SIA Insights TECHNOLOGY

Volume 8, Issue 1
Spring 2020

Welcome

Dear Reader,

This edition of *SIA Technology Insights*, with 11 articles across 92 pages, is the largest that has been printed during the publication's seven years of existence. It is probably safe to say that it also contains the most technologically advanced content of the past seven years. That is in no way a reflection on the quality of the roughly 100 previous articles; it is simply an indication of just how much security technology is advancing from year to year. Sometimes, it seems, from month to month.

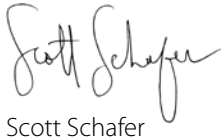
Many of the articles herein address various aspects of the same major issues that are redefining the power and role of security devices – the Internet of Things and connectivity, smart devices made smarter through integration, and the power of data, chief among them.

The articles, which, as always, were written by SIA members, do not get bogged down in dry technical details. Rather, they convey a sense of excitement and wonder at the innovations that are enhancing our security and our quality of life. It is our hope that, in reading these articles, in learning a bit more about where security technology is and where it is going, you will share that excitement and wonder.

If you have any comments, questions or article proposals, please contact our editor, Ron Hawkins, at rhawkins@securityindustry.org. And if you are currently reading a hard copy of *SIA Technology Insights*, remember that you can view and share all articles – past and present – by visiting www.securityindustry.org/techinsights.

Thank you for reading.

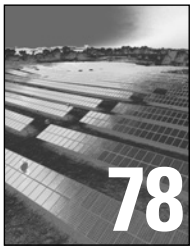
Sincerely,



Scott Schafer
Chairman, Board of Directors
Security Industry Association

Don Erickson
CEO
Security Industry Association

Table of Contents



Search the SIA Membership Directory

The advances in AI provide an added layer to video analytics technology, helping systems to not only immediately identify objects moving within a scene, but also characterize when the behavior of an object is anomalous.

Always Watching, Always Learning

AI-powered analytics and algorithms are making cameras smarter

By Alex Asnovich
Motorola Solutions

Today's leading security solutions are carving a new path for the industry. Innovative technology is optimizing the more traditional aspects of security, like video and access control, giving businesses more autonomy when it comes to protecting their assets, property and – most importantly – people.

From robust storage features and centralized offsite management to dynamic video analytics, modern security technologies present a number of opportunities for providers and operators alike. As digital systems outgrow their analog counterparts, security professionals are no longer restricted to onsite touchpoints, manual video reviews and minimal data storage capabilities.

Recently, the Security Industry Association published its annual

selection of top megatrends in physical security technology. While cybersecurity again ranked first, artificial intelligence (AI) moved into second place, up from fifth a year earlier. Meanwhile, facial recognition, which had never been on the list before, burst onto the scene in third

place. Both of these technologies are optimizing video analytics as a core security function. Match that with the development of centralized, unified systems, and organizations can now rethink their security infrastructure to make it more agile and effective.

Technologies That Are Reshaping Security

Like most other industries, the security space is capitalizing on the opportunities that come with new technologies. In order to remain competitive in a market that is constantly evolving, security providers are investing in several transformative technologies:

- *Deep learning AI* – The ability to train algorithms to learn and make inferences or associations without human intervention. This is accomplished with convolutional neural networks that build programs that mimic the biology of human brains and their billions of connections between neurons. The advances in AI provide an added layer to video analytics technology, helping systems to not only immediately identify objects moving within a scene, but also characterize when the behavior of an object is anomalous.
- *Business intelligence* – The ability of computer programs to identify meaningful patterns and insights in large amounts of information. This enables operators to track trends and make informed predictions, such as when spikes in activity or critical events may take place. Outside of security-related use cases, this can inform retail businesses about the success of merchandising or promotional programs.
- *Edge analytics* – A solution that allows devices to connect to the Internet of Things (IoT), this tool is used to examine and refine data as soon as it is collected at

the "edge" of the network. That way, only relevant information is sent to the centralized server or data store.

As the security industry responds to these shifts in the digital landscape, it comes as no surprise that there have been breakthroughs in access control software, as well. The most advanced access control solutions on the market can be integrated seamlessly with an organization's video platforms, alarm panels and wireless locks so that operators can manage multiple security touchpoints with a single browser-based program. In practice, this functionality allows them, for example, to be alerted to monitor the video feed of an entrance when an individual swipes an access card and enters a facility or controlled area.

Video analytics are among the most valuable applications of AI in modern security systems.

Video Analytics Are Breaking the Mold

Video analytics are among the most valuable applications of AI in modern security systems. Now there are video management system (VMS) solutions on the market that allow security personnel to monitor feeds on a single, simple interface from any location.

The most advanced VMS solutions include built-in analytics capabilities that leverage deep learning AI, enabling security operators to easily browse through recordings and quickly locate specific individuals and events. Even if the only information a practitioner has when looking for a person of interest is a general physical description, some technologies are so sophisticated that, given a specific time period and simple descriptors such as vehicle type and color, clothing color, gender or age, they are able to find, track and verify the subject in video.

In many cases, video management solutions provide users with complete control over video playback so that security incidents can be followed both retroactively and in real time. Meanwhile, AI can find subtle changes in scenery to automatically flag moving objects or atypical activity thanks to self-learning analytics. These capabilities are presenting themselves in a number of use cases:

- Facial recognition technology can be a powerful tool, but there are privacy concerns to take into account. In an effort to help mitigate these concerns as they develop comprehensive AI-enabled solutions, security providers should make data stewardship integral to the capabilities. This means building in compliance controls such as user authentication and log audits and setting data retention periods.
- License plate recognition technology is a valuable tool for identifying vehicles of interest,

homing in on small details to differentiate individual cars.

- Technologies that use AI to recognize and flag unusual activities help provide greater situational awareness. This is vital, since organizations generally capture more video than they will ever have a chance to view. By focusing on abnormal movements, for instance, security teams can get through hours of footage in minutes.
- Some intelligent systems make it extremely easy for security teams to see precisely where action is required by using different colors to highlight and differentiate between motion, analytic events and alarms as soon as an anomaly is detected.

In some programs, it is possible to fine-tune analytics algorithms so that they flag exactly the types of events that a user wants to protect against. These are called teach-by-example capabilities, and they allow users to provide feedback, enabling the AI to adjust its self-learning systems accordingly.

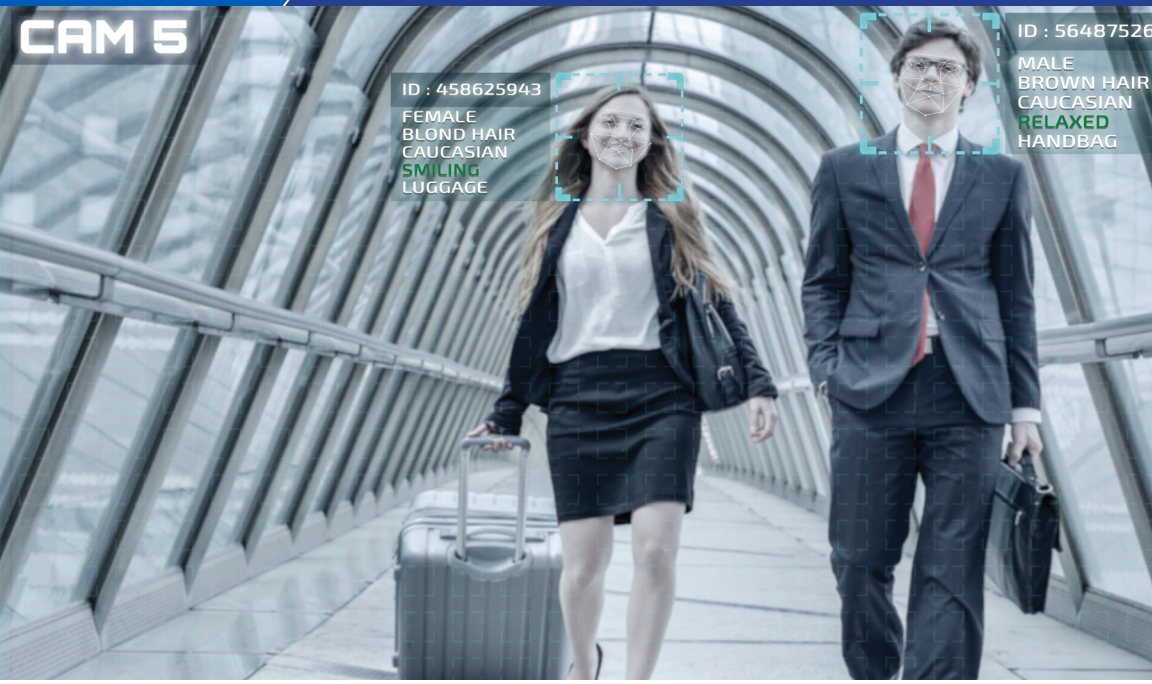
Then there are features that do not need any manual calibration. They are designed to instantly map and memorize their surroundings. These kinds of features are often found on systems that leverage edge analytics – meaning the cameras extract actionable intelligence from the data as soon as they collect it, so only meaningful metadata is transmitted for further analysis. This helps increase the speed of detection, decrease response time, and enable a much simpler deployment.

Centralized Oversight for Unified Systems

Video analytics can be a value-add for modern security teams, but the many new options could be overwhelming without consolidation in a single source. A software solution that centralizes access for security operators and clean, simple, browser-based systems that operate on pre-configured servers can minimize installation time and let security personnel do their jobs remotely, monitoring recorded footage on their devices in real time from anywhere.

A software solution that centralizes access for security operators and clean, simple, browser-based systems that operate on pre-configured servers can minimize installation time and let security personnel do their jobs remotely.

Creating a unified hub from which security personnel can manage their various tools and solutions goes beyond video analytics. Today's sophisticated access



control software can be integrated with on-premises hardware such as camera networks, alarm systems, intercoms, point-of-sale systems, and wireless locks, putting a holistic, user-friendly dashboard at the fingertips of security professionals.

The best solutions of tomorrow will be built on the best solutions of today.

How Leading Security Companies Stay Ahead

One of the most daunting challenges security companies face is the simple fact that technological innovation moves very fast, and digital disruption is constant. Nevertheless, the best solutions of tomorrow will be built on the best solutions of today. The organizations to work with are the ones that stay current, that are willing and eager to be early adopters in the present so they can be better prepared for the future. Their prudence benefits their partners.

Organizations that feature analytics technology across their entire product line – on the edge, in the software, on the servers – are best positioned to adapt to technological advances. The future may be full of uncertainties, but that is all the more reason to understand analytics, AI and machine learning right now. ■

Back to TOC

Alex Asnovich (alex.asnovich@motorolasolutions.com) is head of global marketing, video security, for Motorola Solutions (www.motorolasolutions.com).

Search the SIA Membership Directory

Access control, intrusion detection, video surveillance, facilities management, and communications systems are connected, helping to reduce complexity while increasing control.

You Say You Want an Evolution

Built-in intelligence enables security devices to expand beyond their usual functions

By Sean Murphy
Bosch Security and Safety Systems

Safeguarding people and property remains the top priority for the security sector, but the industry is evolving into more than that. The Internet of Things (IoT) and increasing connectivity are expanding the role of security devices, making them an integral part of the vast, connected digital infrastructure.

This is possible through the expansion in intelligent security devices – like IP cameras with built-in video analytics – and systems that seamlessly integrate to enhance security, automate processes, and increase efficiency in monitoring and control. Software and services are also beginning to play an increasingly important role.

Connected Systems for Customized Solutions

Security systems are no longer isolated. Access control, intrusion detection, video surveillance, facilities

management, and communications systems are connected, helping to reduce complexity while increasing control. By receiving alarms from various devices and using those alarms to trigger actions, connected systems focus the attention of security and facility personnel on the events that matter most.

For example, at the perimeter of a facility, access credentials with the correct authorization will open a gate or door. However, when access is denied, video from a nearby camera can display at the security operator's workstation, while a text message with a video snapshot alerts the facility manager to a condition that may require action as a potential attempted breach of the perimeter. By integrating access control and other systems like intrusion detection within a video management system, users gain centralized control of devices and doors across the enterprise. This increases efficiency for the operator and simplifies management of the system.

The layering, or integration, of multiple systems allows for multi-sensor verification of events, dramatically reducing the chance of a false alarm or of an event being missed. This efficiency gain reduces employee workload.

Inside the building, when a camera with on-board video analytics detects an object blocking an emergency exit door, it can trigger the public address system to play an automated message over a nearby loudspeaker with instructions to move the object. In addition, the system can help users enforce no-parking zones by triggering a message when a vehicle parks or loiters in a fire lane. These solutions enhance safety while also reducing the risk of fines when violations occur.

In many larger office buildings, the elevator lobby is the main artery

to move people. It is possible to limit access to floors based on individual need via access control and, using analytics like crowd detection, redirect traffic during peak congestion. Making the process faster while maintaining safety and security can have a major impact on the productivity of a workforce and on the perception of a building's accessibility.

Building staff can gain the ability to handle events, like a mass evacuation, more dynamically and efficiently than before. Elevators are typically disabled during these types of events, but that leaves occupants searching for the quickest way out along paths they rarely use. IP cameras, motion detectors and access control elements can provide the system with a real-time understanding of where people are and how best to guide movement patterns. With the addition of a building-level communications system, automated or manual announcements, individualized and localized, can quickly inform people of their best options.

For sensitive areas of a facility, such as a server room, combining video security with access control and intrusion detection limits access. Together, these technologies provide enhanced security and can even protect the individual hardware racks inside the room. For example, each server rack can have its own access reader, keypad and camera. This can keep unauthorized individuals from gaining access to the equipment and restrict authorized people to scheduled days and times, limiting after-hours access to pre-determined times for maintenance or upgrades. Using a keypad and a reader on the racks enables the use of dual authentication, so the individual must

> With built-in intelligence, security devices are moving beyond their traditional roles.

present something he or she has – a credential – along with something he or she knows – a PIN – for greater security. The IP camera ensures that attempts to open the racks by unauthorized individuals will trigger a text or email alert, complete with a video snapshot, to the facility manager. Just as important, there is now an auditable history of access events.

These are just some examples of the possibilities with connected systems. This type of integration adds flexibility for integrators, making it possible for them to customize solutions that fully address a user's security pain points and provide added benefits for an organization.

