal building assistant who does double duty as a user's confidential assistant, continuously anticipating needs while delivering secure and seamless access to doors, IT systems, networks, data and services.

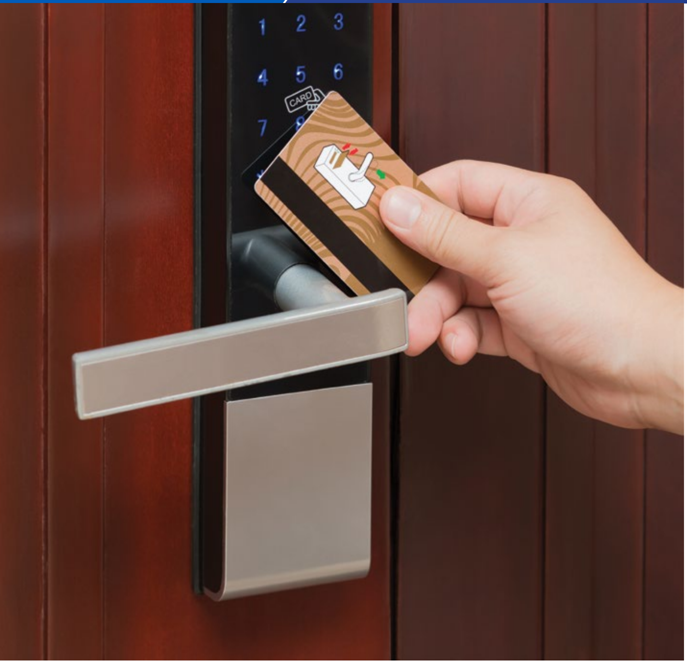
These and other changes will have a dramatic impact on everyday activities for businesses and consumers. In the enterprise, new capabilities for managing and using trusted IDs will be driven by the increase of temporary offices, mobile knowledge workers and the evolution of tomorrow's more connected workplace, where adapting to the preferences of the talent pool will drive the need for more open, flexible workspaces.

"Distributed work" models that combine independent workspaces, social interaction and formal/informal collaboration in the office space will need a more seamless, secure access experience. When breakthrough technologies allow management of identity across the organization, there can be a universal approach to identity that connects disparate systems and assists in achieving regulatory compliance mandates.

Biometrics will provide the most convenient and reliable way to associate a digital identity exclusively with the person who truly owns it.

Trusted IDs Beyond the Enterprise

Trusted identities will become an embedded feature of more "use cases" rather than simply an add-on capability.



The trend of "security by design" will lead to many more convenient approaches to using digital identities across a variety of activities, services and industries.

Consumers will see trusted identities used in such scenarios as guaranteeing authorized use of corporate and heavy machinery fleets, as well as creating new ways to safeguard students and validate drivers. Indeed, as digital identity technology becomes an embedded feature in wearables, there is an opportunity for it to pervade virtually all aspects of daily life.

Digital identity will open every door, connect us to cloud-based applications and services, and control our environment at home and where we work, shop, learn and play.

In banking, trusted identities will help drive consistency across multiple service channels to improve the user experience, from faster, anytime/anywhere instant issuance that is revolutionizing the way customers receive new or replacement debit and credit cards to "out-of-band" mobile push capabilities that increase trust, reduce fraud, and deliver an easier path to compliance for financial institutions.

Digital IDs will also push the banking industry to increase trust levels by better associating a user's physical identity (via biometrics) with his or her digital identity. And by combining multiple types of biometrics with mutual authentication, mobile certificates and other technologies, banks will be able to deliver a game-changing user experience across all channels. A user will be able to "be present" for his or her transaction on the phone, at the bank or automated teller machine, or online.

Similar dynamics are changing the way citizens interact with government agencies and systems. Passports, national IDs, driver's licenses and other credentials will coexist with new disruptive technologies and change the way IDs are issued by government agencies and used by citizens. More citizen IDs are poised to move to mobile phones this year, with some state governments offering mobile driver's licenses as an option. Physical passports and national IDs will be more secure, with more ways to encode information onto and inside more durable cards featuring contactless microcontroller chips.

Digital IDs will move beyond paper and plastic documents to phones, starting with driver's licenses and other government-issued documents – all with a focus on meeting policy, privacy, interoperability and security requirements.

Physical IDs and government documents will coexist with mobile credentials and will feature improved card quality and security, higher resistance to cloning and counterfeiting, and streamlined methods of personalization, printing and issuing.

In the increasingly connected health care environment, trusted identities are improving the patient experience and increasing efficiencies, while safeguarding and managing access to equipment, facilities, patient data and electronic prescribing of controlled substances (EPCS). Physicians will have a much better experience writing, monitoring and tracking online narcotic prescriptions, in full regulatory compliance, from any location.

Patients will also have a better experience since prescriptions and refills can be sent ahead for fulfillment, usually on the same-day – a savings of at least two to three days as compared to waiting for paper-based prescriptions. These and other developments are being enabled through new ways to leverage the power of trusted identities using flexible and unified management platforms.

A Simpler, More Efficient Approach

Cloud-based solutions for IT access management are well established and widely used, and there is growing interest in using cloud-based solutions for physical access control and ID

management, as well. These systems could cover the full identity lifecycle, from the printing of badges or issuing of cards or mobile credentials through system management and assigning of access rights.

Organizations across a wide range of industries will increasingly pursue the goal of truly converged access control that consists of a single security policy, one credential, and one audit log, delivered through a fully interoperable, multi-layered security infrastructure that is based on a flexible and adaptable platform.

Credential issuance for physical ID cards will also experience a digital transformation, as the use of cloud technologies will enable service-focused models for badge printing and encoding. Cloud-based models for ID badge issuance will feature the security of end-to-end encryption and provide the choice of on-premises or cloud models for card personalization. This will transform the user experience and the operational management of ID badge printing, reduce costs, eliminate capex outlay, simplify system maintenance, and improve security as compared to on-premises solutions.

Organizations are also recognizing the interdependencies of technologies and platforms needed for business agility, cost management and providing a better user experience within a mobile workforce, as well as for digital commerce and relationship management, which require more reach, flexibility and security.

To support these technology interdependencies, breakthrough advances will allow identity management across the organization and will connect multiple platforms for a unified approach that delivers a single, comprehensive security view. This model will make it easier for administrators to deploy and maintain an integrated system and will help lower the total cost of ownership. It also will support extending strong authentication from the desktop to the door, and other advanced security, such as digital signing, full disk encryption and boot protection.

A good example of this can be seen in a connected health care environment. Across the health care continuum, from hospital to home, identity technologies will simplify all aspects of operations, from opening hospital doors, accessing records and e-prescribing to how health care professionals interact with patients and log their activities.

Hospitals will explore leveraging

their e-prescribing architectures for other valuable capabilities, such as authenticating to VPNs and enabling remote access using credentials, key fobs, smartphones and other smart devices and on-time password (OTP) tokens.

Growing Importance of Trust and Biometrics Identity

The shift in the use of identity technology is also exposing the crucial difference between biometrics identity and ownership of a digital identity, pushing the industry to increase trust levels and combat fraud by better associating a user's biometric ID with his or her digital identity.

The use of passwords or PINs to validate who is presenting a digital identity will become an increasingly unacceptable approach as cyber criminals continue to assume and use false digital identities across a growing number of transaction channels and access platforms.

To solve this problem, the industry will look at biometrics as much more than simply a PIN or password replacement that makes it somewhat harder for cyber criminals to falsely assume another digital identity. Instead, biometrics will provide the most convenient and reliable way to associate a digital identity exclusively with the person who truly owns it.

In applications that require the highest levels of trust and security, the industry will begin moving toward integrated solutions that use this biometrics-based identity-proofing process to create an unbroken chain of trust. Biometrics identity will be verified and bound to a digital identity at the time of set-up, and then verified again each time it is used.

Emerging IoT Use Cases

New ways to connect more people, places and things will drive the need to use trusted digital identities throughout the IoT. These identities will help to connect people with things to streamline processes and make it easier for users to manage their world. They will also increasingly be employed to help secure, customize and enhance the user experience across a growing range of industry segments.

Organizations will also look toward streamlining processes and operations using real-time location systems, presence and proximity-based location functionality and condition-monitoring solutions, and cloud infrastructure, gateways, beacons and software-as-a-service (SaaS) models, leveraging emerging solutions that secure IoT use cases.

BLE-based solutions will also advance existing secure proof-of-presence capabilities to include predictive analytics and functionality using location-based technologies.

As a result, there will be a variety of new and emerging energy efficiency, productivity and safety-oriented applications in the enterprise that need to know the identities of occupants in a physical space. BLE-based identity credentials will be an enabling technology in applications, including heating, lighting and other environmental management, coordinating meeting room booking, auto-configuring audio-visual equipment, and facilitating emergency mustering and alarms so organizations can determine who is in a building in real time.

> As trusted identities are used with unified platforms that align facility and information security, previously independent teams will need to work together to understand and follow best practices for both physical and logical access control.

In the health care environment, there will be continued momentum toward the adoption of electronic visit verification (EVV) that helps streamline in-home patient visits and eliminate billing fraud using "proof of presence" applications that make it easier to document the time, location and delivery of prescribed care.

Health care institutions will embrace trusted IDs, predictive analytics and new IoT solutions that use real-time, location-based services to effectively connect, monitor and manage patients, mobile clinicians and staff. These solutions will also help to quickly locate critical medical equipment, beds, crash carts and other devices by providing the missing link between physical assets and a trusted ID ecosystem.

