Catch 'em All
What Pokémon and security have in common

Laser Show
Using active energy to enhance intrusion detection

A Face in the Crowd
Financial institutions look to biometrics

SIA Technology Insights

Volume 4, Issue 2
Fall 2016

Welcome

Dear Reader,

Drones. Augmented reality. Event-driven intelligence.

This is not your father's security industry. Really, it's not even your older brother's.

The pace of technological change in physical security seems only to increase, so much so that the very definition of the security industry is changing. A sector that includes the technologies listed above – each of which is addressed in this issue – and that overlaps more and more with cybersecurity is not the same as the one we knew not too many years ago. The ends remain the same – managing risk and deterring, detecting and defeating intruders – but the rapidly evolving means are altering the ways that we think about achieving those goals.

If you've been in the industry for a while, think back to how differently a security system looked at the start of your career, as you read these articles. And, whether you're a veteran or a newcomer, try imagining what security solutions will grow out of the technologies described in these pages during the next few years. The possibilities are both exciting and important, as the role of security is no longer just crime prevention, but anti-terrorism and business continuity, as well.

We hope that *SIA Technology Insights* will not only provide you with information about the security technologies that are available today but also give you a glimpse of what could be coming. We encourage you to let us know how we're doing by submitting comments and article suggestions to the editor, Ron Hawkins, at rhawkins@securityindustry.org. And if you're holding this publication in your hands, please note that an online version and all past editions are available at www.securityindustry.org/techinsights.

Thank you for reading.

Sincerely,

Don Erickson

Denis Hebert
Chairman, Board of Directors
Security Industry Association

Don Erickson
CEO
Security Industry Association

How to Navigate Through the Magazine

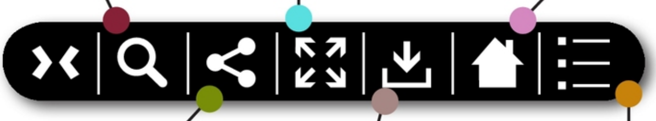
Navigation Bar

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

Click the search button to look for keywords.

Click the fullscreen button to view page.

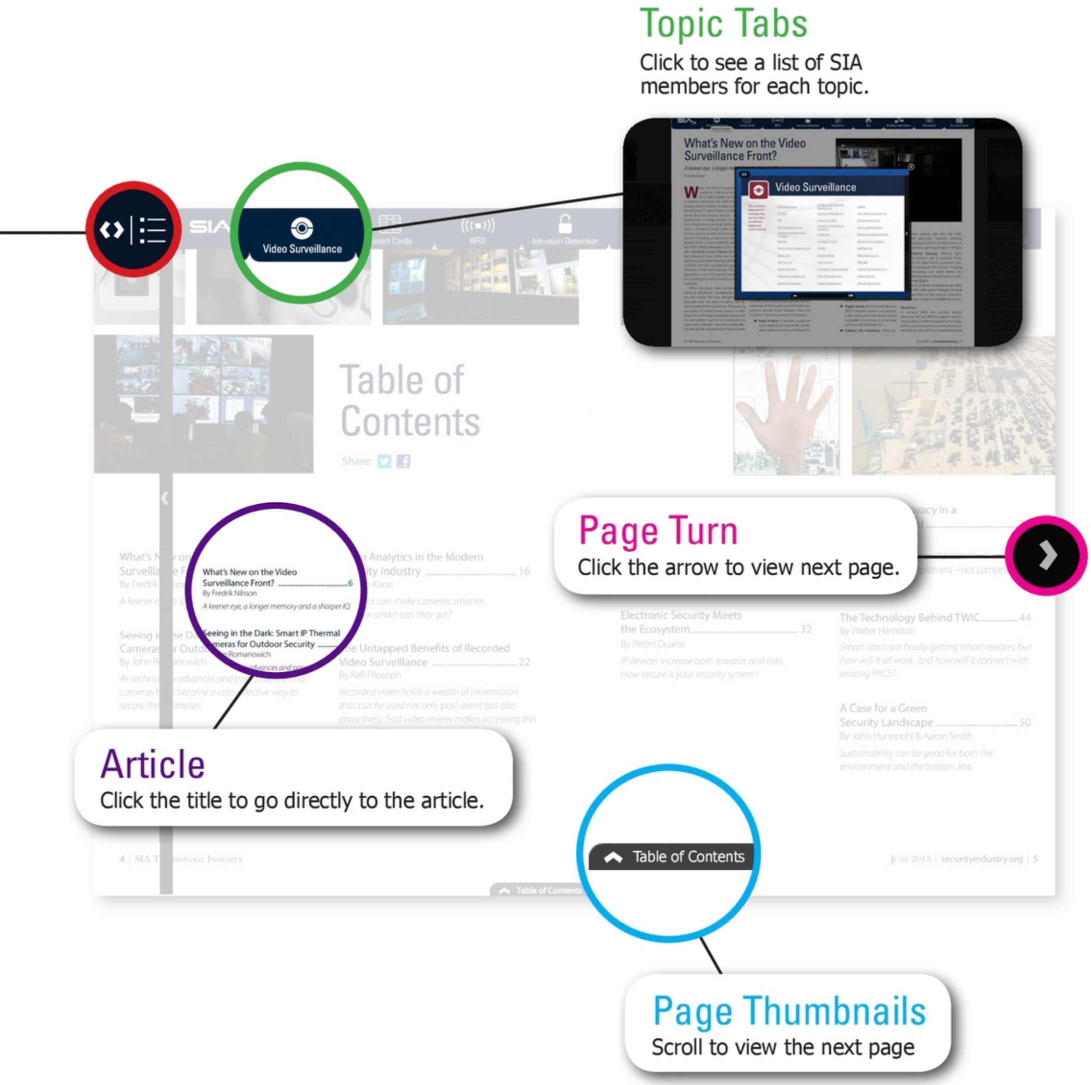
Click the home button to go back to the cover of this Magazine.



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

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

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


SIA
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
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
Table of Contents
What's New on the Video Surveillance Front?
Video Surveillance

Topic Tabs

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

Page Turn

Click the arrow to view next page.

Article

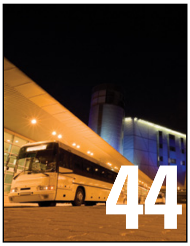
Click the title to go directly to the article.

Page Thumbnails

Scroll to view the next page

Table of Contents

36


44

52

60

Because of the potentially disastrous consequences posed by improper drone use, there has been a recent upsurge in the development of technology that can be used to mitigate drone threats.

Threat from Above

How can potentially dangerous drones be detected and defeated?

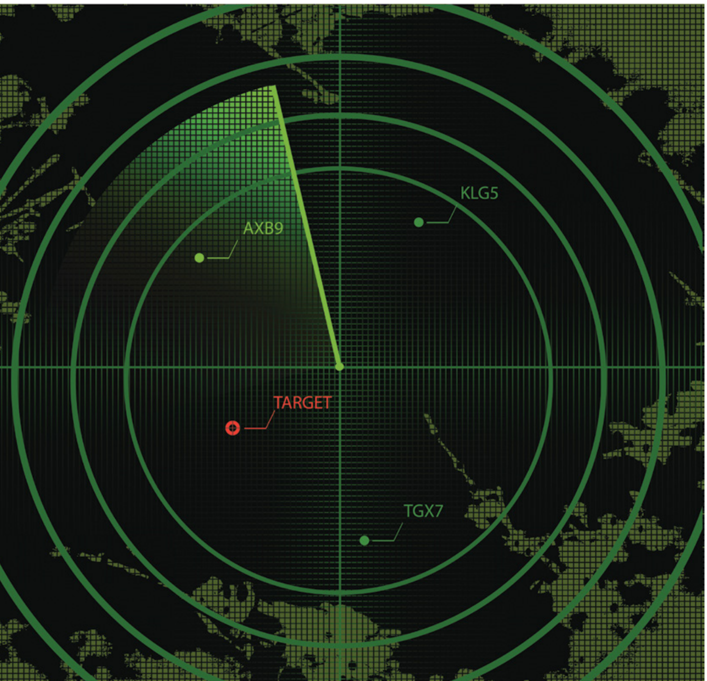
By Logan Harris
SpotterRF

Unmanned aerial vehicles (UAVs), or drones, have been in use for many years, but had not been widely adopted by the mass market until recently. With that adoption has come many new and productive applications of drones, but new threats have also emerged in a wide variety of areas. For example:

- "The Pentagon has seen both commercially bought quadcopters and fixed-wing type unmanned aircraft systems used in an improvised manner to both deliver IEDs and for reconnaissance," Joint Improvised-Threat Defeat Agency spokesman David Small wrote in a July 6 email to *Inside the Pentagon*.
- In 2015, 21 drone sightings were reported to the U.S. Fire Administration in Arizona alone and nine of those forced the grounding of firefighting aircraft.
- According to sports security experts, finding a football game without a drone is now the exception. How long before

one disperses a chemical or biological agent over a crowd of 50,000 or more fans?

- In 2014, the Federal Energy Regulatory Commission reported that destroying as few as nine electrical substations could take out the entire U.S. power grid for more than one year. How long before terrorists try launching a coordinated attack using low-cost drones?
- According to a recent report by Open Briefing, a London-based civil society intelligence agency, some drones are capable of carrying payloads of as much as 1,000 kg of explosives, which is more than three times the amount said to have been used by al Qaida to bomb the U.S.S. Cole in October 2000. How long before a terrorist delivers such a payload to a nuclear power plant or a busy bridge carrying 200,000 cars per day?



Because of the potentially disastrous consequences posed by improper drone use, there has been a recent upsurge in the development of technology that can be used to mitigate drone threats, though many of the approaches have not yet been approved by the Federal Aviation Administration (FAA).

Technology Solutions

Geofencing of Commercial Drones

Drone manufacturers are now embedding programs into their drones that do not permit them to fly above areas such as airports and the White House. However, these can be easily circumvented by disabling the GPS and flying under manual control.

There are many companies that use a variety of technologies to detect, identify and respond to drone events. Each of these technologies has pros and cons.

The first step in the security workflow is to detect the threat. There are four main types of sensors that are being used to detect drones.

Video

Cameras, both optical and thermal, are limited by a very narrow field of view (less than 4 degrees for detection out to 300 meters) in order to get enough pixels on target to detect that there is a drone in the area. Plus, environmental conditions such as rain,

Summary of Detection Technologies

	Night and Day	Rain	Fog	Snow	Clutter	Wide Area	Auto Detect
Optical	X	X	X	X	✓	X	✓
Thermal	✓	X	O	X	X	X	✓
Acoustic	✓	X	✓	X	X	X	✓
Radio	✓	✓	✓	✓	X	✓	O
Radar	✓	✓	✓	✓	O	✓	✓

fog, snow or dust can severely affect camera performance. Combining different lighting conditions and video analytics, cameras are unable to reliably detect a drone outside of very short ranges (less than 100 meters).

Acoustic Sensors

Acoustic sensors listen for the sound that a drone makes. In certain quiet conditions, these sensors have proven to be successful in detecting particular types of drones within a 50 to 100 meter radius, but they are unable to precisely determine the location. Acoustic sensor effectiveness is significantly reduced when rain or snow is falling because the sound from the drone is obscured. This same effect occurs with background noise, such as in urban environments.

A new class of radar has arisen called compact surveillance radar (CSR), which picks up small, slow-moving targets and provides precise location information about them.

Radio Sensors

Radio sensors listen for the radio communication between a drone and its controller. Because drones are able to operate autonomously with no communication to the controller, however, radio sensors are not always able to detect them. Another limitation of radio sensors is that they have to recognize the unique type of communication that occurs for each and every make and model of drone, which means there will always be drones that the radio sensors do not recognize. The benefit of radio sensors is that they are able to cover wide areas, as long as there are not a lot of other radio transmitters in the area; otherwise, the radio signal of the drone can be lost among all of the background signals.

Radar

Radar has been used since World War II to detect airborne objects at long ranges and over wide areas. Radar is not affected by weather conditions and does not require there to be any communication between a drone and its operator. However, radar in the past was designed to detect fast-moving planes, not small drones that are moving very slow and low. For this type of older radar, the drones are just background clutter that is rejected. Recently, though, a new class of radar has arisen called compact surveillance radar (CSR), which picks up small, slow-moving targets and provides precise location information about them. These small radar devices can be pointed up at the sky so that they do not pick up ground clutter. A limitation of CSR is that it will also detect and track birds, which increases the number of false detections. New artificial intelligence algorithms, however, have been successfully applied to train systems to recognize the difference between birds and drones.

