

**Security Can
Be Social**

Tapping into social
media in the security
operations center

I See You

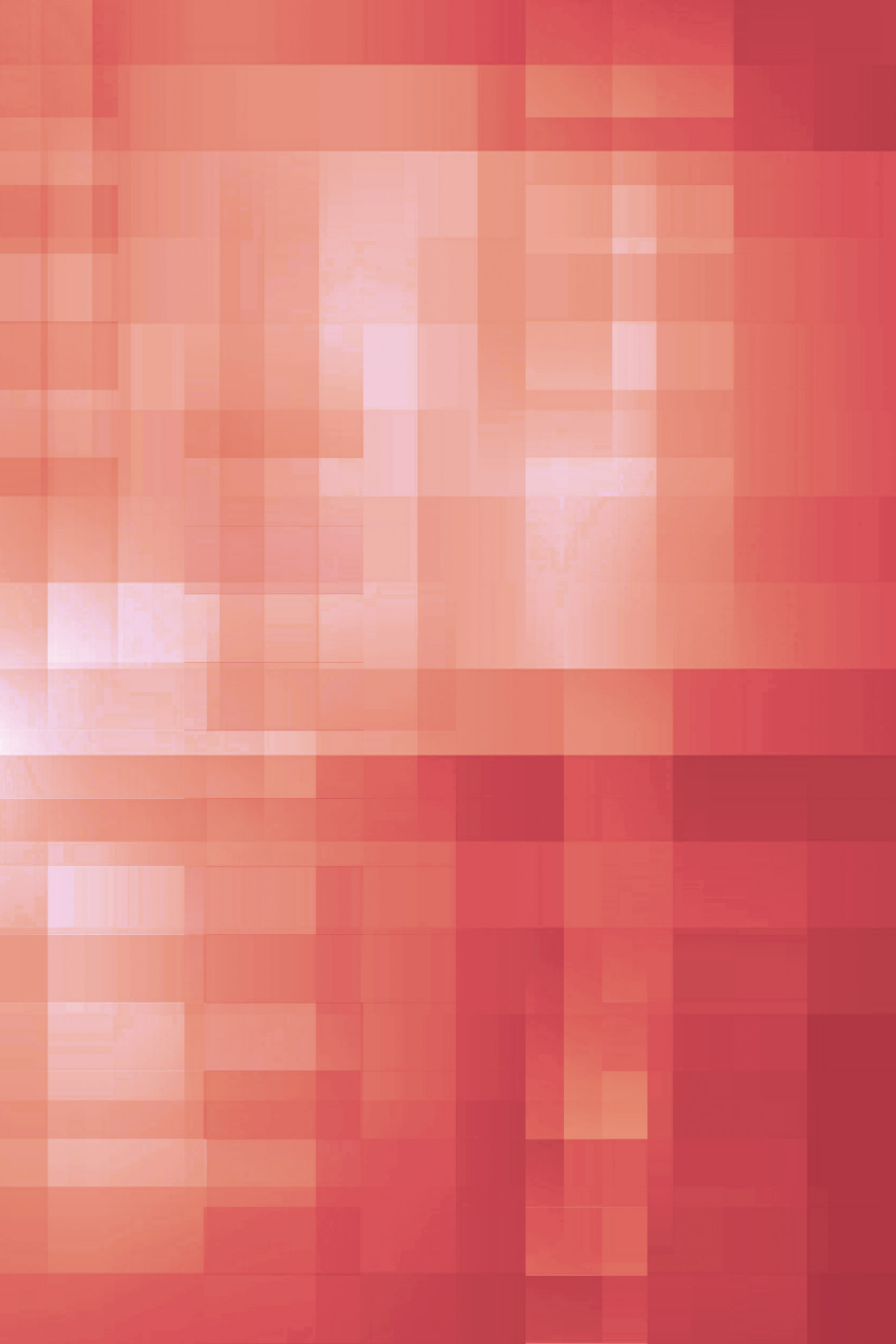
Radar and dual-
sensor thermal
imaging complete the
security picture

**Now Hear
This**

Audio analytics for
physical security

SIA
Insights
TECHNOLOGY

**Volume 6, Issue 1
Spring 2018**



Welcome

Dear Reader,

In every issue of *SIA Technology Insights*, we try to look to the cutting-edge (and sometimes even to the bleeding edge) of security technology, to ensure you stay current with the steady whirl of technology change.

In that spirit, we start this issue off with two technologies – social media and facial recognition – that are seeing great adoption in the consumer space, and which are poised to be adopted for security and safety applications.

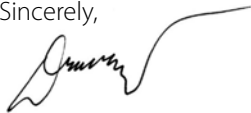
Did you know that around 500 million tweets are sent per day? That volume of posts and status updates is a deep well of information, and as Dillon Twombly of SIA member company Dataminr writes in this issue, that publicly posted social media content, once seen through the proper lens, can offer powerful insights for corporate security teams.

But it's not just the emerging technologies you will find in this issue; we're also tracking emerging advancements of existing solutions – like applying on-camera audio solutions (something that has been part of networked cameras for years) and delivering smart power solutions to security solutions on the network.

Remember that all editions of *SIA Technology Insights* are available online at www.securityindustry.org/techinsights. We welcome your feedback about the articles, and we encourage you to propose an article or otherwise contact the SIA staff via info@securityindustry.org.

Thank you for reading.

Sincerely,



Denis Hébert
Chairman, Board of Directors
Security Industry Association



Don Erickson
CEO
Security Industry Association

Table of Contents



Early Alerts Spur Action..... 6

Why corporate security teams rely on social media for real-time information

By Dillon Twombly, Dataminr



Modern Face Recognition Systems..... 16

Living the revolution as algorithms based on Deep Neural Networks (DNN) come to market

By Alexander Khanin, Vision Labs



24-Hour Perimeter Protection..... 22

Relentless defense for critical infrastructure

By John Distelzweig, FLIR Systems Inc.



Securing Healthcare Facilities 30

Maintaining 24/7 parking lot security

By Alex Doorduyn, Siklu Communication

Listen Up..... 36

How audio monitoring raises the surveillance bar

By James Marcella, Axis Communications Inc.



Smart Power 46

The paradigm has shifted to intelligent networking solutions

By John Olliver, LifeSafety Power Inc.



Navigating Technological Change 54

The way to success is ensuring new technologies impact your customers in a positive way

By Todd Graves, Allegion



The Puppy Movement 64

A new vision for security

By Doug Haines, Haines Security Solutions



SIA Technology Insights Article List..... 73

Social media gives corporate security teams an edge they've never had — the ability to detect and understand critical events sooner.



Early Alerts Spur Action

Why corporate security teams rely on social media for real-time information

By Dillon Twombly
Dataminr

Social media is transforming information distribution. Increasingly, it is where breaking news first appears. It's where high-profile politicians make announcements, share opinions and shape public debate on the issues. It's instantaneous, pervasive and truly global.

And social media is deeply embedded in popular culture. Social media users number in the billions (2.46 billion in 2017), and they're doing more than just sharing jokes. In fact, many individuals use the medium primarily to share what they are experiencing at any given moment. When news happens, these eyewitnesses can post a description or share a video instantly.

New tools exist which allow practitioners to harness the power of publicly available social media and



deliver real-time alerts to corporate security teams across the globe. In the age of real-time information, pressures on security teams are rising considerably. Influenced by an incredibly fast-paced news culture, stakeholders across the enterprise expect security teams to know

everything immediately and develop strategic responses faster than ever. Of course, social media also gives corporate security teams an edge they've never had — the ability to detect and understand critical events sooner.

To study these dynamics more closely, Dataminr interviewed corporate security leaders from a range of industries. These stakeholders represent five firms, ranging in size from 2,150 to 300,000 employees and from \$260 million to \$8.6 billion in annual net income. Our objective was to learn how these companies handle the flow of information to and from the global security operations center (GSOC). We also wanted to see how real-time alerts generated from social media were changing the way these companies responded to breaking news.

The results were informative. Here are some of the key takeaways:

- Social media alerts arrive earlier, giving security teams extra time to respond.
- Efficiency depends more on established processes than a specific organizational structure.
- There is not a direct relationship between team size and scope of responsibility.
- Well-established GSOCs excel at cataloging events for future analysis and trend detection.

Security Without Reservation

Hospitality Provider

200,000 employees

6,000 locations in 122 countries

Net income \$260MM

This hospitality company has more locations than any other company





we interviewed. With thousands of properties in its domain, the company's corporate security team must use resources wisely and maintain an efficient flow of information.

It does this through a GSOC established more than a decade ago, staffed by a team of 25 analysts who share a wide range of security responsibilities. Open source data feeds and finished intelligence assessments from subscription vendors provide the bulk of their security information.

The hospitality provider is currently focused on dealing with rapid growth and scaling robust processes. Another top priority, with which any corporate security team can identify, is demonstrating its value internally as lines of business compete for limited budgets.

Favoring a centralized flow common in large organizations, this company has all information arrive at its GSOC. Depending on the initial assessment, the regional security director is notified of a relevant event or crisis, along with a designated executive. Then locations in the

affected area are notified. Security analysts develop an appropriate response, adjust the threat posture, and notify the relevant head of operations.

Interestingly, security communications are distributed widely. On all communications, the "cc" list includes the PR crisis team, fire and life safety team, medical personnel, and the claims and insurance team. This partnership helps each team maintain awareness and carry out their own efforts as necessary, while supporting a coordinated response across the company. All incidents and GSOC actions are recorded for subsequent analysis.

Social media played a critical role in the company's response to the Brussels airport bombing in 2016. An alert sourced from social media informed the GSOC of the rapidly unfolding incident 20 to 30 minutes prior to any other information source. This early tip spurred analysts to perform additional research on social media to corroborate and contextualize the event.

While this research was performed, local facilities were notified along with

the European security director. As a clearer picture emerged, the company sent a report to key stakeholders via email so they could carry out their own notification responsibilities. Later, a second social media alert provided a similar time buffer when a second coordinated attack hit the city's metro station.

Banking on Reliable Information

Global Bank

52,000 employees

3,000 locations in 35 countries

Net income \$3B

This leading global bank's security operations team provides security for tens of thousands of employees as well as the brand's reputation. As the largest company we interviewed, with the largest security team, the bank demonstrates how a complex

global organization can streamline information flow in the GSOC with a well-defined process fueled by real-time, open source information.

The bank's security team is seasoned, having been assembled before 9/11. It includes approximately 100 people, plus contractors, and most of work is focused on dealing with alarms and physical security. The GSOC receives information from several subscription services, as well as a variety of news feeds.

These sources can trigger an event analysis, which follows a rigorous process designed to distribute important details to local resources as quickly as possible.

1. Information arrives from various open sources.
2. Analysts at the GSOC perform preliminary vetting.
3. If the information is valid,





- analysts create a spot report.
4. If the event is critical (such as a terror attack) analysts call stakeholders directly.
5. The spot report is emailed to a select group of decision-makers.
6. Analysts perform a deeper dive, sharing details with affected regional managers.
7. In an emergency, the GSOC notifies all employees and security centers in the affected area.

Analysts catalog events in a historical database so they can be referenced during similar future events. This is a popular tactic with many applications. For example, a string of social media alerts can be used in training modules to help security teams understand how conflicting reports emerge during a chaotic event, such as a natural disaster or active shooter. This can help teams resist the

urge to disseminate information too rapidly in a crisis, risking false positives.

Stakeholders outside of corporate security can also use this historical database to inform business decisions. For example, when deciding where to locate a new office, the risk management team can use the frequency of proximate security incidents to assess the relative physical security risk.

When asked to share an example of how social media has changed its information flow, the bank volunteered its experience dealing with the Las Vegas shooting in October 2017, when a gunman opened fire at concertgoers, killing 58 and wounding more than 500.

According to the bank, a real-time alert from social media provided the first indication that something was wrong. The alert arrived within a minute of the first shots being fired. The team immediately pulled up a

map to visualize its local facilities and determine whether any employees were traveling in the area. Analysts put the essential details together in a spot report and distributed it to the first tier of stakeholders, including the Las Vegas regional manager. Relevant stakeholders and senior executives received the security team's initial assessment of the incident before the event appeared on mainstream news channels.