Preparing for the Future

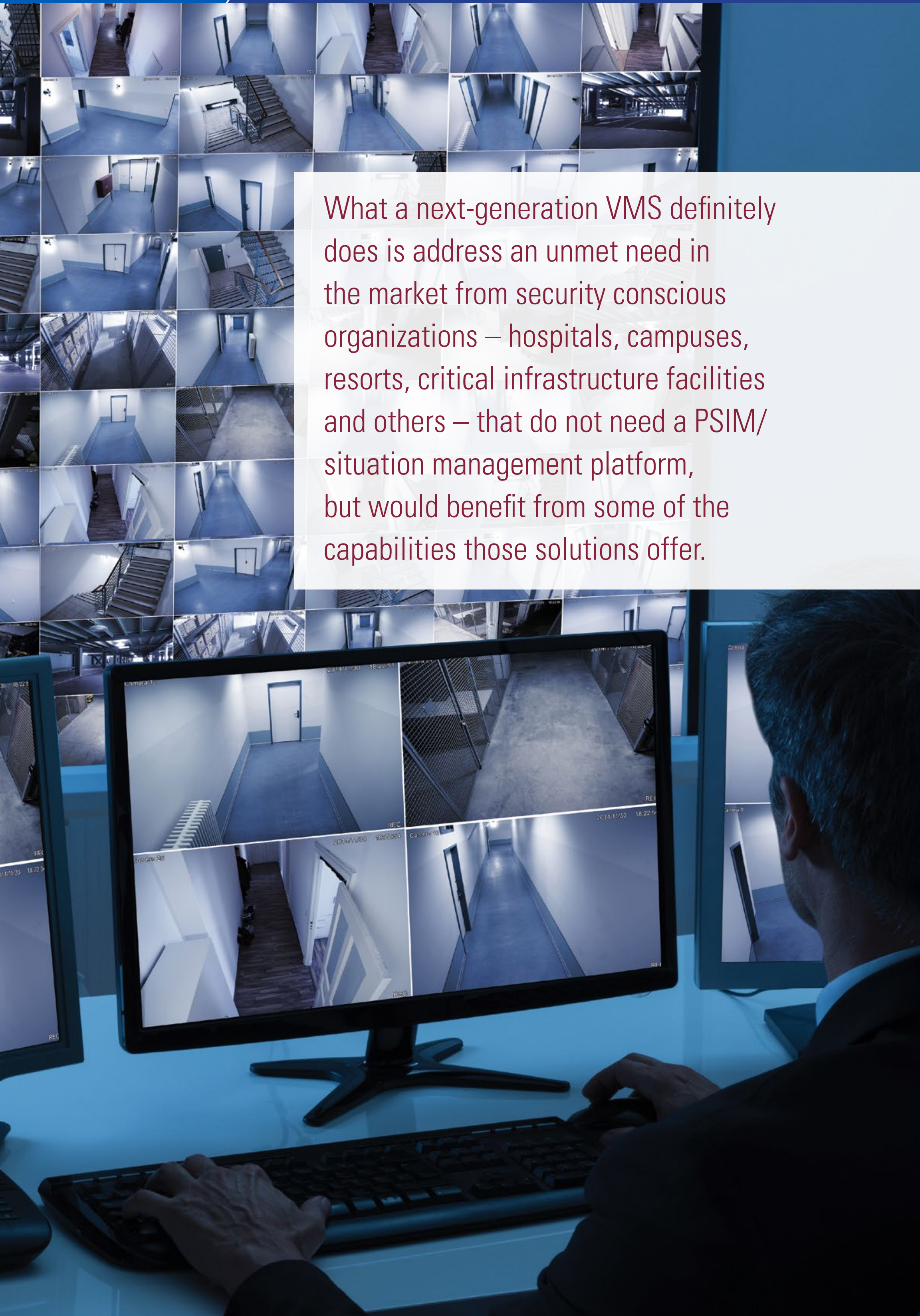
Organizations across a wide range of industries will increasingly pursue the goal of truly converged access control that consists of a single security policy, one credential, and one audit log, delivered through a fully interoperable, multi-layered security infrastructure that is based on a flexible and adaptable platform.

Such a platform will enable organizations to preserve their investments as they grow, evolve and improve their security capabilities in the face of ever-changing threats, while also simplifying deployment and management and lowering the total cost of ownership. This unified platform will also improve the user experience, deliver a more comprehensive security view and facilitate a more coordinated approach for protecting privacy.

The use of trusted identities is entering a new chapter that will drive profound changes across a variety of industries. As trusted identities are used with unified platforms that align facility and information security, previously independent teams will need to work together to understand and follow best practices for both physical and logical access control.

Organizations will also need to explore opportunities to combine authentication and new IoT applications to address a variety of current and future challenges. When they do, there will be an opportunity to simplify all aspects of their operations – from opening doors and accessing data, networks and cloud applications to how they manage assets and streamline processes – while creating a better and more secure user experience. ■ **Back to TOC**

Stefan Widing (info@hidglobal.com) is president and CEO of HID Global (www.hidglobal.com).



What a next-generation VMS definitely does is address an unmet need in the market from security conscious organizations – hospitals, campuses, resorts, critical infrastructure facilities and others – that do not need a PSIM/situation management platform, but would benefit from some of the capabilities those solutions offer.

VMS: The Next Generation

Facilities can now extend video management systems to provide a more complete security solution

By Shawn Mather
Qognify

Since video surveillance was first used as a security tool, the control room and security operations have undergone a transformation, several times over. Video and video management systems (VMS) have evolved. Whereas once the view from video footage was fixed, low-quality and unreliable, control rooms now have reliable, analytics-powered, high-definition, pan-tilt-zoom-enabled video that is able to deliver much more information and insight.

And, as we know, video is not the only thing that has taken leaps forward. Today, organizations have access to advanced systems that increase situational awareness and ensure effective and compliant incident management. This technology is commonly referred to as physical security information management solutions, or PSIM. In the same way that the brain and nervous system monitor, manage and control the body's functioning, a PSIM solution unifies and manages all security and safety-related systems to provide an integrated and complete picture of an organization's current state. Advanced

PSIM and situation management solutions go even further and provide incident management capabilities. But these technologies do not function in a vacuum, they continue to rely on video as one of the key components of the system.

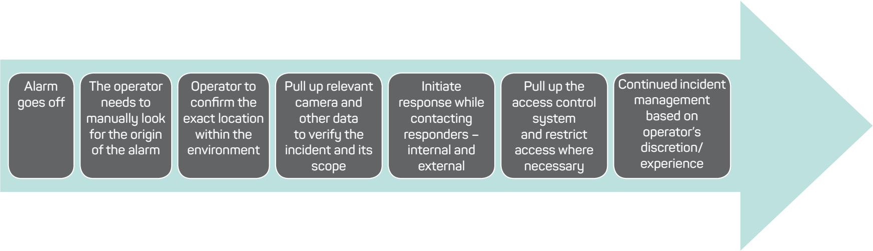
While a PSIM system is ideal for large and complex environments, not every organization, no matter how security conscious, requires a solution as specific and complex as a PSIM or situation management platform. The gap that exists between traditional VMS and PSIM solutions is one where many organizations' needs fall. Those organizations would benefit from the enhanced security that greater situational awareness and incident management capabilities bring. It is from this need that the next generation of VMS was born.

The gap that exists between traditional VMS and PSIM solutions is one where many organizations' needs fall.

Next-Generation VMS

As mentioned above, a PSIM solution integrates various sensors and systems within the control room, then correlates, analyzes and visualizes the information to present a complete picture to security operators. Video is critical to this. With this in mind, next-generation VMS goes beyond video management by integrating additional layers of information from a range of sources.

Figure 1. Fire alarm scenario without next-generation VMS.


Alarm goes off
The operator needs to manually look for the origin of the alarm
Operator to confirm the exact location within the environment
Pull up relevant camera and other data to verify the incident and its scope
Initiate response while contacting responders – internal and external
Pull up the access control system and restrict access where necessary
Continued incident management based on operator's discretion/ experience

Here is how next-generation VMS works, along with the benefits it provides. Video remains the main sensor, but, in addition:

- Data from other security systems, such as access control, fire detection, intrusion detection and alarm panels, are integrated with the VMS.
- The VMS is augmented with management capabilities over these same systems. Integrating the data from these core systems gives control room operators greater situational awareness, which can be further increased through geographic information system (GIS)-enabled visualization. Operators manage all of these integrated systems from the same interface (VMS), meaning no more switching between systems and applications.

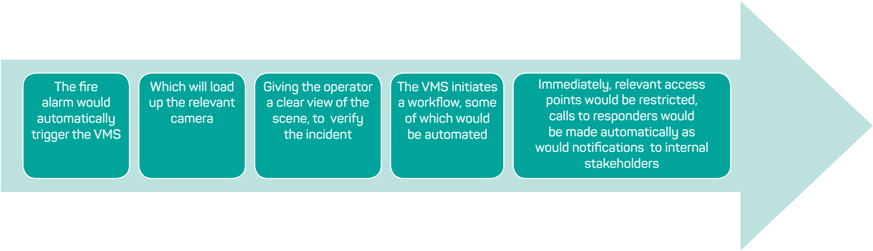
So what does this mean in real terms? Without the integration of these systems, a typical fire alarm scenario might go something like what is depicted in Figure 1. At a minimum, all of these steps would need to be taken. Ideally, they would happen in conjunction, rather than sequentially.

With next-generation VMS, however, many of these steps would be either eliminated or automated, and pre-defined workflows would ensure that everything gets done as it should. The scenario would be very different and might go something like what is seen in Figure 2.