Extending Beyond Security with Intelligent Devices

With built-in intelligence, security devices are also moving beyond their traditional roles. For example, the video security camera is no longer a passive system that simply records events, with about 90 percent of recordings never being viewed. With recent advances in analytics, security practitioners have a never-tiring assistant that can help them to manage, and extract more value from, their vast quantities of video data.

In this increasingly connected world, the smart video security camera becomes a versatile sensor that enables other "things" to extract and interpret the recordings to bring security, life safety and business intelligence to another level, enabling nearly 100 percent utilization of the video. The data is fed to solutions that collect information from multiple devices, aggregating and interpreting it to provide valuable insights. These solutions increase efficiency, reduce costs and create more business opportunities with new revenue streams.

Intelligent cameras, for example, can help large organizations or city planners monitor parking space utilization. In lots, cameras can count the number of open parking spaces, the availability of specialized spots – such as those for handicapped drivers or electric vehicles – or track ingress and egress, then relay this data to parking management systems without the need for a series of ground sensors. Sharing this information, along with alternative parking locations, on a dynamic message sign can help people to find parking more quickly, improve efficiency and reduce emissions.

In addition, cities and parking lot managers can take advantage of machine learning to track how long a vehicle remains in a time-limited space, which can boost revenue streams from parking violations. This same concept applies at the airport curbside for passenger drop-off and pick-up, where parking time is restricted. Video analytics with machine learning can detect and alert law enforcement to parked vehicles that exceed the time limit. Machine learning also enables video analytics to function in application-specific ways, as it can identify objects and situations that have been defined by the user.

> Using video analytics to integrate with other systems requires high-quality images at all times to ensure reliability and accuracy.

On roadways, intelligent cameras can improve safety by alerting to risks with automatic incident detection and identification of slow or stopped vehicles, queues of vehicles at exit ramps, vehicles traveling the wrong way, objects in the road, and other traffic events. Video sensors can also

classify objects as cars, trucks, bicycles or pedestrians, and can detect speed and trajectory. With this real-time information, city traffic planning directors and engineers can analyze flow patterns on networks of roadways to develop safer and more efficient intersections.

Machine learning can also enable intelligent cameras to gather data in heavily controlled environments, such as airports, where awareness of traffic flow and plane status is critical. Data collected could include information on how long an airplane parks at a gate, the time it takes to load passengers' luggage, or how long it takes to refuel. This information is helpful for reducing turnaround times, improving efficiency and reducing costs.

In retail stores, video security cameras can capture anonymous shopper data that provides merchandisers and operations managers with actionable insights. With cloud-based processing, the data shows where customers walk, dwell and engage with product placements, providing information that can be used to maximize customer engagement and increase sales. By analyzing the data, operations managers can enhance service by adjusting staffing to accommodate peak days and times, thereby increasing customer loyalty. This can all be done without video streams ever leaving the retailer's premises, thus maintaining shoppers' privacy.

In a large building, meanwhile, sensors can provide data on occupancy to help facilities managers

identify patterns in the arrival and departure times of employees on each floor in order to better manage costs associated with HVAC and lighting.

Considering the Essentials

Using video analytics to integrate with other systems requires high-quality images at all times to ensure reliability and accuracy. If image quality is lacking, the accuracy of the data is at risk, as is any video evidence.

Video analytics technology must also be robust enough to differentiate between genuine events and false triggers such as snow, trees, rain, hail and water reflections that can make video data difficult to interpret. It should also be trainable. The camera should be able to retain information on user-defined objects and situations and refer to it when processing scenes.

With the right platform, devices like IP cameras have the potential to be as flexible as a smartphone, creating unlimited new uses within their lifetimes. Capturing data and putting it in a usable structure is a foundational piece. Just as important is funneling that raw data into a platform that transforms it into intelligence. This is key to enabling both automated and human decisions. It is a quickly evolving area with exciting advances in artificial intelligence powering new abilities every day.

With the right platform, devices like IP cameras have the potential to be as flexible as a smartphone, creating unlimited new uses within their lifetimes.

Equally important is a high level of data security. Users need to know that the data they are capturing is protected when in transit and when stored. A system approach is the key to achieving the highest standards in end-to-end data security. For video systems, this means assigning every component in the network an authentication key, securing data from hackers by encrypting it at the hardware level using a cryptographic key that is safely stored in a built-in trusted platform module, managing user access rights, and supporting the setup of a public key infrastructure.

Fueling Innovation

The continued proliferation of connected devices will change customer requirements and preferences. Extending the role of security devices beyond their standard usage enables solutions designed to help users address the challenges they face in their businesses and organizations. This approach will help to shape the future of security – one in which the security department can make the transition from a pure cost center to a profit center – and continue to fuel innovation. ■ **Back to TOC**

Sean Murphy (sean.murphy3@us.bosch.com) is director of vertical markets development for Bosch Security and Safety Systems (www.boschsecurity.com).

Search the SIA Membership Directory

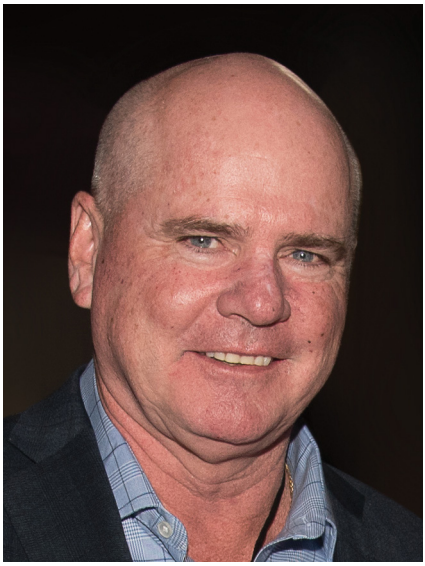
The migration of intelligence to the edge has dramatically increased situational awareness and created an ecosystem of predictive analytics that not only makes for more robust security operations but also a healthier bottom line.

Gaining an Edge

Embedded analytics are enabling proactive security and business solutions

By William Brennan
Panasonic i-PRO Sensing Solutions

During the past 10 to 15 years, a savvier video surveillance end user has emerged demanding solutions that feature high-performance cameras, versatile installation, flexibility to expand, cost efficiency in storage, and advanced analytics to help realize a system's full potential. Increased public and private security concerns have driven a technology shift and altered business models in the video surveillance marketplace, while end-user demands have forced vendors to conform to their needs.



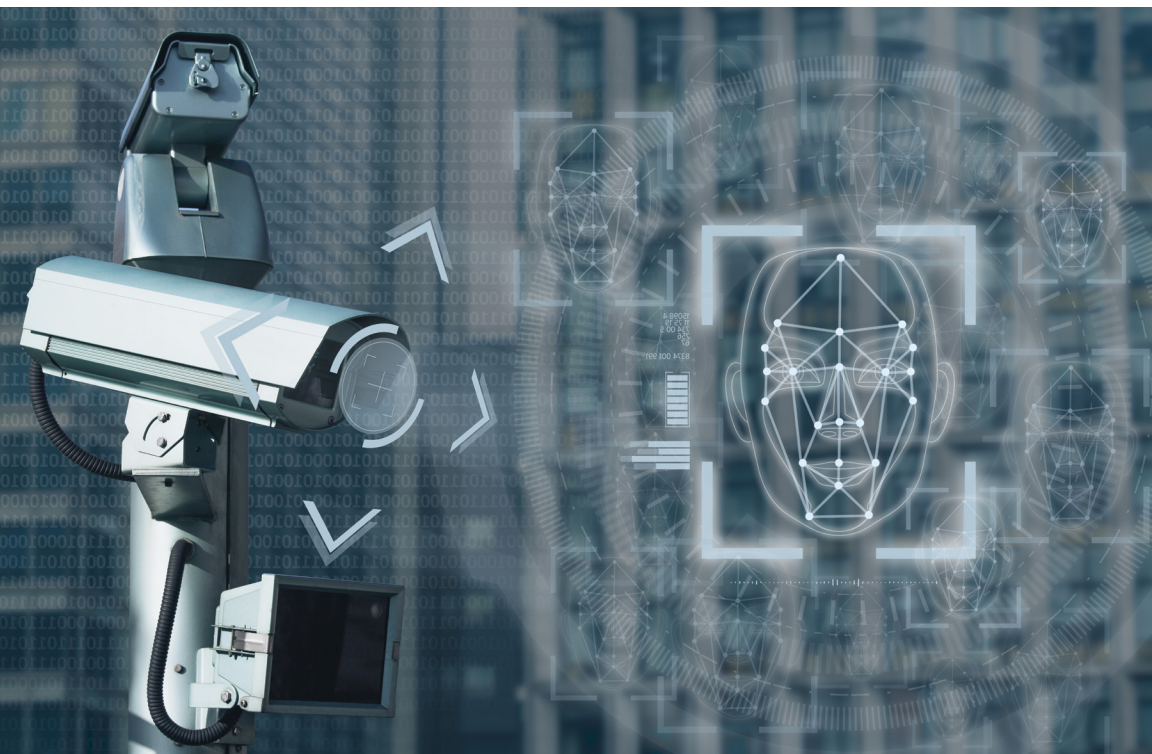
According to IHS Research, the surveillance market's migration from analog to IP video systems continued to accelerate in 2018, when 70 percent of all security cameras shipped were network cameras. At the same time, global shipments of HD CCTV cameras, also known as analog HD cameras, fell in 2018. And that trend, which began in 2014 when IP cameras first overtook analog in total sales, is expected to increase.

The rapid growth of IP video surveillance has been driven by end users' needs to expand the capabilities

of traditional CCTV beyond simple monitoring of facilities and assets. While the market demand for smaller and less robust analog systems remains, an increased appetite for next-generation solutions powered by artificial intelligence (AI) and machine learning, along with advanced analytics and cloud computing, has broadened the capabilities of video surveillance beyond just security. Attention to business metrics and an expanded systems team that may include facilities and IT has added new uses like posture and demeanor detection, traffic monitoring and heat mapping, people counting, and facial recognition.

The evolution of commodity hardware into a convergence of advanced software and interoperable hardware has allowed systems designers and systems integrators to meet the expectations of end users. This convergence has moved systems solutions from being reactive to proactive, permitting users a seamless integration of technology no matter what level of investment. For example, a relatively small system of 50 cameras or fewer could provide basic video surveillance solutions at a cost-effective price point that would include video management software (VMS) licensing and servers for 30 days of retention as a technology bundle.

A similar scenario unfolds for users who move into the mid-level systems of 50 to 150 cameras. Now, however, the system may feature more advanced solution-driven devices such as multi-sensor cameras or pan-tilt-zoom (PTZ) cameras that possess higher retention times. Mid-level system users may even request fail-over options for their servers as an upgrade. These servers match the exact specifications that run the main system, but in the event of a power surge or loss of power to



the main server, functionality would automatically jump to the fail-over server in a seamless transition.

Advanced Video Technology Raises the Bar

As the digital revolution alters the landscape of video surveillance and security rises to a board-level priority for private and public organizations, security leaders have an opportunity to enhance risk management. Both traditional on-site surveillance and integrated remote security solutions are benefitting from the proliferation of AI-driven proactive solutions that push intelligence to the edge with embedded analytics. This has been a game-changer not only for security but for business as well, altering how video surveillance systems are designed, configured and operated.

As the digital revolution alters the landscape of video surveillance and security rises to a board-level priority for private and public organizations, security leaders have an opportunity to enhance risk management.

According to a 2018 "Future of Physical Security" survey conducted by Microsoft and Accenture, security/risk executives identified "reactive threat management" and "intuition-led decision-making based on subjectivity" as the two leading challenges facing physical security operations today. These challenges – reactive operations and sub-optimal decision-making – make it difficult to be proactive. Operating in this manner puts an organization's people, brand and reputation at risk.

The survey said that, in an ideal environment, security end users would possess the tools to proactively assess

and manage their security risk. However, in many cases, the complexity of incoming threats and the sheer volume of information overwhelms security personnel who still rely on manual processes to translate data, which can then inhibit their ability to focus on proactive threat management. The survey added that it is nearly impossible to monitor all security video content without advanced analytics, which is "why it is commonly estimated among security professionals that more than 90 percent of security video footage goes unseen" and video is typically watched only during reactive investigations.

To that end, more than 80 percent of surveyed security participants identified big data and analytics as a top-three investment for the next three to five years. They also said their teams will concentrate on technology investments in cloud computing and storage (58 percent) and advanced identification (56 percent), concluding that a digital video solution "empowers these operators with systems that contextualize data to identify threats before they occur, mitigate risks and better ensure life safety."

It seems that 2019 became the year that AI technology in video surveillance established itself as mainstream. In a market report released last year by Research and Markets, experts stated that significant improvements are being made in AI video analytics software, and over the next 10 years, it will become a standard feature in most surveillance solutions. The research added that "there is a critical need to make full use of the massive amounts of data being generated by video surveillance cameras and AI-based solutions are the only practical answer. Modern chip architecture with AI software can comb through vast volumes of data and boost security and safety. Granted, there is a lot of development in this field that we are yet to see, but the path towards AI seems quite clear."

Make no mistake as to what is driving this rapid technology

advancement: intelligent hardware and software that allows users to put all of this data to work in a proactive manner. The migration of intelligence to the edge has dramatically increased situational awareness and created an ecosystem of predictive analytics that not only makes for more robust security operations but also a healthier bottom line.

It takes 150 to 200 milliseconds for data to travel from endpoints to the cloud and just 10 milliseconds from endpoints to the edge. This speed allows for more effective detection and response.

Meeting End User Expectations

End user expectations will continue to push video surveillance to the edge – literally. Video surveillance has traditionally been a tool of the physical security community, who could monitor or recall video footage to identify suspicious activity. However, legacy and closed systems were limited and could only assimilate and translate so much data. The advent of AI technology provides the security user a machine partner that can learn, identify and interpret suspicious activity.

As James McHale, the managing director and founder of Memoori Research, put it, "AI is a tool of the IT community and offers a far more powerful video surveillance solution than traditional approaches. Meaning the security department needs to develop IT skills, utilize the skills of the IT department, or ignore a technology that is changing the physical security landscape."

Oddly enough, it has been product innovation on the consumer technology side that has helped spur a revolution in the security industry as the integration of advanced analytics and edge computing in everything from smartphones to smart refrigerators shapes the burgeoning Internet of Things (IoT). Video data processed at the edge – that is, in the camera itself – lowers bandwidth consumption and reduces communication latency, allowing end users to create more proactive security strategies and take appropriate action in critical situations.