Essentially, this spot report provides all stakeholders with a "single version of the truth," eliminating the risk of discrepancies and confusion during a chaotic event. With a common report in hand, the team confirmed the details and produced follow-ups as more news reports emerged. Fortunately for the bank, none of its employees was affected by the shooting.

Driving Toward Decentralization

Transportation Provider

12,000 employees

430 locations in 55 countries

Revenues \$6.5B

This company built its corporate security team in 2014. Its team of 100 professionals spends much of its time on executive protection and threat assessment because threats to the company's drivers are frequent. Unfortunately, threat assessment is a manually intensive task. In fact, the team's top priority for the next five years is to increase automation and relieve this pressure.

In addition to these priorities, the GSOC handles intelligence analysis, crisis management, and engineering

response, events that require the company to rapidly implement changes to its app or online properties.

The company uses a variety of open source feeds, as well as select online forums and social media platforms. Information flow is decentralized, with regional managers responsible for relaying information and executing the response. It's important to note that this approach works very well because it aligns with the company's highly distributed business model.

1. Regional security managers receive incoming information.
2. Information of interest gets forwarded to the GSOC.
3. GSOC analysts vet the information and return it to the regional security manager.
4. If action is required, the regional manager coordinates with relevant teams.

Just like the bank, this company catalogs every event within an incident management platform with more than 70 categories. Detailed records help identify trends and inform security planning and process development. Because this team is relatively new, its second priority for the next five years is developing resiliency through more well-established processes, including event-specific playbooks and procedures.

The company indicated that social media played a key role in its response to the London Bridge terror attack of June 2017, which killed seven and injured 50. Social media provided the first indication of the event, with subsequent real-time alerts



providing details and confirmation from increasingly credible sources. The social media alerts prompted the security team to notify employees in the area, and to begin working with communications to coordinate public messaging.

Building a Culture of Security

Biotech Manufacturer

2,150 employees
16 locations in 13 countries
Revenues \$1.7B

This fast-growing biotech company established its GSOC in 2015. It is the smallest team we spoke with and has just three full-time employees plus contractors. Its GSOC is staffed by two team members 24/7 and a third during weekday business hours for additional support.

As both a new and small team, this GSOC demonstrates how the size of a team does not necessarily indicate the scope of responsibility or the size of the daily workload. The biotech's

security team, for example, takes full advantage of technology to cover its global locations with limited resources. The centerpiece of the GSOC is an impressive common operating picture used to maintain awareness of events. The display includes open source information feeds and a mix of local and global news outlets.

What's more, the company's growth accentuates the GSOC's focus on efficiency because it must continually cover new sites without increasing its staff. To do this, the GSOC uses subscription social media analytics software to help automate coverage of wider geographic areas. Standard operating procedures — an absolute essential for efficiency — expedite incident response times by delineating clear responsibilities. The core team triages and contextualizes incoming information before disseminating to relevant stakeholders, often including site security leaders, communications, and senior executives. Subsequent updates are provided proactively.

The April 2017 terror attack in Stockholm, Sweden, illustrated the effectiveness of the team's reliance on automated real-time social media alerting and standard response procedures. A subscription social media alerting service detected the event and provided imagery from the scene several minutes before other information sources. Early notification allowed the security team to execute their response procedures before the incident appeared across major news services.

Dealing With Crisis

Industrial Manufacturer

300,000 employees
300 locations in 170 countries
Net income \$8.86B

The GSOC function for this very large manufacturing concern

is fulfilled by a dedicated crisis management team based in Europe. It was established in 2012 and involves four professionals whose sole focus is reacting to crisis events in concert with the larger corporate security apparatus. The bigger group includes three regional teams, each with its own regional security director.

Like the other teams we interviewed, the crisis management group uses a mix of open source feeds, OSAC reporting, major news feeds, Twitter and an in-house travel management system. One of its top priorities for the next five years, however, is improving its approach to data streams. According to our interview respondent, filtering high volumes of incoming information is a significant challenge.

Social media inputs are a key part of the crisis team's information flow.



Specifically, the team uses real-time alerts driven by social media to access event data within a 10-miles radius of each property. The combination of automated social media event monitoring and tight geofencing reduces inbound noise and increases efficiency. This is another example of how a relatively small team takes on a large responsibility by taking full advantage of available technology, including social media.

The team's process was put to the test in July 2017 when a train accident in Barcelona, Spain, injured 56 people. A real-time social media alert notified the team of the crash before mainstream news outlets, giving the team extra time to react. The company has hundreds of employees who work in the city. Fortunately, only a small number were traveling that day and none was affected. With the early notification, however, the team could quickly review the available details, and confirm to senior leadership that none of their employees needed assistance.

Preparing for a Social Future

Social media is changing what corporate security teams are expected to do, as well as helping them meet these new expectations. It is clear

Social media is becoming a standard source of information in the GSOC, across industries and among both new and more experienced teams.

from these interviews that social media is becoming a standard source of information in the GSOC, across industries and among both new and more experienced teams. In many cases, real-time alerts sourced from

social media content can give security organizations valuable extra time during critical events.

Social media has other built-in advantages as well. When cataloging

events for future reference, teams can easily refer to specific alerts (or a series of posts) for images, video and other contextual details. Social media content lends itself to analytics that can help teams understand how information travels during common high-risk events.

The utility of social media data for corporate security teams will increase as these public platforms assume a larger role in modern life. Teams armed with the best social media services and standard operating procedures will be well positioned to respond optimally to diverse and unexpected threats. ■ [Back to TOC](#)

Dillon Twombly is vice president and head of corporate risk and PR/corporate communications in sales at Dataminr (www.dataminr.com).

A woman in a dark blue business suit is shown from the chest up, looking down at a silver smartphone she is holding in her right hand. Overlaid on her face is a white wireframe mesh representing facial recognition technology. To the left of the phone, there are several concentric, glowing teal circles with white lines, suggesting a data visualization or a scanning process. The background is a soft, out-of-focus grey and blue.

We are entering the second wave of face recognition technology adoption, now driven by commercial businesses willing to give the technology a second chance.

Modern Face Recognition Systems

Living the revolution as algorithms based on Deep Neural Networks (DNN) come to market

By Alexander Khanin
Vision Labs

Face recognition as a technology experienced its first wave of adoption in 2000s, mostly in government projects. We must admit that the quality and performance of the previous generation of face recognition products simply doesn't hold up against criticism, although many global vendors introduced face recognition as newly created solutions (using available third-party face recognition engines) or rose to success with their own face recognition technology.

The limitations of such legacy technology and systems will affect government agencies around the world for another 10 years (at least) since they both can't immediately give up already implemented and supported systems. That would basically be admitting the expenditure



of hundreds of millions of dollars on technology of questionable quality. In addition, agencies face a stumbling block in the lack of a legal framework setting minimal requirements for the face recognition engines/systems.

Luckily, commercial businesses that have tried face recognition for

their tasks during the first wave of adoption quickly learned that the technology was not there yet to bring measurable value to their day-to-day operations. And it was for a very solid reason: Businesses didn't have a need nor the resources for sophisticated suspect profile investigation software (for investigating a customer or employee in their case) with a variety of manual tools for face image treatment or ISO standard-based reports.

As business itself went digital, the need to interact with customers and employees in an interconnected environment allowing contactless person identification (which face recognition enables) has led to the concept of cross-platform and cross-domain face recognition. Breakthroughs in the approach to face recognition happened in 2012

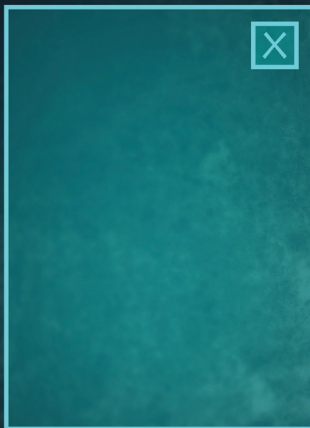
with the introduction of deep neural networks (DNN)-based algorithms that now penetrate the full-face recognition pipeline with state-of-the-art products. We are entering the second wave of face recognition technology adoption, now driven by commercial businesses willing to give the technology a second chance.

Imagine modern business working today through the following multiple channels where it interacts with employees and customers, who are typically divided into controlled or uncontrolled scenarios:

Controlled (user interacts with the system in the process of acquiring the best shot of the face for recognition)

- Mobile
- Web (including web-based software)
- Standalone devices (digital signage)

FACIAL RECOGNITION
STATUS: FAILED
NO FACES DETECTED
TRY AGAIN



DATABASE COUNT: 6.391.554.897
MATCHING RESULTS: 0



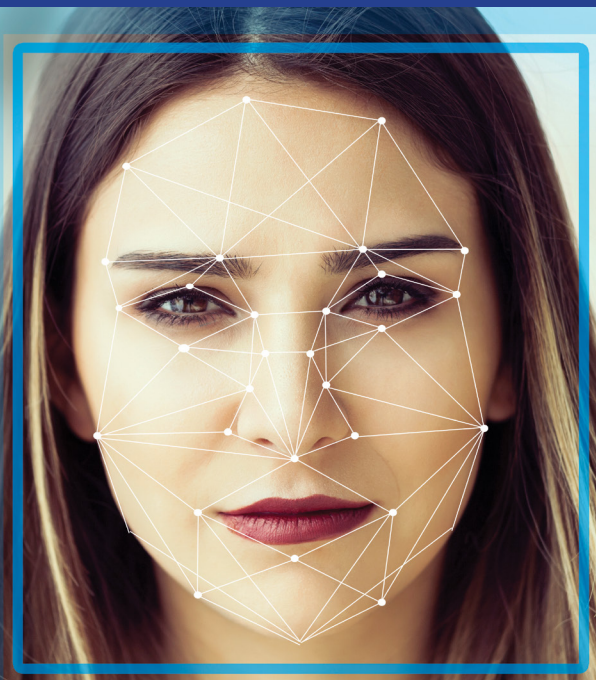
Facial
recognition



name:
password:

```
0100010110010100101001
0001001000101010000101
0100101100001000101010
```

Security



Uncontrolled (no interaction/cooperation of the user required to capture the best shot of the face for recognition)

- IP camera surveillance (doesn't have to be security-oriented)

Having the seamless customer/employee journey across all the domains described above is the key for any business case of modern enterprises. This, in turn, dictates a set of "must-haves" facing recognition engines and solutions providers.

Let's have a look at them below:

Mobile

- Work with mobile camera stream for face detection/best shot selection (no selfies anymore)
- Support offline 1:1 face matching with the acceptable face recognition speed (less than 500ms)

- Have liveness (anti-spoofing) algorithm
- Have stable performance across a variety of at least iOS- and Android-based devices

Web

- Work in JavaScript with no performance decrease
- Have liveness (anti-spoofing) algorithm
- Standalone devices
- Work with commonly available web cameras
- Support both 1:1 and 1:N face matching with the acceptable face recognition speed (less than 500ms)
- Have stable performance across a variety of embedded system on chips

IP camera surveillance

- No special "special face recognition camera" acceptable:

solution for employees either through an IP camera or standalone devices (could be mobile devices as well).

Step 5: Finally, the company would like to track and measure the conversion of the unidentified visitors of the branch office to the enrolled customers in a database.

While the use cases may be straightforward, traditional face recognition solution vendors would

find it challenging

to build up such new functionality

on top of an

existing database

or users, or

dynamically

changing a

database of

prospective

customers,

leading to parallel

operation of

face recognition engines that meet

the expectations of performance

and quality of each business unit.

That brings us to the most important

part of this article: How to make sure

that cross-domain face recognition

is possible with a specific face

recognition solution vendor or engine?

The best way to ensure that a

face recognition engine would cover

most of your evolving business needs

is to refer to “The Ongoing Face

Recognition Vendor Test” collated by

the U.S. National Institute of Standards

and Technology (NIST) and see the

performance of algorithms listed there

across such domains as visa, webcam,

selfie, mugshot and wild (uncontrolled).