Identification or Classification

The next step in the threat response chain is to identify or classify the nature of the threat. While acoustics, radar and radio are able to detect a drone, it is difficult for these technologies to provide much information on the nature of the threat that the drone may present. For instance, is the drone carrying a camera or other payload? Is it a hobby drone or one with a larger payload?

If precise location information is known, then an optical/thermal camera can be used to evaluate the threat. Using cameras with sufficient zoom and resolution allows an operator to identify the type of drone and any payload that is visible. High-quality continuous zoom thermal cameras have the best contrast and image capability across both day and night operations.

Summary of Response Methods

	Liability	Legal	Difficulty	Availability
Kinetic	X	X	X	✓
Drone vs. Drone	O	X	X	O
GPS Spoofing	X	X	X	X
Hacking	✓	X	X	X
Jamming	✓	X	✓	✓
Locate Operator	✓	✓	O	✓

Various mechanisms can be used to alert an operator that a drone is in restricted airspace. These methods include pointing a laser dazzler or spotlight at the drone, which requires an accurate real-time location reading. If the drone continues into the restricted area, then it can be inferred that the operator has ill intent and is not just an uninformed hobbyist. A higher-level response is then warranted.

Response

There are a number of ways to respond to drones, ranging from shooting them out of the air to jamming their communication link and GPS. Some are considerably easier to accomplish than others, and legal advice should always be sought before purchasing or deploying any solutions.

> There are a number of ways to respond to drones, ranging from shooting them out of the air to jamming their communication link and GPS.

Kinetic

Shooting a drone is viable at ranges of less than 100 meters. Beyond that, it is very difficult to aim a rifle or shotgun precisely enough to damage the drone. One must also consider the liability and legal issues related to firing a weapon at a drone, which includes responsibility for wherever the discharged rounds may end up. In most cases, this type of response is illegal.

An alternative to a shotgun is a net gun that shoots a net to envelope a drone. The main limitations of this method are range and accuracy. The farthest that these guns can shoot a net is 100 meters, and hitting a moving target with one is very difficult. However, for short-range stationary drones, net guns can be effective.

Drone vs. Drone

Drone wars can be fun to watch but they are not very practical. It is very difficult to fly a drone into another drone, especially when the other drone is moving at a high rate of speed and is trying to avoid the attacking drone.

Also, given FAA regulations stating that all commercial drones must only be flown within line of sight of the operator, it is very difficult to scale this solution at this time. This option may develop in the future as regulations change and on-board drone sensing capabilities improve.

GPS Spoofing

Another electronic response method is to make the drone's GPS receiver think that it is much higher than it is. The drone then drops down to a lower altitude and comes in contact with the ground. The problem with GPS spoofing is that it could also affect the GPS receivers of other devices. GPS spoofing devices are still very much in the R&D phase and are not something that can be purchased at this time.

Hacking

Hacking a drone's communication link has been done with a number of commonly used drones that have unencrypted communications. Commands can be sent to the drone to return home or land. While effective for some drones, the rapidly changing protocols and the addition of encryption to drone communications mean that there will always be drones that cannot be intercepted by this method. Some companies are starting to offer these systems commercially, but they have a limited number of drones that they are able to intercept.

Jamming

Currently, all drones rely on either a communication link or GPS for navigation. The frequencies used for communication and video are typically in the WiFi bands of 900 MHz, 2.4 GHz and 5.7 GHz. If precise location information is known, the communication link can be jammed with a focused beam of energy that is not dangerous to people or other devices. This type of jamming has been shown to be effective up to ranges of 1 kilometer. Once a drone loses its communication link, the default action is typically to return to where it took off. This allows security personnel to follow the drone and, possibly, find the drone operator. This method is effective against all drones and knowledge of the exact model is not required. There are a number of jamming systems that are commercially available where regulations permit.

GPS jamming should only be used as a final resort after attempts to jam the communication link have failed and the drone is considered an immediate threat. GPS jamming is similar to communication link jamming but at the GPS frequencies of 1.575 GHz and 1.227 GHz. When a drone loses its GPS lock, it will attempt to find its way back home using a digital compass or will, in many cases, just land. The main drawback to jamming

GPS is that this may interfere with other aircraft that are in the area. When using an antenna that focuses the beam, the chance of this happening is greatly reduced, but the possibility remains, so this method should only be used as a last resort and when other aircraft are not in the vicinity.

Besides the technological questions, there are many regulatory and legal issues surrounding the interception of drones.

Locate the Operator

The most common response method at this time is to find the drone's operator. The FAA even has a reference card to be used by law enforcement officers who make contact with a drone operator.

While this method is legal and does not require any specialized technology, it can be difficult to put into practice and it will not prevent a drone from causing damage, as a drone operator usually cannot be located until after the fact.

What Needs to Be Done

Besides the technological questions, there are many regulatory and legal issues surrounding the interception of drones.

How to respond to drones is still very much up in the air because of countries' differing regulations about restricting interference with aircraft or other electronic equipment. In the United States, it has been illegal to intercept drones, though there have been instances of civilians shooting down drones that were over their property and not being prosecuted. In July, President Obama signed into law H.R. 636, which, among other things, authorizes the FAA to conduct a pilot program on drone countermeasures. It is expected that the FAA will use a number of detection, classification and response mechanisms to counteract drones around airports and other critical infrastructure. In general, however, it is not legal for even state or local governments to stop or interfere with drones, other than by locating the operator and having him or her land the drone. Often, this is not effective, as has been seen in the western United States, where drones have interfered with airborne firefighting efforts and have cost the government millions of dollars. Because of this, in July, Utah passed legislation authorizing firefighters to disable drones flying around active wildfires.

This is just one of many such state laws that will likely be passed, and some may be in conflict with federal regulations. What is needed is a comprehensive FAA rule regarding permissible responses to drones around critical infrastructure. ■ Back to TOC

Logan Harris (lcharris@spotterrf.com) is the CEO of SpotterRF (www.spotterrf.com).

AR is a niche technology at present, but it has tremendous potential. As connected devices grow, the case for leveraging AR grows as well.

Augmented Reality is for More than Capturing Pokémon

When combined with IoT, the technology could have a big impact on security

By Rob Martens
Allegion

This year, Pokémon GO captured the mobile gaming world by becoming the most popular application in both the Apple and Android app stores, with more than 100 million downloads within the first few weeks of its public release in early July.

The mobile application blurs the lines between the virtual and physical worlds by utilizing GPS to navigate cities and uncover digital characters and items. The game attracts a wide demographic – young, old, professionals, students and more. It is relatable, intuitive and fun. The concept of integrating virtual reality into real-world environments is formally known as augmented reality, or AR.

AR is not new; the technology has been around for some time in the automotive and other industries. A simple example would be projecting dashboard information onto the interior of a car's windshield so that the driver can easily see it without taking his or her eyes off the road. Another would be the screen of an air traffic controller where a digital overlay is presented to point out key information and simplify decision-making. So what makes the use of AR at this time any different or particularly special? The availability of real-time data. Lots of clean, affordable, proactively delivered data. Many industries are recognizing AR's potential, especially in conjunction with connected/ smart devices, otherwise known as the Internet of Things (IoT).

What makes the use of AR at this time any different or particularly special? The availability of real-time data.

In 1999, the phrase "Internet of Things" was coined by British tech pioneer Kevin Ashton. On a large scale, it is defined as billions of sensors and smart devices that connect and share information with each other to enhance the collective experience of the end user in a variety of ways. This is done by collecting, cleaning and analyzing the data provided, allowing for predictive and real-time actions to take place on behalf of the user and the associated community.

IoT's recent rise in popularity stems from its newfound affordability and accessibility. Since 2010, sensor costs are down 50 percent, and bandwidth and processing costs have plummeted more than 97 percent. Put more simply, the cost of devices, information transport and information cleaning is lower and the technology is easier to use than ever before.

Today, IoT is becoming clearer in what it can do. Better business

cases are continuing to help drive productivity. Businesses are starting to use the abundance of data collected from sensors to gain an advantage over their competition. Consumers are able to control and manage more with less effort.

One of these advantages is a company's ability to create a more positive, personalized experience for the end user throughout the work day. This can be in the form of automatically performing complex repetitive actions such as adjusting lights, controlling the temperature, or locking doors.

AR has the potential, like IoT, to turn opportunity into reality, but for now, it is only scratching the surface.

Augmented Reality Overview

AR overlays graphics, audio and even smells across a real-world environment in real time with an end goal of making things more convenient for the user. This technology is already being adopted on smartphones, and it will continue to evolve and become more consumer-friendly as years pass.

Taking another look at Pokémon GO, the application allows users to locate characters through a smartphone GPS signal and camera. By using the mobile application, one can see digital characters located in the real-world environment. While it is fun to catch Pokémon while commuting or in the office, AR is more than just a game and businesses are taking notice.

For example, one of the leading AR companies has created an application that incorporates the cell phone camera and GPS to collect data from surrounding areas. This data allows the user to access information about restaurants, hotels, etc., and it overlaps onto the phone's screen for easy accessibility in a matter of seconds.

Imagine this: A young person is looking for a summer job and is not sure which companies are hiring. Rather than spending countless hours going from building to building, he or she could point a phone at a structure and have the app pull up the hiring status of any of the participating companies within it. In addition, the technology could allow consumers to be able to see company hours, sale prices and even images.

Challenges with Augmented Reality

Although AR has a large amount of untapped potential, there are also significant challenges and concerns that will need to be addressed.

- *Privacy concerns*. What images are private? Who gets access to what information? What information or status is acceptable to "attach" to a building, site or object? Who makes that decision? There are plenty of situations that could potentially cause legal disputes over privacy.
- *Technology*. In many applications, GPS is a major functional component of AR. It is typically available in most smartphones today, but signals can regularly get lost and are largely unavailable indoors. For AR to take off, either GPS needs to scan farther distances and improve its indoor accuracy, or complementary technologies will need to be introduced and embedded on common devices.

Augmented Reality's Impact on Security

It is easy to recognize the large number of potential applications of AR in the security space, despite the challenges. As is typical, the size of

the opportunity and the difficulty associated with change go hand in hand.

Consider the evolution of door locks over the past 5-10 years. Mechanical keys were once the only option for security professionals to implement. Then came the introduction of electronic access control and the adoption of smart cards/mobile credentials by commercial businesses. These new credentials are continuing to trend upward in the security marketplace, especially on college campuses, and some of the benefits include:

- Greater security
- Lower costs and ease of installation
- Efficiency
- Convenience
- Peace of mind

Imagine being in a facility service role and being able to walk onto an unfamiliar campus and identify issues immediately from devices that are actively calling out through a smartphone.

Forward-Thinking Applications

Imagine being in a facility service role and being able to walk onto an unfamiliar campus and identify issues immediately from devices that are actively calling out through a smartphone. Sound a little bit like Pokémon? It is. The big win for facilities, however, is that this is no game. Those devices are not disturbing the people around them with annoying noises or flashing lights; rather, they are calling to the user, specifically, via AR, saving time, frustration and money while also enhancing the experience of everyone involved in the process. Every time a smart device is installed, it has the potential to interact in an AR environment. When designing a new facility or retrofitting an old one, this is something that should be considered, as the productivity and enhanced experiential benefits could be significant.

There is a clear future for AR in the security industry. Provided below are a few examples of possible solutions.