End users appreciate the lead time provided by the rapid transmission of data offered by edge computing, especially considering that it takes 150 to 200 milliseconds for data to travel from endpoints to the cloud and just 10 milliseconds from endpoints to the edge. This speed allows for more effective detection and response.

Lower bandwidth consumption is another major benefit of edge computing as all the processing is done at the source of the data. While bandwidth issues have improved for many organizations, applying advanced analytics on video that runs through a central server and is,

thus, heavily compressed, reduces the accuracy of the analytics. Moving the processing of the original data to the edge is an obvious advantage when it comes to response time and image resolution.

Camera latency is a major concern for end users, especially in critical infrastructure and gaming environments. Edge computing reduces latency since video does not have to be sent to the backend for processing and analysis. This has significant advantages in applications like facial recognition, where detection of significant situations at the edge triggers an alarm response from the device itself, skipping the round-trip transmission to the backend servers. There are also aspects of cloud computing, such as "fogging," that can extend cloud computing to the edge of a network while also placing data, compute, storage and applications in the most logical and efficient location between the cloud and the origin of the data itself.

What Drives Technology?

Technology continues to develop and come to market at an incredible pace driven by new intelligent hardware and software with AI that deliver improved outcomes. For example, new IP camera systems with embedded analytics and sensors are capable of detecting far more than a conventional camera (or human eye) can see. These intelligent edge devices dramatically increase situational awareness for conventional security applications through predictive analysis capabilities, while providing reams of data for business intelligence applications. Meanwhile, advanced algorithms and analytics like facial recognition and various forms of object detection further capitalize on the powerful imaging and detection capabilities of edge devices.

Physical security is only as good as the intelligence the technology offers. End user demands, now more than ever, are helping to chart the course for the technology advances of the

future. For years, the security industry strived to achieve networkability, and now that it has arrived, it is dramatically changing the dynamics of the industry. In this age of IoT, users are looking for interoperability and open architecture systems.

Users want to converge systems and integrate everything, which has inspired many companies to think outside the box and develop more easily integrated and operated system solutions. Where cameras were once deployed simply to monitor activity and document events, they are now being used to detect abnormalities, count people, monitor motion direction and speed, and so on. Users want proactive performance that captures and analyzes more data for applications that can help them improve merchandising on retail floors, increase manufacturing throughput, detect traffic violations, get alerted to unauthorized site visitors and more. As users demand more performance, versatility and intelligence from their systems, the opportunity to fulfill their requests creates new growth opportunities for solutions providers. ■ **Back to TOC**

Where cameras were once deployed simply to monitor activity and document events, they are now being used to detect abnormalities, count people, monitor motion direction and speed, and so on.

William Brennan (william.brennan@us.panasonic.com) is vice president, Security Division, for Panasonic i-PRO Sensing Solutions (www.ipro.panasonic.com).

As with any other type of data analysis, video analytics depend on accurate input to provide reliable results and reduce false positives and false negatives as much as possible.

Quality in, Accuracy out

To be effective, video analytics must be applied to high-quality images

By Sophie Gigliotti
Immervision

For the past 15 years, the accuracy and range of video analytics have tremendously improved, from basic people counting to facial recognition. Indeed, what was yesterday's imprecise line crossing has given way to artificial intelligence (AI) and deep learning-based people and object recognition.

Several factors directly affect the precision and efficiency of these applications, including processing power, algorithms, and – one that is frequently undervalued – image quality. It is important to remember that, as with any other type of data analysis, video analytics depend on accurate input to provide reliable results and reduce false positives and false negatives as much as possible. The most powerful processor and the most sophisticated algorithms will still produce erroneous findings if the image quality is poor.

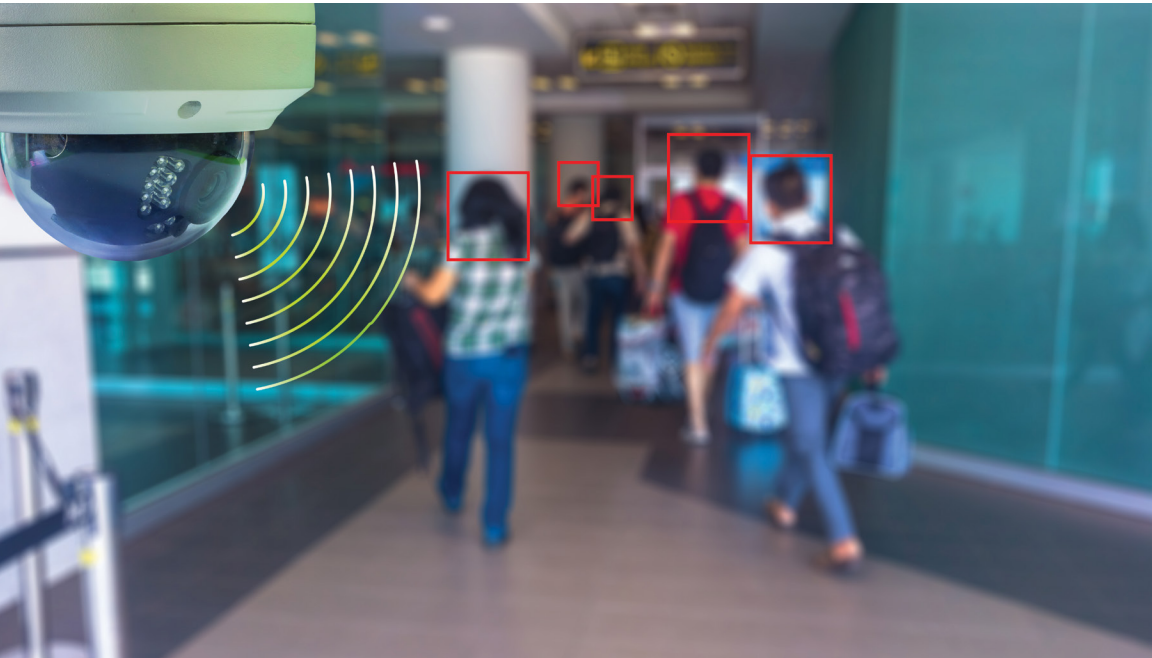
Video Analytics in Brief

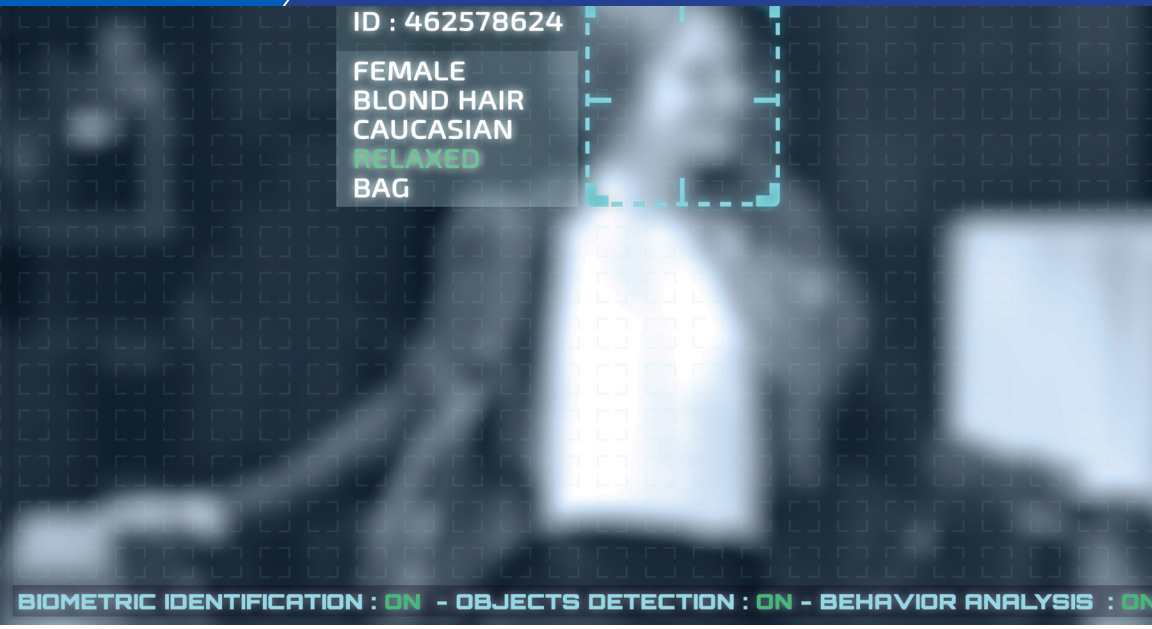
Depending on the desired usage and the security surveillance system configuration, analytics can be done at the video management system (VMS)

level, the network video recorder (NVR) level, or the camera level. While some post-processing analysis is performed, most of today's analytics are done in real time, whether centrally or at the edge, delivering information to users as events occur. Furthermore, with the power of processors rising and their costs decreasing, more complex analytics, including AI and deep learning, can now be achieved at the edge, providing more system flexibility and efficiency. As such, several equipment manufacturers have cameras with various analytics suites, either for multiple purposes or for specific applications such as license plate recognition and facial recognition. With this increase in complexity, image quality becomes of paramount importance to ensure that the correct information is captured, analyzed and learned by the system.

Video analytics are based on rules set by the user. When these rules are met, a notification is sent. A simple rule could involve, say, a person crossing a specific area or a piece of luggage left unattended. More complex rules could, for example, identify all black cars in a certain zone or all people who are carrying a red backpack. To carry out simple rules, the system will apply specific algorithms. These algorithms analyze the image captured by the camera – that is, the pixels composing the image – to determine if the conditions specified by the rule are met or not. Typically, at this level of complexity, the algorithms search for certain defined changes in pixels within a specific zone of the image and within a certain timeframe.

While more complex rules also use algorithms, they perform a more precise analysis of the image, which may involve eliminating irrelevant information such as foliage or animals and very often includes some machine learning. For example, for the system to recognize and understand what a black car is or what a cat is, it must be





taught. In addition to deep learning techniques, there are other machine learning methods that use statistical and mathematical models. And while the choice of machine learning type usually depends on several factors, including the algorithms used and the application, the starting point is still image analysis. Even at this complexity level, a small change in some pixels may result in a false response. For example, when teaching a system about facial recognition, a discrepancy between some pixels and reality can make a trait look completely different.

Understanding Image Quality

In the context of analytics, image quality can be defined as the accuracy of an image captured by the camera. It is important to mention that, when analytics are performed, they are not affected by human perception, unlike when a display is viewed by a person under various lighting conditions. Furthermore, the analytics are performed on uncompressed images to ensure the accuracy of the input. When done at the edge, they are completed before compressing the image and transmitting it. When done in an NVR or

> Principal factors affecting image quality can be divided into three categories: the optical system components of the camera and their related characteristics, the environment, and human interaction.

a VMS, the image is first decompressed and then the analysis is applied.

While image quality may seem to be subjective, it is in fact possible to assign it measurable attributes. Indeed, image quality is directly correlated to the modulation transfer function (MTF) of the optical system and the *f* number and relative illumination (RI) of the lens. Whereas low-light performance increases as the *f* number decreases, high MTF and controlled RI are defined by optical designers based on the type of lens and its applications. Distortion is another attribute of image quality, and although it should be minimized in most cases, controlled distortion is an important characteristic in wide-angle cameras that maximize the magnification factor or pixel density where needed.

Principal factors affecting image quality can be divided into three categories: the optical system components of the camera and their related characteristics, the environment, and human interaction.

In regard to the optical system, near perfect image quality can be achieved by pairing up a high-quality lens with an appropriate sensor. If the lens is of low quality, the image will be as well, regardless of the sensor's specifications and performance. In addition, the entire image processing pipeline has a direct effect on image quality: A camera that has a high-quality lens, sensor, image signal processor and encoder will still display poor images if the image processing is inadequate.

Probably the best-known image quality factor related to the sensor is the image resolution/pixel count. With multi-megapixel cameras now common, state of the art image quality should be achieved. However, the effects caused by digital zooming must be accounted for. As the camera zooms digitally within an area to analyze it, pixels are interpolated, the resolution

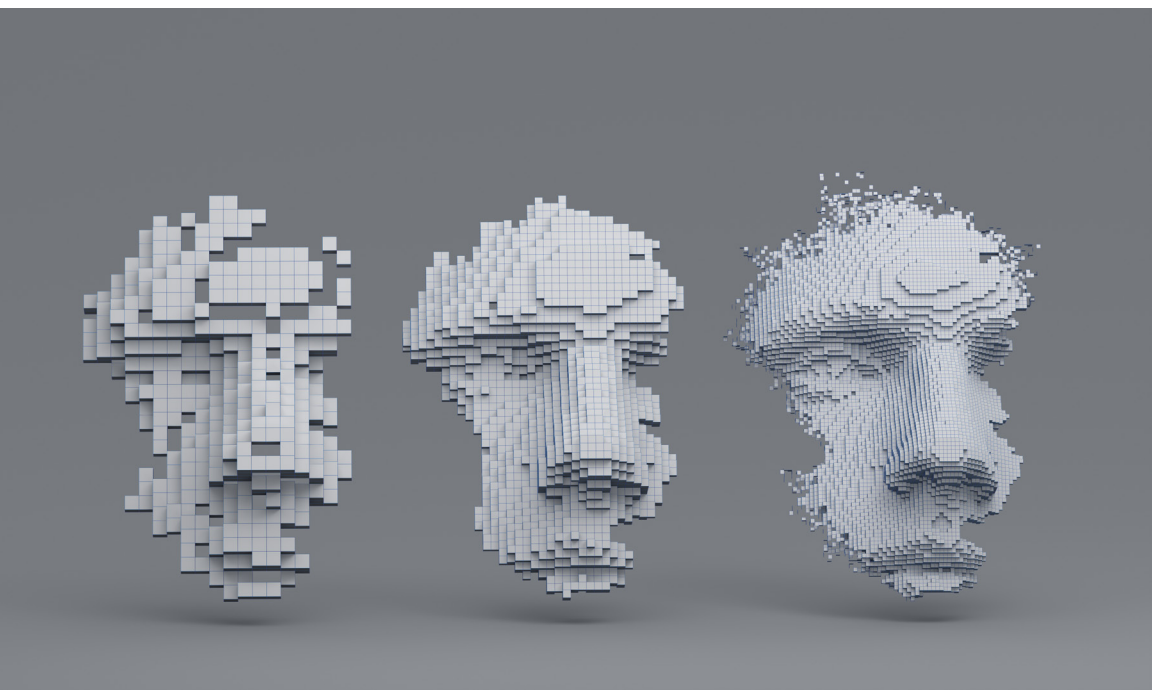
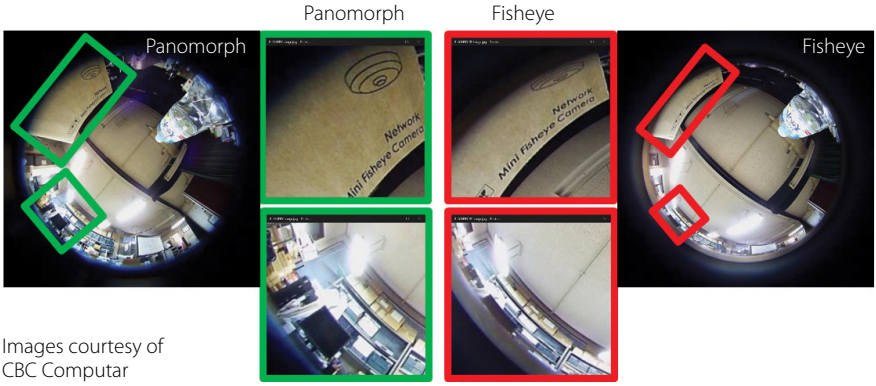


Figure 1. Panomorph vs. Fisheye Lens



Images courtesy of CBC Computar

decreases, and the image quality may suffer, especially for cameras with lower resolutions, such as 1.3 megapixels.