You should pay attention to the most stable (leveled) top results of a vendor across all categories.

There is another set of face recognition engine parameters to pay attention to that directly influence the performance: face template size. There needs to be a balance between the face template size and the achieved quality across domains. Face template creation time directly affects the ability

of an algorithm to

run on a mobile

device in offline

mode. Take care

to compare times.

The algorithm

may be tops in all

categories but 100

times slower than

its competitors.

State-of-the-art

face recognition

algorithms are

evolving fast and aim for the mass

adoption in many industries in the

near term. The only suggestion for

any business would be to closely

monitor available trusted resources for

algorithms evaluation, keeping in mind

that more and more business units are

becoming interested in face recognition

as an enabling person identification

technology. A key competitive

advantage in businesses with a rapidly

changing technology landscape is

adaptability, so flexible face recognition

technology that efficiently meets most

business cases is a must. ■ **Back to TOC**

The reality is that today face recognition solutions are being used by several business divisions of companies pursuing various goals as a part of an overall user experience.

Alexander Khanin is CEO at Vision Labs (www.visionlabs.ai).



Combining technologies to create solutions with multiple complimentary capabilities results in an overall system that is greater than the sum of its individual parts.

24-Hour Perimeter Protection

Relentless defense for critical infrastructure

By John Distelzweig
FLIR Systems Inc.

The challenges to perimeter protection seem to grow more nefarious every day. The bad news is that intruders are increasingly inventive and unscrupulous. The good news is that the security operators are leveraging more innovative technologies to mitigate and deter these threats.

Effective perimeter protection on a 24/7 basis is a crucial part of the defense of critical infrastructure – the assets, networks and systems, either virtual or physical, that are so vital to security and safety.

The Challenges

Over the past few years, securing the nation's critical infrastructure has become a top priority. Security has arguably become the most important aspect of any airport, seaport or utility's



business. Operations managers must continually answer the question, "Are we protected?"

The common concerns involve a combination of factors:

- Physical plants cover enormous areas, with many points of

entry and extended perimeters, often in remote areas that make monitoring difficult.

- Campuses contain complex, highly restricted and expensive equipment where proper access and use must be controlled.
- Facilities such as airports have areas with varying levels of access authorization, from the check-in area to the airline gate to the baggage claim.
- Operations at these locations take place 24-hours a day in heat, rain, sunshine or darkness.

When designing an effective solution to secure the perimeter, there is no one-size-fits-all solution, primarily because no two perimeters

In a time when threats are varied, systems must be as flexible as possible to adapt quickly to challenges.

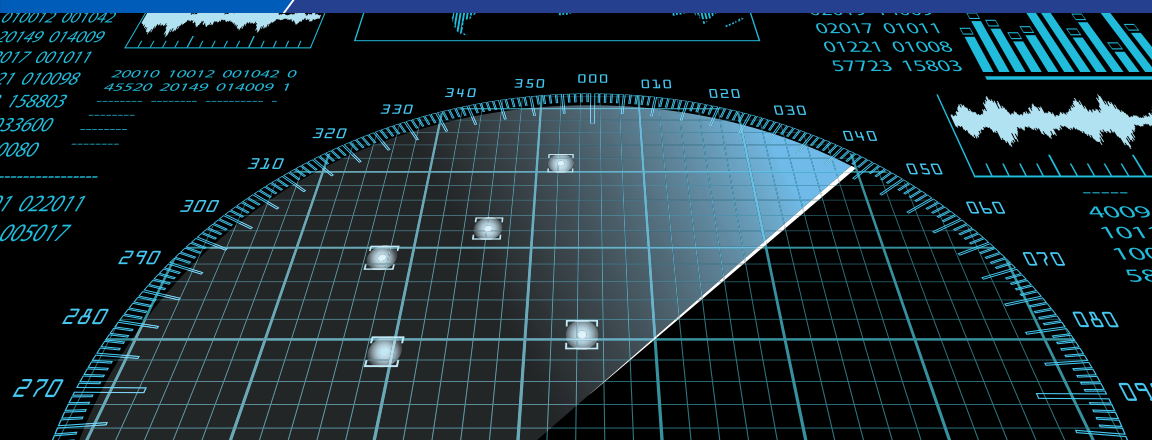
are the same. Terrain, climate and threat profile all affect the decisions of what technologies are required for the best solution. Typical choices include patrolling personnel, fences, walls and/or trenches, unattended

ground sensors, unmanned aerial sensors, radars and thermal imaging.

Even with this variation, the technologies that are being increasingly

deployed in the critical infrastructure sector for intrusion detection are radar, thermal imaging and multisensor cameras, which are controlled through advanced Physical Security Information Management (PSIM) solutions. Combining technologies to create solutions with multiple complimentary capabilities, like combining radar with mobile cameras, or high-definition surveillance cameras with thermal





imaging technologies, results in an overall system that is greater than the sum of its individual parts.

Radar

As always, understanding the nature of a threat is key to intercepting and defeating it. Fixed, mobile or trailer-based, the latest ground surveillance radar systems can detect and track multiple threats simultaneously, even beyond perimeter lines. This enables security personnel to monitor and control their security zone by intercepting threats early, before they have had opportunity to complete their mission. Today's ground surveillance radars are also exceptionally fast in terms of target detection and acquisition.

In maritime search and rescue operations, as an example, improved radar surveillance can work together with infrared thermal imaging to cover

a wider area and interpret images quickly so that crews can rapidly decide whether to continue the search pattern or investigate a target.

Airborne systems operate on helicopters, fixed-wing aircraft, ships, land vehicles and observation towers around the world. In a time when threats are varied, systems must be as flexible as possible to adapt quickly to challenges.

In fact, the most effective border surveillance systems combine

Effective long-range dual sensor thermal imaging easily networks with other sensors, as well as with command and control software.

performance, coverage and reliability to create the most efficient solutions on the market today for border protection, coastal surveillance, vessel traffic monitoring, airport security

and other large perimeter security applications.

Effective radar detects threats over great distances, providing important reaction time. In addition, it is virtually impossible for targets to

advance without detection, including slow-moving targets. Radar provides important targeting parameters, including range, bearing, course, speed and GPS coordinates.

Dual-Sensor Thermal Imaging

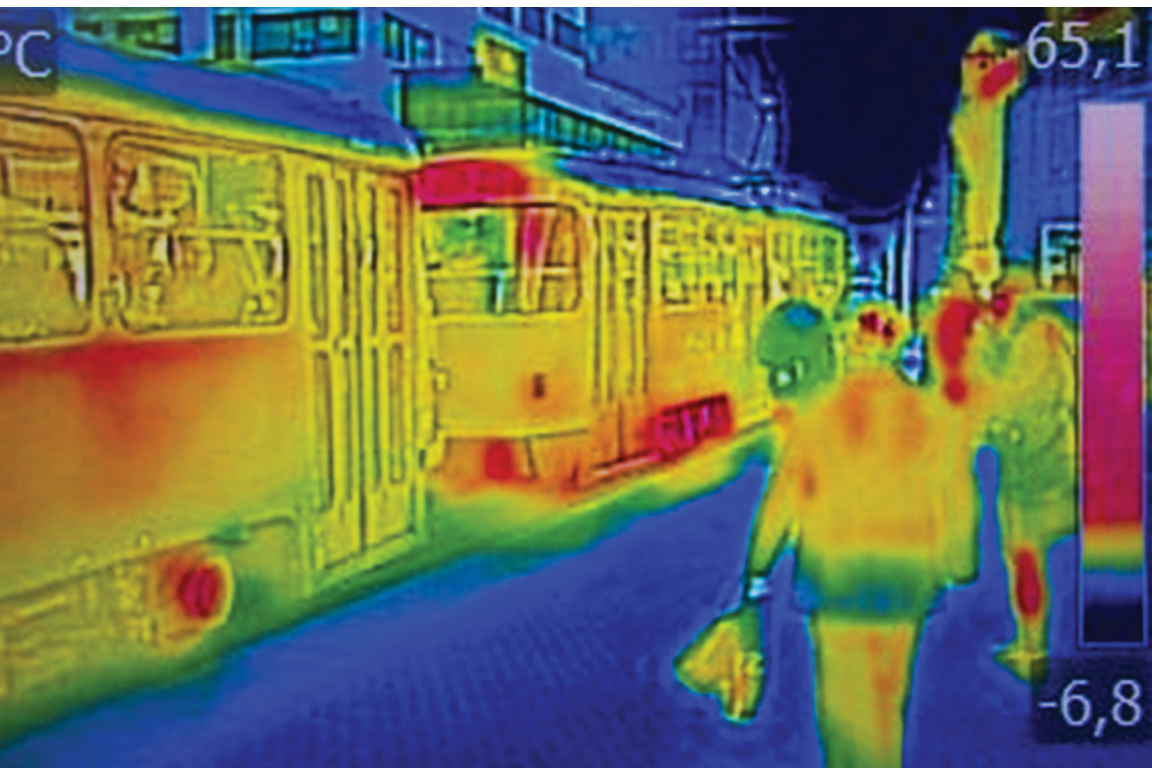
Detecting a potential threat, of course, is just the first step. Once an object is detected, it must be identified and its threat level determined. Without clear, long-range visual analysis of detected threats – on land or on water – operators are unable to discern the difference between false alarms and alerts that require some sort of action.

Effective long-range dual sensor thermal imaging combines thermal and high-definition visible-light imaging sensors that easily network with other sensors, as well as with command and control software. Although many believe that

thermal imaging is only effective at night, thermal imagers equipped with powerful zoom optics often outperform their visible-light counterparts. These systems can provide such reliable threat detection at ranges so extreme that they're limited more by topography than by the energetic limits of the sensors themselves.

Multi-sensor cameras are an extremely versatile solution for critical infrastructure protection in total darkness, bright sun and/or adverse conditions. The best are equipped with a continuous optical zoom lens for superior image quality, and are designed for system integration.

Additionally, thermal cameras are ideal for video analytics. Visible light cameras can be easily fooled by many naturally occurring phenomena, such as blowing trees, shadows, insects,





birds or oncoming cars. In terms of motion detection, microwave, fence sensors, motion sensors, and radar can all detect a possible intrusion, but they are essentially “blind” technologies compared to thermal imaging. When a motion sensor is triggered, a user still needs an additional method of assessing the nature of the alarm, to determine the most appropriate response. For example, is it a person climbing the fence or just a harmless squirrel?

Because of thermal security cameras’ high-contrast video output, security professionals have found that they work very well with video analytics that are capable of classifying humans and vehicles, which is an obvious important factor when determining

The value of command and control software is that it seamlessly integrates all elements from multiple manufacturers on multiple sites.

the correct response. They can provide more reliable alarming with fewer false reports than visible-light cameras, even during the day. Thermal imaging security cameras offer both alarming capabilities and reliable images – two solutions in one.

Command and Control Software

The command and control software is the brain of the overall system, the link that enables integration of all the elements.

As such, it is important that this element provides security and surveillance in a high customizable, user-friendly environment. The best command and control

systems can control virtually any number and combination of disparate devices with point-and-click simplicity.

The value of command and control software is that it seamlessly integrates all elements – cameras, displays, analytics, radars, fence detection, unattended ground sensors and other devices – from multiple manufacturers on multiple sites. This capability supports existing legacy devices as well as allowing systems to add new technologies. It provides unparalleled situational awareness from one control room.

One defining feature of PSIM platforms is their scalability, accommodating the addition of servers and clients as needed. The benefit of having an intuitive and configurable client interface is that it provides operators with access to external monitors and monitor walls through simple drag-and-drop actions. The server environment is powerful enough to provide such features as device prioritization, system security and granular permissions control, alarm

management, archived video storage and retrieval.

Among the additional tactical features a robust command and control software system should offer:

- Automated camera tracking: As intruders monitored by radars pass into defined detection zones, visible/infrared cameras are triggered to track and identify the moving objects.
- Radar support: The capability to overlap multiple radars will provide a detection area of virtually unlimited size.
- Infrared imagery: The capability to slew thermal cameras to follow moving objects in the dark. Users can toggle between infrared and visible imagery while viewing infrared video.
- Total position awareness: The capability to snap cameras and radars to their real coordinates on GPS-aligned maps,



monitoring real-time positioning of radar tracks and GPS-enabled mobile resources.