Along with the increased situational awareness, next-generation VMS also comes with:

- Procedure enforcement tools
- Automation of tasks
- Customizable user interface
- Dynamic workflows that guide

Figure 2. Fire alarm scenario with next-generation VMS.


The fire alarm would automatically trigger the VMS
Which will load up the relevant camera
Giving the operator a clear view of the scene, to verify the incident
The VMS initiates a workflow, some of which would be automated
Immediately, relevant access points would be restricted, calls to responders would be made automatically as would notifications to internal stakeholders

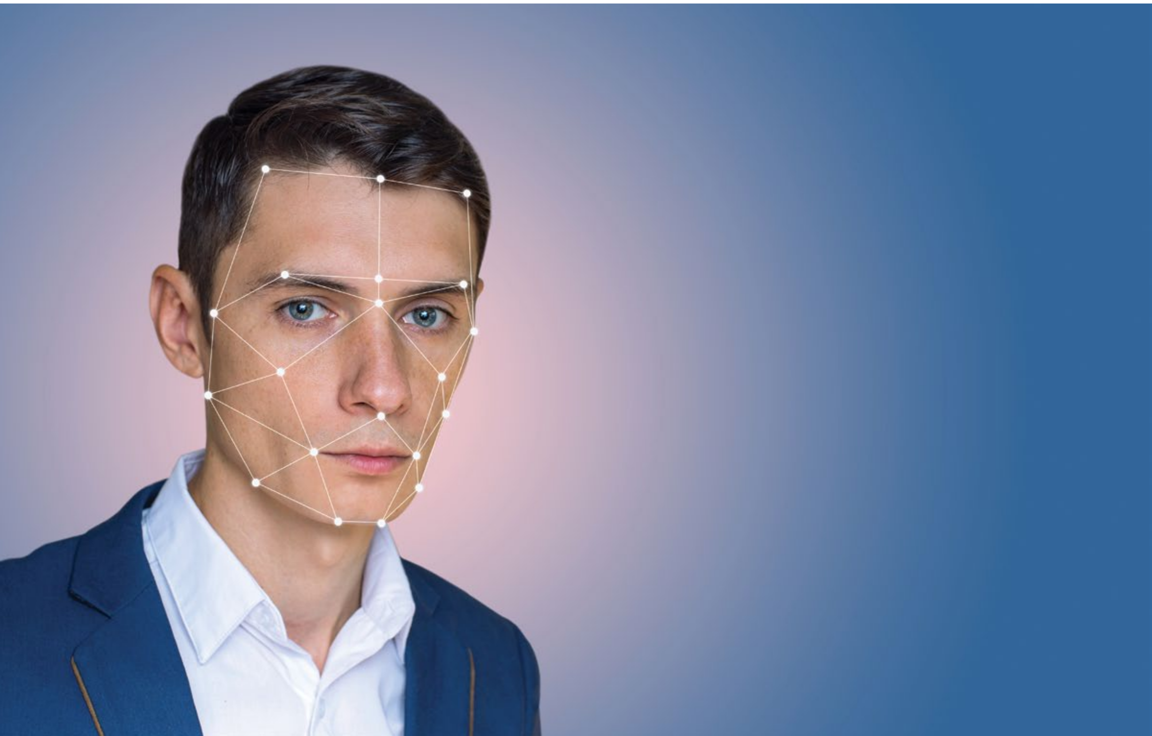
operators to a consistent, effective response

Adding More Data Layers

By integrating core security and safety systems – video, access control, intrusion, fire detection, etc. – layers of information can work together. And the more layers that are added, the smarter the system becomes.

As already mentioned, control room technology has gone through a tremendous transformation during the last decade, and that includes the use of video analytics. One of the more exciting and important developments in video analytics has been in the field of advanced search. Put simply, advanced search performs rapid forensic searches across extremely large volumes of recorded and live surveillance video, in order to track, locate and pinpoint missing people and suspicious persons and objects during time-critical situations. It can rapidly process data from thousands of camera feeds in a matter of minutes, even seconds. What used to take law enforcement or security personnel hours, days or

By integrating core security and safety systems – video, access control, intrusion, fire detection, etc. – layers of information can work together. And the more layers that are added, the smarter the system becomes.



even weeks – manually reviewing video – can now be done in minutes or seconds.

Advanced search works by continuously indexing every person that passes by every camera on the network in the facility. Because of this, it is always ready to conduct a search either in real time or after an incident. Operators just need to either upload a photo, use an existing image from a camera, or create an "avatar" based upon a description of the person who needs to be located. This image or avatar is used to filter out 95 percent of the images and present the operator with the most likely matches. And because advanced search also provides geospatial awareness, it is able to retrace the person's movements across cameras, identifying his or her current or last known location.

Now think about adding that layer of data to the integrated, next-generation VMS described above. One of the largest Level I trauma and burn research centers in the United States has done just that. Covering about 2.1 million square feet, the expansive medical center wanted to be able to more effectively track and locate missing, vulnerable patients and suspicious persons and to prevent infant abductions. They did this by combining wireless radio frequency technology, RFID bracelets and video surveillance with advanced search video analytics. If an infant is removed from a designated area, an alarm automatically triggers streaming video and advanced search.

VMS, Next-Generation VMS, PSIM or Situation Management?

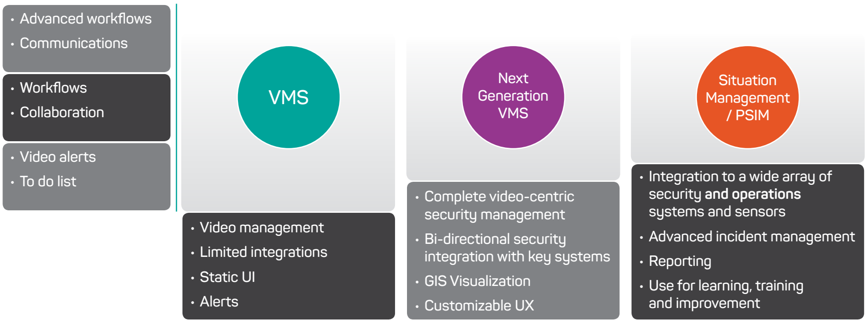
So, on the spectrum of available security solutions, where does next-generation VMS fit in? It is actually closer to a PSIM solution in terms of capabilities than it is to a traditional VMS. This is because a traditional VMS is focused on managing and extracting value from video, while next-generation VMS is a security management solution, similar to a PSIM, just not as extensive. And a situation management solution goes even further than a PSIM system, with organization-wide operational impact.

> Next-generation VMS is actually closer to a PSIM solution in terms of capabilities than it is to a traditional VMS.

In the past, the decision to implement either a PSIM, situation management or VMS-only solution was fairly clear-cut because the gap between traditional VMS and the other approaches was big enough that organizations were forced into one category or another. Next-generation VMS closes that gap, making the choice easier for some, but potentially more difficult for others.

What a next-generation VMS definitely does is address an unmet need in the market from security conscious organizations – hospitals, campuses, resorts, critical infrastructure facilities and others – that do not need a PSIM/situation management platform, but would benefit from some of the capabilities those solutions offer.

Figure 3. Capabilities of different video-based technologies and solutions.


· Advanced workflows
· Communications
· Workflows
· Collaboration
· Video alerts
· To do list
VMS
· Video management
· Limited integrations
· Static UI
· Alerts
Next Generation VMS
· Complete video-centric security management
· Bi-directional security integration with key systems
· GIS Visualization
· Customizable UX
Situation Management / PSIM
· Integration to a wide array of security and operations systems and sensors
· Advanced incident management
· Reporting
· Use for learning, training and improvement

For example, unifying systems into a single interface makes management of them much easier and less time-consuming. In some cases, the various systems become more effective as the merging of information enhances their performance.

System performance is not the only thing that can increase by introducing advanced management capabilities to the control room. The enforcement of procedures via prompting, notification and escalation helps ensure that operators are responding according to organizational standard operating procedures. This helps reduce the potential risk from operator error.

Standardization in the Control Room

In much the same way that most of the world works with a unified and integrated set of office computer tools, aptly named Office, mission-critical control rooms will increasingly move closer to a similar model. Control room technology will be managed by software that brings everything that is needed together. Next-generation VMS moves one step closer to that inevitable development.

Deciding Between Next-Generation VMS and PSIM

When is video management-only enough for an organization? And when does it need a wider-ranging, next-generation VMS, or an even more comprehensive solution? Answering these questions depends on an organization's challenges, needs, resources and budget.

Understanding the functionalities and benefits of the available options is a first step, but sometimes the distinction between the solutions is not clear, and it can be hard to tell what each provides. The information in Figure 3 can be used to help organizations match their needs with today's technologies and solutions.

When a traditional VMS cannot adequately address the needs of an organization, yet the scope and scale of challenges, or the available resources, do not support the implementation of a PSIM or situation management solution, then next-generation VMS may be just the right fit. ■ **Back to TOC**

Shawn Mather (smather@qognify.com) is director of global video and channel strategy for Qognify (www.qognify.com).

No longer the exclusive domain of complex, enterprise-wide security systems, sophisticated and cost-effective electronic access control is now available for smaller companies and single facilities with the same need for protection as larger organizations.