- *Digital mapping*. AR has the ability to capture structural images of a building and create a 3D virtual map. When applied to physical access control, this map could be used to generate specifications, support building information modeling (BIM) or other building models and facility guides at all stages of the building lifecycle. These digital maps could be valuable assets that could evolve and even be transferred to new ownership as needed over time.
- *Space planning*. Having a digital map could help when planning for the implementation of

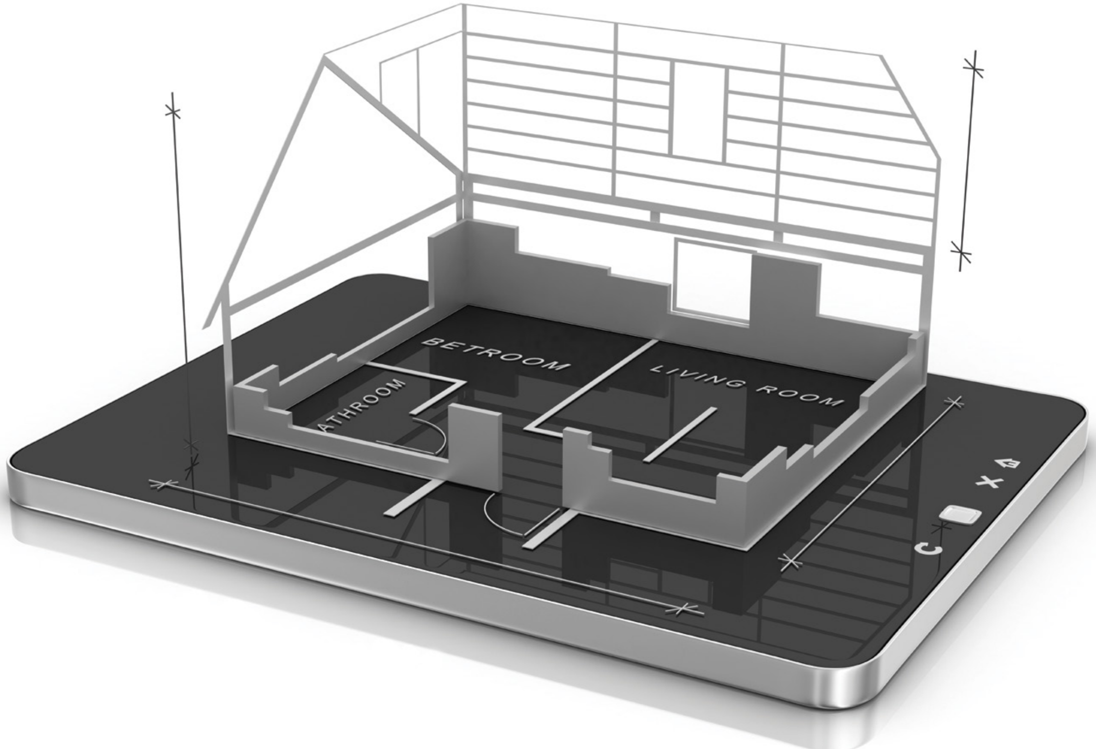
access control and security systems. Measuring and installing security devices while present at a facility could also be a potential benefit of AR. By utilizing the ability to overlay a virtual object within a physical space, security professionals, contractors and locksmiths would have the ability to visualize an entire room as a finished project before they even start, or to see existing infrastructure that they need to be aware of in the case of a retrofit project. This could help to avoid costly errors, and in some cases, even help to avoid accidents.

- *Reduced rate of error.* If specifications are written into the AR platform, a user would be able to receive notifications of inconsistencies or misplaced hardware before an error occurs. The platform may also have the ability to reduce or eliminate errors in order quantity when checking a confirmation sheet or integrating with an existing BIM system.

Although hypothetical, these are some of the possible instances in which AR could play a role in the security industry by assisting building planning, enhancing operational efficiencies, and improving the ease and convenience of building maintenance.

Augmented Reality and IoT

It is not hard to see that building security is advancing at an exponential pace. Each year, more aspects of security are being managed remotely from a computer, smartphone or



other device with fewer and fewer staff required. Many of these control options are made possible by the support of IoT devices. They have the ability to actively communicate with each other and to the cloud with little or no human interaction. They can proactively send updates on the status of a facility without the need for an administrator to be there in person.

In most buildings that house an integrated security and access control system, there is an opportunity to manage much more with IoT-enabled devices. It is projected that by the year 2020, there may be as many as 200 billion connected devices across the globe. That translates to roughly 26 smart objects per person. With all of this smart technology being implemented at a rapid rate, AR begins to make sense for facility executives and building owners. A smart device needs to be connected to communicate proactively with AR, and AR can provide a cleaner, simpler way to see what is happening without creating additional churn and chaos in an already busy environment.

> With all of this smart technology being implemented at a rapid rate, AR begins to make sense for facility executives and building owners.

Things to Consider with Augmented Reality

AR is a niche technology at present, but it has tremendous potential. As connected devices grow, the case for leveraging AR grows as well. A good implementation of AR is dependent on clean, accurate and easy to manage data and an applied business case that delivers real value for users. The improvement curve for this data is steep, and IoT is helping to drive it forward with the mass proliferation of smart devices and integrated systems across many industries. The business cases are improving as well, as users are more aware of what data is of value, and how they can deliver it in a way that improves the condition of the community using it.

Conclusion

AR is new, dynamic, interesting and fun. It may appear most prominently in a mobile game today, but there are many interesting potential uses waiting to be discovered across a variety of industries. The technology is evolving, and as it continues to advance and grow, we will learn how to apply it in more practical ways. Only time will tell which uses for this technology will reach the security industry, as many are now only hypothetical, but the potential is great. ■

Back to TOC

Rob Martens (robert.martens@allegion.com) is the futurist and director of connectivity platforms at Allegion (www.allegion.com).

With intelligent tools, such as built-in video analytics, critical details can be easily and quickly identified to facilitate rapid response, while allowing facilities to maximize manpower and ensure a high level of safety.

A Needle in a Video Haystack

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

By Steve Birkmeier
Arteco

Today's global security teams are faced with a complex set of threats, from vandalism, violence and severe weather to more extreme dangers, such as terrorism, all of which can be unpredictable. Because of the nature of these threats and the devastation that each one has the potential to inflict, comprehensive building management and security solutions are required to safeguard people, facilities, critical data and assets.

Security managers often rely on video surveillance and captured video data to assist them in maintaining awareness of the happenings within a facility at any given time. Since manpower is not sufficient to cover all areas and budgets tend to be constrained, video surveillance typically serves as the "eyes" of a security team.

It is clear that the need for more comprehensive surveillance and situational awareness is spiking, as evidenced by the more than 200 million cameras in use around the globe since 2014. The industry is also in the midst of a sea change, with IP cameras outpacing analog camera sales for the first time in history. However, in terms of combining security approaches and taking them to the next level of interconnectivity, barriers to entry remain.

This surge in software-enabled solutions has increased the potential for comprehensive, real-time safety measures, but it can also leave users with a sense of weariness from trying to keep up with the constant turnover of technology.

New Challenges in the Security Market

An exploding global population and a growing risk environment has resulted in a staggering rise in the sheer amount of data that is used for security purposes. IHS estimates that the amount of data produced in a single day by all new video surveillance cameras installed worldwide reached 566 petabytes in 2015. This is the equivalent of 11.3 million standard double-layer Blu-ray discs, or twice the amount of all user data stored by Facebook.

Secondary systems of protection are also facing a revolution in technological innovation, with many platforms reconfiguring notification centers to better mesh with intelligent devices such as computers, smartphones and tablets, allowing users to have eyes

and ears in many more places than ever before. This surge in software-enabled solutions has increased the potential for comprehensive, real-time safety measures, but it can also leave users with a sense of weariness from trying to keep up with the constant turnover of technology.

To develop a proactive approach, security managers need an intuitive way to identify the most valuable pieces of captured video data and corresponding system alerts.

The information provided by video surveillance is often overwhelming to operators, especially since video systems are typically set to record 24/7. It can be a challenge to identify the specific data that is important, since it takes hours of sifting through seemingly endless amounts of recorded information. Now add all the data coming from other alarm-based platforms and Internet of Things (IoT) devices, such as access control equipment, analytics, mobile platforms and alarm and life safety systems, and the amount of incoming data per application becomes massive.

To develop a proactive approach, security managers need an intuitive way to identify the most valuable pieces of captured video data and corresponding system alerts.

What is Event-Driven Intelligence?

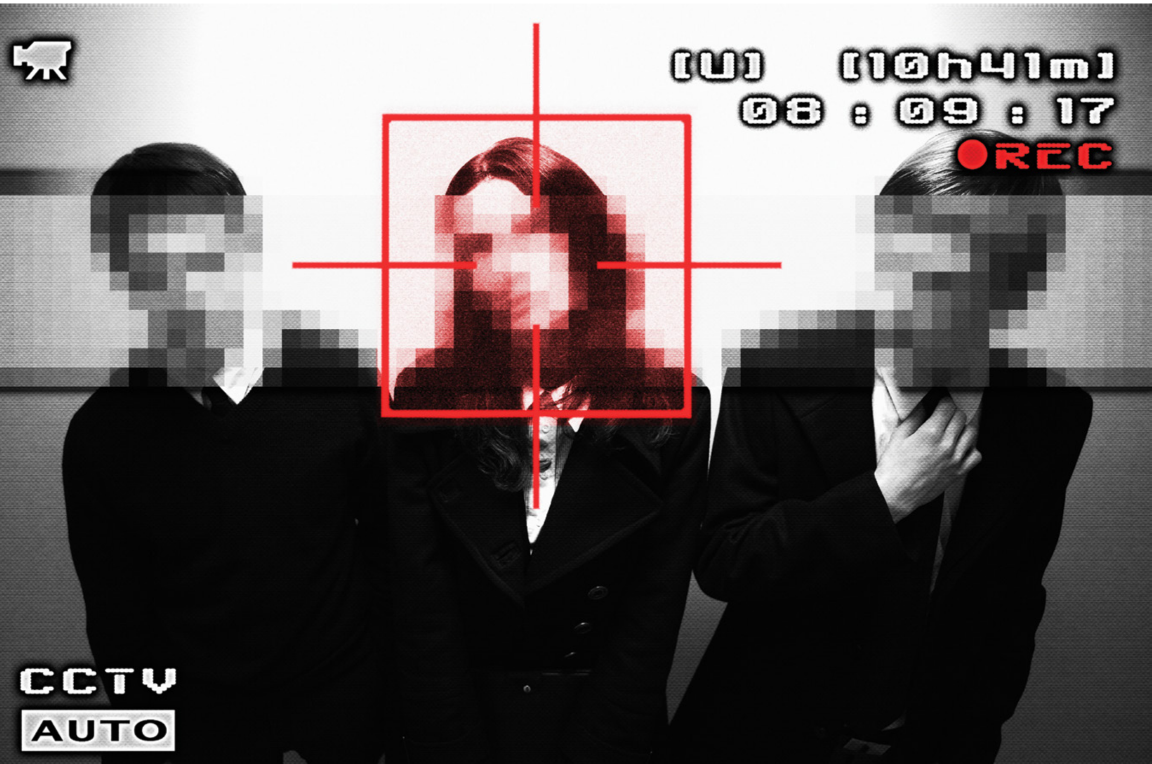
Event-driven intelligence (EDI) is a highly streamlined method of collecting, analyzing and responding to security data that allows users to use the incoming information to their advantage for emergencies and investigations. EDI platforms, such as video event management software (VEMS), rely on streaming, notification and management of data from multiple third-party devices, such as video surveillance, access control, building automation, and fire and intrusion alarms. These systems shift the burden from hardware to software as they link facility device notifications into a single easy-to-use interface, using high-level configuration for increased customization and, eventually, more efficient tactical responses to prioritized events.

Event-driven solutions are applicable across a number of markets, making them the nimblest and most intelligent security solution for users seeking organization, clarity and increased awareness of the incidents that matter (as well as peace of mind in false alarm situations). Applications ranging from education facilities and retail to critical infrastructure sites and city surveillance are adopting an event-based intelligence approach as a way to gain insight and improve operations in security and enterprise applications.

Event-driven intelligence allows users to intuitively and easily recognize key trends to drive informed and effective incident management and emergency response. With intelligent tools, such as built-in video analytics, critical details can be easily and quickly identified to facilitate rapid response, while allowing facilities to maximize manpower and ensure a high level of safety.

Advanced Detection, Robust Intelligence

Video cameras traditionally collect video data, but it is how this data



is used that makes it so valuable to security managers. They need a solution that is able to home in on specific events to collect details that can be used to properly address incidents. The quicker an operator can find video evidence of the incident in question, the quicker a problem can be remedied and security restored. Moreover, security teams should identify a video solution that will meet these needs in a cost-effective manner while empowering users with intuitive options. And an easily scalable solution is critical to taking advantage of growth possibilities.