- **Advanced controls:** The system should control advanced camera features used in perimeter surveillance such as range finders, trackers, and the ability to control all camera parameters.
- **External display control:** The platform should provide users with seamless control of monitor walls using sharing and collaboration features accessed through simple drag-and-drop actions.
- **Scalability:** The platform should support scalability by the capability of adding servers and clients as needed.
- **Workspace configurability:** Client applications should support the ability to create the most efficient layouts for the mission. Allowing multiple panes for maps, event lists, live and archive video, as well as enabling cooperation between these components, creates a truly “intelligent” user interface.
- **Operator security:** System security should be controlled by operator passwords, priorities and access privileges, as well as by controlling access to features and devices independently.

The Future of Perimeter Protection

As we've seen, the technology of safety and surveillance, especially as it applies to perimeter protection, will

continue to evolve. What else will soon be seen?

Watch for these systems coming to your security zone soon:

- **Aerial surveillance:** The use of personal drones will only increase, especially now that the Personal Reconnaissance System (PRS) is now pocket-sized. This game-changing technology provides immediate situational awareness at a safe distance. In the civilian sector, they're particularly useful in search and rescue missions, firefighting and law enforcement applications.
- **Advanced biometrics:** Go beyond traditional ink fingerprinting for identification with such solutions as an optical fingerprint scanner, an iris scanner, and a palm print scanner.
- **Connected technology:** The emergence of place-specific solutions that range from Internet and communication systems to document imaging, archival security and document sharing services.
- **Perimeter patrol robots:** They're already entering the market.

Any business that wants to achieve the maximum level of security and protection of their intellectual and physical property should consider deploying these cutting-edge technologies, along with thermal imaging and radar systems. ■

Back to TOC

John Distelzweig is general manager of FLIR Systems Inc. (www.flir.com).



For healthcare facilities, protecting patients, staff and visitors has become increasingly important in addressing patient privacy, safeguarding against infant abductions and ensuring an overall safe environment.

Securing Healthcare Facilities

Maintaining 24/7 parking lot security

By Alex Doorduyn
Siklu Communication

Many hospitals today currently have large parking garage complexes containing multiple levels of parking supported and protected by an extensive parking gate entry system and surveillance system; however, deploying these types of solutions in remote and outdoor parking lots can be a challenge.

Unlike a retail environment, which has a set open and close time and a parking lot that empties out in the evening hours, parking lots at hospitals are typically full around the clock. Not only are employees walking to these parking lots at all hours of the day and night, meaning that their safety needs to be protected, but it is also important to monitor parking lots and their surrounding areas to deter against vehicle vandalism and theft.



It's fair to say that over the past 10 years, many hospitals have made a significant investment to improve the security within and around the perimeter of their facilities. For healthcare facilities, protecting patients, staff and visitors has become

increasingly important in addressing patient privacy, safeguarding against infant abductions and ensuring an overall safe environment. Tighter rules and regulations require healthcare facilities to keep under lock and key and provide an audit trail of those with access to prescription medication.

The desire to provide better security and safety at healthcare facilities also extends to areas outside of the walls, sidewalks and outdoor gardens that are part of these campuses to include the parking areas used every day by employees and visitors.

As many large hospitals already operate their own command centers to monitor their security, it's important to integrate video surveillance of the parking lot into the hospital's existing security system.

Infrastructure Challenges

In remote lots, the lack of a power source or access to fiber can make it very difficult to deploy a video surveillance system that can be actively and continuously monitored. As many large hospitals already operate their own command centers to monitor their security, it's important to integrate video surveillance of the parking lot into the hospital's existing security system.

In some instances, the remote parking lot can be located half a mile away from the main campus, according



to Craig Lerman, president and CEO of LTW, a systems integrator in Pine Brook, New Jersey — which can make this type of project more challenging.

“Putting fiber up to the parking lot from the hospital can be expensive and it can take a long period of time to get it there, especially if you need to get a right of way approval across multiple properties,” says Lerman. “We routinely deploy wireless solutions to overcome those obstacles.”

Wireless Parking Lot Surveillance Options

If fiber is not an option, due to unavailability, cost, time or disruption to deploy, it’s important to consider a few points before implementing a wireless system.

First, review your current and future bandwidth consumption needs to ensure you implement a system that can handle multiple video sources without impairing the video quality while maintaining low latency. This capacity analysis needs to address future bandwidth requirements as technologies such as 4K hit the video camera market and become commonly deployed. Second, account for all data traffic requirements of the link. In addition to video, the same wireless link may also carry voice and data. Therefore, quality of service (QoS) must be factored into the design process.

Millimeter (mmWave) wireless, a next-gen, gigabit fiber-like technology, uses spectrum that is located at much higher frequencies than traditional



wireless consumer products and can provide reliable connectivity and enough available bandwidth to accommodate multiple HD cameras and even 4K cameras on a wireless video surveillance network.

If you’re mounting cameras to existing light poles, check to make sure that there is continuous power at the pole. When continuous power isn’t available, a continuous power bridge (CPB) is another option to consider. One benefit of using the Power over Ethernet (PoE) power sourcing capabilities of mmWave radios: some systems can also provide power to a camera, which can reduce installation time and the number of power supplies required.

Surveillance Network Deployment Options

Wireless networks that use mmWave radios to transmit data are much simpler to design and pre-installation preparation is minimized because no spectrum analysis is typically required — the only requirement is to ensure that there is direct line of site and calculate the distance of transmission. mmWave's transmission beam width is very narrow, and its high frequency short-range propagation

characteristics greatly reduce the possibility of interference in the environment due to other RF systems.

"You have to consider many factors when installing a wireless networked surveillance system, so it's important to do a comprehensive site survey and use the path propagation tools provided or specified by the vendor," says Lerman. "The up-front engineering has to be correct and wireless radio links have to be mounted correctly to a very rigid pole to ensure reliability." In addition, it's important to ensure

Millimeter (mmWave) wireless is a next-gen technology that provides reliable connectivity and enough bandwidth to accommodate multiple HD cameras and even 4K cameras on a wireless network.





the network will not get jammed due to heavy Wi-Fi traffic or malicious intent. The narrow beam technology and frequencies associated with mmWave radios means they are extremely robust, dramatically reducing the already small risk associated with typical wireless systems.

“The surveillance system for a hospital parking lot may incorporate a variety of different security cameras, such as high-resolution cameras that can identify a license plate or to clearly identify facial features of an individual,” according to Rick Adams, director of security solutions for LTW.

“Hospitals will install cameras on the roof for general surveillance purposes to see the street and a parking area,

but will also install cameras closer to the ground to capture better details,” said Adams.

Regardless of which type of wireless security system you implement, Adams advises users to make sure the wireless system can provide reliable connectivity and enough available bandwidth to accommodate future growth as customers are always looking to upgrade both the number of cameras and the resolution of their cameras to include 4K and beyond. ■ [Back to TOC](#)

Alex Doorduyn (alex.d@siklu.com) is business development and sales director, security and surveillance, at Siklu Communication (www.siklu.com).

Audio has been a standard feature in professional network cameras for at least a decade, yet the integration of audio has had little impact in the overall scope of physical surveillance installations.



Listen Up

How audio monitoring raises the surveillance bar

By James Marcella
Axis Communications Inc.

Did you know that the “See something, Say Something” campaign originated with the New York City Metropolitan Transportation Authority? The citizen participation program was so successful as a force multiplier for local law enforcement that the Department of Homeland Security (DHS) licensed the idea and turned it into a nationwide campaign.

Video surveillance manufacturers are taking this lesson to heart by placing a new emphasis on the audio capabilities of their systems that enable their security tools to not only “see things” but “say something” as well. Coupling audio with video has been shown to increase a surveillance system’s overall ability to deter crime, increase public safety as well as improve situational awareness among responders.



Why Aren't More People Using Their Audio Features?

Audio has been a standard feature in professional network cameras for at least a decade. Yet the integration of audio has had little impact in the overall scope of physical surveillance

installations. Why? The challenges to adoption have been twofold: one legal and one technical.

- For many users, the legal ramifications of adding audio to the surveillance system have pushed this technology out of consideration. As you read further, you'll learn that there are several ways to approach audio that fall within legal bounds.
- The complexity of integrating systems that are operating on different infrastructures can be costly. In many cases, audio equipment ranging from public address, phones and hand-held radios are all analog. As this article will explain, that siloed approach to systems is rapidly being replaced with standards-based, open solutions that run on the network.

Changing Your Perspective on Audio Surveillance

Most security professionals think of "listening" when you talk about implementing audio with surveillance cameras. But what they really should be focused on is monitoring. You should also take the "human" out of the equation and think more in terms of "audio analytics," where the camera uses a decibel threshold or an acoustic signature to establish that an event has happened – such as glass breaking. Or, the camera uses a video analytic to trigger an audio response to an event – such as a broadcasting a verbal warning. These events could also be layered creating a tiered response based on a subject's behavior.

To illustrate this point, imagine waiting for a train at the station. Notice the yellow line on the floor meant to protect people from coming too close





to the tracks. Using a video analytic such as crossline detection, the video surveillance system could detect a person who is in the yellow space and then play a pre-recorded message over the networked speaker to “Step away from the tracks.” If that person does not comply, an operator in the security operations center receives an alert, reviews the video live and then engages in a two-way conversation with the person. It’s one thing to hear a generic message, it’s another thing entirely to be identified by what you are wearing and asked to step back from the yellow line. If the person still does not comply, then the next tiered response might be

Most security professionals think of “listening” when talking about audio surveillance – but what they really should be focused on is “audio analytics.”

to send a uniformed response to the location.

This defense-in-depth approach to physical security is prevalent in many facilities. It relies on a combination of people, processes and technology across multiple layers moving from the outer perimeter inward. Usually, these facilities mount cameras on the outside of a building to record activity along the perimeter of the property. But what they rarely do is mount loudspeakers on the outside of the building. And given that some security professionals argue that due to the prolific use of video surveillance, cameras are not as much of a deterrent as they used to be, these

facilities are missing an opportunity to enhance their deterrence.

Case in point, loitering can be as innocuous as some kids choosing the wrong spot to “hang out” or it could be as threatening as someone casing your establishment or waiting to rob one of your customers.

Either way, most business owners would rather not accept the risk and prefer that people move on. You can detect loitering with visual assessment

of the scene, but you still need to communicate your intent, which typically involves approaching the offenders and asking them to leave. By adding loudspeakers to the equation, business owners and security professionals can address the offenders remotely from the safety of their building, thereby avoiding a possibly risky face-to-face confrontation. People

Automated audio monitoring is a different story because it doesn't involve a human eavesdropping on a conversation.

are more likely to comply if they know someone is watching and recording their behavior.

Drilling Down on Legal Barriers

Most network cameras shipping today have embedded audio features

that are disabled by default – for legal reasons. In the United States, federal and state wiretapping laws legislate when audio recordings are permitted.

Since many end users and system integrators don't understand the legal framework, they prefer to avoid audio altogether.

Depending on the state, you may be okay recording a conversation as many have enacted “one-party consent” laws with you being one of the parties providing consent. Other states require all parties to grant consent before a conversation can be recorded.





Especially for companies operating across state lines, the simple solution has been not to record audio, period.

But *automated audio monitoring* is a different story because it doesn't involve a human eavesdropping on a conversation. The audio analytics just detects sound waves by acoustic signature and makes no attempt to translate sound into words. (More about this later in the article.) So, there is no breach of privacy. In most cases, listening in and archiving an audio recording really isn't necessary anyway. You just need to be made aware that something is happening so that you can respond. When the analytics detects certain sounds, it can automatically alert you to watch the live video – which is perfectly legal – so that you can ascertain whether it's necessary or not to communicate with the target individuals to let them know you're observing them. Usually, a simple verbal warning is sufficient to stop the behavior. In more serious

cases, an audio component can enable you to inform the perpetrators that law enforcement is on the way.