Furthermore, the camera angle of view directly influences the image quality and is correlated to the resolution, as well as the type of lens used. For angles of view of less than 80 degrees, the pixel density is generally rectilinear across the entire image, and the quality is mostly constant, with a little MTF drop toward the edges. With conventional lenses, as the angle of view increases, the pixel density tries to remain constant up to a decrease at the edges. This is a well-known challenge for wide-angle cameras using a traditional fisheye lens, which displays significant distortion at the edge of an image, where the pixel density is lower than at the center.

> A camera that has a high-quality lens, sensor, image signal processor and encoder will still display poor images if the image processing is inadequate.

In these cases, the image quality in the center is adequate for analytics processing, but closer to the edge, it is not. Alternatively, wide and ultra-wide cameras equipped with panomorph lenses generate less distortion at the image's edge, because of a higher pixel density, which provides sufficient quality for analytics processing throughout the image. Figure 1 demonstrates the difference between a traditional fisheye lens and a panomorph. On the edge of the fisheye lens image, one can observe a simple black rectangle, whereas in the same zone with the panomorph lens, one can clearly see a computer screen.

Other important factors that affect image quality are related to the environment, with lighting conditions having the most direct effect. While

some surveillance occurs under constant lighting conditions, a large proportion takes place in light that varies. Bright light and low light can affect how a camera captures a scene, producing over or under-exposed images, which results in inferior image quality for analytics processing. To mitigate the impact of bright and low light on image quality, cameras with wide dynamic range (WDR) are highly recommended. Similarly, for very low-light conditions, such as at night, cameras with infrared (IR) sensors are good options.

Additional environmental factors that influence image quality are the ambient temperature and the humidity level. Extreme heat and cold, abrupt temperature changes, and high humidity can hinder the functioning of the camera sensor and processor, as well as the camera focus adjustment, all of which affect image quality. Also, mist may form on the camera bubble, degrading visibility. Where weather factors are a concern, ruggedized and extended temperature cameras with autofocus mechanisms, heaters and ventilated housings should be considered.

Lastly, a highly variable type of factor in image quality is human interaction, primarily through the installation and configuration of the cameras. While camera configuration is becoming more automated, it still has a human element that can influence image quality. Proper physical mounting and alignment and accurate setup of all parameters, including focus, are important steps to ensure sharp images. Special attention should be paid to the impact of varying lighting conditions to ensure that the parameters address all of the conditions

mentioned above. Consequently, it is of vital importance to make sure that the technicians installing the cameras are properly trained.

Summary

Tremendous advances have been made in the field of video analytics, especially with the use of AI and deep learning, which allow for sophisticated rules and analyses, whether handled at the edge, on an NVR, or in a VMS. As the complexity of analytics increases, so does the need for images to be of excellent quality. To ensure high image quality, several aspects must be considered: the design of the entire optical system and imaging pipeline, the environment, and the human factor. Thus, as for any process, the quality of the input directly affects the accuracy of the output.

While the lens-to-display pipeline has shifted from analog to digital and has been improved by new technologies, it has remained centered on the expectation that humans are looking at the images. When the human observer is removed, as in the analytics process, the entire imaging pipeline must be revisited to accommodate the new technical demands and enable AI to open up new areas of innovation. ■ **Back to TOC**

As for any process, the quality of the input directly affects the accuracy of the output.

Sophie Gigliotti (sophie.gigliotti@immervision.com) is manager, sales and business development, video security, for Immervision (www.immervision.com).

Search the SIA Membership Directory

As data is continually collected, organizations are tasked with identifying the best ways to use the information to their advantage. For forward-thinking enterprises, this can be achieved through the implementation of data sharing and integration between systems.

Data, Data Everywhere

Integrated systems can use information from multiple sensors to enhance security and efficiency

By Lynn Wood
Vanderbilt

When thinking of data, it usually is not associated with anything of an artistic nature. Instead, images of spreadsheets, wires or dark server rooms often come to mind. However, true data integration must be more than that. It needs to combine pieces of information that come from a number of sources and display them in a way that is meaningful and valuable to the user. This unified view paints a full operational picture from a security perspective, while individual brushstrokes made up of unique data points can be further dissected when necessary. Taken together, this viewpoint can provide valuable insights into the security and business inner workings of an organization.

In the security world, data integration enables users to streamline

processes. Ensuring that software platforms work well together allows managers to kickstart a workflow with the press of a button, instead of taking multiple independent steps to systematically change numerous data points. Data across today's modern enterprises is collected in

many ways, such as through human resources, employee records, and event management software, all of which are typically used in corporate, healthcare or educational environments. Integrating these platforms with access control and visitor management software can create a cohesive system for managing access to a campus and much more.

Data-Driven Decisions and the IoT

The amount of data produced daily is astounding. According to Raconteur, it is estimated that, by 2025, 463 exabytes of data will be created each day. That is 463 billion gigabytes, or the equivalent of more than 212 million DVDs, per day. This growth can be attributed to multiple factors, one of which is the Internet of Things (IoT), the network of interconnected devices embedded with sensors and software that collect and exchange data.

The security industry has a pretty good idea of what the IoT means for organizations, and at its core, these connected devices are providing a foundational element: data. As data is continually collected, organizations are tasked with identifying the best ways to use the information to their advantage. For forward-thinking enterprises, this can be achieved through the implementation of data sharing and integration between systems. The IoT introduces a new capacity for connectivity that is proving to be a real benefit, changing the way business is done, as well as how employees work, and the interconnectivity between the two.

Data and Access Control

In the realm of access control, IoT technology can provide a wealth of options for granting and restricting access to various parts of a facility or campus, working seamlessly with

other software and providing security leaders with more information about incidents in the event of an emergency. Additionally, advanced connectivity through smartphones and other IoT devices allows for a much more personalized experience through the use of mobile credentials, biometrics and analytics in new and innovative ways.

On a large scale, the IoT can be applied citywide, using data, for example, to measure energy use and identify waste, which can help to improve the way we live and work as a society. Within security, this might mean intelligent cameras, intrusion-detection alarms and other sensors that are analyzed at a central point within a security department.

A critical component to venturing into IoT-friendly systems in the security space is protecting data and privacy.

An increased level of connectivity and integration in an organization can provide enhanced insights into the physical security posture, such as by measuring throughput rates and identifying traffic patterns. Additionally, the information gathered through network-enabled readers allows an organization to set specific "rules" that can be applied depending on the time of day and the day of the week, and those rules can be adjusted for special events.

Without software platform integration, in order for a new employee to be added to a system and given a security badge, his or her data has to be entered into not only the employee management software,

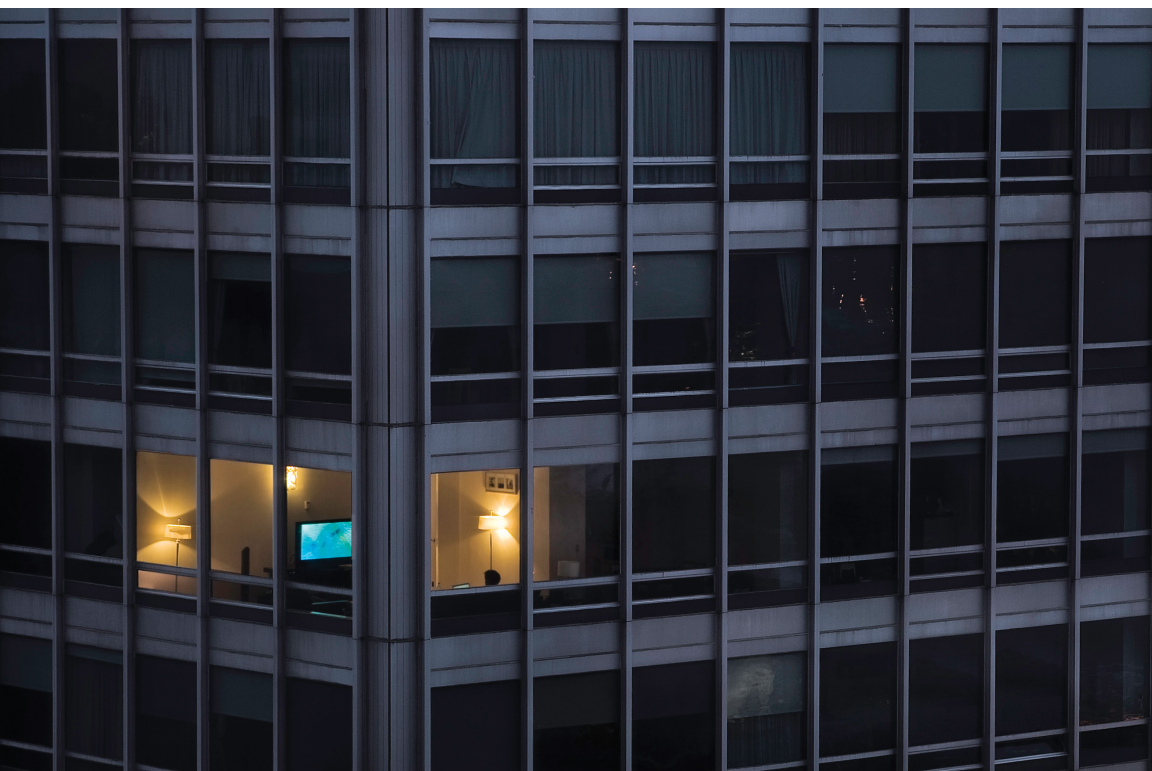
but also the IT network, the security manager's access control software, and other systems. The art of data integration centers around the concept that each of these software platforms is linked in order to streamline workflows and make it easier to keep information current across an organization. So when a person is added to (or deleted from) one platform, multiple systems are updated in real time.

A critical component to venturing into IoT-friendly systems in the security space is protecting data and privacy. Systems integrators, dealers and consultants play a crucial role in the deployment of access control systems that use advanced IoT-enabled devices in a safe and secure manner. If an end user or facility manager wants to use connected devices, security professionals must educate them about best practices to protect organizations from threats. For these entities, effective cybersecurity is a prerequisite to success.

Going Beyond Security

Integration between access control technologies and other types of systems, like HVAC or building controls, can help enterprises identify ways to save energy and become more efficient, such as:

Lighting control – Automatic lighting is not a new phenomenon, but this technology has been slow to spread. However, with the addition of "smart" devices (think Google Home or Amazon's Alexa, but for large facilities), there is a significant shift toward streamlining control of a facility's lighting. Software integration between access control platforms and smart lighting technology can help make this a reality by signaling when someone



has entered or exited a facility and triggering a response to turn lighting on or off in a specific location. This can produce cost savings by reducing energy usage.

Heating/cooling management – For many facilities, climate control is a significant expense, which means measures that link usage directly to need are getting a lot of interest. When the first person of the day enters a facility, that information from the access management software can trigger an automatic notification for the HVAC system to turn on for the day, and the opposite occurs when the last person leaves at night. Further, software integration can be customized to the point of controlling the temperature based on someone's preferences within a specific office space.

Using access control software to determine how many people are present in a building, along with integrating roll call systems to ensure accurate reports, can be invaluable tools in emergency situations.

Lockdowns, evacuations and attendance reporting – The benefit of using access control to assess building occupancy becomes clear when lockdowns or evacuations are necessary. Using access control

software to determine how many people are present in a building, along with integrating roll call systems to ensure accurate reports, can be invaluable tools in these emergency situations. Having accurate records is essential for making sure people are safe and accounted for as an event unfolds.

> Each and every system and sensor that a building leverages can contribute crucial information to an organization's overall safety and business goals.

Human resources records – When an HR department or school registrar is tasked with the management of employee or student information, they require innovative technology platforms. This technology can be integrated with access control software to streamline the onboarding of staff and students. Additionally, with the use of a visitor management platform, visitors can be granted access to certain parts of the facility based on their reason for being on the campus, and credentials can have assigned time limits to ensure that they will not be used beyond their expiration or outside of their approved times of day.

Strengthened security – The goal of integrating access control software with other platforms, ultimately, is to deliver enhanced security to both employees and assets within an organization. The ability to gather insights about visitors, building

occupancy, and who is present at any given time can prove useful for officials during an incident, allowing them to obtain critical information with the push of a button.

The ability to gather insights about visitors, building occupancy, and who is present at any given time can prove useful for officials during an incident.

The Future of Data Integration

As the amount of data being generated by devices grows each day, it is important to recognize the value of integration. Each and every system and sensor that a building leverages can contribute crucial information to an organization's overall safety and business goals. Access control technology is at the center of this effort, enabling operators to protect the occupants of a facility while enhancing everyday efficiencies through the incorporation of additional systems. The true art of data integration lies in having the vision to bring all of the incoming information together to obtain a cohesive operational picture that allows for more informed decision making. ■ **Back to TOC**

Lynn Wood (lynnwood@vanderbiltindustries.com) is product portfolio manager for Vanderbilt (usa.vanderbiltindustries.com).