By the Power of Ethernet

PoE gives smaller facilities more access control options

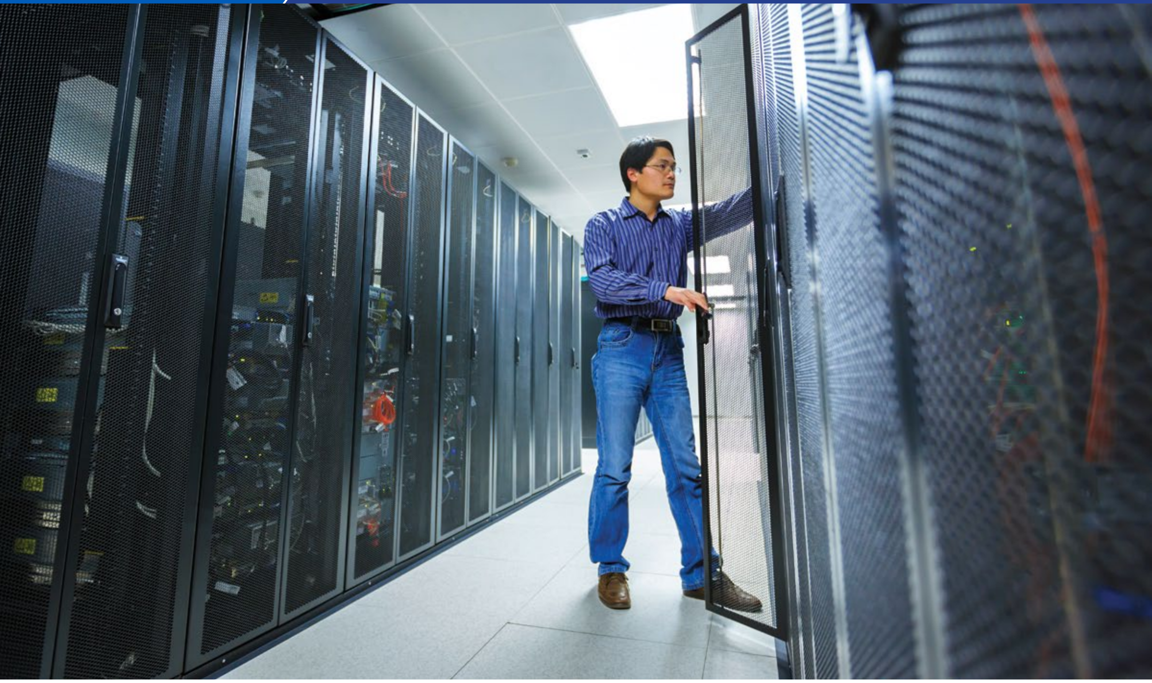
By Kerby Lecka
Security Door Controls

Physical electronic security for non-enterprise applications is now as simple as tapping into the nearest Ethernet connection to power and control doors via web browser and low-voltage access and egress devices. There are a variety of cost-effective, code-compliant, low-power solutions for electronic access control of door openings in smaller companies and single facilities that do not require complex and costly enterprise-wide systems.

Regulatory Compliance

Besides meeting national fire and life safety codes, physical electronic security via Power over Ethernet (PoE) hardware and IP-based access control can also meet the compliance requirements of many regulations not typically associated with access control, including:

- The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for



Economic and Clinical Health (HITECH) Act – Hospitals and health care facilities must comply with these two laws regarding the protection of personal health information and electronic health records, including limiting physical access to information systems, equipment and IT operating environments to authorized individuals.

- Sarbanes-Oxley Act – Requires organizations to store certain financial information in an auditable trail, have physical security, and maintain a system for monitoring and reviewing access on a periodic basis.
- Payment Card Industry Data Security Standard – Covers all businesses that accept credit card payments; Requirement 9 states that any physical access to data or systems should be appropriately restricted, with entry controls used to limit and monitor physical access to systems that store, process or transmit cardholder data.
- SSAE 16 – An auditing standard issued by the American Institute of Certified Public Accountants that restricts physical access to data centers through a combination of physical security systems and biometric identification.

There are many possibilities for cost-effective IP security and PoE hardware applications to meet these compliance requirements in smaller installations. Typically, medical and financial data records reside on computers or servers located onsite within these small organizations.

Data Rooms

No longer the exclusive domain of complex, enterprise-wide security systems, sophisticated and cost-effective electronic access control is now available for smaller companies and single facilities with the same need for protection as larger organizations. Data rooms are no exception.

From the outer door to the inner door separating visitors from employees, and even to the entrance to the "data" part of the center, low-voltage access control devices (PoE hardware) can be controlled via web browser. This includes creating "mantraps" that allow only one door to open at a time and require authentication for both doors. It can also include access control at the door to an individual computer processing room (data room) where the actual server, mainframe or other critical IT equipment is located. Even individual computer cabinets can be secured and connected to the network via low-power electronic cabinet locks.

Applicable, low-voltage PoE hardware solutions for access control include magnetic locks, key and exit switches, electrified exit devices, electric strikes, electrified locksets, electric bolt locks, and cabinet locks – all connected by Ethernet cable to an IP-based access control system.

Real-time monitoring, detecting unauthorized access or attempts, and keeping track of people, especially during a building evacuation in an emergency, is critical. Low-voltage keypads, card readers and proximity readers are popular key technologies for door access control, all tied to an IP-based controller that provides audit trails and user management to define who has access. These are also suitable for entrances like loading docks and other exterior facility doors.

Should the small company or single facility grow, these PoE hardware solutions and IP-based access controllers and software can serve as a foundation for unlimited, cost-effective expansion. Instead of paying upfront for a large and expensive access control system, users can add security and protection incrementally as budgets and needs increase.

Generally, applying the principle of least privilege is appropriate. Physical security is the key to all other IT security measures. Unauthorized physical access to servers and equipment is the weakest link in IT security and can have profound consequences.

> Using low-voltage PoE hardware and IP-based access control for physical electronic security is one of the easiest and most cost-effective means for preventing health care crime and violence.

Clean Rooms

Clean rooms require rigorous controls to protect products and processes from contamination by chemical vapors, aerosol particles, dust and airborne microbes. Prevalent in pharmaceutical, biotechnology, and high-technology industries, clean rooms provide protection primarily by limiting physical access and logging all access and egress activity.

As with data rooms, most physical electronic access control systems for clean rooms have been designed at the enterprise level for large facilities and organizations. Yet the clean rooms in smaller or single facilities must also prevent contamination using solutions within their budgets. Enter low-power PoE hardware devices and IP-based access control connected and powered by existing Ethernet connections.

Clean rooms typically utilize airlocks for entry and exit, a combination of a mantrap with two doors interlocked to prevent simultaneous opening and special timing functions to avoid unwanted passage between areas to ensure sterile and safe conditions. These procedures also maintain constant temperature, humidity and air pressure in the clean room. Access to these secure areas can be limited to authorized personnel through the use of low-voltage keypads, key switches and card readers. Of particular benefit

is the use of proximity readers to provide touch-free high security and contamination avoidance.

As with data rooms, all access and egress activities can be controlled with low-voltage PoE hardware connected to – and monitored in real time with – an IP-based controller, with records stored for future audit trails. This can ensure compliance with organizational policies and regulatory compliance with GMP and FDA 21 CFR Part 11.

Low-voltage, cost-effective clean room security also helps to maintain consistent product quality, preventing costly recalls and regulatory actions that can negatively affect reputation and the bottom line.

Health Care

The health care industry has recently experienced disturbing trends toward visitor impatience, patients in behavioral health facilities being more easily upset, and staff being unprepared to respond appropriately to bad behavior. These problems can involve access and egress of unauthorized people into higher-risk areas, potentially leading to violent incidents. All of this can be particularly acute for small, single facility entities like urgent care centers, outpatient surgery centers, and rural medical clinics that do not require enterprise-wide security systems but still need viable solutions.

Once again, low-power PoE hardware devices and IP-based access control powered with existing Ethernet cable offer a practical alternative. Although it is generally not an accepted practice to lock entry and exit doors to everyone who enters a hospital, clinic or health care facility, it is acceptable to control access to specific areas. Physical electronic security applied to funneling patients and visitors into areas can provide them with a positive, safe and secure experience. Restricting access into high-risk areas is also part of a well-designed program. These areas may include:

- Emergency Room
- Pharmacy
- Maternity
- Pediatrics
- Geriatrics
- Behavioral Health

Using low-voltage PoE hardware and IP-based access control for physical electronic security is one of the easiest and most cost-effective means for preventing health care crime and violence.

> Physical security is the key to all other IT security measures. Unauthorized physical access to servers and equipment is the weakest link in IT security and can have profound consequences.

Pharmaceutical facilities have come under increased scrutiny by the Food and Drug Administration (FDA) and the Drug Enforcement Administration (DEA) and greater pressure to comply with good manufacturing practices, good distribution practices, good storage practices and international World Health Organization (WHO) standards. Additionally, physical security and access control regulations from the Department of Homeland Security (DHS) and DHS's Chemical Facility Anti-Terrorism Standards (CFATS) must be adhered to in order to prevent access to dangerous chemicals by terrorists.

Small pharmaceutical manufacturers, wholesalers and logistics providers have few alternatives for physical electronic security solutions beyond the large, enterprise systems currently offered them. Yet they must also meet the many guidelines of FDA Title 21, Subchapter C, dealing with the security of facilities that "must be secure from unauthorized entry" and whose "access from outside the premises shall be kept to a minimum and be well controlled." Here, too, low-power PoE hardware devices and IP-based access control connected and powered by existing Ethernet cable is a viable, cost-effective, code-compliant solution for the needs of a small facility.