A word of caution: If you do plan on recording audio, then I strongly suggest that you discuss it with a lawyer to ensure that you are operating your system within the letter of the law.

Drilling Down on System Complexity Barriers

Over two decades ago when the first network camera was introduced to the surveillance market, it was met with skepticism from the traditional CCTV integration channel. The technology was a paradigm shift from analog, and it required a whole new skill set – computer networking – which they did not understand.

That same shift is repeating on the audio side with the transition from traditional analog silos to a digital world. The good news is that the same hard-earned computer networking skills learned from the network camera

world can be applied to the latest generation of audio equipment as well so the learning curve will be short.

Traditional physical security companies need to understand that the barriers to audio integration are quite low and adding audio to their portfolio of solutions can greatly enhance their value. Every job that requires video surveillance, particularly ones that involve the monitoring of public access spaces, should be evaluated as a potential candidate of audio augmentation. There are certain vertical markets where internal audio components are standard such as schools, hospitals and public buildings. These "overhead" paging systems are on the move to digital and could also be incorporated into the physical security discipline.

So, what should an integrator or security practitioner know before adding audio monitoring to their repertoire? Let's start with the easy

part: the network. Most of you reading this have been exposed to or have embraced network cameras over the past decade. The infrastructure you have deployed for these systems is the same for audio: Ethernet on an IP backbone. What you need is experience with Session Initiation Protocol (SIP), which is the predominant communications protocol used by manufacturers to ensure interoperability between devices. This you can acquire through internal training or hiring external expertise.

As an historical side note, SIP was introduced in 1996, the same year as the first network camera, and ratified as standard in 2000. Like other network protocols, it sets forth the rules for devices to establish, maintain and terminate connections. Most voice-over-IP (VOIP) phone systems use it, which makes these systems compatible with physical security devices.





For example, if a network camera supports SIP, you could pick up your VOIP phone, dial the IP address of the device and converse with the person you're observing. This assumes that the camera is equipped with a microphone and speaker. Most cameras ship with an embedded microphone but rarely do they have a speaker unless they are purpose-built solutions such as a networked door intercom. So, in many cases, you have the basics on the networking side. You just need to add SIP to your already long list of acronyms that were thrust upon you by the IT world.

Understanding How To Optimize Microphones

To ensure that you use the camera's microphone to its best advantage, you need to understand how its operation is affected by the environmental aspects of the scene you're monitoring as well as what you're trying to accomplish. Most built-in microphones

are omnidirectional, meaning they pick up ambient noise in all directions around the camera. Depending on the size of the area monitored, this often does not meet the needs for security professionals unless the camera is placed indoors in a relatively small room.

There are also limitations with using built-in microphones outside because the camera needs to be installed in an enclosure that effectively cancels out the ability of the microphone to pick up any sound. In most cases, a separate, standalone microphone is used by connecting to the camera and co-locating it with the camera. By using a separate microphone, you can choose the best "audio pick-up pattern" for the given scene.

For instance, you might find that a directional or "shotgun" microphone is more appropriate for monitoring audio at your front gate because you can eliminate the sounds of your employees talking inside your

perimeter. Manufacturers can provide you with the specification on the effective distances these microphones can pick up sound as well as best practices for installation. Most cameras will have a standard “line-in” jack located on the camera for using third-party microphones. Make sure you confirm the size of the connection before purchasing to guarantee compatibility. Also check for outdoor ratings for both temperature range and water/dust ingress. There are many IP66-rated solutions you can choose from on the market today.

Understanding How To Optimize Loudspeakers

Speakers come in many shapes and sizes, but most external speakers used today resemble wall-mounted bullhorns. Networked loudspeakers, which have been available for a few years, are now enabling some interesting opportunities for integration that were not possible with their analog cousins. By sharing the IP backbone, these network devices can be integrated with other physical security countermeasures providing the “say something” for more than just

video. An example would be a Passive Infrared Detector (PIR) triggering a pre-recorded message that is played over the networked speaker. This form of hands-off approach can be leveraged across many video management systems and provides an added layer of deterrent.

Speakers also provide a valuable option for mass-notification across buildings and campus environments. As stated earlier, if your organization leverages VOIP for telephone communications, the networked speaker becomes one more “number” to dial giving security professionals the ability to address people across the entire system as necessary. Of course, that assumes the speakers are all in functioning order. But what if that is not the case? How do you find out which speakers are inoperable? Here, too, manufacturers have put some forethought into the problem. Today’s networked speakers have an incorporated testing function. Basically, it is conducted by a limited microphone embedded in the unit that picks up an acoustic pattern played by the speaker and reports back that it is operational. This saves valuable

maintenance time and ensures that your investment is functioning when you need it.

Where Audio Analytics Comes Into Play

Most reading this article don’t have staff that monitors your video daily. So, your video is primarily a reactive



tool that you view after the fact to determine what happened at a given scene. But with audio analytics, you can be more proactive with your security system, learning about potential problems in real-time without the legal constraints barring a live operator from eavesdropping on a conversation.

So how does it work? Embedded on the camera, audio analytics can detect such sounds as aggression, a car alarm, glass breaking or gunshots, and trigger a proactive notification should audio be detected that represents those acoustic signatures. Audio-enabled cameras equipped with audio analytics become intelligent, dual-technology sensing devices that security professionals can leverage with low incremental investment.

Municipal monitoring provides a great use case for several audio analytics when you consider the high number of people and vehicles in a relatively small area. Most aggressive acts, such as fights, start with a verbal altercation prior to the physical confrontation. Audio analytics can detect aggressive voices and alert law enforcement or private security that an altercation of some sort is happening in view of a particular camera.

Responders could then remotely monitor the situation to determine

if this is a situation that requires intervention of some sort. It could be just some guys celebrating their team's win or it could be aggressive posturing that might quickly escalate.

Regardless, audio analytic detects aggressive sounds and quickly sends out the alert while the video verifies and records what is happening. Timely response is important so anything that can provide early indicators of behavior helps

security professionals resolve issues or determine cause.

Traditional physical security companies need to understand that the barriers to audio integration are quite low and adding audio to their portfolio of solutions can greatly enhance their value.

Not Just Video Anymore

Audio has been used for many years by security professionals but in limited situations and often as standalone systems that were not integrated with other security solutions. With the introduction of IP networked speakers, the use of audio has the potential to increase the value of surveillance systems at a relatively low incremental cost. Moving forward, it would behoove you to become acquainted with SIP. Furthermore, every time you install a camera you should ask yourself whether it is also an opportunity for installing audio. ■ **Back to TOC**

James Marcella (jmarcell@axis.com) is director of industry associations at Axis Communications Inc. (www.axis.com).

With continuous power supply system monitoring comes the opportunity for creating real-time action alerts and reports for system maintenance and management.



Smart Power

The paradigm has shifted to intelligent networking solutions

By John Olliver
LifeSafety Power Inc.

In the past, power wasn't smart. It was simply a static piece of hardware – still necessary but not connected or integrated with other physical security components and certainly unable to tap into analytics, predictive data or history reporting.

That's no longer the case. Now, the paradigm of power has shifted from unintelligent device to network-connected component that yields rich data for the user and allows the security integrator to provide remote monitoring and managed power services – producing numerous residual benefits to installers and customers alike.

This transformation of power has coincided with the move of many products and solutions to the network and IP connectivity. Now, not only are surveillance, access control, audio and other devices IP-based, but power



solutions have moved to the network, providing real-time information and intelligence on connected technologies across the enterprise and protected premises.

The movement of security devices to reside on networks gives rise to a

host of capabilities and opportunities that not only enable these devices to work together to provide more effective security but also allows the monitoring and supervision of integrated solutions to ensure their *continuing operation*. Too often, the latter point is overlooked.

Increasingly, humans face an array of devices that help us monitor our own body performance – pulse, heart rhythm, skin temperature, light exposure and noise levels, for example. Of these and others, cardiovascular functions are arguably the most important. A network may be compared to the body's nervous system; meanwhile, power bears closest resemblance to the circulatory system. Monitoring and managing the current flow through the system can lead to increased longevity and performance, as well as avoidance of unexpected surprises in the form of device failures.

The base concept of power monitoring and management is not new. For decades, electrical utilities have deployed intelligent systems to maintain a continual flow of energy to their customers, constantly balancing energy supply with user demands and rerouting flows when problems arise. Over the past several years, this thought process has entered the conversation in the electronic security market, where random device failures or loss of power are unacceptable.

If the power supply can be compared to the heart and current to blood flow, monitoring and managing the health of both will contribute to the continued safe operation of physical security solutions.

The benefits of smart power management solutions to end users are clear. Predicting and gathering data on the health of systems provides a high return on investment (ROI) for the user, low overall total cost of ownership



(TCO), reliable uptime and assured business continuity.

Smart power systems improve the security of equipment, protected assets and people.

For the systems integrator, managed power provides the ability to provide a new suite of services to the customer that monitor, alert, manage and provide detailed reporting on systems solutions remotely.

History of Evolution

Power solutions have changed dramatically in performance and design. In the '70s, power systems used linear regulation, an older and inherently inefficient technology. Linear systems required a large, step-down transformer and would burn off extra voltage as heat – an enemy of electronics.

Linear power supplies continue to be phased out, in favor of offline switching supplies (OLS). OLS provides a cleaner output than linear, less noise and ripple, removing the need for a step-down transformer while improving efficiency, reducing weight and decreasing heat output. When power supplies began to move to OLS, the higher efficiency offered a greater feature set and power solutions started their transition to smart, network-connected systems.

With smart power, a quick look at system health is possible at a moment's notice and trouble conditions are reported in real time. With proactive power management

systems and predictive analytics data from networked components, an end user can be informed, ahead of time, of impending lock failure or

With smart power, a quick look at system health is possible at a moment's notice and trouble conditions are reported in real time.

battery fatigue, offering the ability to replace components in a timely manner and maintain system operations. With continuous power system monitoring

comes the opportunity for creating specific action alerts and reports for comprehensive system maintenance and management.

The Possibilities to Perform

Managed power can encompass several physical elements: the main power supply, power system outputs, supervised inputs and standby batteries. When it comes to power, there are different ways to accomplish managed monitoring and remote servicing. Managed monitoring can include: event reports, AC loss notification, service due reminders, overcurrent alert and low-battery warning. Remote servicing capabilities of power solutions can include: output supervision, battery load testing, remote power cycling and system health logs/trouble alerts.

The enhanced monitoring provided by managed power sends immediate notification of current or impending problems. Once notified, the monitored parameters allow basic troubleshooting remotely without sending a technician to the site.

With continuous power monitoring also comes the opportunity to create

real-time action alerts and reports for system maintenance and management. Alert formats may include email, XML, web-browser notification or Simple Network Management Protocol (SNMP). For example, a short circuit or integrated lock that is running “hot” and could present a fire hazard will instantaneously generate an email alert or SNMP “trap” to notify the integration company or end user of a potential problem.

Moving the Industry to Fully Integrated Solutions

Network monitoring and management systems typically rely on SNMP. When a managed power system supports SNMP, it becomes eligible to be monitored, and possibly controlled, by a high-level system. This creates the opportunity for IT departments to have greater ownership in addressing selected problems affecting security. Through the development of security industry standards, such as with the Physical Security Interoperability

Alliance (PSIA), which encourages “plug and play” interoperability, managed power systems can share the information and intelligence they generate with a wide range of other devices, services and systems.

Intelligent power systems with appropriately provisioned web browser interfaces provide the capability to not only predict but to implement actions in critical situations. Managed outputs may be individually activated or deactivated to shut down or recycle equipment through an embedded browser interface and then monitored for voltage and current values via the network or internet.

Other specific managed capabilities may include the following:

- Battery load tests can be scheduled or performed via network connection to check a site’s real backup capability against what’s required. Sites with underperforming battery backup are immediately flagged, so servicing can be performed





in a rapid, efficient and proactive manner.