VEMS can track which alerts are triggered most and least frequently as well as identify gaps in security. This can be the difference between proactively securing an area and reacting to a situation after the fact.

Fast-Tracked Interoperability

Interoperability between systems, devices and applications is important when making the whole system more intuitive. Solutions should offer the ability to detect and manage any and all events captured by video cameras while simultaneously integrating other security-focused measures, such as access control, intrusion detection, fire detection, license plate recognition, etc. The more information that is available about a certain event, the quicker the resolution. When choosing a solution, users should make sure it is based on open standards so that it will easily integrate with other third-party systems, devices and applications.

End users seek to retain as much of their initial investment as possible while looking for ways to improve these systems as risks and business needs evolve. Integrators should look to bring an end user's diverse security devices into one integrated platform. The ability to integrate with building management systems is critical, as well. The combination of multiple devices and platforms into one interface allows security managers to realize new levels of awareness, as well as increased functionalities, across networked systems. Without question, integration and interoperability are crucial for scalability and for "future-proofing" these installations, and it is imperative that integrators look into the innovation capacity of high-quality manufacturers.

Higher Levels of Situational Awareness

Opting for an event-driven intelligent solution with video analytics and video management software allows users to recognize key trends in data. Video analytics enhance video intelligence by performing event detection. For example, VEMS can track which alerts are triggered most and least frequently as well as identify gaps in security. This can be the difference between proactively securing an area and reacting to a situation after the fact. Security managers can define a specific set of events when alerts are necessary while, at the same time, the software continuously analyzes incoming video data, providing an immediate alert upon detection of a relevant incident.

VEMS and School Security

One way that VEMS is helping security managers improve and secure operations is by lending a hand in some of the most data-driven environments: school campuses.

Campuses range from semi-closed environments with high-level access control to more open perimeters with multiple sites spread across town, which can make a unified security approach difficult to achieve.

Many universities and K-12 campuses have strict budgetary requirements from trustees or school boards and try to maximize security allowances while still balancing the books for all other operational functions. Now more than ever, these schools are facing a growing demand for increased security within a tight budget, making it difficult to dedicate a larger portion of funds to one particular department.

Event-driven intelligence and video event management software are changing the way schools visualize, analyze and tackle security operations by allowing stakeholders to maintain existing security infrastructure, but they also take it a step further by funneling video alerts, alarms and notifications into one interface. As a result, the return on investment for VEMS is increased through its interoperability and reduced need for costly upgrades. This highly streamlined approach has allowed schools to absorb the increased video security presence at a custom level and identify key trends for emergency protocols, all while promoting significant cost savings by avoiding expensive end-to-end solutions.

Increased Return on Investment

Platforms that are able to remember patterns of behavior for a particular camera scene are most beneficial to security managers. Once users adopt EDI-based technology, they are able to retain their initial security investment and run proper VEMS, along with other third-party integration and reporting tools. They are also able to reduce investments in physical guards and move toward fewer operators manning more cameras through one platform, delivering robust ROI.

The "event" – a particular activity that seems suspicious or otherwise draws attention – should always be the focus when it comes to increasing situational awareness and enhancing facility security. When events occur and security managers are able to tune into them by using event-driven intelligent solutions, this enables optimal security and safety for all. ■

Back to TOC

Steve Birkmeier (sbirkmeier@artecous.com) is vice president, sales and business development, for Arteco (www.artecous.com).

In today’s enterprise, an organization’s physical access control should adhere to the same standards and deployment models that any other IT application would.

Raising the Standards

Physical access control can benefit from adopting an IT-centric approach

By Scott Sieracki
Viscount Systems

The convergence of physical and logical access is certainly not a new phenomenon. Ever since security systems and related peripheral devices made the jump to IP, there has been a desire to combine the two functions to derive greater intelligence and value from these solutions. In addition, security systems on the corporate network closely align security and IT departments within an organization because of the growing concern about cybersecurity threats and the need to view access and identity across the enterprise more cohesively.

In today's enterprise, an organization's physical access control should adhere to the same standards and deployment models that any other IT application would. This is not the world that most organizations live in, however, because most access control systems – the platforms that monitor physical access to facilities – are based on legacy architectures that operate in a standalone nature. Increasingly, though, end users are looking for ways to eliminate these silos as part of a larger effort to build unified systems that operate with common practices. The first step in that process occurs when organizations start to view access control as an extension of identity management.

End users are looking for ways to eliminate these silos as part of a larger effort to build unified systems that operate with common practices. The first step in that process occurs when organizations start to view access control as an extension of identity management.

Because of the growing need for robust identity management across the enterprise, an increasing number of organizations are looking to provision the physical and logical identities of users through a common set of rules and policies. Many organizations in both the public and private sectors have invested millions of dollars into managing and protecting virtual identities because of increasing cyber threats, and now it has become necessary to apply those rules, policies and procedures from the virtual world to elevate and transform physical access control.

The U.S. government has been at the forefront when it comes to achieving unification of physical and logical security with the issuance of the Federal Identity, Credential and

Access Management Roadmap and Implementation Guidance, better known as FICAM. Released in 2009 and revised in 2011, the goal of FICAM is to streamline logical and physical access among federal government agencies. Although FICAM was developed with government entities in mind, it can also serve as a guide that private sector organizations can use when building comprehensive access control policies.

Unification as a Business Tool

The cost savings and operational efficiencies that can be achieved through the unification of access control in an IT-centric security environment are numerous. In a true IT-centric access control model, the application software platform looks and responds like any other native IT application, deployed and supported by in-house IT staff. This access control model delivers myriad benefits in a wide variety of environments, including government, enterprise, education and health care.

Cybersecurity

The many high-profile data breaches that have occurred over the past several years have been a source of great concern for security professionals. From retail giant Target to the U.S. Office of Personnel Management, the number of people whose personal data has been compromised by hackers is astronomical. Given the increasing pace of migration to digital technology, the chances that more network-based systems will fall victim has risen.

An IT-centric access control platform is, by the nature of its design, an inherently more cyber secure solution.

Organizations face a multi-layer threat situation when it comes to cyber vulnerabilities, especially with the growth of the Internet of Things (IoT) and the demand for a secure, mobile enterprise. Malicious viruses can either infiltrate or disable IP-based devices, or hackers can use unsecured endpoints to gain access to corporate networks. The Carbanak cyber gang, for example, was able to steal nearly $1 billion from 100 financial institutions with such tactics. After using a spear phishing campaign to infect the IP devices of employees, the cyber thieves tapped into video surveillance systems via administrators' computers, allowing them to view what was happening within the facility.

A report issued by the U.S. Government Accountability Office (GAO) in December 2014 found that the Interagency Security Committee, which is responsible for developing security standards for non-military federal facilities, had not addressed the risk of cyber threats to building and access control systems as part of its Design Basis Threat report. This risk needs to be addressed; from fiscal year 2011 to fiscal year 2014, the GAO found that the number of cyber incidents reported to the U.S. Department of Homeland Security involving industrial control systems increased from 140 to 243, a spike of more than 70 percent.

Cybersecurity experts also generally said that building and access control systems are vulnerable to cyber attacks. One expert, for example, plainly stated that access control systems were not designed with cybersecurity in mind, the GAO reported.

Additionally, individuals within the white hat hacker community have tried to draw attention to the cybersecurity gaps that exist in access control by detailing specific vulnerabilities. At the annual hacking convention DEF CON, security researcher Shawn Merdinger demonstrated how he was able to successfully attack a network controller manufactured by one of the most venerable brands in the industry.

Experience Freedom

An IT-centric access control platform is, by the nature of its design, an inherently more cyber secure solution. The architecture leverages encryption bridges that are used to communicate with the application software. The entire application – decision-making, software, etc. – is located behind the firewall to ensure the highest level of cybersecurity protection.

End users need to be asking their integrators about the types of compliance tools that have been used on access control systems to better gauge the cybersecurity safeguards in place in comparison with standards established by industry bodies.

A key advantage of this software architecture is that, when any cybersecurity or operating system-level patches need to be installed, the work can be done

on the server in real time, under the same policies and practices as other IT systems. Companies can push out updates without having to worry about the security and compatibility of databases and an embedded system outside the firewall.

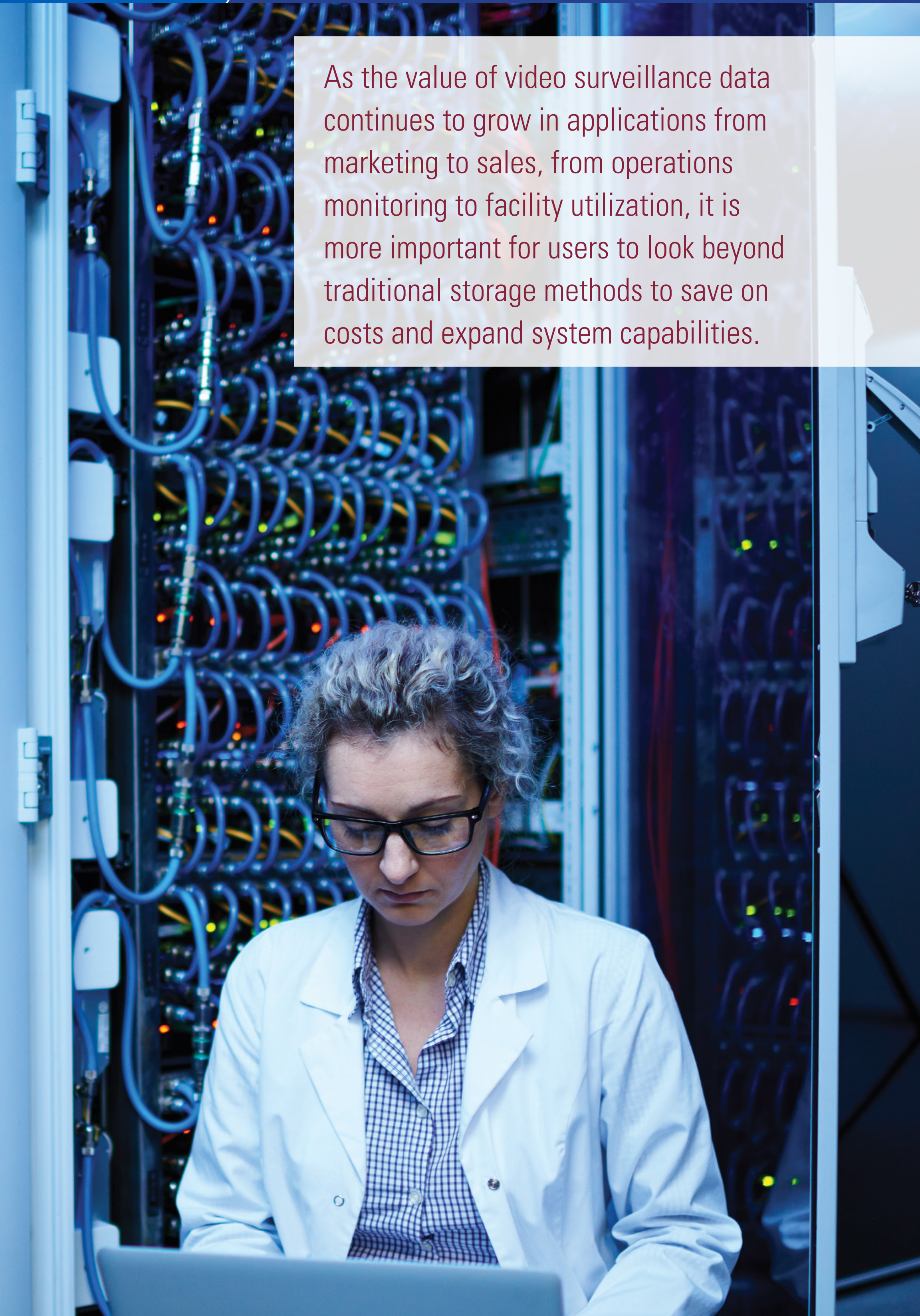
In addition, access logs can be exported to other network security or business intelligence systems running on an organization's IT infrastructure, which, in essence, makes the identity management platform a part of the overall information security strategy. For instance, if a company has a business intelligence software suite and it receives an alert that an attack is under way against the system, it can make immediate changes throughout the entire security enterprise.