Search the SIA Membership Directory

With the exponential increase in data gathered by smart cities, it is essential to implement measures to protect, preserve and process it.

Smarter Cities Through Secure Data

The first step to leveraging sensor and other information is ensuring that it is protected

By Jason Bonoan
Seagate Technology

As the world becomes increasingly urbanized, growing pains felt by large cities can be seen across a number of indicators, from rising crime rates to increased traffic to housing shortages. In 1950, only 29 percent of the global population occupied urbanized areas. In contrast, a recent United Nations study found that 1.3 million people now move into cities every week, and by 2040, 65 percent of the world's people will be living in cities. As populations become denser and municipalities grow at a breakneck pace, there is a need to implement measures that will maintain a high quality of life.

Once thought of as a futuristic aspiration, smart cities have positioned themselves, in many ways, as the answer to these challenges. By collecting information from a variety of

devices and sensors, municipalities are able to manage assets and resources more efficiently than ever before. Utilizing surveillance cameras equipped with high-definition optical sensors and advanced video analytics, these systems are part of the Internet of

Things (IoT) revolution in which an unprecedented amount of data is being collected and processed.

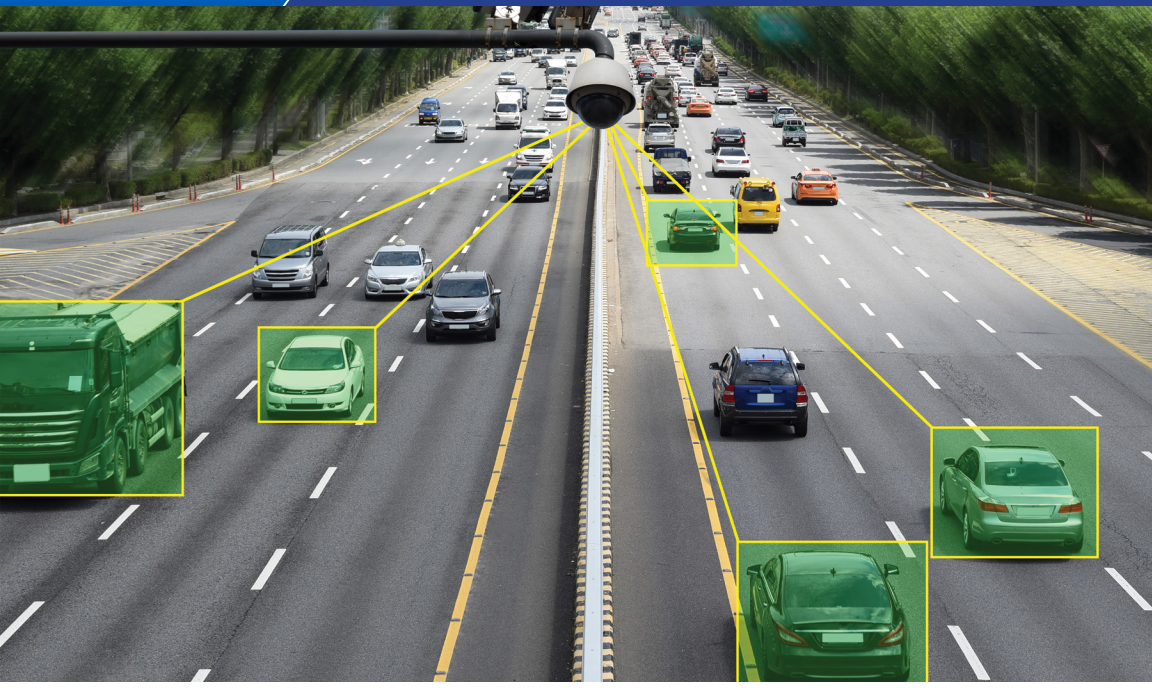
Thanks to innovations in artificial intelligence (AI) and deep learning technologies, surveillance systems are now able to aggregate, structure and analyze complex sets of data. By identifying characteristics such as hair color, iris patterns, thumbprints, movement, license plate numbers and more, surveillance systems can use this information to perform important tasks. Object classification, license plate recognition, pattern analysis, heat mapping and facial recognition are just a few examples.

At the center of it all lives data, collected by devices and leveraged by analytics. This data enables the features of a smart city, making the integrity of the systems that collect and process it of the utmost importance.

Data at the Center of Smart Cities

In smart city deployments, data is the central force driving improvements across numerous sectors, from health and safety to mobility to energy. Pairing IoT-connected devices with AI allows for real-time intelligence that can protect residents and optimize resources to keep municipalities operating smoothly.

Body-worn cameras, city-wide surveillance systems, and gunshot detectors are only a few of the notable security devices being deployed in smart city applications to enhance public safety efforts. Enabling real-time crime prevention and mapping, these sensors help to reduce robbery, burglary and assault incidents by 30 to 40 percent, according to a McKinsey Global Institute report titled *Smart Cities: Digital Solutions for A More Livable Future*. In the area of public health,



the data captured by IoT devices in smart cities can be utilized to improve the quality of healthcare, while also enhancing preventative measures to aid in creating a healthier population. In healthcare facilities, sensors that enable remote patient monitoring can provide staff with a patient's vitals in real time, alerting to potential issues and crises prior to escalation.

Across the globe, many cities are in the midst of a housing shortage, causing both home prices and rents to skyrocket. While expanding the housing supply is a seemingly simple solution to address the issue, bureaucratic policies often hinder progress. Digitizing land acquisition, permits and design approvals can greatly ease a builder's ability to begin new projects, simultaneously increasing both housing availability and affordability.

When it comes to resources, intelligent energy meters allow for more regular readings and enhanced tracking for both homes and businesses. This provides citizens with insights that can be used to make lifestyle adjustments, ultimately lowering utility bills and strain on the grid.

Smart streetlights, meanwhile, can help optimize routes based on traffic data collected by surveillance systems. As a result, commutes are shortened, roads are safer, and emergency response times are reduced by as much as 35 percent, according to the aforementioned McKinsey Global Institute report.

In the private sector, local businesses are able to better serve their patrons thanks to the data collected by smart city technology. By analyzing an area's demographic

makeup and buying habits, retailers can enhance their tactics for more potent marketing campaigns and enhanced customer engagement. Business owners can use AI-powered surveillance technology to develop heat maps, track visitor flow, and monitor employee-customer interactions. This leads to an overall improvement in customer satisfaction, reduced theft, and more efficient staffing. Additionally, municipalities that deploy smart city systems can more easily automate the business filings process, eliminating common roadblocks for would-be entrepreneurs while growing the local economy.

Deploying smart city technology has also been shown to have positive effects on the local community, enabling municipalities to better appropriate assets and disseminate information to residents. Platforms are now becoming available that provide the public with helpful information, such as roadblocks to avoid on a morning commute or neighborhood disturbances to be aware of. These systems also invite participation through incident reporting, resulting in enhanced safety and community engagement.

With the exponential increase in data gathered by smart cities, it is essential to implement measures to protect, preserve and process it. While the collection of personally identifiable information (PII) can help to improve the lives of city dwellers, it also demands a higher level of privacy protection than the standards associated with traditional surveillance footage.

Understanding the Risks

The primary risk to smart city surveillance data containing PII is that it could be stolen. If not properly encrypted, data can be accessed from the camera wire (during transmission), the network (through stolen passwords), hard drives (during disposal), and physical security equipment sabotage. Stolen data leads to unauthorized access to networks and personal accounts, which can result in crippling cyberattacks on businesses, individuals and even government entities.

> If hackers were to gain access to the networks of electrical substations, power plants, transportation systems, communication lines, or military or law enforcement systems, entire cities, even governments, could be shut down.

Prime examples are the Mirai and Reaper Botnets. In October 2016, a distributed denial of service (DDoS) attack was launched by exploiting default usernames and passwords of IoT devices, including IP cameras,

routers and digital video recorders (DVRs). Together, these hacked devices comprised the Mirai Botnet, which made the Internet inaccessible in several regions of the United States. A year later, the Reaper Botnet used "software hacking techniques to break into devices" and infected more than a million networks, according to an October 2017 article in *Wired*.

Cyberattacks through malware and stolen data can have serious ramifications, as these examples illustrate. However, the reality is that many IoT devices lack basic data hardening features. In fact, as many as 46,000 commercial and residential DVRs can easily be accessed by hackers, according to a recent report from Risk Based Security.

The concern escalates when considering what unsecured data could mean for the critical infrastructure sector. If hackers were to gain access to the networks of electrical substations, power plants, transportation systems, communication lines, or the military or law enforcement, entire cities, even governments, could be shut down.

> Insufficient data security standards not only reflect poorly on integration firms, they can also make them liable if breaches occur.

Decoding Data Privacy Regulations

Partially in response to these threats, the General Data Protection Regulation (GDPR) was enacted by the European Union. The GDPR is the most significant change in the world of data protection in a generation. The goal is twofold: one, balance an individual's right to protection, and two, allow a data-based economy to thrive without stifling innovation. The GDPR also imposes direct obligations on service providers (known as processors) for the first time. Furthermore, the European concept of personal information is broader than the U.S. concept of PII and includes personal identifiers that may result from AI processing of surveillance video.

Industry experts expect the GDPR to have a ripple effect on legislation across the globe. For example, in the United States, the California Consumer Privacy Act (CCPA), one of the most significant data privacy laws in America, is now in effect. Companies that store large amounts of personal data, including corporations like Google and Facebook, will have to be transparent about the type of data they collect, and they will also have to provide an option for consumers to opt out of having their data sold. Many other changes will continue to take place as policymakers respond to the need for stricter data management practices.

The implementation of the GDPR ushered in a new era of security. Because many of today's advanced security solutions collect some form of PII, systems integrators, security operators and end users can no longer deploy solutions that employ mediocre cybersecurity measures or none at all. Security professionals will

now be held responsible for ensuring that this information is safeguarded.

While there is an immediate impact on security manufacturers, dealers and end users in the EU, companies who are based in other geographic regions but have a global customer base can also fall under the purview of this policy. Moreover, as technologies continue to evolve and data aggregation increases, it is likely that the United States and other countries will follow the EU's example and implement similar legislation. Consequently, it is essential for security leaders around the globe to act now by deepening their understanding of the risks associated with unsecured data and implementing best practices to protect it.

While many cybersecurity discussions revolve around the theft of "data in transit," safeguarding "data at rest" is just as crucial. Protecting data at rest begins with ensuring that storage solutions utilize solid state hard disk drives alongside appropriate data protection protocols.

Data Protection Best Practices for Systems Integrators

Despite data's central role in the security industry and the increasing importance placed upon data security, many systems integrators have a hard time knowing where to begin. In the 2019 State of the Industry report by *Security Business*, 43 percent of survey respondents selected cybersecurity as a key technological disrupter in the security market. Yet only 23.5 percent have added cybersecurity features to their service plans, highlighting the disconnect between thought and action.

> Hardware encryption is often the most effective data security strategy for systems integrators.

So what can be done about these unseen digital threats? And why should integrators take note? As mentioned previously, locking down a security system starts with the integrator, and part of this crucial responsibility is understanding which practices offer the highest level of data protection. Insufficient data security standards not only reflect poorly on integration firms, they can also make them liable if breaches occur. For example, in 2018, a major home security company paid $16 million to settle several class action lawsuits that accused it of installing systems that left users vulnerable to digital threats.

For these reasons, systems integrators should adopt the latest data protection measures. Examples include software encryption, pseudonymization, hardware encryption, and secure erase features. All of these tactics have their own important and distinguishable characteristics.

- *Software encryption* utilizes tools that run on the same processor as the security system, which

can lead to system slowdowns.

- *Pseudonymization* is another form of reversible data encryption. Simply put, this is a data management and de-identification process, placing PII with one or more artificial identifiers, or pseudonyms, within data records. This process of masking data and keeping the key to reversing the process separate is greatly encouraged throughout the GDPR.
- *Hardware encryption*, which uses a separate processor for continuous authentication and encryption, is another optimal solution for data hardening. Self-encrypting hard drives work 30 percent faster than encrypting software and are cost-effective lifecycle solutions. Self-encrypting drives also provide important benefits to businesses. In the event of a breach, the GDPR states that organizations do not have to publicly report the incident if the data is encrypted, making self-encrypting drives valuable assets to companies for both data protection and reputation management. For these reasons, hardware encryption is often the most effective data security strategy for systems integrators.
- *Secure erase*, used when a hard drive reaches end-of-life status or when the stored data is no longer needed, is another key best practice to implement for total data protection. Alternative methods of retiring or repurposing a drive can be time or labor-intensive. Physically shredding a drive is both expensive and environmentally hazardous, while overwriting data software is a costly process that can tie up a system's resources for days at a time. Long-term storage of decommissioned drives in a warehouse puts the data at high risk of theft. The

most reliable option is a secure erase function, which quickly eliminates all data on the drive, instantly resetting it to factory defaults and automatically changing the encryption key so that any remaining data is cryptographically erased. This means all data that was once housed on the drive is permanently unreadable.

Systems integrators and end users who implement end-to-end encryption, pseudonymization and secure erase procedures will experience the greatest peace of mind. In addition, integrators should focus on partnering with trusted security suppliers who are committed to data security and regulatory compliance. By deploying hardware that encrypts from verified sources, systems integrators can provide end users with a secure, comprehensive surveillance solution.