- Since impending failure of electric strikes and magnetic locks can be indicated by unusual changes in current draw, intelligent power systems, through tracking and reporting of power consumption, can often predict when and where a lock is starting to go bad.
- Ambient air temperature of the Intermediate Distribution Frame (IDF) security closet can be monitored and trigger an event notification for investigation if temperatures reach an unusual level.
- Security integrators can configure managed power systems to provide notifications for scheduled service or battery replacement.

In a managed power solution, there are many factors that contribute to a healthy ROI, focusing on the ability to be alerted to problems, remotely diagnosing those problems and maximizing system uptime without having to dispatch a service vehicle. Other factors to consider are the profitability loss to the business due to system downtime or malfunction, or having to hire security support personnel at the protected premises.

In addition, by monitoring current to a device and being alerted to system values moving to an unacceptable range, the chances of sudden catastrophic failure of security equipment may be minimized. Monitoring voltage, current and power draw of attached devices can help spot performance degradation and predict impending failure. Problems may relate to device temperature,

fan performance, mechanical or component issues. Batteries attached to power supplies will degrade over time and become incapable of providing backup power for the required period of time. A system that can verify battery performance, optimize its charge profile and maintain its history helps ensure the battery will be there when needed.

Remote Monitoring

Remote monitoring of power solutions adds value to the integration firm and makes them more proficient in the field, and that translates to more money to the bottom line from direct time and labor savings. Managed power services can be added to the suite of services currently offered by the integration company.

Here's how remote monitoring of power solutions works:

- You are notified by email, text or while online that one of the

power solutions is running hot, the access control won't engage, or the security solution might somehow be compromised should a real emergency occur.

- You can remotely, from anywhere, access the graphic user interface, assess the system health and even reboot or reset necessary components.
- If a site visit is required it can be scheduled immediately if necessary or conveniently the next business day.
- The proper parts and accessories can also be planned for, so ideally the work is completed during a single call.

As the Internet of Things (IoT) progresses, sophisticated electrical components will need to be up and running consistently. When there is a problem, the ability to remotely service connected components, such as power solutions, will become increasingly



important. No longer will technicians have to trudge out to the field during regular and even off hours, because many problems can be solved over the Internet, thanks to smart, connected power solutions.

When there's trouble with a networked solution, the systems integrator should be the first to know, not the customer upon failure. Intelligent, networked power solutions allow trouble alerts to be sent automatically and immediately, so the integrator is the hero and not the bad guy. Now you can detect problems before or as they occur, so the customer is assured that their system is operational 24/7 and especially in the event of a security breach or life safety event. Intelligent power system solutions will regularly assess power operation and the health of connected solutions and pick up failures immediately.

Other Valuable Benefits

Customers like metrics and data and connected power solutions allow systems integrators to generate detailed reports on the operating status of devices. These health reports can be produced on demand, daily, weekly, monthly or scheduled at intervals the customer desires. Reports can be saved for yearly status updates or other accountability purposes, such as in meeting compliance or regulation requirements. Reporting can provide valuable insights into device or system history and available on demand or as defined periodically. Maintaining a site's operational history

with data logging of 1,000 events is possible with managed power systems now providing more than a year's history.

For systems integrators, there's no ongoing profitability from static hardware they simply install and leave behind. Intelligent power solutions bring a new value proposition in the way of monthly recurring revenue from managed services and keen situational awareness to the customer's facility and their networked power solutions. It's the future of connectivity, here today.

Smart power is a *tangible asset* that security companies can offer to their customers to expand their business. When cost savings are properly related to the end user and the ROI is calculated, it provides an even stronger value proposition that ultimately lets the installing company make more money and provide additional services that are useful – and make the customer stickier.

In industries where security and reliability truly matter, power is the most critical platform of any system. Power has a new look and technological design for mission critical and security industry systems responsible for saving lives and property. Now, it can detect, report, assess and help respond before potential negative consequences occur. ■ **Back to TOC**

John Olliver (jolliver@lifesafetypower.com) is senior vice president of sales and business development at LifeSafety Power Inc. (www.lifesafetypower.com).

A willingness to employ emerging innovations enables us to deploy and exploit technology in a way that benefits us and our customers.



Navigating Technological Change

The way to success is ensuring new technologies impact your customers in a positive way

By Todd Graves
Allegion

Technological change is continuing to accelerate, impacting every part of our industry. We experience this year after year, as electronics get smaller and more powerful and bandwidth and storage become more readily available and affordable – accelerating the pace of innovation of products and services.

At first glance, the acceleration is sometimes hard to perceive. But consider the state-of-the-art technology in 2005: Most households owned home computers, wireless technologies had emerged and mobile phones were pretty much ubiquitous. The most advanced consumer electronics were flip phones, the iPod classic and digital cameras. At the time, these all seemed so cutting-edge. But today, over 10 years later, the technology of 2005 seems surprisingly



antiquated. Those devices have all been replaced by smartphones that do each job better than the special-purpose devices of 2005. Now think ahead: By 2025 – roughly 10 years from today – we will have autonomous cars and trucks occupying the road with

us. Today's devices, with their touch interfaces, will seem quaint.

Without a doubt, technological change will affect our personal and professional lives.

But our focus as an industry should be on how it will impact the spaces where

we will live and work. 5G cellular technology means that we will have access to unimaginable amounts of data, bandwidth and processing power everywhere we go. We will no longer be tethered to fixed locations to be productive. As part of this transformation, work and living places will be flexible and people will gather into workgroups dynamically.

Today, we are at an inflection point. Technology has reached a point where we're able to see the future state materialize. We are seeing flexible work spaces and hoteling. The sharing economy is changing the way to travel. Unattended delivery is changing the

way we shop. And the first generations of autonomous vehicles are emerging. We can see the horizon from here.

Those radical changes of 2025 have already begun.

But to reap the benefits, we need to embrace the future now so we can drive the

change, rather than be disrupted by it.

The term disruptive innovation was coined by Clayton Christensen. He defined it as an innovation that disrupts established businesses by offering to meet the needs of customers who are not getting the attention of incumbents, and then uses technology and that beachhead to replace the incumbent altogether. Netflix is an example of a disruptor. When it first emerged, most customers wanted the instant gratification of renting a movie from a nearby store. But Netflix addressed the enthusiast segment of the market that was willing to trade on-the-spot rental for

**The question for all of us:
Will we be disrupted or will
we be the disruptors?**





the wide selection available online – even though it meant waiting a few days. For a time, Netflix and video rental stores coexisted, but Netflix had established a beachhead by addressing a niche market. With the expansion of bandwidth in homes that enabled video streaming, Netflix was then able to deliver the same catalog — now with instant gratification.

Technology is inherently a disruptor; change driven by technology will happen one way or another. The question for all of us: Will we be disrupted or will we be the disruptors? The way we succeed is to ensure new technologies are affecting our customers in a positive way. No one knows our customers better than we do. Collectively, we need to ensure that as new technologies arise, we find and create real customer value. It can't be about technology for technology's sake. It's not about gadgets. For us, it's about using technology to design better spaces for people to live and

work – blending security, safety, convenience and efficiency.

Becoming comfortable with emerging technologies is critical. A willingness to employ emerging innovations enables us to deploy and exploit technology in a way that benefits us and our customers. Though keep in mind, advancing technology brings associated risks. It's just as important to understand how to identify and prevent threats, and be able to communicate the pros and cons effectively.

Understanding Technology Trends and Threats

Big Data

As we connect more devices to the Internet of Things (IoT), we generate exponentially increasing amounts of data. There are the obvious devices like readers, thermostats, occupancy sensors and video feeds. In the future, other data sources will layer on top of that, including Bluetooth and RFID

location data for the occupants and assets throughout the building. In isolation, that data has little value beyond the device that generates it. But in aggregate, the data set starts to generate new value.

Analysis of Big Data will give us new insights into how buildings are really used. What are the usage trends throughout the day? Are occupancy levels what we thought they would be when we designed and built the spaces? Are there bottlenecks to productivity? Are we running the building systems as efficiently as possible? Is reliability and durability as

good as we expect? Not only can we gain insights about a particular building, but we can use comprehensive information collected from other buildings to identify larger trends.

Machine Learning

Big Data exists today. Huge data sets are being assembled in a variety of industries, providing insights that were not possible before. But we are in the midst of a huge technological breakthrough that will change the way we can analyze and respond to data sets, large and small. It's called machine learning.

Differential Privacy

This all sounds great, but there are associated risks, as with most technologies. In this case, it's privacy. And that's where differential privacy comes in. The term was coined by Apple and refers to the ability to collect user data to create a Big Data set, while obscuring the contributions of individual users. Think about how much private behavior can be monitored in the home or business by connected systems. That data, in aggregate has value. But users are not going to consent if they have any fear that their individual data can be accessed.

In Apple's case, they are going to be collecting a lot more data from their phones, computers and IoT devices connected through their HomeKit platform. They don't really have any interest in a particular user; their main objective is to improve their services. So, they want to be able to aggregate the data and make it impossible to parse out any user-identifiable information. To guarantee this, Apple intends to apply sophisticated statistical techniques to ensure that this aggregate data – the statistical functions it computes over all your information – doesn't leak your individual contributions. This sounds simple, but there have been cases where it has been done poorly.

In the end, we need to be able to get the benefits of Big Data without compromising privacy. Like the other aspects of Big Data, it is going to require collaboration among all of us to create data strategies that incorporate differential privacy.



Machine learning needs data that is identifiable and can be correlated to the real world. Often called training data, this is data that has been tagged or categorized. Mega techs like Google, Facebook and Amazon are spending tremendous resources to build training data for their machine learning systems – and you're likely part of their labor pool. Every time you tag a face with someone's name on Facebook, you are providing free labor to its machine learning training data for its facial recognition system. In the future, these systems will become autonomous, learning how to do what humans do today.

To date, there hasn't been industry buy-in to go through the work of collecting and tagging data to feed a machine learning system. But the mega techs have already demonstrated that the value proposition exists. For example, last year Google announced that it used the machine learning algorithms from Deep Mind, a U.K. company it purchased, to cut data center energy usage by 40 percent, saving hundreds of millions of dollars

a year. Now, machine learning systems are running the HVAC systems in all Google data centers, adjusting fans and cooling systems in real-time to continue those savings.

Google may have been the first to use machine learning to change the way they operate their infrastructure, but it's coming soon for everyone else. But as I said before, we have to have good quality data for machine learning to use. Now is the time for us to identify how all the equipment in a building will tag, store and deliver data. The actual machine learning algorithms will be provided as a service, so we don't have to become machine learning experts, but we do have to focus on building in the sensors, collecting the data and eventually tagging it to reap the benefits of machine learning for our customers.

Artificial Intelligence

A related trend to machine learning is artificial intelligence (AI). As we integrate connected devices in the building's access control, HVAC, video and more, AI systems

can create new levels of security, safety and convenience based on the combination of those various inputs, replacing what we count on humans to do today. Human beings are incredible at pattern recognition, especially with visual data. Our brains are essentially big image processors. Humans are much better than today's computers at pattern recognition. But humans don't have the attention span of computers, and computers are starting to gain the artificial intelligence to do those tasks as well as a human.

Think about an access control scenario. Today, we rely typically on one thing to make an access decision: the credential. Perhaps two if we add a PIN or biometric to the system. AI allows a security system to use every piece of data in the building to make intelligent decisions about access or egress. It can monitor video for behaviors, perhaps asking for a PIN if pre-credential behavior looks suspect.

Like with machine learning, AI is dependent on good quality data, meaning that the systems within the building need to produce data in common formats. We need to build those requirements in from the beginning.

Augmented and Virtual Reality

A megatrend that is a little less radical and a bit easier to implement is augmented and virtual reality. To get a sense of augmented reality, think about Pokemon Go. Players use their phones to view the real world with a virtual overlay. The game may sound like a gimmick, but there are highly productive applications that have relevance in our industry.

Augmented reality (AR) is the overlaying of data on top of what you see. Virtual reality (VR) is creating something that does not exist. Both have practical applications for customers. For occupants, an AR overlay on their mobile device can





direct them to where they need to go in the building. It could overlay every door in the field of view with the occupant's name and availability. It could indicate whether assets are free or being used. In the flexible workspace or hoteling environment, it could provide an overlay showing where everyone is working in that moment so employees could easily find each other. In a safety situation, AR could direct people to the safest exit based on real conditions in real time, pointing out a path for safe egress.