End users need to be asking their integrators about the types of compliance tools that have been used on access control systems to better gauge the cybersecurity safeguards in place in comparison with standards established by industry bodies, such as PCI, NIST, etc. If researchers, like the aforementioned Merdinger, are searching out the vulnerabilities in access control, then we can assume that malicious hackers are, as well. That is why it is paramount that organizations take steps to harden any network-based system.

Looking Forward

It is clear that the role of IT in deploying security will only increase moving forward. CISOs, CSOs and IT security managers require solutions that operate on the standards they are used to seeing in their environments, and that offer greater efficiencies and cybersecurity safeguards. The days of closed systems and devices are coming to an end, while the dawn of IT-centric, unified solutions is just beginning to break. ■ Back to TOC

Scott Sieracki (scott.sieracki@viscount.com) is the CEO of Viscount Systems (www.viscount.com).



As the value of video surveillance data continues to grow in applications from marketing to sales, from operations monitoring to facility utilization, it is more important for users to look beyond traditional storage methods to save on costs and expand system capabilities.

Video Storage Wars

Hyper-convergence technology can simplify surveillance storage and enhance security

By Brandon Reich
Pivot3

The physical security systems and devices of today are more connected via LANs and the Internet than ever before. This extension of the network creates great opportunities, such as the growth of the Internet of Things (IoT), but it also creates additional vulnerabilities. Any IP-enabled device serves as an entry point to a network, and with that access point can come hackers trying to obtain valuable data. Therefore, these devices, including physical security solutions, must incorporate the same protocols and protections as any other IT devices to help protect the data being collected as part of the overall security posture of an organization.

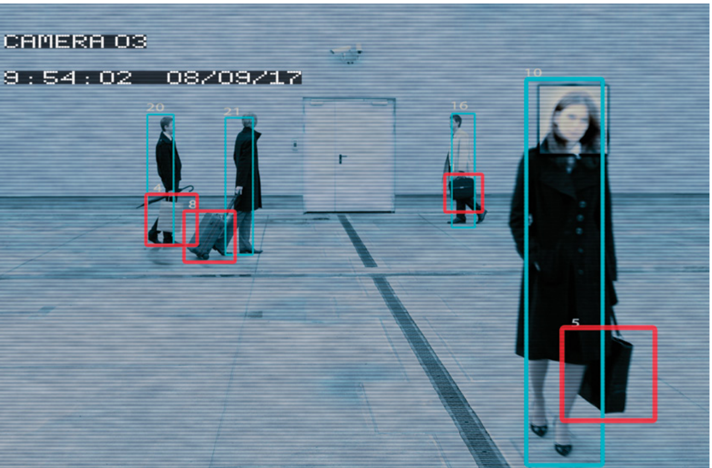
The industry is evolving in many ways: Devices are more connected; IT and physical security functions have merged even more than was previously imagined; and IT threats continue to emerge. Security is not limited to the security department. IT and cybersecurity professionals have a growing influence in overall security decisions, and this trend continues to accelerate at a rapid rate. Significant changes are occurring within the data center and within the security operations center, creating major disruptions to the large enterprise server infrastructures often relied on by IT departments. The emergence of virtualized solutions that enable advanced mobility is changing user expectations, fundamentally altering the way the industry thinks about IT.

> Any IP-enabled device serves as an entry point to a network, and with that access point can come hackers trying to obtain valuable data.

IoT is also affecting the security and surveillance market. Network-enabled devices and the demand for more actionable data are driving increased security spending. A report from Gartner projects that 6.4 billion connected devices will be in use worldwide in 2016, up 30 percent from 2015, and the total will reach 20.8 billion by 2020. Gartner also estimates that IoT will support total services spending of $235 billion in 2016, up 22 percent from 2015.

Today's IT and surveillance leaders are constantly on the lookout for new ways to gather, manage and store data to run their departments more efficiently, as well as maintain budgets and contribute to the overall success of the business. Video surveillance is a valuable tool to help maintain a secure environment and drive actionable business intelligence, and as a result, the number of video surveillance tools deployed continues to increase.

With the growing number of cameras – especially high-resolution models – more surveillance video is being collected and analyzed today than ever before. At the same time, customers of all sizes and in all markets are finding new ways to capture and leverage information from multiple sources – including video surveillance cameras, access control systems, video analytics and physical security information management (PSIM) platforms – to develop reports and identify trends that not only enhance security, but optimize internal operations as well.



The flood of video and business data is driven by the widespread adoption of megapixel IP cameras. A recent IHS report found that new video surveillance cameras worldwide in 2015 produced

566 petabytes of data daily. In 2017, that number is expected to exceed 1,500 petabytes per day. Newer technologies, such as 4K surveillance solutions and video analytics, are also gaining traction in markets ranging from corrections to retail. Such innovations transform large amounts of video from noise into "intelligent" data. As more users lean on surveillance to play a role in big data analysis, the demand for video storage grows exponentially. This trend has another effect: The detailed image quality provided by high-resolution cameras generates enormous requirements for storage capacity and bandwidth. In fact, a single megapixel camera can generate a terabyte of data every day.

As the need for storage grows, so too does the demand for data to be easily accessible over the Internet or networks within an enterprise organization. Keeping that data safe and secure has become a priority for both physical and IT security professionals.

Storage and Security

Surveillance video is only useful if it is reliably captured and stored. Today's advanced camera systems use more bandwidth and require greater storage, which is often the most costly piece of a video surveillance installation. So how can surveillance users manage the growing need for storage and the growing costs associated with it?

Before addressing the ways in which vulnerabilities are identified and rectified, we must first understand the opportunity we have for video storage in today's marketplace. There are several different video storage technologies: direct attached storage

(DAS), network attached storage (NAS), and storage area network (SAN).

Digital video recorders and network video recorders with DAS were designed to be simple digital replacements for VCRs. DAS is an acceptable option for small applications, generally fewer than 30 cameras. However, these single-box products with fixed storage capacity and performance cannot offer the scalability and reliability that IT and surveillance professionals demand.

NAS was designed to provide a much larger and more flexible storage resource for the read-intensive needs of large businesses and associated applications such as email and document storage. NAS offers better scalability than DAS, but it has limitations in video surveillance environments. Its file system layer creates additional traffic on the same network as video data recording, and the need for defragmentation adds significant overhead. This results in poor throughput performance that inhibits the systems' ability to ingest larger amount of data, leading to frame drops and video loss.

SAN offers seamless consolidation and sharing of storage space, which is more efficient than NAS devices. A SAN enables video data to go straight from the camera through the network to a generalized pool of storage. IT SANs are sold based on an average level of performance and are optimized for read-intensive workloads – not ideal for the surveillance environment because video systems require a minimum level of performance at all times and are very write-intensive. As with NAS, any slowdown in the system's computing or write ability can cause frame drops and video loss.

SANs are engineered to be highly reliable and scalable. They are a good solution for general purpose IT environments with many small, random reads and writes. However, the SAN design leads users to over-provision appliances to manage the fluctuation of incoming video from hundreds, or at times thousands, of cameras. In addition, IT SANs are very complex to set up and manage, requiring the services of a trained IT administrator.

Innovations in the market have resulted in new options beyond traditional IT storage methods. Hyper-converged infrastructure (HCI) solutions offer a much simpler, more practical and cost-effective alternative. HCI greatly reduces datacenter costs and complexity by integrating SAN and server virtualization capabilities into a single software-defined infrastructure deployed on commercial off-the-shelf server hardware. The advantage of HCI is that it provides the benefits of enterprise-class IT infrastructure – performance, resiliency, efficiency and scalability – without the high cost and complexity.

HCI appliances designed for the needs of the video surveillance market are simple to deploy and scale. Better performance and availability is achieved when compared to traditional enterprise-class storage, but without the cost, complexity and skill requirements imposed by legacy SAN/NAS with separate physical servers. Because the storage pool is virtualized, storage is completely scalable: Individual appliances can be added to meet growing surveillance needs. Adding a camera here or there when a hot spot or interest area is identified or increasing resolution is easily accomplished.

> The advantage of HCI is that it provides the benefits of enterprise-class IT infrastructure – performance, resiliency, efficiency and scalability – without the high cost and complexity.

System uptime and data availability is critical in video surveillance, especially in mission-critical applications. While redundant array of independent disks (RAID) technology is typically used to protect data within a single server or group of disks, HCI appliances use more advanced erasure coding to protect data across all of the appliances in an array. This approach protects data against disk drive failures, as well as against the loss of an entire appliance, and ensures that the data stored on that appliance or those disks is immediately accessible even during a failure. Built-in failover means the video application never goes offline and never stops recording. This level of resiliency cannot be accomplished with DAS, even if software-based failover solutions are deployed.

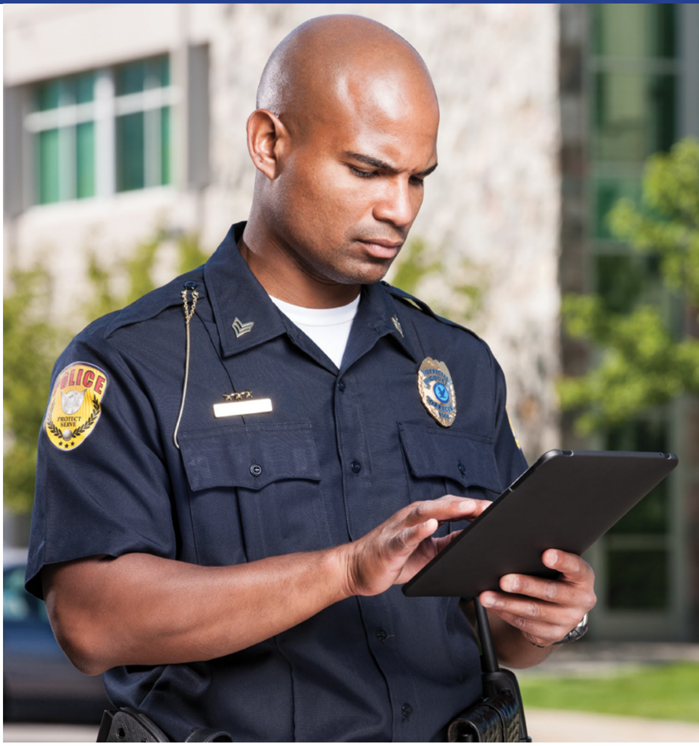
As the value of video surveillance data continues to grow in applications from marketing to sales, from operations monitoring to facility utilization, it is more important for users to look beyond traditional storage methods to save on costs and expand system capabilities. HCI is a technological development that is causing a fundamental shift in the IT sector, and video surveillance users in a wide variety of markets can realize benefits from this technology.

HCI is even ideal for mid-market applications because it can deliver enterprise-class IT capabilities that provide users with highly efficient shared storage, server consolidation and built-in failover, without the complexity or cost typically found with SAN storage. In fact, mid-market video deployments of as many as 200 cameras can realize the IT benefits of SAN at a price point competitive with DAS servers and NVRs. Built-in server failover protects system performance and data during hardware failures, a highly sought after feature typically only found in large, complex enterprise surveillance implementations.

> As the need for storage grows, so too does the demand for data to be easily accessible over the Internet or networks within an enterprise organization. Keeping that data safe and secure has become a priority for both physical and IT security professionals.

Ensuring the Safety of Data in the Operations Center

Security personnel in the field require access to critical data, such as video surveillance footage and information from other pertinent integrated systems. Traditionally, the process of accessing video and security data remotely has been challenging, but innovations in infrastructure platforms are enabling the mobilization of security client workstations without limiting functionality.



The ability to view security data on a mobile basis can reduce costs, improve situational awareness and enhance the effectiveness of responses in the event of a security situation. But, at the same time, the potential IT risks associated with accessing this critical information remotely are of utmost concern. Important surveillance data must be properly encrypted and protected from individuals or groups who might attempt to steal, tamper with or otherwise breach this information.