As smart city solutions enhanced by AI capabilities continue to evolve and aggregate mass amounts of personal data, cybersecurity measures will continue to increase in importance. Systems integrators must lead the way in recommending and installing surveillance systems that contain the necessary protections. By partnering with manufacturers who prioritize data privacy, integrators can be assured that their security solution is protected. ■ **Back to TOC**

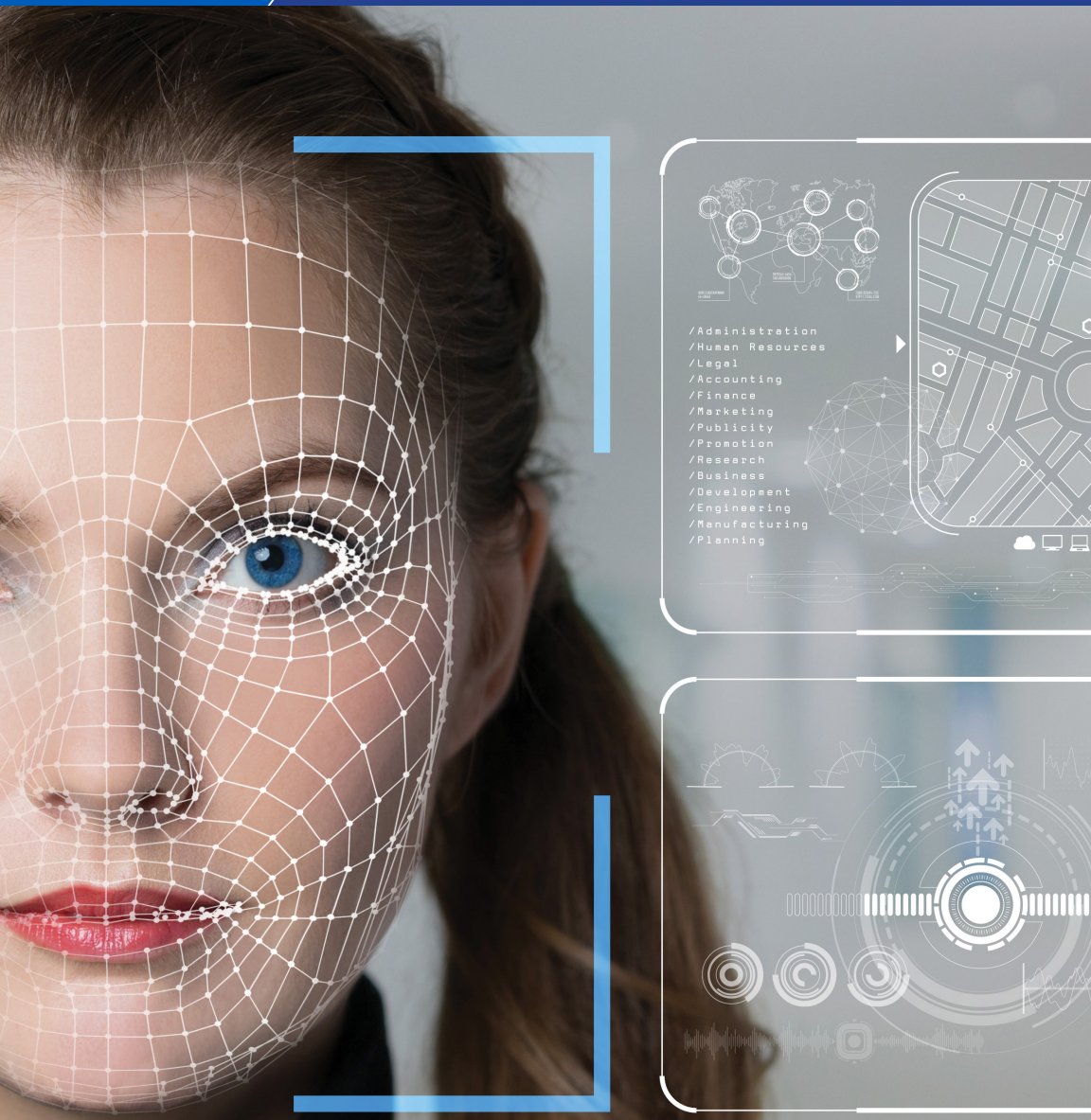
Jason Bonoan (jason.bonoan@seagate.com) is global product marketing manager for Seagate Technology (www.seagate.com).

Features Checklist

When sourcing storage solutions for smart city deployments, it is important to look for a few key features:

- *Secure supply chain* – Know where the hardware is coming from. Ensure that a manufacturer's components are sourced securely from trusted partners in compliance with the Open Trusted Technology Provider Standard (O-TTPS).
- *Self-encryption* – Seek out devices that utilize hardware-based encryption to protect against attacks.
- *Secure download and diagnostics* – Establish that a manufacturer's firmware is protected from attacks during its working life through precautions such as digitally signed firmware and rogue firmware detection, blocked cross-segment downloads, locked diagnostic ports, and a secure boot process.
- *Secure erase features* – Look for storage devices that offer instant and secure erase functionality so that administrators can easily replace encryption keys on any device, rendering the data cryptographically erased, making device retirement or repurposing much simpler.

Search the SIA Membership Directory



Although the use of biometric data in the physical security industry has been mainstream for many years, the understanding of the ramifications of collecting and storing this kind of data is clearer now than ever before.

Who Am I? Why Am I Here in this Database?

As security technology advances, privacy concerns must be addressed

By Antoinette King
Axis Communications

The definition of personal data, also known as personally identifiable information (PII), has expanded in recent years. Previously, personal data typically referred only to the most sensitive information, such as name, address, Social Security number, health records and date of birth. Today, it has expanded to include things like location data, IP address, MAC address, biometric data, behavioral patterns, and browsing history.

The sources of data collection are many. When online, browser cookies record things such as IP address, MAC address and browsing history, while offline, behavioral activity is recorded by surveillance video and analytics. Additionally, people give varying degrees of consent to the collection of their data. In some cases, people

freely give away their most personal information, as when they turn over their DNA information to ancestry services in return for a glimpse at their family tree. That same data is highly protected by HIPAA when it is being processed by a healthcare facility.

The current climate of data privacy is unstable at best. According to a recent study by Pew Research Center, approximately 62 percent of Americans believe that it is impossible to go through a single day without having their personal data collected by private companies, and 63 percent think it is impossible to go through a single day without the government collecting data about them. Most people feel like they have no control over the collection of their data by companies or the government. The same study found that 59 percent of Americans indicate a lack of understanding about how their data is used by companies, and 78 percent express similar concerns about the use of their data by the government. Understanding what PII is, how it is collected, and how it is used is essential when considering technologies to implement in business.

Personal Data and Physical Security

The commercial use of physical security has traditionally been concerned with creating safe and secure environments for assets (people and property) in a given location. Physical access control, perimeter protection and video surveillance are combined to form a comprehensive system of protection. Video surveillance has also been a key tool in helping law enforcement to investigate and solve crimes. With the rapid advancement in technology, the physical security industry now finds itself in the throes of transformation. Biometric technologies, such as fingerprints, iris scans and facial recognition, require identifying information to be collected and stored as a means of secure access control and as an aide to investigations. Although the use of biometric data in the physical security industry has

been mainstream for many years, the understanding of the ramifications of collecting and storing this kind of data is clearer now than ever before. If the biometric template is compromised, the subject can never use it again.

Facial recognition has been getting a lot of attention in recent months. To understand the technology, it is important to note the difference between facial recognition and facial detection. For a system to "recognize" a person, there needs to be an enrollment process in which a master photo is taken and associated with the person, then stored in a database for future comparison. A direct link is created between the picture and the identity of the person in the image. A person can be "enrolled" into a system consensually, as when an employee's ID photo is used as a template, or without their knowledge, perhaps when an image from a video surveillance system is used as the template. Consent plays a very important role in the controversy surrounding facial recognition. Citizens are very sensitive to their image being used without their consent. Facial detection, in contrast, simply determines that there are faces in the field of view, and sometimes through software, a box is drawn around the face to bring attention to it. Facial detection does not create a link between the image and the identity

To understand the technology, it is important to note the difference between facial recognition and facial detection.

of the person in the image. Facial detection may be used as a deterrent, as in the case of public view monitors in retail applications. As people enter the store, they are made aware of the use of video surveillance in order to discourage theft.

There are many beneficial applications of facial recognition. In the state of New York, it is used to detect identity theft and to find people with multiple licenses. The technology enables law enforcement to efficiently scrub through many hours of video to identify suspects and collect evidence. In August 2019, the New York Police Department was able to apprehend an attempted rape suspect within 24 hours of the incident in part because of facial recognition. The technology is also being implemented in airport security applications for more accurate identification of passengers. In addition, it can be used by retailers to identify known shoplifters and to alert security personnel when people on watchlists enter the establishment, a modern-day equivalent to taping a shoplifter's photo to the entrance wall of the store.

Some people are highly concerned about how their biometric data is being used and consider the use of facial recognition in security and surveillance to be a threat to their privacy. However, facial recognition, in conjunction with geotagging, has been widely implemented by Google and Facebook, as well as many other social media platforms that consumers use daily, for years. People have been putting their image and location – their PII – out there for all the world to see at least since the days of MySpace. When a person "tags" someone in a photo on social media, they are essentially

supporting the learning engine for that platform. Somehow, social media giants have convinced consumers that facial recognition use on their sites is not only OK, but cool, and they have been profiting from it for years. Yet when use of the same technology has been suggested to improve safety and security, consumers resist, citing invasion of privacy. Along similar lines, many cell phone manufacturers use fingerprint and facial recognition technology to unlock their devices. The security behind the management of that biometric information has fallen under very little public examination or scrutiny.

Legislation on Data Privacy and Physical Security

Despite the myriad benefits of the technologies, many individuals and organizations fear that video surveillance and biometric device advancements may be abused by both commercial entities and government agencies. Commercial entities stand to make a lot of money from consumer data, and government agencies can use the information in many ways that would infringe on citizens' rights. As a result, legislation and regulations have been enacted in several places around the world to respond to these concerns.

The European Data Protection Board recently published its *Guidelines on Processing of Personal Data Through Video Devices*, which outlines how and when video surveillance can be used in commercial environments. It sets very strict standards regarding the process that needs to be followed if video surveillance is implemented, including:

- Video based solely on general security is no longer a sufficient reason to implement a surveillance solution; the purpose must be specific and documented.
- It must be demonstrated that video surveillance is necessary and that less intrusive technologies or alternatives would not suffice.
- There must be an existing threat or situation sparking the need for video surveillance.
- It establishes a clear definition of how and when consent is required.
- It sets very specific requirements regarding disclosure of video surveillance to subjects.

These guidelines apply to all video surveillance, not just systems that include facial recognition.

> There need to be mechanisms in place to safeguard citizens' privacy.

In the United States, Pennsylvania, Oklahoma and Oregon have all passed legislation pertaining to the use of facial recognition technology. Oregon has prohibited its use with body-worn cameras; Oklahoma prohibits the sharing of biometric data (including images of its residents) with the federal government; and Pennsylvania requires any agency that uses facial recognition to create a written use

policy. Several cities have also passed laws completely banning the use of facial recognition by the government and law enforcement, including San Francisco, Oakland, and Somerville, Mass., and at least nine states are considering legislation concerning law enforcement's use of the technology. The California Consumer Privacy Act, meanwhile, creates a comprehensive set of rules pertaining to consumer privacy that are akin to the European Union's General Data Protection Regulation.

Industry Response to Data Privacy Concerns

Citizens are concerned about how their biometric data is being used. Given the negative attention that facial recognition technology has received recently, these concerns are understandable. There need to be mechanisms in place to safeguard citizens' privacy. If a person is recorded as they pass through a public area, there is no basis for any expectation of privacy. However, if a person is recorded over an extended period of time, and there is a mass of data that can be used to identify the behavioral patterns of that person, then they could certainly make a case that their privacy has been violated.

At the same time, businesses are using video technology not only as a security measure, but to collect behavioral information about their customers for many reasons, including:

- Knowing how many people enter and exit the facility
- Learning which displays customers are most interested in
- Determining how long customers are in the store
- Measuring how long people wait in line
- Determining the average number of customers in line when a waiting customer decides to abandon a cart

While collecting this kind of information is important to the overall business plan, upstanding employees do not want to feel like they are being "watched" their entire shift if they have never given their employer a reason to suspect them of any wrongdoing. Surveillance camera manufacturers are now incorporating solutions, such as redaction and real-time privacy shielding, so that the employee, and other innocent people in the scene, are not necessarily identifiable. An unredacted view would also be recorded in the event the video is required for evidence in an investigation. In addition, the use of static masking enables the user to block out sensitive areas in a camera's field of view, effectively eliminating the ability to view parts of the scene live and on

> Options such as live privacy shield and redaction provide businesses with the ability to collect data about their operations while also being sensitive to privacy concerns.

playback. Another alternative to video surveillance is using thermal imaging technology as a detection tool. Rather than relying on visible light, this technology measures and displays the temperature differences in the scene, making it an excellent option for perimeter protection.

The use of video surveillance by businesses to improve service offerings and the customer experience is growing each year. Options such as live privacy shield and redaction provide businesses with the ability to collect data about their operations while also being sensitive to privacy concerns. Behavioral patterns can be examined and shared without compromising the personal information of the subjects in the video.

Outlook for the Future

Artificial intelligence and machine learning are the wave of the future. As society becomes more reliant on Internet of Things devices to perform security and safety functions, the subject of data privacy will become more pronounced. Having a strong understanding of what information is being collected and how it is being stored and used is paramount in creating a trust relationship between data subjects and those collecting the data.

It is up to security industry professionals to demonstrate the value of using these technologies to protect the assets. Educating the public on how the technologies work, listening to their concerns, and developing use policy recommendations are all fundamental to security and surveillance innovation. ■ **Back to TOC**

Antoinette King (antoinette.king@axis.com) is key account manager for Axis Communications (www.axis.com).

Search the SIA Membership Directory

Unlimited Access

Cloud and open source solutions allow for greater access control scalability and efficiency

By Jeff Bransfield
RS2 Technologies

Jumping into the world of entrepreneurship is not for the faint of heart. In addition to managing finances, hiring competent employees and creating a sustainable business plan, there are many other important considerations to be aware of, such as ensuring the comprehensive protection of the people and assets inside a facility. Entrepreneurs are responsible for the safety of their business and those that help operate it, which requires making strategic decisions when it comes to what type of security solution will work best now and in the future. It is difficult to predict business trajectory, so it is imperative to have a security system in place that allows for scaling up or down as needs change.

Manufacturers and integrators alike, especially in the access control sector, are responding to this growing concern by offering more customized solutions than ever before. From "as a service" offerings to the cloud, the industry understands the need for operational longevity and is working to improve the solutions available. When it comes to choosing an access

control system that will fit a business's unique needs both today and in the future, there are a few things to keep in mind.

Should an Access Control System Be in the Cloud?

Over the past few years, the availability of cloud-based security solutions has exploded, and for good reason. The benefits the cloud provides to end users are numerous, ranging from cheaper installations to increased scalability potential.