AR will be mainstream in the very near future. The biggest challenge for the industry is to have good data that can quickly be integrated into an AR system. For AR, it comes down to having building system data in common formats, so that integration is easy. For VR, it means products need to be supported by good 3D data in common formats, which need to be

integrated with beacons and mobile devices.

Cybersecurity

A multitude of systems, sensors and devices in smart buildings connect into the Internet of Things to automate and optimize security, HVAC, lighting, surveillance and other parts of building operations. However, the connection of more and more devices to the IoT carries risks. And we have seen cases already where the IoT has been used as an attack point for hackers.

One reason is that many of these products and controllers that are being connected run on legacy operating systems that have not been hardened against cyberthreats. They may use old versions of Linux, for example, that have known vulnerabilities.

Many access control systems, along with other building components, usually connect using nonstandard protocols. Nonstandard could mean a

protocol that is proprietary to a certain manufacturer, or it could even mean one that is only used by a certain class of systems but isn't standardized outside the industry.

At first glance, nonstandard protocols might not seem like attractive targets for hackers. After all, hackers know TCP/IP and HTML, so they have the skills to attack systems using those standard protocols. That's not the issue. The problem is that the IT department's cyberdefenses don't understand these protocols and often can't detect malicious activity on the network. They typically have cutting-edge defensive tools against attacks, but these systems only work to monitor traffic on standard protocols like TCP/IP and HTML. I'm not advocating a complete shift to these standardized protocols for building systems, but we need an industry-wide strategy on how to be more open and collaborative.

Cybersecurity risks are substantial. A cyberattack can freeze elevators, cut power to the building or turn IoT devices into a botnet to do further harm to other victims. Any of these connected IoT devices, if compromised, could be a backdoor into the customer's entire corporate IT network, making all their data vulnerable.

Our approach to security must be more integrated in the future. We need a new security architecture that provides visibility across IT systems, operational devices and IoT devices. And as an industry, we need to plan for this from the start and use open and more standard protocols that are hardened against attack. These considerations need to be part of the design process, something that manufacturers, integrators and even architects need to cooperate on for their customers.

In fact, a well-designed system can provide enhanced levels of security. As our connected systems are hardened against attack, integrated building systems are more resistant to social

engineering. Social engineering is defined as the manipulation of people into performing actions or divulging confidential information, and it's perhaps a greater security threat than true cybersecurity. In

Manufacturers are often in the best position to keep abreast of technology trends. They monitor technologies as they develop and are constantly working to integrate those technologies into our products.

fact, it is estimated that two-thirds of all cybersecurity attacks have an element of social engineering.

As we prioritize convenience and productivity, we open increased vulnerability to social engineering. An access control system with both credentials and biometrics is pretty immune to social engineering, as



long as gates are in place to prevent tailgating. But those systems aren't very good for throughput and can be a pretty big productivity hit.

The good news is that artificial intelligence and machine learning will provide a solid defense against social engineering. Despite years of training, employees still fall victim to the simplest email and phone phishing scams, giving up usernames and passwords and creating backdoors into IT systems. On the other hand, AI doesn't easily fall for social engineering. Social engineering often comes down to playing on the emotions of the victim, exploiting his or her desire to be helpful. AI systems don't have emotions to exploit.

The Integrator's Role

Ultimately, it's up to the systems integrator to help customers blend security, safety, convenience and efficiency in ways that meet the needs of the owner, operators and occupants. These can often conflict, but with the

proper systems – and early planning – they can be in optimal balance.

It starts with an understanding of new innovations and the ability to communicate these technologies in a way that alleviates customers' fears. Knowing how to prevent privacy and security threats is essential because technology will only continue to accelerate. Leverage your manufacturing partners. Manufacturers are often in the best position to keep abreast of technology trends. They monitor technologies as they develop and are constantly working to integrate those technologies into our products.

Let's put ourselves in the driver's seat as innovation and technology change the way we design, build and operate the places where we work and live. We can be our own disruptive innovators. ■ **Back to TOC**

Todd Graves (todd.graves@allegion.com) is senior vice president of engineering and technology at Allegion (www.allegion.com).

We cannot lose sight of the human aspect of using new technologies as we move forward. The use of invasive technologies will need to give way to nonintrusive technologies.



The Puppy Movement

A new vision for security

By Doug Haines
Haines Security Solutions

When we think of security, we often think of products. We think of fences with concertina wire on top, big bold cement blocks, or at the very minimum a jersey barrier to prevent vehicular threats. We think of armed soldiers walking the streets in Europe and stationed in “places of interest” here in major U.S. cities and in places like Times Square or Union Station. At sporting events and outdoor concerts, we think of metal detectors and bag searches. And when traveling, we think of bag searches, emptying pockets or standing for a body scan.

These mechanisms are designed to be very visible. They’re almost designed to be “in your face.” They are saying, “Hey, scumbag come over here, and we’re going to get you. So just try us!”



And there are also the electronic systems like cameras or biometrics and a whole slew of other technologies that add to a “Big Brother is watching” feeling, almost as if we’re in a warzone and are expecting an attack by the hordes at any minute. I call this type of

security implementation the “Big Dog” concept.

It’s like the big black and white sign with red letters on the garden gate that warns of a big slobbering Rottweiler on the other side of the gate just waiting to “take a bite out of somebody.” It’s bold and in your face on purpose – like John Wayne slinging his side-arm. But this Big Dog attitude and the big “Woof” that goes with it really doesn’t do much in the way of preventing bad things from happening. It transfers some of the threat likelihood to somewhere else. But most of the time, a dedicated threat will not be deterred. The “bad actor” only brings a bigger, better ladder or bolt cutters or a gun to the party.

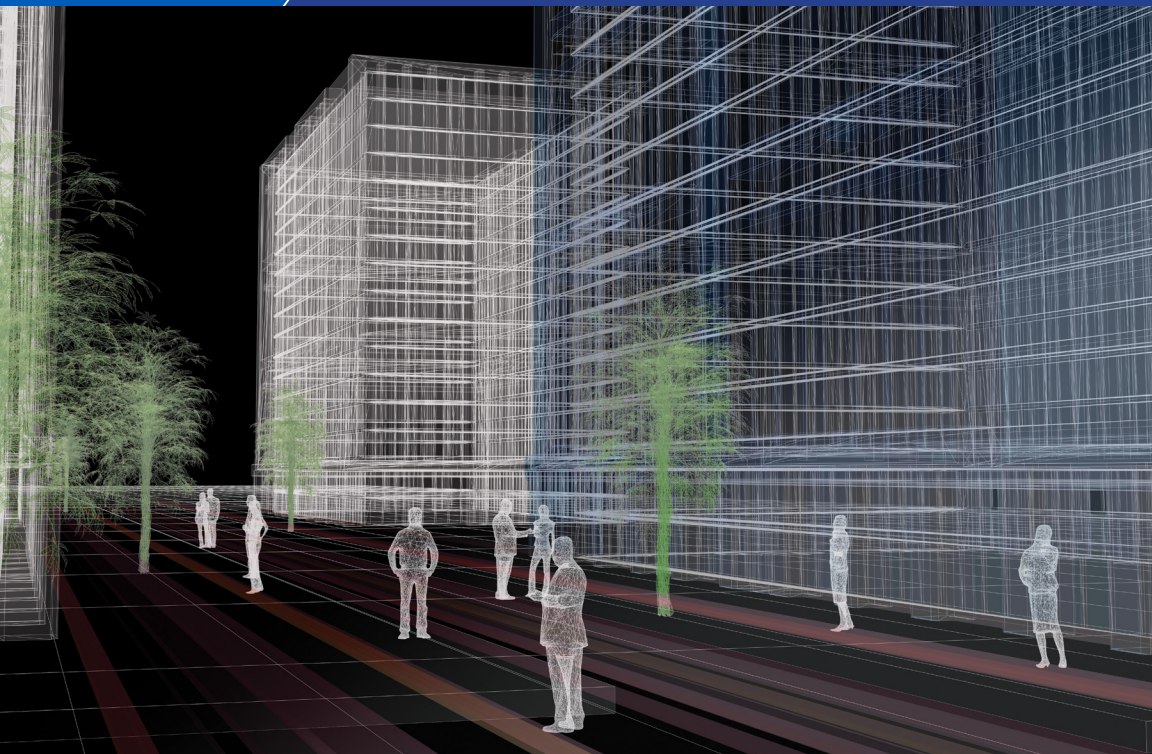
The real value with all this physical security lies in the fact that it helps distinguish good behavior from bad.

The real value with all this physical security lies in the fact that it helps distinguish good behavior from bad. After all, that’s security in a nutshell, isn’t it? Reward good – deny bad. Good behaviors are those actions that people can do and we reward them for it. For example, if you have the right debit card and PIN at the ATM, the machine will give you your money; bad behavior, on the other hand, stolen debit card or wrong PIN and no money is dispensed.

A Place for Big Dog

Now that said, there is a place for the Big Dog, but not in every circumstance or in every occasion. One of those circumstances involves





uniformed armed security forces on-site. Having security forces on-site allows for immediate intervention when the normal good behavior is just slightly off – for example, when an employee forgets their access badge at home. A guard can look them up in the database and allow temporary entry.

This is a good thing, and is the best argument for having a guard force. Their real value comes in their ability to assess and decide the right course of action when things are off.

The reliance on physical security engineering will become paramount as we use inhabited space to mitigate unwanted behaviors and reduce its effects. We cannot lose sight of the human aspect of using new

technologies as we move forward. The use of invasive technologies will need to give way to nonintrusive technologies. We want users of the space to do the right thing because it's the right thing to do, not because "Big Brother" is watching them. This will take time. But there's no better time to start than now.

A Change Is Afoot

As the great migration from the countryside to urban centers becomes an increasing phenomenon, community leaders must meet the challenges that lie ahead. As systems of urbanization become ever-more complex, so will the solutions to resolve the problems they cause. Cities are becoming more and more

complex. The systems they incorporate are being evermore intertwined. There is no such thing anymore as an independent system.

And the collection of data has evolved into a business vertical itself. As connectivity to the Internet of Things (IoT) becomes the norm, so will the need for other types of technologies that are not relying on this connectivity. We saw what happened recently during Hurricane Maria. Loss of the electric grid had catastrophic results, from which people are still recovering. I imagine that in the future, every electronic gadget will have self-sustaining power, but we are a long way from that now. So, in the meantime, we should concentrate on nonelectronic solutions. It's imperative that not only will smart cities be highly functioning and efficient but they must also be – first and foremost – safe.

It will require good infrastructure systems, good inhabited space design, good governance and good community involvement. The right

mix of technology from all sectors and behavioral sciences will be needed. Due to this holistic approach to city planning, companies wishing to compete in this space will need to bring in a variety of specialties to adequately meet the consumer's needs. As an example, inhabited space design cannot be a function of only architects and engineers. It must also include security professionals, transportation experts, government officials, behaviorists and community members, both retailers and residents.

Research is showing us that we can create environments that reduce crime by using a variety of "social behavior engineering mechanisms." I hate to use the words "manipulating behavior," but that's exactly what is happening. All large electronics companies and very large retailers are using your data, which you willingly agreed to provide when you signed a user agreement, so that they can harvest your behavior to their advantage. In the end, they want to get your money.





Good Stewardship

City planners, building designers and others involved in developing mitigation strategies will need to embrace other nonelectronic, nonaggressive technologies. One of those technologies is the use of Crime Prevention through Environmental Design (CPTED) principles in the development of neighborhoods.