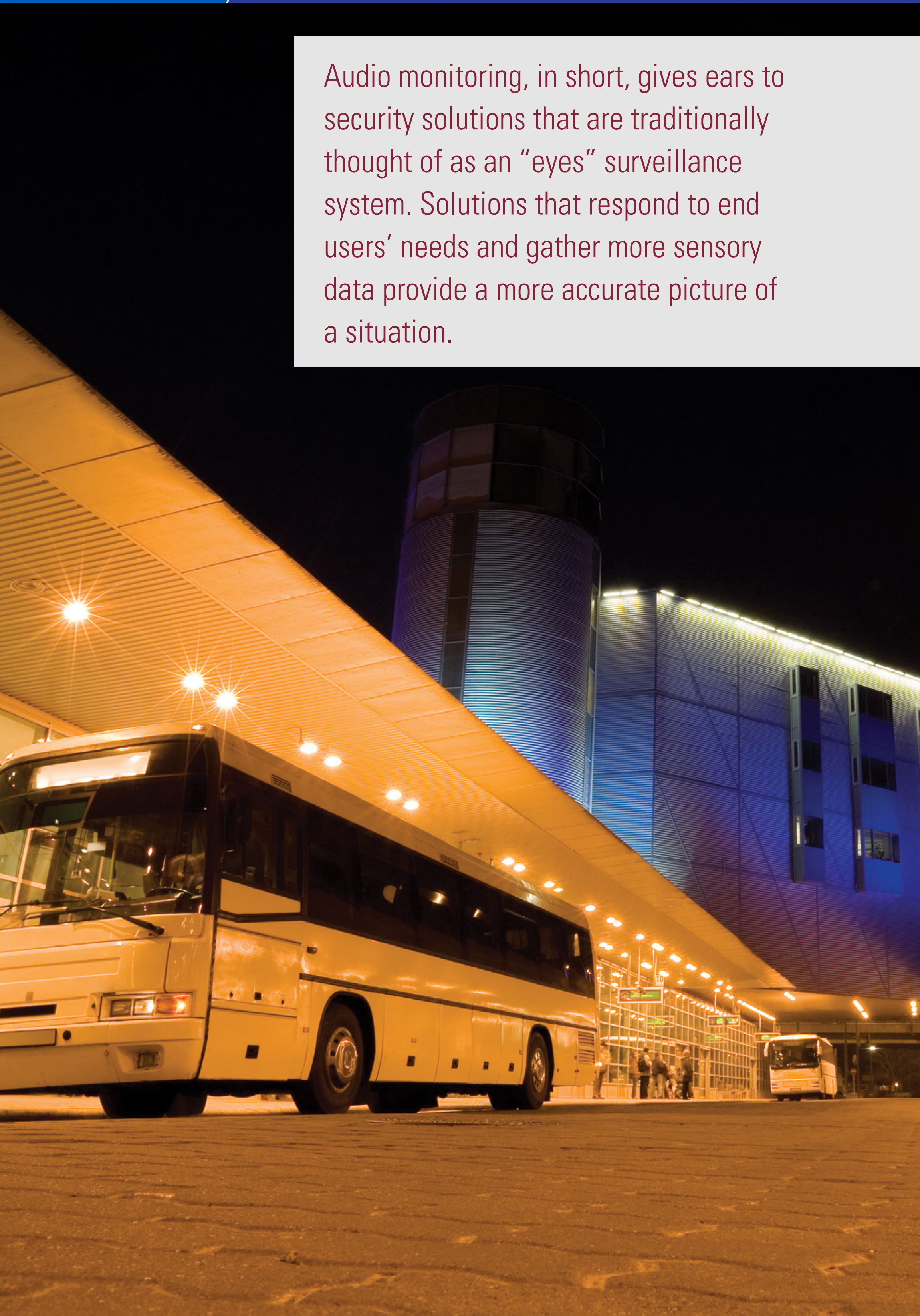
Security leaders can leverage the latest IT innovations to improve physical security operations and effectiveness, while ensuring that IP devices and critical security data remain secure, even as users demand mobility and remote access to data. The once siloed IT and security organizations must collaborate to ensure robust data protection strategies are successfully implemented.

IT trends, and the convergence of physical security and IT, have driven innovation in the security market, including the use of hyper-converged solutions for video surveillance server and storage needs. HCI ensures system reliability and high availability of video data, leading to more resilient security and business intelligence efforts.

Overall, advanced technologies like HCI deliver myriad benefits. These platforms work in conjunction with a business's security posture to reduce risk, improve response times and effectiveness, and enhance protection. But all of this must be accomplished in a manner that protects sensitive security data and reduces the likelihood of exposing organizations to cyber and physical security risks. Ensuring security across the enterprise is always the most critical goal. ■ **Back to TOC**

Brandon Reich (breich@pivot3.com) is director of surveillance solutions for Pivot3 (www.pivot3.com).

Audio monitoring, in short, gives ears to security solutions that are traditionally thought of as an "eyes" surveillance system. Solutions that respond to end users' needs and gather more sensory data provide a more accurate picture of a situation.



A Sound Solution in Transportation Security

Audio monitoring can enhance situational awareness, reduce crime

By Richard Brent
Louroe Electronics

In 2014, the transportation sector contributed $1.45 trillion to the U.S. economy and represented 8.3 percent of the gross domestic product (GDP). While transportation is paramount to a thriving economy, it also presents some of the greatest security challenges.

Millions of people rely on transit systems to commute to work, and the public's need to board buses, trains and airplanes every day requires the system to be both easily accessible and secure. Currently, video surveillance, access control and intrusion detection systems are the security and safety solutions of choice for transportation agencies, but there are other tools that can significantly enhance situational awareness. Audio capture, or monitoring, is one of them.

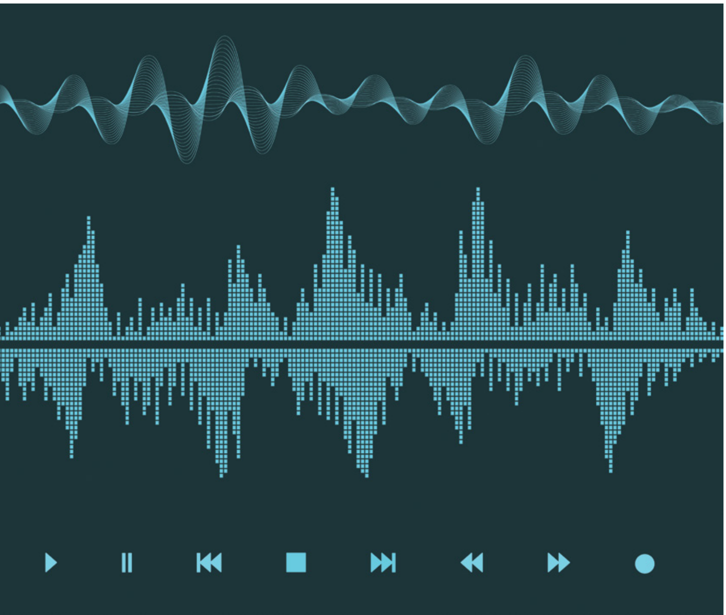
Power of Audio

Audio technology can detect auditory signals, filter what sound is significant information and enable decision-making that video surveillance alone cannot. Names, languages, and dialogue that contain important real-time information are just some of the additional things that can be captured. Audio recordings also can help transportation officials determine forensically what actually occurred, say, in a dispute between a passenger and a bus driver. Audio data collection has the power to eliminate the "he said/she said" arguments. The sound captured provides a record that can be convincing in a court of law.

Sound capture is an important security practice because it enhances monitoring and makes it more efficient. With audio technology engaged, systems will analyze auditory triggers that would have otherwise gone unnoticed. These acoustic indicators can alert central station guards to what zones should be more carefully observed. Secondary verification for incidents such as break-ins, vandalism, workplace safety mishaps, assaults, harassment and even malfunctioning equipment can be captured with audio technology.

Hands-free, two-way sound solutions, like intercoms, speaker-microphones, and talk-listen outdoor monitors, make real-time interaction and response a reality for security personnel. Through the interconnected audio solution, agency staff can speak to people on site from a remote location. For example, two-way audio solutions provide security guards the opportunity to speak to employees during a safety stand-down event or to warn trespassers to vacate the property.

Audio monitoring, in short, gives ears to security solutions that are traditionally thought of as an "eyes" surveillance system. Solutions that respond to end users' needs and gather more sensory data provide a more accurate picture of a situation. This allows security personnel to better determine the needed course of action. Consequently, audio monitoring is no longer an optional safety and security component for transportation applications, but a necessity. This is evident when looking at the current risks that mobile transit vessels, such as cabs, buses, trains and trucks, face. It is also clear when considering the perimeter challenges for mobile transfer stations such as bus terminals, train stations, truck yards, airports and seaports.



Buses and Trains

The primary security challenges for buses and trains are bullying, aggression, theft and robbery. Additionally, the safety of the driver is always at risk and, therefore, behaviors should be monitored. With the right technology and public knowledge, these crimes can be deterred. The Chicago Transit Authority (CTA) is a prime example of how investing in surveillance equipment can be a game-changer.

Over the past few years, the CTA has expanded its surveillance network to 23,000 cameras, and the system has proven to be a tremendous resource for police. In 2015 alone, cameras aided police in the capture of 256 individuals. Overall, crime in the CTA system fell by 25 percent in 2015, the fourth consecutive year that it decreased. Much of the success has been directly attributed to the security equipment.

> What many transit agency executives likely do not realize is that, by not utilizing audio, they are significantly limiting their ability to accurately analyze a situation.

Clearly, monitoring technologies play a critical role in crime deterrence. However, many transit agencies, including the CTA, still primarily deploy security cameras without audio. What many transit agency executives likely do not realize is that, by not utilizing audio, they are significantly limiting their ability to accurately analyze a situation. Viewing a video recording without audio is akin to watching a silent movie; it excludes a key component of the story. Consider this: How much more could security officials lower crime rates if audio was professionally integrated into their surveillance solutions? Passenger complaints could be resolved. Suspicious sounds in truck yards could immediately alert security guards, allowing them to apprehend suspects before they tamper with or steal equipment. Key evidence could be gained in an incident such as a train derailment, since investigators could listen to, as well as watch, what the driver did.

If transit authorities seek to increase safety for passengers by deploying a complete monitoring solution, audio must be part of the picture. The best audio solutions for buses and trains are appropriately selected, strategically placed microphones that can pick up sound even in areas with excessive levels of background noise. For directional audio capture technology placed near the operator, everything taking place behind the driver will be captured. When connected to a video management system, the audio solution can be set up to automatically record in the event of a verbal dispute, attack or crash. Installing weather-resistant, omnidirectional microphones and intercoms along the perimeters of bus terminals, train stations and rail yards is an optimal solution as well.

Airports

For airports, ensuring perimeter protection and strong access control and eliminating public safety threats are at the top of the security priority list. In particular, intercepting unsafe

items that endanger other travelers has been a focus for security personnel. In 2015, the Transportation Security Administration (TSA) reported that it confiscated 2,653 firearms in passenger carry-on bags at 236 airports in the United States; this number is about 20 percent higher than the previous year. Of those confiscated weapons, 82 percent were loaded.

How much more could security officials lower crime rates if audio was professionally integrated into their surveillance solutions?

Intrusion is an increasing concern for airport personnel. The Associated Press estimates that a U.S. airport experiences a perimeter breach about once every 10 days.

And perhaps most perilous of all, airports have had to increasingly respond to terror attacks. In 2016, there have been two high-profile incidents in Belgium and Turkey. On March 22, two explosions sounded in Belgium's Zaventem airport, tearing apart the check-in area. An hour later, another bomb went off at the nearby Maelbeek Metro station. The attack left 32 dead and 340 injured. On June 30, three men opened fire at Istanbul Ataturk Airport in Turkey before detonating three bombs. Forty-two people died and another 239 suffered injuries.

These shocking events illustrate that staff need to use all the skilled personnel and advanced technology at their disposal to mitigate threats. One technology that every airport security director should consider adding is audio analytics, specifically glass break and gunshot detection.

Glass break sensors placed in restricted areas of airports or along perimeter fences can provide for early detection of intruders. The sensors are set to identify breakage of most types of glass, including laminated, single or double plate, tempered and wired. In the past, each monitored surface had to have an individual sensor. Today, the solution requires just one high-quality, omnidirectional microphone that can pick up sound for the target area and be connected to a network camera, which integrates the audio analytics software with its video management system. The result is greater coverage with fewer microphones, leading to enhanced security at lower costs.