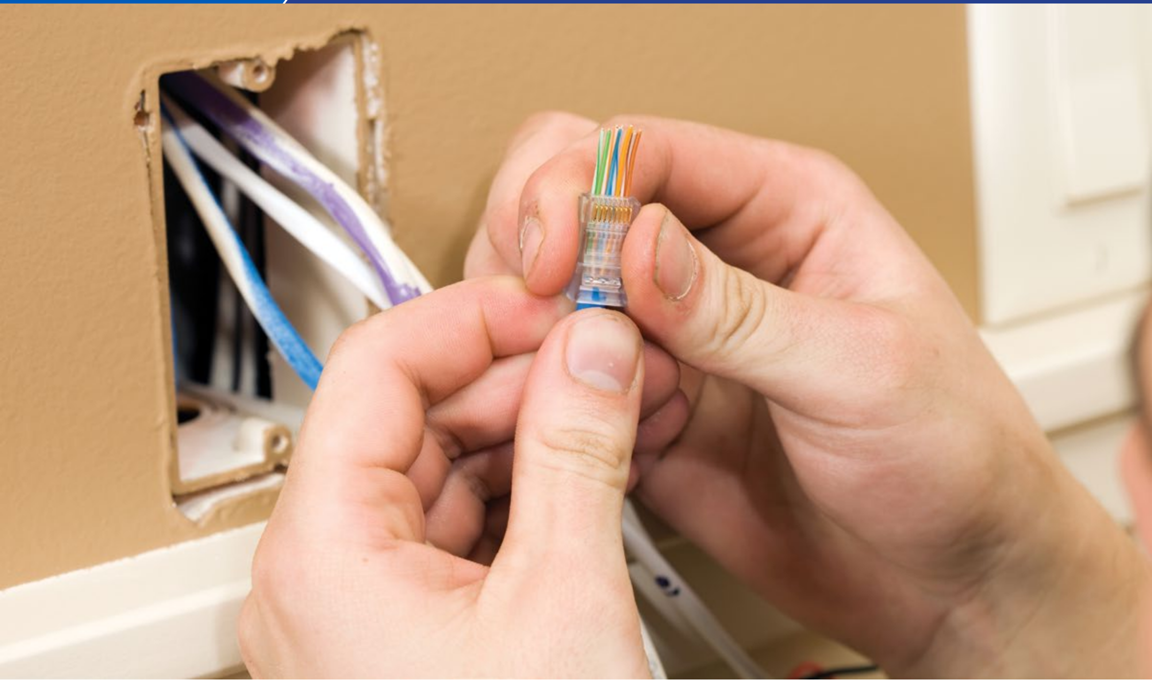
Imagine the savings in cost and installation time from being able to avoid long cable runs and power supplies for every door by simply tapping into the nearest Ethernet connection.

Data rooms and clean rooms are commonly found in pharmaceutical facilities, and the physical electronic security solutions previously described are equally effective here. The protection of people – e.g., researchers, executives, managers – is foremost, followed by the facility's critical assets, including the research/intellectual property and raw materials used to develop and manufacture products. As with other facilities, all perimeter exit doors and loading entrances can be included in the solution.

Retrofit Projects

Ethernet cable is everywhere. Buildings are smart. Imagine the savings in cost and installation time from being able to avoid long cable runs and power supplies for every door by simply tapping into the nearest Ethernet connection. Low-power, PoE-capable locking hardware connected to IP-based access control does just that by allowing easy integration and connection to a physical electronic access control system.

Physical electronic access control solutions are particularly suited to tenant improvement and retrofit



projects, providing the ability to purchase and install just what is needed without having to invest in a more costly enterprise system designed for larger facilities. The beauty of the PoE hardware and IP-based access control approach is that it is easily expandable as needs grow without a big upfront commitment to an oversized solution.

As with any tenant improvement or low-voltage implementation via Ethernet cable, it is recommended that installers be comfortable with Ethernet network best practices and test any installation by using an Ethernet cable tester before startup. Also, by following industry standards – ANSI/TIA-1005 (MICE) and ANSI/TIA-569C.0 (cable lengths) – many issues that are residuals of previous installations can be avoided.

Without a doubt, using viable, legacy Ethernet cable with PoE hardware and an IP-based controller will save money, time and manpower when retrofitting for physical electronic security. Plus, the building or facility can remain operational without the need to remove, install and recycle cable.

A smaller organization or facility can now meet many of the physical electronic security requirements of their industry by using lower-cost, low-voltage, easy to install and operate PoE hardware and IP-based access control solutions with existing Ethernet cable and avoiding the heavy cost commitments of complex, oversized, enterprise-wide systems. ■

Back to TOC

Kerby Lecka (kerby@wmwinc.com) is director of marketing for Security Door Controls (www.sdcsecurity.com).

From a lack of evidence stability and security to difficulties with sharing and cross-referencing, law enforcement is facing real challenges when it comes to video surveillance footage.

Law & Order & Video

Police and prosecutors need enhanced case management systems

By Pota Kanavaros
Genetec

In the security sector, while information is great, what we strive for is clear and actionable data. Both seeing and understanding are vital. To that end, we continue to deploy more cameras in physical security systems and collect and share more data than ever before. But this increase is not without its challenges. Managing and storing growing amounts of data can overwhelm systems that were not designed to accommodate the new types of digital data and metadata that are being collected by today's law enforcement tools.

In 2016, a national security researcher filed a federal lawsuit against an agency in the United States claiming that they were using an outdated software system for processing Freedom of Information Act (FOIA) requests. The issue for the researcher was that, by using what is essentially a computer-based card catalogue instead of a web-based search tool, this agency is not conducting searches in good faith.

According to the claim, while the agency is technically complying with FOIA requests, the time it takes to search its databases is unnecessarily long, and the results are often incomplete as they rely on outmoded and restrictive search methods. Regardless of the legal outcome, the filing of the suit points to the importance of data and how analog – in some cases, archaic – technology can hamper an organization's ability to search and manage it.

The Impact on Law Enforcement

One area that is particularly affected, both positively and negatively, by the changes in the amount of data being collected, is law enforcement. In an ideal world, an increase in the quantity and variety of digital evidence would mean that law enforcement would have more information with which to prevent and prosecute crime. However, when departments have to deal with old processes, unsearchable data, or an inability to keep up with the costs associated with data storage, video evidence may be underutilized.

Currently, many systems used by law enforcement agencies in North America are based on old technologies that use CDs/DVDs and agency computers to store digital evidence. The potential problems with this are extensive. From a lack of evidence stability and security to difficulties with sharing and cross-referencing, law enforcement is facing real challenges when it comes to video surveillance footage.

While the volume of evidence being collected and managed is increasing, law enforcement is not seeing an equivalent rise in cases being closed. Before we can begin to change this, we have to understand why the amount of data being collected by law enforcement is growing so dramatically.

Body-Worn is Booming

More than three-quarters of police cars in North America are equipped with dash cams and the number of sworn officers wearing body cameras is increasing. As of 2013, more than 30 percent of local police departments in the United States used body-worn cameras, and the percentage is significantly higher among major cities. The Department of Justice recently announced that it will make $75 million in federal grants available to provide as many as 50,000 body-worn cameras to local police departments.

We have seen that dash cams and body-worn cameras have the potential to help law enforcement improve relations with the communities they serve while increasing transparency and accountability. Researchers from the University of Cambridge's Institute of Criminology published the first scientific study on the impact of body-worn cameras. They found that the very fact that police were wearing cameras contributed to reducing both unnecessary use-of-force by officers as well as abusive behavior toward the police by the public.

But putting a camera in every patrol car and giving every sworn officer a camera is far more complicated than just purchasing a lot of hardware. When we consider the amount of footage being captured by these cameras as well as the metadata associated with this footage, we start to see why data collection, storage and management are such important issues.

When departments have to deal with old processes, unsearchable data, or an inability to keep up with the costs associated with data storage, video evidence may be underutilized.

More Data to Store and Archive

Overall, law enforcement is producing a lot more data. One of the reasons for this is that it would be counter-productive for them to capture low-quality video footage. To this end, the Department of Homeland Security (DHS) has published recommendations regarding body-worn cameras for police departments that include an image resolution of at least 640x480 pixels and a frame rate of at least 25 frames per second. By following these recommendations, law enforcement can ensure that they work with high-quality footage. However, this also means that they produce very large files, which can create storage and retention problems.

Recently, a police department in California began investigating the possibility of providing body-worn cameras to their officers. During this process, they learned that a 30-minute video took about 800 MB of storage space. If they were to provide every one of their 200 sworn officers with cameras, the department could potentially generate 33 terabytes of data each year.

Factoring in government-defined retention rates relating to each category of crime and the fact that, when data is used as evidence in a court case, the requirements become even longer, it is very likely that a large portion of this data will have to be stored for years, even decades, after it is collected.

The Institute of Criminology research highlights this concern. While it found that body-worn cameras appear to be cost-effective, with every dollar spent saving about four dollars in complaint litigation, it also found that the sheer volume of data storage required to support these programs has the potential to become crippling. Even as the equipment and technology has become less expensive over time and the return on investment has increased, other costs have the potential to skyrocket.

Putting a camera in every patrol car and giving every sworn officer a camera is far more complicated than just purchasing a lot of hardware.

Video from Other Sources

The police are not the only ones who are capturing more video evidence content. The number of civilians carrying smartphones capable of capturing high-quality video is increasing. People everywhere are now able to contribute to police investigations. Whether it is video taken intentionally of an incident or event in progress or captured accidentally when a person is filming something else, private smartphone video can play a pivotal role in helping to keep communities safe.