The main advantage of selecting the cloud when considering the future of a business is financial. The cloud eliminates the need to invest in an access control server – one of the more expensive parts of a traditional access control solution. Capital expenditures become a thing of the past, and system maintenance is more cost effective.

In addition, cloud solutions are typically part of a subscription-based model that allows users to pay a set monthly fee for the services they receive. This ensures that users only pay for what they need, with the ability to change the services as a business grows. If a business only requires support for four doors at launch, but experiences growth and later needs support for 10 doors, this can be done easily and efficiently within the cloud. And, conversely, if a business experiences slower growth than anticipated, it can scale back on the services. The cloud provides the means by which users, for the first time, can scale up or down seamlessly, creating cost-saving measures and the flexibility needed to accommodate to ever-evolving technology.

With no software to install and with automatic updates, the cloud ensures

delivery of the most up-to-date, secure version of the system possible. Since there is no need to create an entirely new network, installations are streamlined, saving users both time and money compared to traditional access control solutions that require extensive wiring and network configuration. This further reduces installation costs while simultaneously allowing users to add more services without having to pay to rewire the entire network. No wires, no capital expenditures, and a dedicated team monitoring the system positions the cloud as an ideal option in terms of affordability and scalability.

The benefits the cloud provides to end users are numerous, ranging from cheaper installations to increased scalability potential.

What about Open Source?

Open systems are having an impact on all aspects of physical security, from development to installation. In general, these systems are being increasingly accepted and implemented, though not all companies have recognized the benefits yet.

Open source systems provide a level of flexibility that is unmatched by other options on the market. Instead of choosing a single manufacturer and getting locked into purchasing products and services only from that vendor, users can instead mix and match to develop a true "best of breed" solution. An open system means being able to use equipment from a variety of companies

to customize the solution to a user's unique needs. There is no cookie cutter approach to access control, and open systems provide the means by which integrators can create tailored solutions.

As a result of this flexibility, users can start small and add more system components as the company grows. With no vendor lock-in, users are free to choose equipment at a price point they are comfortable with, while also staying on the cutting edge of new technologies. An open source access control system can easily integrate with a video management system (VMS), human resources and HVAC to provide a full operational view of a facility. From there, the systems can work together to grant and revoke credentials, schedule lighting and heating based on occupancy, and more. This integration provides situational awareness, which ensures that a business is being run in the most streamlined and efficient way possible, with the flexibility to easily add cameras or other devices as needed.

In contrast, with proprietary systems, users are forced to make up-front commitments that do not easily allow for adaptation as new technologies are developed. Open systems ensure that users are at the forefront of innovation, on whatever scale works best for them, while also providing the freedom of choice to make security decisions based on functionality rather than manufacturer agreements.

Some companies have open APIs, which can be modified by integrators depending on what users are looking for. Are they interested in

advanced technologies, such as facial recognition and machine learning? Open systems can accommodate that. There are minimal limitations to what can be done, ensuring the solution that is implemented is fully customized to user demands, with the ability to switch out equipment from different manufacturers as needs change. Gone is the "build once and maintain forever" mindset. Open source provides users with more flexibility to choose than ever before.

> An open system means being able to use equipment from a variety of companies to customize the solution to a user's unique needs.

Do I Need Remote Monitoring?

Remote monitoring provides both short and long-term benefits to technology investments and is especially useful for companies that do not have the resources to support full IT departments. According to Gartner, the average cost of IT downtime is $5,600 per minute. While there is variation among businesses, this translates to about $140,000 to $540,000 per hour, with the average being around $300,000. Regardless of where users land on this scale, one thing is certain: Downtime means money lost.

The benefit of remote monitoring is that users have an offsite dedicated team in place watching over the network to respond to any incidents that could result in downtime. The moment a potential issue occurs, it is either taken care of automatically or, if human intervention is required, is

routed to the correct person and dealt with immediately. Since users pay a set monthly price to receive remote monitoring services, there are no hidden fees incurred when an event arises. Remote monitoring is like insurance: It is not always needed, but when it is, it can quickly pay for itself and more.

Remote monitoring can also be useful to companies that have an onsite IT team by increasing productivity and allowing members of that team to focus on other essential job functions. If employees are constantly responding to every single IT event, that leaves little room for other tasks to be accomplished. Remote monitoring takes the guesswork out of what tasks need human intervention, streamlining internal operations and providing the means for talented employees to use their skills elsewhere.

> The benefit of remote monitoring is that users have an offsite dedicated team in place watching over the network to respond to any incidents that could result in downtime.

Overall, remote monitoring saves money by reducing downtime, which is especially important for businesses that are just starting out, as a large financial setback could be devastating for a fledgling company. And for companies that already have an IT team in place,

remote monitoring helps users allocate resources and respond to events in a more effective way. In both of these situations, remote monitoring positions companies to be more successful in their responses to threats, both now and in the future.

Preparing for the Future

There are many ways to ensure that an access control system is ready for the technological challenges of the future, and all of the suggestions above can be combined to achieve that goal. All of these services provide high levels of cybersecurity, ensuring that technology investments are longstanding and worthwhile. It is not practical to update systems completely as new technology is developed, but the cloud and open source systems provide a way to effectively accomplish the same thing in a cost-effective manner. Combining the cloud, open source capabilities and remote monitoring ensures that access control systems are on track to stay competitive in a changing technological landscape. ■

Back to TOC

Jeff Bransfield (jbransfield@rs2tech.com) is national sales manager for RS2 Technologies (www.rs2tech.com).

Over the past 15 years, electronic access control has shifted from solely controlling access to become a multidimensional ecosystem that addresses a variety of functions.

The Keys to Electronic Access Control

Security and convenience can both increase with modern lock technology

By Rob Lydic
Allegion

Electronic access control is growing at a rate that outpaces other security technologies. This growth is driven by the desire to manage access and to know definitively which doors are secured and which are not. In addition, facilities are demanding security and safety features like lockdown, which is especially important for K-12 schools but is growing in other markets. Further driving this growth is the consumer preference for using mobile credentials. All of this is leading to greater adoption rates of wireless technology and expansion into new markets, such as multifamily properties.

Over the past 15 years, electronic access control has shifted from solely controlling access to become a multidimensional ecosystem that addresses a variety of functions. It is no longer as simple as controlling who enters a space. Expectations have evolved along with technology, and end users want to see their security solutions do more.

The IHS Markit 2018 Access Control Intelligence Report found that only 9 percent of all doors are protected with electronics, meaning that this technology is just scratching the

surface of its market potential. Heading into the next decade, electronic access control will continue to take shape and drive innovation in the marketplace.

Top 5 Emerging Electronic Access Control Trends

1. Mobile Credentials and Identity

The mobile movement is just ramping up and all markets should prepare for the seamless experience a mobile credential offers. The most notable examples have been in the higher education and multifamily markets, both of which were early adopters of mobile ecosystems.

Mobile credentials are becoming more closely tied to how an individual manages his or her identity. Users are enjoying the convenience of having a single credential to log in to disparate applications and are now pushing this into the world of access control. Apple and Google are both active in the mobile identity conversation, so advances are likely in the coming years.

2. Open, Interoperable Platforms

Traditionally, companies have offered a closed, proprietary solution that did not integrate well with other pieces of the access control puzzle. Customers became locked into a specific manufacturer's system, limiting their choices in technologies. Today, customers are becoming more knowledgeable about the topic and expressing their desire for freedom when it comes to the future of their security solutions. It is essential that the security industry listen to their demands for openness and flexibility. Open, interoperable platforms allow users to select best-in-class solutions to create a customized security ecosystem.

While some manufacturers are sticking to proprietary solutions, many have combined to create standards for openness in the industry. The

LEAF Consortium defines itself as an association of partner entities intent on bringing interoperability to the access control and identity credentials market and beyond. It is influencing the market at a time when customers are demanding to take credentials across multiple sites and introducing mobile into their security plans. Interoperability is key to future-proofing their choices.

3. Wireless Technology

Wireless solutions have transformed electronic access control by reducing the deployment cost and, thus, increasing reach and enhancing security, convenience and efficiency. The cost effectiveness of wireless solutions has helped users in a variety of markets extend the benefits of electronic access control beyond main entrances. This increase in popularity, coupled with user demand for more features, will result in improvements in battery life, communication, WiFi protocols and more.

4. Electronic Access Control Beyond Security

When hardwired devices first grew in popularity, security was the most important consideration. Efficiency and convenience were secondary. Like other technologies, access control has evolved, and so have customers' expectations.

On a macro level, the use of electronic access in an individual's environment pushes the envelope for its use in other areas. It goes beyond security to offer a more convenient experience.

In the multifamily space, residents can use their phones to gain access to their building, unlock their door, and utilize the gym. In addition, electronic access control makes it easier for dog walkers, grocery services and delivery persons to enter an apartment.

These expectations of convenience bleed over into the commercial space. With the swipe of a credential, an

office building can be made to turn on the lights, adjust the temperature and possibly unlock certain areas. Throughout the day, the system is monitoring the building and providing alerts if abnormal activity is detected. Managers maintain greater control over their properties in a more efficient manner.

5. The Marriage of Video Surveillance and Electronic Access Control

Physical security solutions like video provide value but are, ultimately, reactive. Electronic access control, though, can prevent unauthorized users from entering while granting access to those permitted. Marrying the reactive capabilities of video with the preventative measures of electronic access will create a more powerful and holistic security ecosystem.

Customers want a more comprehensive view of what is going on in their facilities. They want machine learning and artificial intelligence to be linked to alarms and they want to understand how those can be used to trigger a lockdown. Gartner estimates that 20 percent of physical access control solutions will be shaped by mobile technology and cloud architecture this year. With these real-time solutions, users can make the technology work for them and their facilities optimally at a lower cost.

Top Markets for Electronic Access Control

Education

K-12 and higher education facilities are the largest adopters of electronic access control with the most pressing needs. Lockdown, an essential piece of a K-12 school security strategy, is much more efficient and secure when electronic hardware is integrated into the school's security software.

Lacking the strict routines and well-defined perimeter that K-12 schools typically have, colleges and universities trust electronic access control to maintain control and visibility over a sprawling campus. This is simply not feasible with mechanical access hardware. Another major reason for electronic access on campus is that a majority of a student's routine is driven by an electronic credential, either a physical card or mobile student ID. In fact, many facilities are striving for a keyless campus, where everything is accessible via the campus card.

A major reason for electronic access on campus is that a majority of a student's routine is driven by an electronic credential, either a physical card or mobile student ID.

Furthermore, electronic access control provides schools with a streamlined solution that allows administrators to remotely issue and deactivate credentials over-the-air.

Multifamily Dwellings

The advancement of access control solutions will continue to be influenced by the on-demand, mobile-first, millennial generation. For example, college students who have grown accustomed to using electronics to navigate a campus expect a similar experience when they set out to rent an apartment. Using one key to access the main

door, another to get into an apartment and something else to get into the parking garage or fitness center is a foreign concept to this generation. Why would they want multiple credentials interrupting their flow?

It is no secret to property managers that people gravitate to properties because of the amenities and experiences offered. Providing seamless access and secure entry for services are among the ways that electronic access control makes a multifamily property more profitable, on top of the operational efficiencies it offers to those managing the day-to-day tasks.

Costs, Benefits and Adoption

Cost is a major factor in the adoption of any new technology. But what makes the expense of electronic access control in one market different from another? Features certainly play a role, and it is important to examine the unique characteristics of each vertical and identify the cost barriers associated with each.

> The advancement of access control solutions will continue to be influenced by the on-demand, mobile-first, millennial generation.

There are many doors throughout a multifamily residence, and these properties are often up against tight budgets. The need to keep costs low while still delivering the experience expected by potential residents is a difficult balance. A higher education campus, meanwhile, may have twice as many doors, but increased connectivity is needed for the campus experience and student safety. Students control

their entire campus lives with a single credential or mobile device, from accessing residence halls and libraries to paying for meals. Electronic access is also essential for an efficient campus-wide lockdown strategy. While shiny new features of an all-encompassing access control platform are nice in a multifamily facility, they may not be as essential as they are on a higher education campus or in a K-12 school.

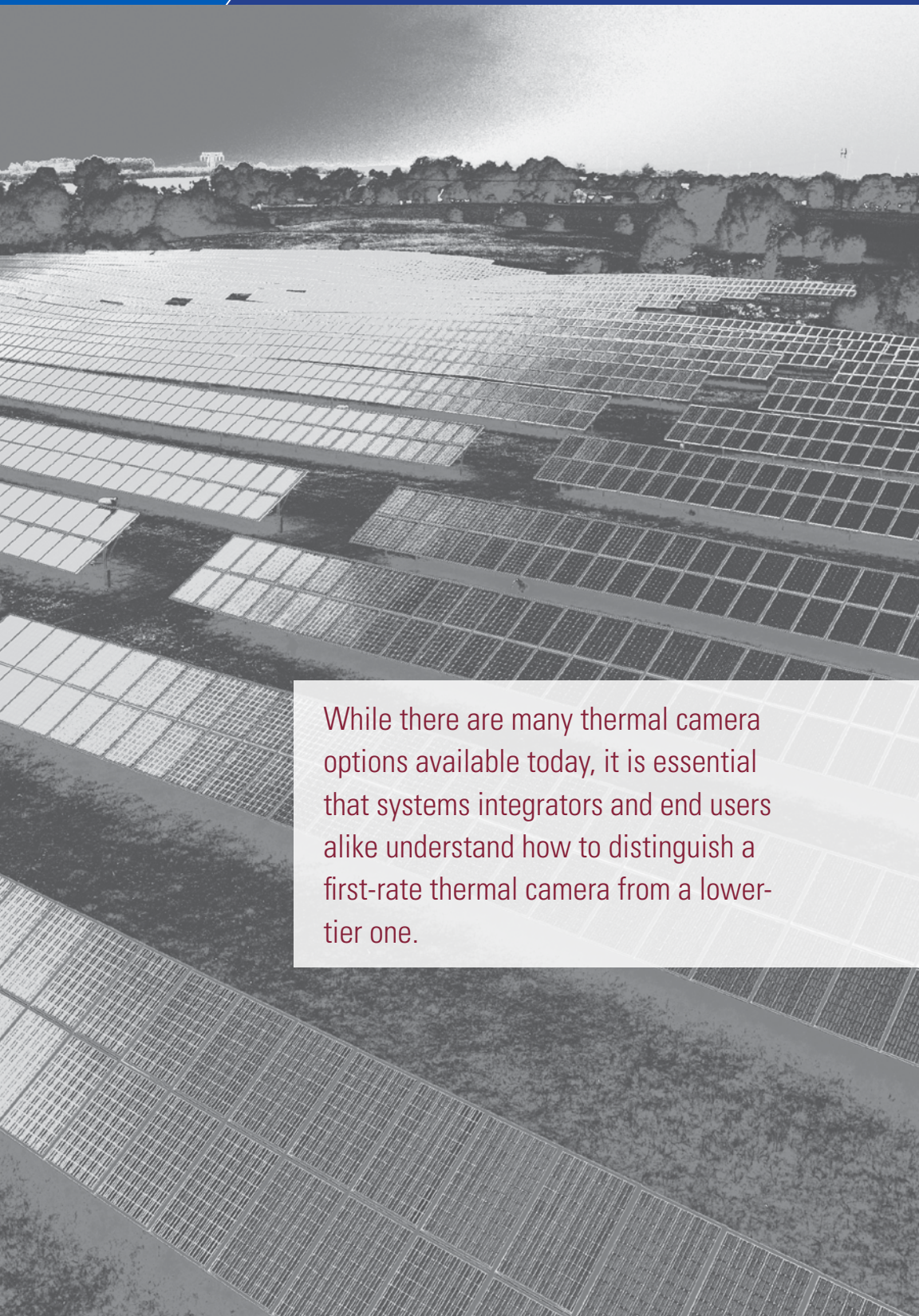
As seen with other technological evolutions, costs will continually decrease over time with new improvements and innovations in the market.