Amidst the chaos and confusion of an active shooter incident, a gunshot detector can ensure that critical information is relayed to the right personnel without delay. Upon recognizing the sound of a firearm, the detector sends a notification to law enforcement and other authorities, reducing reaction time for first responders in situations where every second counts. Traditionally, gunshot detection solutions have been standalone systems that accompany video surveillance and access control systems. However, new providers have developed solutions that directly integrate with IP cameras and video management systems. Not only can this save users thousands of dollars, but in the event of a shooting, control room monitors can access the cameras closest to the gunshot for visual identification of the suspect. Audio analytics are the next generation of audio monitoring, and airports would do well to adopt the technology.

Seaports

At seaports, security teams are trying to protect ships from being intercepted and used as weapons or platforms to smuggle dangerous materials into the country. In the U.S., there are more than 300 sea and river ports and 3,700 cargo and passenger terminals. Each year, thousands of ships pass through these ports with millions of tons of cargo. With such a high volume of traffic and goods, physical security and visitor management is key.

Biometric systems have become an important solution for identification and authorization at ports. Beyond those systems, two-way intercoms have proven to be an invaluable add-on. By installing an access control-integrated intercom, port personnel have an additional checkpoint for guests at main entrances and restricted areas. This secondary verification provides a much needed extra layer of security.

When responsible for monitoring vast areas of goods, port managers need all the help they can get. Weather-resistant microphones are great tools to listen for suspicious

noises, fraudulent claims, non-compliant employees, etc. The audio flags potential problems for agency staff, so they have time to intervene before the situation escalates. Given the minimal installation and maintenance costs and high return on investment, audio solutions should certainly be part of the discussion for port security systems.

> In places where there is no expectation of privacy, monitoring is perfectly fine.

Dispelling Misconceptions About Privacy

Implementing audio monitoring in a security solution is a sound decision, but many people hesitate to take the first step in deployment because of misconceptions about privacy laws. The question is whether audio recording is permitted or is considered an infringement on privacy.

The U.S. Code, specifically Title 18, Section 2510, 2, defines a private conversation as one in which people believe that the communication will not be intercepted. In these cases, monitoring would be prohibited. However, in places where there is no expectation of privacy, monitoring is perfectly fine. Buses, trains, airports and seaports are all public settings in which one's conversation might be overheard by passers-by. For this reason, audio monitoring is an acceptable and positive security practice.

As a result of decades of misunderstandings and inaccurate sayings, though, people fear audio monitoring and mistakenly think of it as a "Big Brother" tactic. What gets lost in the conversation is the whole reason why audio monitoring was considered in the first place, which was to enhance security and safety.

In 2014, Pennsylvania Gov. Tom Corbett signed into law a bill that permitted the use of audio monitoring on school buses. Two years later, a school bus driver in Jeanette, Penn., asked an 11-year-old boy to get off the bus and move a live power line out of the road. Afterward, the audio and video were both used to confirm that the driver did, in fact, make that request. As a result, the driver was charged with endangering the welfare of a child. Here, audio played a key role in defending not just the boy, but all of the students who were unnecessarily placed in a risky situation because of the driver's poor judgment.

Conclusion

The transportation industry is ever moving. As it continues to grow, so will its security needs and vulnerabilities. To combat these risks, audio monitoring must be part of the sector's security plan. ■ Back to TOC

Richard Brent (rbrent@louroe.com) is CEO of Louroe Electronics (www.louroe.com) and a member of the SIA Board of Directors.

Biometrics present a significant opportunity to alleviate many security issues that cause stress for banks and financial institutions, and they can help make operations more efficient in the process.

In a Hand or a Face

Fingerprints, facial recognition and other biometrics can make banking more secure

By Amy McKeown
3M

As society becomes more technologically sophisticated, so does the way we manage and protect our money. Long gone are the days of hiding money under the mattress, or even needing to write a check by hand.

But with the convenience of ATMs, online banking and mobile banking apps comes new security risks. The ability to connect from anywhere at any time amplifies potential threats, such as identity theft, fraud and data breaches.

The security risks do not stop at the bank doors. Financial institutions must also address internal security challenges, such as access control and employee verification. New advances in biometric technology, like facial recognition programs, allow banks to enhance their security systems and work in tandem with local law enforcement agencies that are also utilizing biometric-based solutions.

Biometrics present a significant opportunity to alleviate many security issues that cause stress for banks and financial institutions, and they can help make operations more efficient in the process.

What are Biometrics?

A biometric indicator refers to any unique attribute of an individual, either biological or behavioral. This could be a person's finger or palmprint, iris pattern, face, or even vocal patterns and fluctuations. One or several of these identifiers are collected and authenticated using state-of the-art sensors and algorithms.

Authenticating identity is a critical component of banking security. There are three methods used to verify a person's identity:

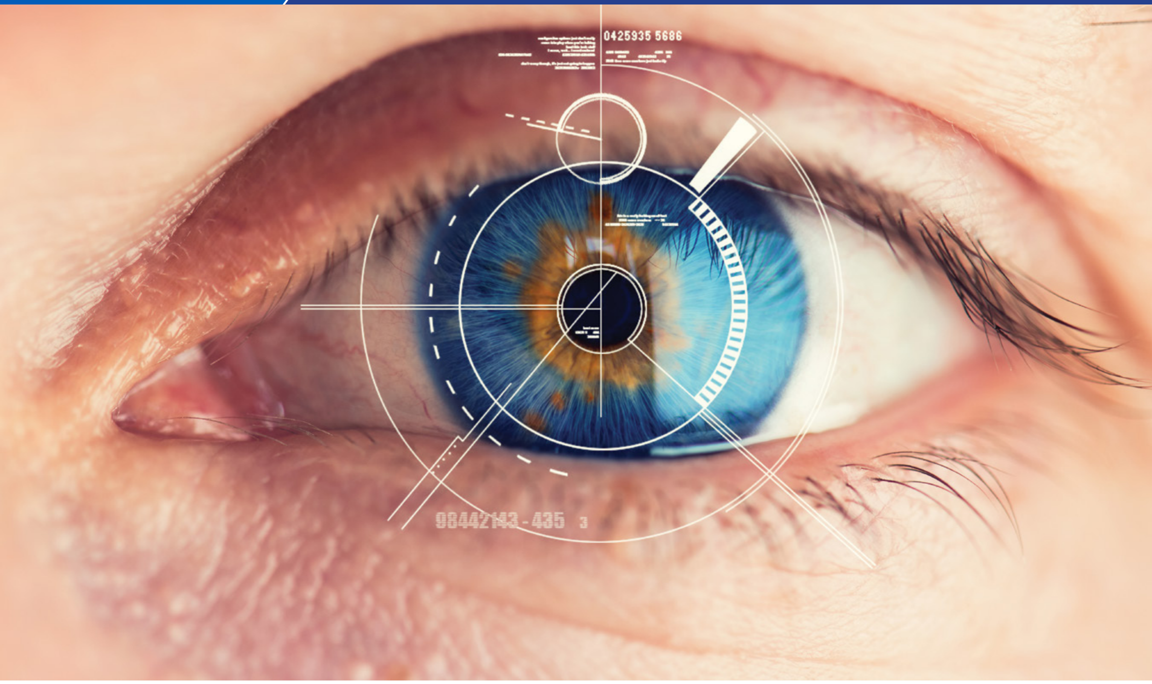
- Authenticate something they know, such as a PIN.
- Authenticate something they have, such as a driver's license or passport.
- Authenticate something they are, such as with a fingerprint. This is where biometrics come in.

For decades, the first two methods were the primary ways to verify identity in financial institutions. With the increase in mobile connectivity and the creation of banking applications specifically for mobile devices, though, the method of identifying people is likely to change. Traditional authentication solutions were not designed for mobile use; they are inconvenient and are proving to be insecure, according to Goode Intelligence in their 2015 report, "Biometrics for Banking."

As more smartphone manufacturers incorporate biometric sensors for fingerprints, eyes and face, biometric authentication is finally primed to take the lead in verifying a person's identity when using mobile applications.

Using biometrics increases the accuracy of authentication as they use a person's unique identifiers when making a match. These physical attributes are more difficult to forge than a password or ID card. As a result, many financial institutions will see a migration toward incorporating biometrics into their multi-factor authentication processes in order to increase security for themselves and their customers.

A recent study by Telstra points to security as one of the most important factors for consumers when choosing a



financial institution: “While factors such as interest rates and ease of accessing funds used to be the most important considerations when selecting a financial institution, today, more than half of U.S. consumers cite the security of their finances and personal information as their top priority, together with their institutions' reputation for security.”

Biometric authentication provides a cost-effective and reliable addition to a bank's overall security program, as well as peace of mind for its customers. In Telstra's survey, more than two-thirds of U.S. respondents said that biometrics such as voice, fingerprint, iris and facial recognition would increase security and help reduce the risk of fraud.

> The ability to connect from anywhere at any time amplifies potential threats, such as identity theft, fraud and data breaches.

Biometrics at ATMs

ATMs typically require a card and PIN to access account information and withdraw funds. However, the Asian market is changing the way ATM security works. Many banks in this part of the world are using biometric authentication at ATMs in large metropolitan areas, such as Tokyo. A recent report by Biometrics Research Group found more than 80,000 biometric-enabled ATMs in Japan and more than 15 million customers using them.

Sometimes biometrics are used in conjunction with a PIN or card, while other times they are a standalone security measure. Fingerprints are the most commonly used biometric indicators for this purpose, but facial and voice recognition are becoming more reliable and, therefore, will become more common.

Biometrics in Mobile and Online Banking

Offering services on the Internet is vital to a financial institution's livelihood; in fact, some banks exist only online. Unfortunately, the ability to log on from anywhere increases the risk of fraud. The ability to authenticate identity for online banking is vital to its utility and success. Biometrics and the Internet, both versatile in their nature, can combine to create a sophisticated and easy-to-use security alternative. Facial recognition is a modality that could easily excel in the online banking arena, as many devices are equipped with cameras.

The advent of smartphones has brought a whole new dimension to banking. With services like Apple Pay and mobile apps specific to financial institutions and payment processors, there is a new virtual vault that banks must secure.

Biometrics Research Group recently reported that PayPal facilitates $1 of every $6 spent online worldwide, and that the total payments volume during the preceding 12 months increased by 26 percent to $203 billion. This makes the need for enhanced and reliable security even more pressing.

Nearly every commerce website that the typical consumer deals with includes online payments, whether it leverages common options such as PayPal or Google Wallet or uses a site's own proprietary payment system. With all of these sites and applications pinging consumers' online bank accounts, banks have to do more to verify the identity of those who are authorizing transactions.

As more smartphone manufacturers incorporate biometric sensors for fingerprints, eyes and face, biometric authentication is finally primed to take the lead in verifying a person's identity when using mobile applications.

Biometrics for Telephone Banking

Voice recognition provides a great alternative to the current methods used for telephone banking security. Typically when calling into a bank, a person is required to verify his or her identity by using the keypad to enter a PIN, bank account number or Social Security number. Voice recognition makes this process more secure by adding a layer of security.

A number of large U.S. banks are receiving positive feedback regarding the installation of voice recognition, according to Biometrics Research Group: "Banks that deploy voice biometrics to automate the 'log-in' process not only enhance customer satisfaction levels, but dramatically reduce their customer care costs through increased automation rates."

Banks are exploring additional uses for voice biometrics in their fraud reduction initiatives. By cataloging voices of fraud suspects, for example, banks can use voice recognition to help protect against criminals gaining access to accounts.

Biometrics for Branch Security

When physically present at a bank, customers are required to present a form of identification and a bank card to verify their identity and gain access to their funds. Providing knowledge of the account, like a current address or the account number, often supports this method. Banks work to make this an easy and quick interaction, but is this the most secure approach?

With more than 50 unique driver's licenses in the United States and with municipal identification cards on the rise, the number and appearance of government-issued IDs is constantly growing and changing. Is it fair to expect tellers to know the exact look and feel of every form of identification that could possibly be used to access an account? With identity fraud on the rise, incorporating biometrics into the authentication process offers a more secure and efficient method that relies on standardized technology to confirm identity and removes the

possibility of human error from the equation.

In 2014, Goode Intelligence reported that 41 percent of all financial fraud in the United Kingdom was identity related. This is largely because of criminals opening up accounts under false identities or changing contact information on existing accounts. This could easily be curbed through the use of biometrics. It is easier to create a fake ID than to fake a fingerprint or iris pattern. Biometric technology offers a more efficient, effective and precise solution compared to an identification card.