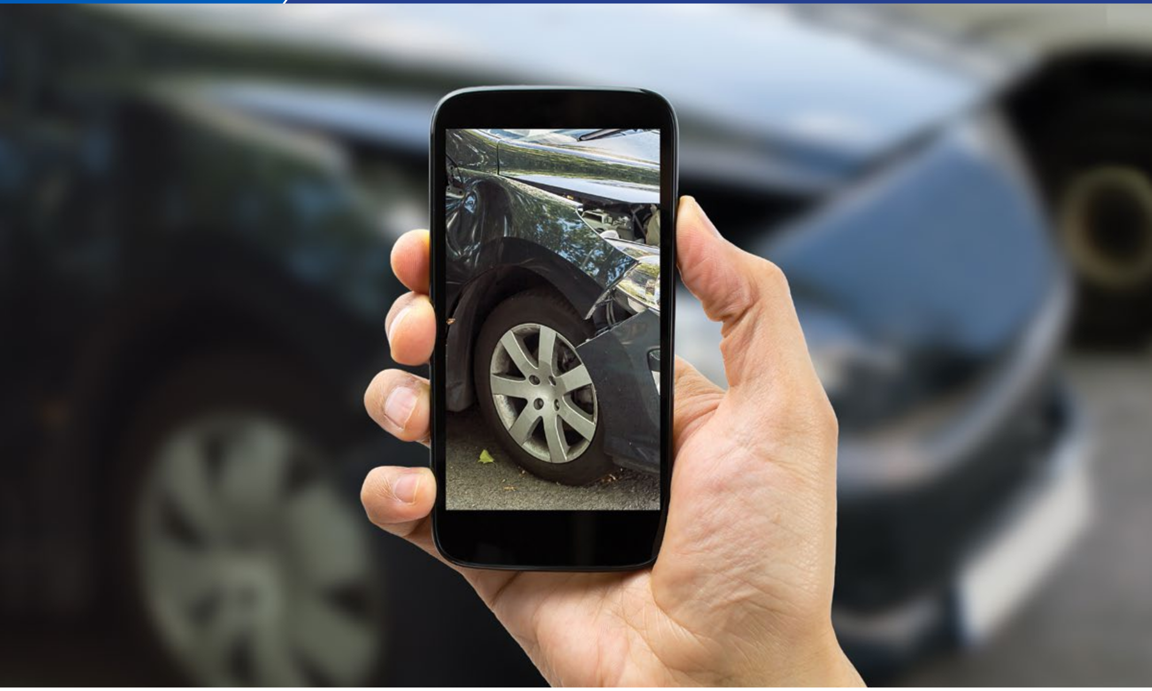
But how can we make this work? It is not feasible to have people just drop off USBs or DVDs of the video footage they collected. At the same time, we do not want to lose evidence that can help prevent or solve a crime.

The same can be said of video footage captured by private businesses, retailers and educational institutions. If they could share that video content with law enforcement, they could contribute to the protection of their communities.

While getting private businesses to share their video surveillance footage with law enforcement is less haphazard than having citizens with smartphones provide their footage, the same challenges exist, but on a larger scale. Namely, how does anyone effectively share video footage with law enforcement?

The Pressing Issue of Data

With the existing system, an average investigation can include multiple CD/DVDs of initial video surveillance footage from a crime scene, as well as other discs that result



from search warrants conducted over the course of the investigation. And, of course, investigations also include footage from in-car dash-cams, officer-worn cameras and footage from non-law enforcement sources. Then, as the case progresses, investigators might add discs from the lab and tape from every suspect interview.

Once law enforcement has finished its investigation, it must prepare the footage to be sent to prosecutors, defense lawyers and insurance companies. Because many law enforcement agencies rely on mail services to transport their video evidence, this preparation involves converting surveillance footage into a readable format and burning it onto a CD/DVD. And, in order to protect privacy, it also means redacting any faces that appear in the video. These manual tasks can take hours to complete.

Then, once the footage is received, legal staff must be able to call up specific pieces of information in the development and prosecution of a case. When everyone involved is forced to sort through CDs/DVDs, costs skyrocket and information can easily be missed.

Understanding the Full Cost

What are we actually discussing when we talk about cost? First, there is the basic expense of the system and all the time that law enforcement officers and technicians spend logging video evidence, converting surveillance footage into readable formats and redacting faces. Then there is the cost of burning and mailing CDs/DVDs. With this, there is also a potential cost associated with the inadvertent loss of footage from incidents, which can lead to case dismissals and millions of dollars in lawsuit awards or settlements.

In addition, this method of sharing video data can have a negative impact on the very system it is designed to support by causing chain of custody problems. When a CD/DVD is burned and transported manually, it can create questions about who has seen, touched or manipulated it. This can make building a solid case difficult and can end up costing law enforcement and prosecutors time, while costing municipalities and taxpayers money.

Finally, the time that officers, prosecutors and technicians spend on these – sometimes fruitless – tasks is time *not* spent on other activities, such as actually patrolling a community and making it safer.

Impact on the Legal System

Legal organizations have started setting policies and defining principles for how to manage data. These policies frequently relate to keeping costs and legal fees low during the discovery, pre-litigation and litigation phases of a case while, at the same time, ensuring the best possible legal support for clients. They focus on evidence management systems that help legal staff reduce the time spent searching data.

When it comes to reviewing video surveillance footage, examiners also face a number of shortcomings and difficulties when using some of the commercially available forensic tools. Many of these tools are costly, complex to use, able to analyze only one data source at a time, and complicated enough to require extensive examiner training in order to be used effectively. In addition, as data sources increase in size, complexity and type, forensic tools have begun to take even longer to perform specific functionalities. This can result in costly delays, as well as lapses in the legal process.

Case Management for the Future

As the amount of digital evidence per investigation continues to grow, the management of it threatens to become operationally and economically unfeasible for law enforcement. When the data being stored doubles every 18 months, it is unlikely that traditional case management systems, which were not designed to cope with these volumes, will be effective.

We need to think differently about digital evidence, and we need to develop solutions that will meet both current and evolving needs. Law enforcement agencies need a case management system that can help them turn the data they are collecting into higher case clearance rates. They need to be able to manage and store digital evidence from cameras and other devices in meaningful and scalable ways. In addition, these solutions must facilitate collaboration and the sharing of information with other departments, agencies and jurisdictions. And, at the same time, they must protect privacy.

A forward-looking case management solution should allow law enforcement to gather and synchronize data from a variety of sources, including video surveillance systems, body-worn cameras, smartphones, in-car dash cams, computer-aided dispatch, and record management systems. It should also save time on labor-intensive tasks related to evidence collection by converting and playing videos automatically, automating facial redaction, tracking chain of custody, automating reporting and helping both law enforcement and technicians locate media quickly.

> Law enforcement agencies need a case management system that can help them turn the data they are collecting into higher case clearance rates.

And, to encourage collaboration, the solution needs to be capable of integrating with multiple systems while also making it possible to manage user and group permissions as well as access rights for documents and cases. In this way, it would work to remove silos and standardize evidence collection by harmonizing digital evidence within an ecosystem of records management and case management systems.

We must not let the increase in video surveillance footage and other data overwhelm law enforcement agencies. It is imperative that we provide them with tools that will enable them not only to collect, store and manage all of this content, but also to use it as efficiently and effectively as possible. ■ **Back to TOC**

Pota Kanavaros (pkanavaros@genetec.com) is product marketing manager for Genetec (www.genetec.com).

Biometric characteristics can be a powerful tool to protect patients, providers and payers from fraud. Among biometric technologies, iris recognition is one of the most convenient, accurate, reliable and hygienic identifiers.

An Eye for Fraud

Iris recognition technology offers one of the most effective ways to prevent medical identity theft and false claims

By Jeff Kohler
Princeton Identity

In 2013, according to the FBI, insurance fraud totaled $80 billion. These costs are borne by insurers, but the companies typically pass them on to providers, who, in turn, may pass them on to patients. At the same time, providers are looking for better ways to protect their patients' medical identities, especially after an IBM report indicated that one out of three Americans had their health care data stolen or hacked in 2015.

While many payers and investigators have adopted new technologies to identify issues after claim submission, fraud is best prevented at the provider's office – before it can occur, as opposed to using "pay-and-chase" methods. Biometric characteristics can be a powerful tool to protect patients, providers and payers from fraud. Among biometric technologies, iris recognition is one of the most convenient, accurate, reliable and hygienic identifiers.

Payers are increasingly using methods such as big data analytics that identify irregularities to combat medical identity theft, phantom billing, and other forms of insurance fraud. However, these analytics are typically applied after a claim is paid.