The concept of CPTED has been around since the '90s and is an effective approach. Communities that use CPTED principles tend to thrive economically and socially. The social engineering of the built-

Due to the holistic approach of city planning, companies wishing to compete in this space will need to bring in a variety of specialties to adequately meet the consumer's needs.

environment can be taken even further. Research is being done in Eindhoven, The Netherlands, to track a person's movement throughout a pedestrian zone by analyzing which

"smells" a person is subjected to as they move through the space. Why do people park in one parking garage and walk all the way over there to get a sweet or why does a person

stop and have a cigarette on that park bench? In Melbourne, Australia, a recently installed art project tracks a person's movement through a simulated ocean to see its effect. The more movement, the more the

whirlpools in the ocean are affected. This “interactive art” tells us something about social behaviors.

Recently, architect Stefano Boeri was cited by Dezeen Magazine as saying, “Cities should be redesigned to include trees with bulky planters rather than concrete barriers to prevent vehicle attack.” He went on to say, “A big pot of soil has the same resistance as a Jersey (modular concrete barrier), but it can host a tree – a living being that offers shade; absorbs dust, CO₂ and

other subtle pollutants; and provides oxygen and a home for birds.”

He’s right. No one wants to sit at an outdoor café sipping their cappuccino while looking at big concrete blocks

No one wants to sit at an outdoor café sipping their cappuccino while looking at big concrete blocks that make them feel like they’re in a war zone.

that make them feel like they’re in a war zone. Environments that are a mixture of color and natural materials are much more soothing and aesthetically pleasing. They give us that

“puppy dog” feeling – the feeling that you get when you cuddle a puppy. You feel safe and protected.





Creating the “Puppy” Environment for Everyone

It seems crazy to me that in some neighborhoods, we allow crime and others we don't. It's almost as if we're saying, "You can be bad over there, and we don't care. But over here you have to play good." That's just wrong! Every neighborhood needs to be safe. Every kid deserves to grow up in a neighborhood that provides opportunities for growth. But parents can't do it alone, we must help them. We must insist that neighborhoods are designed to prevent or deter crime in all its forms, including radicalization – whether ideological or sociological.

The presence of physical security measures in the form of aggressive electronic solutions must give way to nonelectronic countermeasures that are nonaggressive.

The use of concepts such as CPTED must be applied to all neighborhoods. The presence of physical security measures in the form of aggressive electronic solutions must give way to nonelectronic countermeasures that are nonaggressive. They can go a very long way in creating an aesthetically pleasing built-environment.

Criminologists are looking at a variety of mental health issues that affect behavior. After all, criminal behavior, including terrorism, is a type of unwanted behavior in a peaceful society.

Some of those influences are long term and build up over the years of physical and mental abuse, while others are

short term. In any case, psychology is a main factor in why people do what they do. Shouldn't we use them to our advantage and combine social behavior with the engineered space so that they both work together and in fact, complement each other?

When people feel safe in a space, they tend to use it more. When security is a "tax" or burden, people will either avoid the space or figure out a way to circumvent the security solution. Being cumbersome is a delay mechanism that we should use to assist us in assessing behavior – and

When people feel safe in a space, they tend to use it more. When security is a "tax" or burden, people will either avoid the space or figure out a way to circumvent the security solution.

that is useful on its own. The problem comes from the frenetic pace of today's society. In short, people don't want to be bothered.

The use of colors, a variety of natural building materials, water, lighting and even a meandering sidewalk all add to the "puppy" movement. That's the feeling we should be striving to achieve as we

design security into the environments of the future. ■ **Back to TOC**

Doug Haines (doug@hainessecuritysolutions.com) is owner of Haines Security Solutions (www.hainessecuritysolutions.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:

S18: Spring 2018

F17: Fall 2017

S17: Spring 2017

F16: Fall 2016

S16: Spring 2016

F15: Fall 2015

S15: Spring 2015

F14: Fall 2014

S14: Spring 2014

W13: Winter 2013-14

J13: June 2013

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

Access Control/Identity Management

Modern Face Recognition Systems (S18)

Living the revolution as algorithms based on Deep Neural Networks (DNN) come to market

By Alexander Khanin, Vision Labs

More than Just a Silver Lining (S17)

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

By Denis Hébert, Feenics

Walk this Way, Talk this Way (S17)

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

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

A Matter of Trust (S17)

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

By Stefan Widing, HID Global

By the Power of Ethernet (S17)

PoE gives smaller facilities more access control options

By Kerby Lecka, Security Door Controls

An Eye for Fraud (S17)

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

By Jeff Kohler, Princeton Identity

Raising the Standards (F16)

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

By Scott Sieracki, Viscount Systems

In a Hand or a Face (F16)

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

By Amy McKeown, 3M

From Legacy Systems to Advanced Access Control (F15)

New solutions can offer extensive benefits to municipalities

By Robert Laughlin, Galaxy Control Systems

Unlocking the Door (F15)

Next-generation access control systems can offer new insights and greater security

By Scott Sieracki, Viscount Systems

Striking the Balance Between Security and Safety (F15)

Classroom door locks are invaluable, but they must allow quick egress

By Mark Berger, Securitech

Get Up and Bar the Door (F14)

Access management and door hardware play a critical role in school security

By April Dalton-Noblitt, Allegion

Who Is Entering Your Facility? (F14)

Verifying identities is challenging; partnerships can help

By Daniel Krantz, Real-Time Technology Group

Say Hello to Social Spaces (S14)

Social Applications will transform the security experience

By Steve Van Till, Brivo Systems

Fingerprint Biometrics for Secure Access Control (S14)

Moving beyond passwords and tokens can enhance security while decreasing costs

By Consuelo Bangs, MorphoTrak

Integrating Card Access with Interlocking Door Controls (S14)

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

By Bryan Sanderford, Dortronics Systems

Frictionless Access Control: A Look over the Horizon (S14)

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

By Henry Hoyne, Northland Controls

More Security, From Bottom to Top (S14)

Buildings are increasing entrance controls on the main floor and upstairs

By Tracie Thomas, Boon Edam

Hardware Security, Today and Tomorrow (W13)

Advances in door technology are enhancing both safety and convenience

By Will VandeWiel, DORMA Americas

Secure Authentication without the Cost and Complexity (W13)

New technologies are narrowing the gap between passwords and stronger authentication solutions

By Ken Kotowich, It's Me! Security

From Access Control to Building Control to Total Control (W13)

How innovation drives the need to update product standards – and ways of thinking

By Michael Kremer, Intertek

The Technology Behind TWIC (J13)

Smart cards are finally getting smart readers, but how will it all work, and how will it connect with existing PACS?

By Walter Hamilton, Identification Technology Partners

Big Data**Early Alerts Spur Action (S18)**

Why corporate security teams rely on social media for real-time information

By Dillon Twombly, Dataminr

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

Making Connections (F17)

The Internet of Things and the cloud bring new functionalities to the security industry – and new risks

By Mitchell Kane, Vanderbilt Industries

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**Smart Power (S18)**

The paradigm has shifted to intelligent networking solutions

By John Olliver, LifeSafety Power Inc.

Diagnosing Security Challenges (F17)

Developing the secure hospital of the future starts with planning and collaboration today

By Marianne Iannotta, Kratos Public Safety & Security Solutions

Out of Many, One (S17)

Integrating components of a security system can vastly improve effectiveness

By Brian Wiser, Bosch Security Systems

Commanding the Enterprise (S15)

New software platforms enable security leaders to ensure awareness, manage risk

By Rob Hile, SureView Systems

Tying It All Together (S15)

Integrating video surveillance, access control, building management and other systems can enhance security and reduce costs

By Mitchell Kane, Vanderbilt Industries

Safe on the Water (S15)

Integrated solutions secure the nation's largest independently owned commuter ferry operation

By Kostas Mellos, Interlogix

Broken Promises: The Current State of PSIM (F14)

Physical security information management solutions have so far fallen short of expectations, but next-generation systems could change that

By David Daxenbichler, Network Harbor

Enhancing Continuity Planning through Improved Security (F14)

Web-based systems can tie everything together

By Kim Rahfaldt, AMAG Technology

Technology-Enabled Collaboration Builds Safe Cities (S14)

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

By Itai Elata, Verint Systems

Solving a Big Problem for Small Businesses (W13)

New security technologies offer integrated solutions for small and medium enterprises

By Scott McNulty, Kantech

Intrusion Detection/Alarms**24-Hour Perimeter Protection (S18)**

Relentless defense for critical infrastructure

By John Distelzweig, FLIR Systems Inc.

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**Navigating Technological Change (S18)**

The way to success is ensuring new technologies impact your customers in a positive way

By Todd Graves, Allegion

Listen Up (S18)

How audio monitoring raises the surveillance bar

By James Marcella, Axis Communications Inc.

The Puppy Movement (S18)

A new vision for security

By Doug Haines, Haines Security Solutions

Securing Healthcare Facilities (S18)

Maintaining 24/7 parking lot security

By Alex Doorduyn, Siklu Communication

Dialing Up Security (F17)

Smartphones can be an essential component of a mass notification system

By Jana Rankin, VuTeur

Getting on the Path (F17)

Shortest Path Bridging can enhance network performance and efficiency

By Darren Giacomini, BCDVideo

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

Robotics/Artificial Intelligence**The Rise of the Machines (F17)**

Robots can terminate tedious tasks for security personnel

By Alice DiSanto, Sharp Robotics Business Development

The Not So Friendly Skies (F17)

Drones represent a rapidly growing and evolving threat

By Nathan Ruff, Coalition of UAS Professionals

Combining Man and Machine (F17)

Robots can help human guards to be more effective

By Steve Reinharz, Robotic Assistance Devices

Up in the Air (S17)

Drones powered by artificial intelligence could transform security

By Cary Savas, Nightingale Security

The Real Benefits of Artificial Intelligence (S17)

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

By David Monk, Umbo CV

Threat from Above (F16)

How can potentially dangerous drones be detected and defeated?

By Logan Harris, SpotterRF

Video Surveillance**Know a Lot About History, Know a Lot About Security (F17)**

Data from cameras and other systems can increase understanding of events and contribute to a holistic approach to school security

By Jumbi Edulbehram, Oncam, and Steve Birkmeier, Artec

VMS: The Next Generation (S17)

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

By Shawn Mather, Qognify

Law & Order & Video (S17)

Police and prosecutors need enhanced case management systems

By Pota Kanavaros, Genetec

A Needle in a Video Haystack (F16)

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

By Steve Birkmeier, Arteco

Video Storage Wars (F16)

Hyper-convergence technology can simplify surveillance storage and enhance security

By Brandon Reich, Pivot3

Big Video Data (F15)

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

By Jeff Karnes, 3VR

The Public Safety Data Lake (F15)

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

By Ken Mills, EMC

The Sun Shines on Surveillance (S15)

Solar power enables wireless video solutions in remote locations

By Dave Tynan, MicroPower Technologies

Surveillance in the 21st Century (S15)

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

By Jumbi Edulbehram, Oncam Grandeye

10.7 Billion Security Challenges (S15)

As transit ridership increases, so must security

By Steve Cruz, Panasonic

The Future of Video Surveillance (S15)

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

By Alex Asnovich, Hikvision USA

Making Campuses Safer with Innovative IP Technologies (S14)

Networked systems mean more information, more collaboration and more security

By Kim Loy, DVTEL

Harnessing the Increasing Power of Video (S14)

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

Megapixel Cameras Go Mainstream (W13)

Functionality, versatility, clarity make megapixel video the future of surveillance

By Scott Schafer, Arecont Vision

Seeing the Big Picture: 360-Degree Camera Technology (W13)

High-resolution panoramic video overcomes the limits of PTZ cameras

By Steve Malia, North American Video

Achieving IP Video Management System Scalability through Aggregation (W13)

Video isn't just about security anymore

By Jonathan Lewit, Pelco by Schneider Electric

What's New on the Video Surveillance Front? (J13)

A keener eye, a longer memory and a sharper IQ

By Fredrik Nilsson, Axis Communications

Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security (J13)

As technology advances and prices fall, thermal cameras have become a cost-effective way to secure the perimeter

By John Romanowich, SightLogix

Video Analytics in the Modern Security Industry (J13)

Analytics can make cameras smarter, but how smart can they get?

By Brian Karas, VideolQ

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 by emailing SIA at info@securityindustry.org.



securityindustry.org/techinsights

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