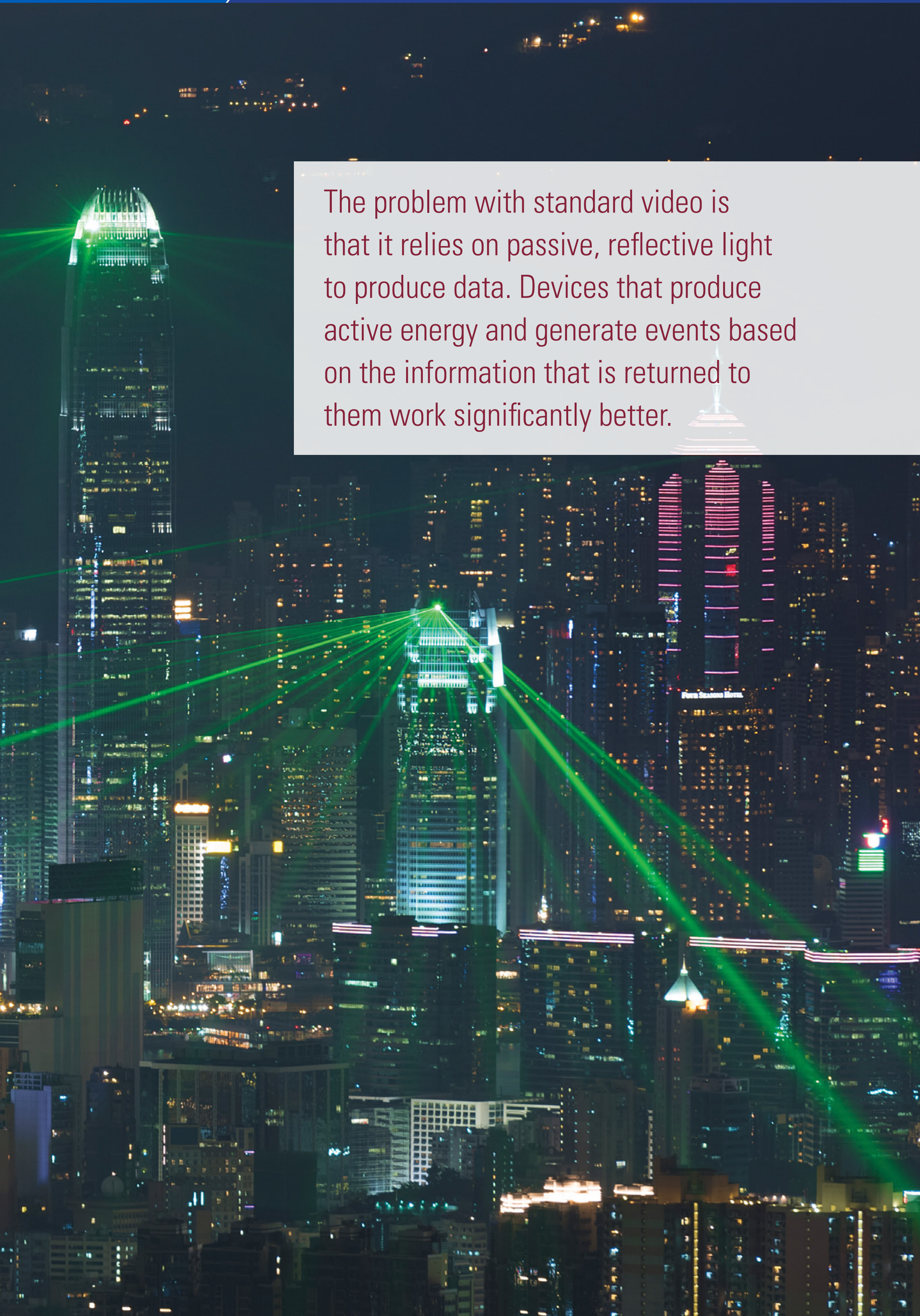
> "More than half of U.S. consumers cite the security of their finances and personal information as their top priority, together with their institutions' reputation for security."
>
> – Telstra

Implementing biometric technology can also help banks combat physical security threats. Large institutions in metropolitan areas with their own security departments could benefit from incorporating facial recognition software into their existing surveillance systems. Using whitelists and blacklists, security departments could monitor patrons and employees alike, providing access to secure areas for employees and being alerted to the presence of unwanted visitors. Smaller banks could benefit from the increased adoption of such technology by law enforcement. Solutions are now available that would allow captured security footage (with appropriate resolution) to be processed by facial recognition software, after the fact. Agencies using the software could take video footage from banks (or any commercial entity using the right security camera infrastructure) and use the software to check facial images against criminal databases. This type of application quickens the process of identifying and potentially capturing suspects. The versatility and preventative nature of facial recognition technology makes it a leading biometric tool for the banking and financial institutions sector.

Conclusion

Biometric technology can provide enormous benefits for the financial sector, removing the element of human error and creating more efficient and secure processes. Using unique personal attributes such as fingerprints, face, iris or voice to authenticate people can help increase customer satisfaction and reduce the risk of fraudulent activity in all areas of banking, while advancing the efficiency and security of the industry overall. ■ Back to TOC

Amy McKeown (almckeown@3m.com) is U.S. biometrics marketer for 3M (www.3m.com).



The problem with standard video is that it relies on passive, reflective light to produce data. Devices that produce active energy and generate events based on the information that is returned to them work significantly better.

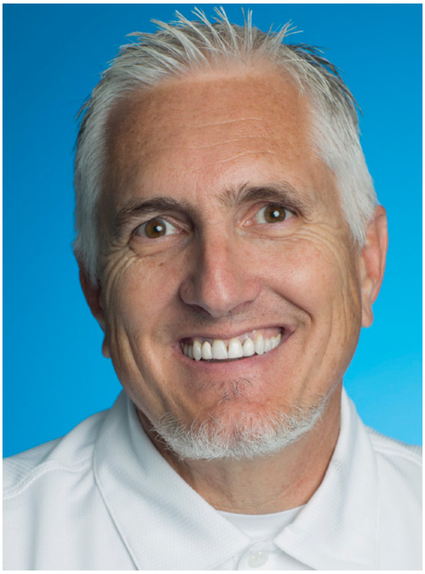
A Laser Focus on Enhanced Security

New scanners can improve the accuracy and reliability of intrusion detection systems

By Patrick Hart
Optex

The electronic physical security industry has done a good job with advancing technology over the past 100-plus years. Current systems are smarter than ever, and that intelligence brings new features and benefits. As more systems migrate to a digital format, larger amounts of data will be available to mine. This increase in data will propel the use of analytics and will move the security industry to a new and better age.

The supply of accurate data is limited by detection devices. Sensors today typically detect in a linear process, with a simple go/no-go for alarm events. The detection technology is adequate but it provides just a limited amount of analog-only information. There is additional information related to troubles, tampers, the environment, and basic device status, but this, too, is all analog. Moving forward with digital alarms – having alarm devices on a network communicating with an alarm system residing on a server



– is the first step toward increasing the functionality of these solutions. Now security devices can add more detail, with defined troubles based on other criteria, like anti-masking, anti-rotation, dirt on the lens or system failure. Alarm zones are also less restricted, with the division of areas defined in multiple zones not limited by the number of relay outputs. This provides more information with fewer connections, points of potential failure (relays), and wiring. Utilizing Power over Ethernet (PoE) devices, the installation becomes even simpler, with a single wire providing both information and power from the network switch. So what is next? The natural progression is toward even more information with sensors sending metadata.

Utilizing a laser scanner for detection eliminates a lot of the problems associated with other types of detection. Heat, lights, wind turbulence and small animals have little or no effect on a laser-based motion sensor.

Metadata can be found in modern security products, but one must look past the basic standard array. Cameras are the usual source of advanced detection data as they have millions of pixels that can be analyzed. The camera metadata is compressed, transmitted and digested to provide alarms and events based on an array of video analytic rules. This is a great advance in the security field, since it turns cameras into sensors and provides feedback with alerts. Too often, though, systems are turned off because of high volumes of false alarms. But camera technologies are improving, and the use of thermal images has produced better results. The problem with standard video is that it relies on passive, reflective light to produce data. Devices that produce active energy and generate events based on the information that is returned to them work significantly better. The main reason for the increased accuracy is the constant stable energy that is projected from the sensor. Both radar and multiplane LIDAR transmit energy at a fixed frequency and use

Covering large areas that can be defined to the inch, a laser scanner can transmit its data to a situational awareness system, a video management system, or an access control system.

time of reply to measure the response. This is a great way to produce accurate results, but the equipment tends to be too expensive for common applications.

A laser scanner can relay information about everything in its line of sight back to an analytic server. This includes not only the location and size of all moving objects, but also all of the information about static objects.

There are some new products, however, that use lasers as the active energy and have a lower cost of ownership. Utilizing a laser scanner for detection eliminates a lot of the problems associated with other types of detection. Heat, lights, wind turbulence and small animals have little or no effect on a laser-based motion sensor. A laser scanner can provide an abundant amount of precise information to determine if an object is a cause for alarm. Size, location, movement and time are all analyzed at the edge to generate event-based alarms. Sending out hundreds of beams of laser light every second, the scanner can identify both the size and exact location of a person inside a detection area. Covering large areas that can be defined to the inch, a laser scanner can transmit its data to a situational

awareness system, a video management system, or an access control system. With the perimeter defined, the sensing area can have custom zones programmed to any size or shape and can easily be networked to a camera to drive pan-tilt-zoom presets to the exact location of detection. The camera could also be programmed to increase framerates, start tracking, send an email, and/or start recording, all based on inputs from the laser.

Security applications are easily accomplished, as the laser scanners can be mounted horizontally or vertically. Horizontally, they create a large, wide detection area that can conform to the desired region of interest. Mounted vertically, they can create a large invisible laser wall. This wall could be as high as 50 feet and cover an area more than 150-feet wide. Typical vertical applications include fence lines, gates and the sides of buildings. For a fence line, a laser scanner can protect the fence and the space above it up to the detector. But unlike other types of detection, a laser can have custom zones for doors or gates that can be controlled independently of the rest of the protection area. For example, a gate could be a driveway with a 16-foot-wide opening, along with a separate 4-foot-wide pedestrian walkway, with the rest of the fence to 70 feet in both directions, all controlled with independent zones. This task is easy for a laser scanner but almost impossible for other types of commercially available sensors or cameras.

False alarms are the primary reason integrators are reluctant to install outdoor motion sensors. Causing police departments to use valuable resources to respond to a false alarm is both costly and inefficient. Video verification is often used but this, too, can result in a "no obvious cause" finding when viewing the location remotely. Either the camera is not in the correct location or the activation is caused by an unknown factor. Even when there is an obvious reason for the false alarm, it is often difficult to pinpoint the exact location because of the camera's perspective. Leaves and branches can cause false alarms, but it is often difficult to determine where to mask, or if masking will remove detection in the background. A laser detector, though, will provide the exact location of the alarm, so that precise space can be masked to eliminate the problem. For example, the detector can determine that the area to be masked is, say, 20.5 feet out and 13.2 feet to the left. The user would then mask that area and eliminate the cause of the false alarm without losing detection past that area. With a remote-accessible, local network server, all of these adjustments could be completed remotely, while saving the time, trouble and cost of having a technician travel to the site.

The most interesting and important aspect for future development is the laser scanner's ability to generate metadata of all the scanning information. A laser scanner can relay information about everything in its line of sight back to an analytic server. This includes not only the location and size of all moving objects, but also all of the information about static objects, including the exact locations of trees, buildings, walls, fences, vehicles and any other objects inside the detection area. This information has great benefits for granular forensic searches, since it allows for the elimination of unwanted detection of objects, and because the data can be processed by video analytics software to be used in conjunction with other sensors or cameras to enhance the performance of security systems.

There are a few manufacturers that understand these benefits and are working to get more than just the basic alarm events into their video management systems. Being able to track intruders and generate events, while excluding environmental factors, sounds too good to be true, but it is not, and these integrated camera and laser technologies can dramatically improve the performance of security systems. ■ **Back to TOC**

Patrick Hart (phart@optexamerica.com) is the field applications engineering manager at Optex (www.optexamerica.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:

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

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

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

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

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.

SIA

securityindustry.org/techinsights

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