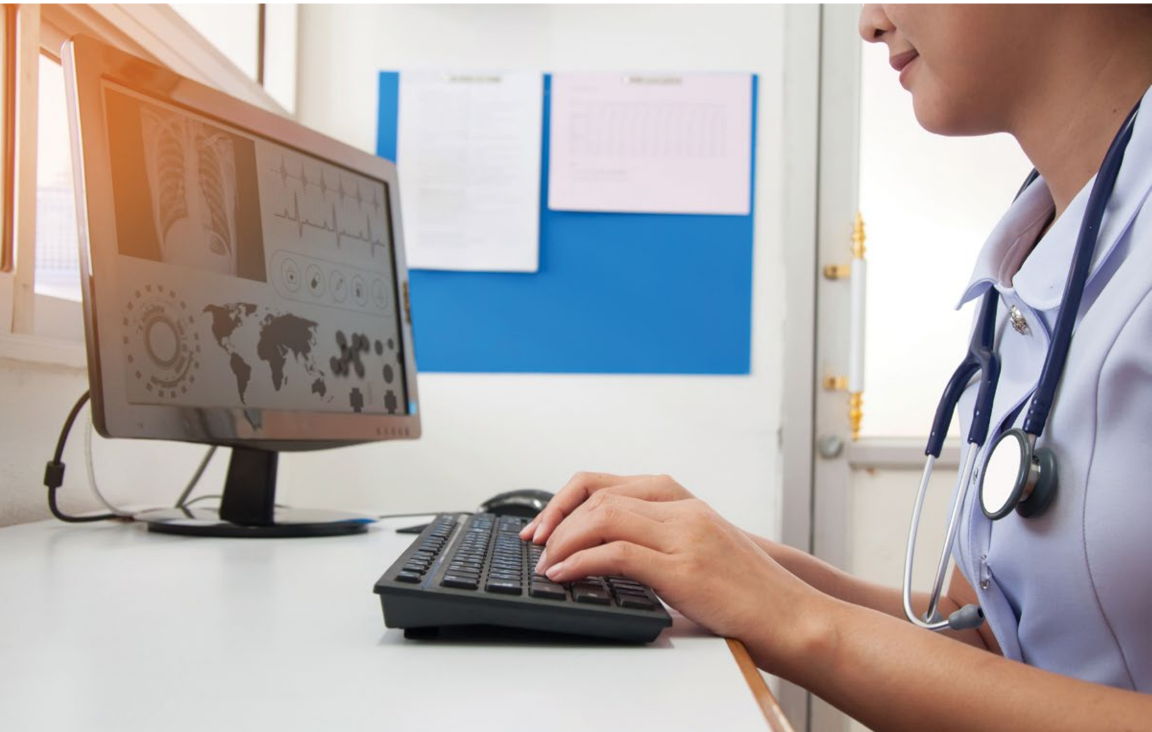
In the case of billing for services not rendered because a patient is not physically present, analytics cannot capture this type of fraud, since a claim can be coded by a fraudulent provider in a way that does not stand out as irregular. The largest provider clearinghouse in the United States, Change Healthcare, which processes more than 6 billion claims a year, estimates that phantom billing – billing for services not rendered – accounts for nearly 40 percent of all medical fraud.

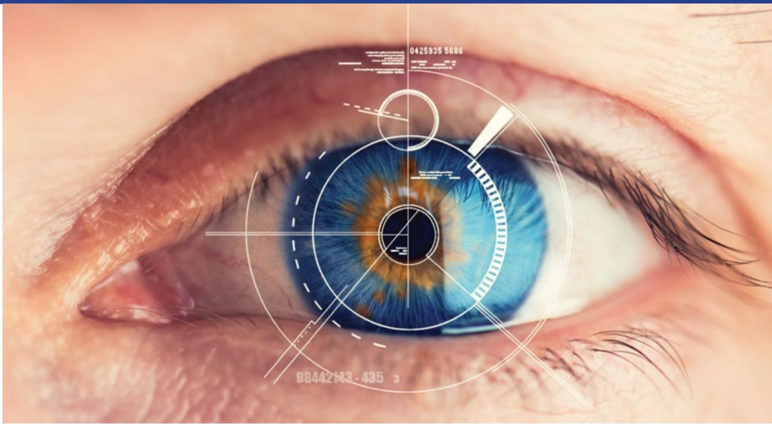
The best approach for protecting against fraudulent payments is to prevent them from occurring by adding a biometric identifier when patients sign in to a medical facility.

Fraud is best prevented at the provider's office – before it can occur, as opposed to using "pay-and-chase" methods.

Traditionally, when patients enter a provider's office, they sign in using only biographic information ("things you know") or ID cards ("things you have"). However, these can easily be stolen or lost. Accurate identification is best achieved by augmenting the biographic information with biometric characteristics ("things you are"). Adding a biometric layer protects patients from medical identity theft, protects providers from mistaken entries in the wrong electronic medical record, and protects payers from phantom billing.

Over the past several years, biometric usage has been expanding in both enterprise and commercial





markets. Vertical markets including border control, airports, data centers, banking, and health care are adding biometrics to increase security in applications for access control, time and attendance, and surveillance. At the same time, the convenience factor of biometrics continues to increase as more mobile phones add one or more modalities. Acuity Market Intelligence projects that 100 percent of the mobile market will include biometrics by the next decade. This combination of security and convenience greatly enhances the effectiveness of fraud prevention efforts.

While biometrics offer substantial increases in accuracy over traditional identification methods, there are multiple modalities to consider. Several characteristics, including fingerprint, voice and facial recognition, can change either naturally as an individual ages or as the result of external factors. To compensate for these potential alterations, patients must be re-enrolled in the system periodically to ensure the most current biometric information is available to provide the most accurate identification possible. This inconvenience can negatively affect both staff productivity and a provider's ability to ensure proper patient identification. Additionally, some biometrics, primarily fingerprint and hand recognition, require patients to make physical contact with a surface. This poses a potential hygiene issue, which can lead to disastrous results in a health care setting. Lastly, the potential of a false acceptance or false rejection varies by biometric type.

Of the many biometric characteristics, iris recognition offers one of the most accurate, reliable and hygienic identification methods. Iris patterns are the least likely to change, and recognition can be accomplished quickly and easily without requiring patients to make physical contact with a potentially unsanitary surface. Additionally, computing platforms and new mobile

Phantom billing – billing for services not rendered – accounts for nearly 40 percent of all medical fraud.

technologies deliver the convenience of performing iris recognition on devices that providers are already using comfortably. Enrolling and verifying patients can be accomplished with a simple click of an iris camera incorporated into or connected to a tablet.

With a mobile biometric solution, a patient's iris pattern becomes the unique key that unlocks access to his or her electronic medical record, guaranteeing that the correct record is opened every time. This also eliminates the possibility of an individual posing as another to take advantage of insurance benefits and protects patients from unknowingly becoming victims of medical identify theft. Ultimately, this streamlines the population management process and eliminates the potential for human error, especially for patients with the same name. This can shorten wait times and office visits, making patients less apprehensive about seeing a provider.

Of the many biometric characteristics, iris recognition offers one of the most accurate, reliable and hygienic identification methods.

All of these factors combine to deliver a powerful, accurate, convenient and reliable means of reducing the insurance and medical identity fraud that costs providers, payers and patients dearly each year. Real-time data is essential to combatting fraud, and iris recognition can provide insurance payers with instant confirmation of a patient's identity, as well as time and location information. The technology allows health care providers and payers to provide enhanced patient care while mitigating fraud with a single device. ■

Back to TOC

Jeff Kohler (jeff.kohler@princetonidentity.com) is senior director for product and business development at Princeton Identity (www.princetonidentity.com).

SIA Technology Insights Article List

All of the articles published by *SIA Technology Insights* since it was launched in 2013 are listed below by subject. The edition in which an article was published is noted after the title:

S17: Spring 2017
F16: Fall 2016
S16: Spring 2016
F15: Fall 2015
S15: Spring 2015
F14: Fall 2014
S14: Spring 2014
W13: Winter 2013-14
J13: June 2013

All editions are available at www.securityindustry.org/techinsights.

Access Control/Identity Management

More than Just a Silver Lining (S17)
Using the cloud for access control enhances scalability, availability, resiliency, flexibility and security
By Denis Hébert, Feenics

Walk this Way, Talk this Way (S17)
Combining gait analysis, voice recognition and other biometric identifiers provides a fraud-resistant security solution
By Maj. Gen. (ret.) Aharon Zeevi Farkash, FST Biometrics

A Matter of Trust (S17)
New digital identity technologies will increase security, functionality and convenience in many areas
By Stefan Widing, HID Global

By the Power of Ethernet (S17)
PoE gives smaller facilities more access control options
By Kerby Lecka, Security Door Controls

An Eye for Fraud (S17)
Iris recognition technology offers one of the most effective ways to prevent medical identity theft and false claims
By Jeff Kohler, Princeton Identity

Raising the Standards (F16)
Physical access control can benefit from adopting an IT-centric approach
By Scott Sieracki, Viscount Systems

In a Hand or a Face (F16)
Fingerprints, facial recognition and other biometrics can make banking more secure
By Amy McKeown, 3M

From Legacy Systems to Advanced Access Control (F15)
New solutions can offer extensive benefits to municipalities
By Robert Laughlin, Galaxy Control Systems

Unlocking the Door (F15)
Next-generation access control systems can offer new insights and greater security
By Scott Sieracki, Viscount Systems

Striking the Balance Between Security and Safety (F15)
Classroom door locks are invaluable, but they must allow quick egress
By Mark Berger, Securitech

Get Up and Bar the Door (F14)
Access management and door hardware play a critical role in school security
By April Dalton-Noblitt, Allegion

Who Is Entering Your Facility? (F14)
Verifying identities is challenging; partnerships can help
By Daniel Krantz, Real-Time Technology Group

Say Hello to Social Spaces (S14)
Social Applications will transform the security experience
By Steve Van Till, Brivo Systems

Fingerprint Biometrics for Secure Access Control (S14)
Moving beyond passwords and tokens can enhance security while decreasing costs
By Consuelo Bangs, MorphoTrak

Integrating Card Access with Interlocking Door Controls (S14)
While there may be implementation challenges, interlocks can greatly enhance portal security
By Bryan Sanderford, Dortronics Systems

Frictionless Access Control: A Look over the Horizon (S14)
New uses of biometric and RFID technologies could make access badges obsolete
By Henry Hoyne, Northland Controls

More Security, From Bottom to Top (S14)
Buildings are increasing entrance controls on the main floor and upstairs
By Tracie Thomas, Boon Edam

Hardware Security, Today and Tomorrow (W13)
Advances in door technology are enhancing both safety and convenience
By Will VandeWiel, DORMA Americas

Secure Authentication without the Cost and Complexity (W13)
New technologies are narrowing the gap between passwords and stronger authentication solutions
By Ken Kotowich, It's Me! Security

From Access Control to Building Control to Total Control (W13)
How innovation drives the need to update product standards – and ways of thinking
By Michael Kremer, Intertek

The Technology Behind TWIC (J13)
Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?
By Walter Hamilton, Identification Technology Partners

Big Data

Transforming Data into Actionable Intelligence (F15)
New solutions can identify insider threats before it is too late
By Ajay Jain, Quantum Secure

The Evolution of Risk (F15)
Banks are using analysis of 'big data' to enhance security
By Kevin Wine, Verint Systems

Reducing Retail Shrink with Business Intelligence Software (F15)
Data mining can be a valuable new tool for loss prevention professionals
By Charlie Erickson, 3xLOGIC

Cybersecurity

IoT Makes New Security Partnerships Essential (S16)
Bringing physical security and IT security together can enhance both
By Rob Martens, Allegion

Because You Can Never Be 100% Cybersecure (S16)
Effective use of strategies for countering attacks can minimize risk
By James Marcella, Axis Communications

Becoming Predictive, Rather than Reactive (S16)
A holistic view of physical and logical identities can help to identify insider threats
By Don Campbell, Quantum Secure

A Standard Response to IoT's Security Challenges (S16)
Technical standards are essential to securing billions of connected devices
By Steve Van Till, Brivo Inc.

Don't Be the Weakest Link (S16)
Security, IT departments must work together to reduce vulnerabilities
By Stuart Rawling, Pelco by Schneider Electric

Creating a Cybersecure Physical Security Enterprise (S16)
Simplicity and convenience are the enemies of security
By Paul Galburt, IPVideo Corporation

A CEO's Guide to Cybersecurity (S16)
Identifying and addressing vulnerabilities must be a priority
By Hans Holmer, Intelligent Decisions

Tackling the Complexities of the Connected World (S16)

Enterprise security must be a team effort

By Herb Kelsey, Guardtime

The Importance of Practicing 'Due Care' in Cybersecurity (S16)

Taking appropriate precautions can prevent security equipment from being a cyber vulnerability

By Dave Cullinane, TruSTAR

Beginner's Guide to Product and System Hardening (S16)

From the SIA Cybersecurity Advisory Board

Keeping the Security System Secure (F15)

Ensuring that video stays online is key to managing risk

By Bud Broomhead, Viakoo

Target, eBay … and You? (F14)

Cybersecurity threats are real, even for small businesses

By Hank Goldberg, Secure Global Solutions

Electronic Security Meets the Ecosystem (J13)

IP devices increase both rewards and risks. How secure is your system?

By Pedro Duarte, Samsung Techwin

Fire and Life Safety

Removing the Barriers: The Wireless Side of Fire Protection and Life Safety (S15)

The industry's wireless movement is fueling innovation

By Richard Conner, Fire-Lite Alarms and Silent Knight

The (Slow) Transition to IP in Fire and Life Safety Devices (J13)

Codes and regulations often force fire and life safety equipment to use older technology, but that is changing

By Christopher Peckham & Walter Frasch, Kratos Public Safety and Security Solutions

Integration

Out of Many, One (S17)
Integrating components of a security system can vastly improve effectiveness
By Brian Wiser, Bosch Security Systems

Commanding the Enterprise (S15)
New software platforms enable security leaders to ensure awareness, manage risk
By Rob Hile, SureView Systems

Tying It All Together (S15)
Integrating video surveillance, access control, building management and other systems can enhance security and reduce costs
By Mitchell Kane, Vanderbilt Industries

Safe on the Water (S15)
Integrated solutions secure the nation's largest independently owned commuter ferry operation
By Kostas Mellos, Interlogix

Broken Promises: The Current State of PSIM (F14)
Physical security information management solutions have so far fallen short of expectations, but next-generation systems could change that
By David Daxenbichler, Network Harbor

Enhancing Continuity Planning through Improved Security (F14)
Web-based systems can tie everything together
By Kim Rahfaldt, AMAG Technology

Technology-Enabled Collaboration Builds Safe Cities (S14)
Better management of more information can enhance the protection of people and property
By Itai Elata, Verint Systems

Solving a Big Problem for Small Businesses (W13)
New security technologies offer integrated solutions for small and medium enterprises
By Scott McNulty, Kantech

Intrusion Detection/Alarms

A Laser Focus on Enhanced Security (F16)
New scanners can improve the accuracy and reliability of intrusion detection systems
By Patrick Hart, Optex

Integrating Intrusion (S15)
Video and access have converged on the network; the time has come for intrusion detection to join them
By Mark Jarman, Inovonics

Integrating Technology with Telephone Service at Central Stations (W13)
IVR implementation can be challenging, but when done well, it can significantly increase capacity and customer satisfaction
By Jens Kolind, Innovative Business Software

Related Issues

Up in the Air (S17)
Drones powered by artificial intelligence could transform security
By Cary Savas, Nightingale Security

The Real Benefits of Artificial Intelligence (S17)
'Computer vision' powered by AI could radically change video surveillance
By David Monk, Umbo CV

Threat from Above (F16)
How can potentially dangerous drones be detected and defeated?
By Logan Harris, SpotterRF

Augmented Reality is for More than Capturing Pokémon (F16)
When combined with IoT, the technology could have a big impact on security
By Rob Martens, Allegion

A Sound Solution in Transportation Security (F16)
Audio monitoring can enhance situational awareness, reduce crime
By Richard Brent, Louroe Electronics

Maintaining Power (F15)
New network communication solutions can minimize system downtime
By Ronnie Pennington, Altronix

Do You Hear What I Hear? (S15)
Audio technology is redefining the surveillance industry and has become an essential component of security systems
By Richard Brent, Louroe Electronics

Enabling Safe Learning Environments (F14)
Securing schools demands a layered approach
By Neil Lakomiak, UL

From Horse-Drawn Wagon to Moving Truck (F14)
Nearly a century after the first VBIED was detonated in the U.S., what can be done to mitigate the risk of car bombs?
By Laurie Aaron, Building Intelligence

What Is in Store for the Physical Security Community (S14)
New technologies will open up great opportunities for the industry
By Bill Bozeman, PSA Security Network

Security and Privacy in a Connected World (J13)
With proper planning and precautions, security and privacy can complement – not compete with – each other
By Kathleen Carroll, HID Global

A Case for a Green Security Landscape (J13)
Sustainability can be good for both the environment and the bottom line
By John Hunepohl & Aaron Smith, ASSA ABLOY

Video Surveillance

VMS: The Next Generation (S17)
Facilities can now extend video management systems to provide a more complete security solution
By Shawn Mather, Qognify

Law & Order & Video (S17)
Police and prosecutors need enhanced case management systems
By Pota Kanavaros, Genetec

A Needle in a Video Haystack (F16)

Event-driven intelligence can identify the most important elements in surveillance data

By Steve Birkmeier, Arteco

Video Storage Wars (F16)

Hyper-convergence technology can simplify surveillance storage and enhance security

By Brandon Reich, Pivot3

Big Video Data (F15)

Video management systems offer a powerful platform for security and business intelligence

By Jeff Karnes, 3VR

The Public Safety Data Lake (F15)

Making the right decisions regarding storage and other issues can vastly increase the value of video surveillance

By Ken Mills, EMC

The Sun Shines on Surveillance (S15)

Solar power enables wireless video solutions in remote locations

By Dave Tynan, MicroPower Technologies

Surveillance in the 21st Century (S15)

Smart, 3-D, 360-degree cameras that see in the dark are on the way

By Jumbi Edulbehram, Oncam Grandeye

10.7 Billion Security Challenges (S15)

As transit ridership increases, so must security

By Steve Cruz, Panasonic

The Future of Video Surveillance (S15)

A rapidly changing security landscape will provide new ways to meet end users' needs

By Alex Asnovich, Hikvision USA

Making Campuses Safer with Innovative IP Technologies (S14)

Networked systems mean more information, more collaboration and more security

By Kim Loy, DVTEL

Harnessing the Increasing Power of Video (S14)
New functionalities and greater ease of use enhance the value of video in both security and non-security applications

Megapixel Cameras Go Mainstream (W13)
Functionality, versatility, clarity make megapixel video the future of surveillance
By Scott Schafer, Arecont Vision

Seeing the Big Picture: 360-Degree Camera Technology (W13)
High-resolution panoramic video overcomes the limits of PTZ cameras
By Steve Malia, North American Video

Achieving IP Video Management System Scalability through Aggregation (W13)
Video isn't just about security anymore
By Jonathan Lewit, Pelco by Schneider Electric

What's New on the Video Surveillance Front? (J13)
A keener eye, a longer memory and a sharper IQ
By Fredrik Nilsson, Axis Communications

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security (J13)
As technology advances and prices fall, thermal cameras have become a cost-effective way to secure the perimeter
By John Romanowich, SightLogix

Video Analytics in the Modern Security Industry (J13)
Analytics can make cameras smarter, but how smart can they get?
By Brian Karas, VideoIQ

The Untapped Benefits of Recorded Video Surveillance (J13)
Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing this data possible
By Rafi Pilosoph, BriefCam

Back to TOC

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md. All editions are available at no charge at www.securityindustry.org/techinsights. Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

securityindustry.org/techinsights

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