Providing seamless access and secure entry for services are among the ways that electronic access control makes a multifamily property more profitable, on top of the operational efficiencies it offers to those managing the day-to-day tasks.

Looking Ahead

With a new decade underway, it is time to usher in actionable security solutions. While electronic access has progressed by leaps and bounds during the past several years, more than 90 percent of doors contain no electrical components, offering a huge testbed for new solutions. Cybersecurity and cloud-based technologies will also affect electronic access control, and new innovations will continue to disrupt the sector. ■ **Back to TOC**

Rob Lydic (allegion@havasformula.com) is vice president of the PACS/OEM business for Allegion (us.allegion.com).



While there are many thermal camera options available today, it is essential that systems integrators and end users alike understand how to distinguish a first-rate thermal camera from a lower-tier one.

The Heat Is On

High-quality thermal cameras can see threats that other security solutions cannot

By Fredrik Wallberg
FLIR Systems

Thermal sensors capture something that the naked eye cannot see: heat. What distinguishes thermal cameras from other security sensors is their ability to use heat rather than light to produce images. By measuring the differences between heat signatures and representing these variances in high-contrast, monochrome images, thermal cameras can "see" even in total darkness, sun glare, rain, light fog, smoke and other adverse conditions.

While a standard surveillance camera may not be able to spot a camouflaged suspect in foliage at night, a thermal camera will easily see the person. This is one of the reasons why thermal cameras have become essential tools for detecting intruders, securing borders, and safeguarding airports, seaports, power plants, electric substations and other critical infrastructure sites.

Demand for Advanced Detection

Following the terrorist attacks of Sept. 11, 2001, mission-critical enterprises expressed increased interest in thermal cameras to enhance

intrusion detection at their properties, particularly at night.

In the 2010s, the Nuclear Regulatory Commission announced its 73.55 policy, which states that nuclear facilities must "provide continuous surveillance, observation and monitoring" to improve threat recognition and crime deterrence. Thermal cameras, given their ability to produce clear images in bright light, low light and no light at all times of day and night, quickly became a preferred option for the nuclear industry.

The 2013 sniper attack on Pacific Gas & Electric's Metcalf Transmission Substation in Coyote, Calif., led the Federal Energy Regulatory Commission to introduce Critical Infrastructure Protection Standard 014 (CIP-014). This standard requires utilities to deploy advanced security systems to identify and mitigate threats to mission-critical assets.

Thermal cameras have become attractive options for utilities because of their long-range capabilities and ability to detect intruders before they reach the fence line. Another advantage is their simple installation. Thermal cameras can be mounted on existing walls and lattices, whereas other solutions, like buried cable sensors, may require trenching and other extensive labor. For these reasons, thermal cameras have frequently been added to the security systems of power plants and substations across the country. Today, thermal cameras have become the go-to perimeter monitoring solution at critical infrastructure sites.

The Market for Thermal Solutions Expands

Thermal cameras have often been considered a niche technology for high-end security applications. However, their success in the industrial and critical infrastructure sectors has

generated demand across a variety of verticals.

In 2017, revenue for the thermal imaging market surpassed $5.5 billion, according to Global Market Insights, and by 2024, the market is predicted to nearly double to $10 billion. This growth reflects integration with various other technologies, including unmanned aerial vehicle (UAV) deployments by the military, hand-held devices sold to critical infrastructure sites, and cooled cameras, which offer superior imaging for life sciences, healthcare, special industrial detection, and automotive applications.

> Thermal cameras have become attractive options for utilities because of their long-range capabilities and ability to detect intruders before they reach the fence line.

The growing interest in thermal technologies can be seen in the security sector, as both traditional and new camera suppliers have debuted their own lines of thermal cameras over the past five years. This mushrooming of the market for thermal devices reflects a growing interest in thermal's value proposition and affirms the demand for innovative technologies that take security solutions to the next level.

Distinguishing Features of Superior Thermal Technology

While there are many thermal camera options available today, it is

essential that systems integrators and end users alike understand how to distinguish a first-rate thermal camera from a lower-tier one. Cutting costs upfront often does not pay off in the long run.

A low-end thermal camera can experience video degradation over time. As a result, low-quality images, inaccurate detection and maintenance calls to fix these issues can increase the total cost of ownership. As a best practice, security practitioners should implement high-quality thermal cameras with a solid track record.

Here are some factors to consider when evaluating thermal cameras:

Resolution

When considering a thermal camera, it is important to know the type of thermal core that it uses. The sensor determines the camera's resolution and, in large part, its price. After considering the options, security practitioners must determine which thermal resolution is most appropriate for their application. For critical infrastructure deployments, where cameras need to be able to detect objects well beyond the fence line, premium thermal cameras with full thermal resolution of 640x480 are a must. These devices offer up to 16 times the number of pixels as a standard thermal device, delivering greater image detail, which is crucial for analytic performance at extended ranges.

When it comes to commercial installations that need wide-area monitoring and a detection range of 50 meters or less, however, 320x240 resolution is acceptable. Developed for small to medium-sized enterprises, these thermal cameras ensure that property size and security funding are

no longer barriers to adoption. Remote storage companies and private marinas are some of the businesses now deploying thermal cameras for 24-hour wide-area monitoring and intrusion detection.

Detection Range

Long-range detection is another differentiator for high-end thermal cameras. These thermal cameras can detect an intruder before the suspect even reaches the perimeter and can send an alarm to the command center. This early detection gives security operators more time to respond.

By providing precise detection of potential threats, thermal cameras with onboard video analytics offer automatic early warning to security personnel so they can intervene before a crime is committed.

Pan-tilt-zoom (PTZ) thermal cameras, when integrated with other sensors like radar, improve tracking and threat assessment. When the radar detects a target, the PTZ thermal camera will "slew to cue" and capture video of the target's exact location. The radar will continue to cue the PTZ camera on the target so that operators can maintain a visual at all times. For security systems that must address threats that can approach from all sides, at all times, advanced thermal cameras with longer detection ranges and PTZ capabilities are essential.

Analytics Capabilities

It is one thing to detect a threat, but it is quite another to classify that threat. In the era of artificial intelligence (AI) and machine learning, superior thermal cameras are delivering sharper images that, when coupled with video analytics, are improving the way security systems operate. No longer are security cameras simple "point-and-shoot" devices. Cameras enhanced by video analytics are able to differentiate between objects like foliage, vehicles, animals and humans. By providing precise detection of potential threats, thermal cameras with onboard video analytics offer automatic early warning to security personnel so they can intervene before a crime is committed.

Integration with Advanced Sensors

At the end of the day, a thermal camera is just a sensor operating within a security system. However, first-class thermal cameras will be able to integrate with other advanced sensors, delivering a higher level of perimeter monitoring and protection. Thermal cameras that integrate with radar are prime examples. Ground-based radars use radio waves to detect moving objects. They provide continuous coverage as they conduct 360-degree scans of a property every few seconds. By deploying a thermal-radar solution, operators increase redundancy and peace of mind, since if both a thermal camera and radar detect a human crossing the fence line, the likelihood that the event is a true alarm is higher. By using information from multiple sensors, operators gain enhanced situational awareness and can prioritize events and responses appropriately.

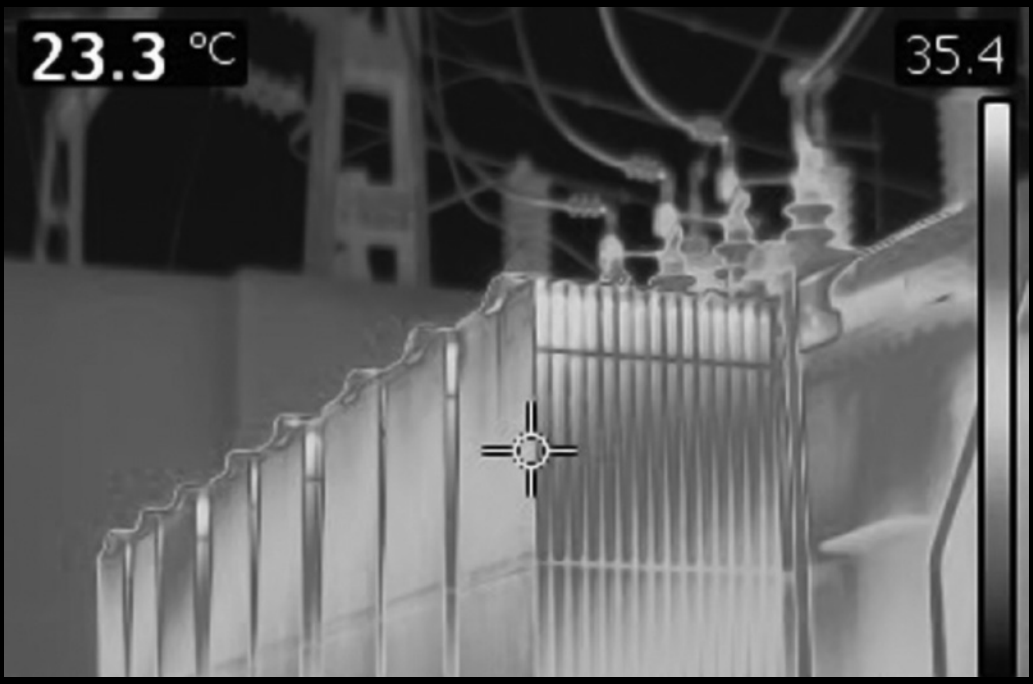
The Future of Thermal Technology

New applications and opportunities to deploy thermal cameras are growing in number every day. Thanks to new partnerships, the value of thermal is being extended beyond traditional use cases.

Utilities, for example, are deploying radiometric thermal cameras with temperature trending software so that substation operators can proactively inspect equipment and identify components that are at risk of overheating *before* they malfunction. This predictive maintenance not only reduces asset failure and the accompanying repair and replacement costs, but it also increases efficiency by reducing machinery downtime.

Utilities are deploying radiometric thermal cameras with temperature trending software so that substation operators can proactively inspect equipment and identify components that are at risk of overheating *before* they malfunction.

There has also been an increase in the number of drones equipped with



both optical and thermal payloads and deployed to sites that are difficult to access. For critical infrastructure enterprises like oil and gas refineries, where assets are housed in remote areas, drones are a viable option to improve security surveillance. The advantage of drones is that they essentially act as mobile security cameras, and when equipped with thermal sensors, they can capture clear images and improve real-time intelligence at night. When integrated with state-of-the-art security systems, a drone, upon receiving a verified alarm, can be dispatched to an area of interest to quickly get eyes and ears on scene to assess the threat. As drones continue to gain traction in the security industry as an emerging technology, the number of thermal sensors deployed with them will likely increase.

Key Takeaways

The future for thermal technology is bright. Physically securing enterprises begins at the first line of defense – the perimeter. And thermal cameras have demonstrated their value as a superior perimeter protection technology through their ability to detect and classify threats in challenging lighting and weather conditions in which other cameras simply cannot perform. Security practitioners should remember to consider quality, total cost of ownership and track record of performance when evaluating thermal cameras. Not all thermal cameras are created equal, and selecting a reliable, high-performing product is key. ■ **Back to TOC**

Fredrik Wallberg (fredrik.wallberg@flir.com) is director of marketing for security for FLIR Systems (www.flir.com).

Search the SIA Membership Directory

New possibilities for a shared customer experience and new economic models that benefit everyone are emerging.

The Sharing Economy

Integrators and manufacturers must work together to improve customer care

By Steve Wagner
Open Options

For the past 30 years, a core set of assumptions has remained the same in the security industry, despite the fact that customer expectations, economic realities, technological complexities and the availability of skillful technicians have changed.

The unchanged assumptions are that integrators "manage" and "control" the relationship with end users; manufacturers don't have any direct relationship with end users; but the manufacturer needs to provide top-notch technical support when the integrator cannot figure something out for the end user. The underlying belief is that a shared customer experience is simply not possible.

However, the changing dynamics of the security industry are challenging

these assumptions and perceptions that have prevented the industry from progressing as fast and efficiently as other technology sectors. New possibilities for a shared customer experience and new economic models that benefit everyone are emerging.

The cracks in the existing model of customer support are being exposed. The proverbial dam is about to burst.

Will this be the security industry's breaking point? Will this be the industry's much needed "paradigm shift," with a positive outcome for integrators, manufacturers and end users?

The following are defining elements of the security industry today. They must be recognized and understood before they can be improved:

- An incomplete, fragmented or downright broken customer care ecosystem for end users
- A lack of qualified talent in the industry, as a whole
- The need for more training
- An outdated financial model for customer support that is putting manufacturers at higher risk, while leaving integrators wandering, as if in a desert
- End user expectations that are fundamentally changing, including an increasing desire to see integrators and manufacturers work together more to solve problems
- Technologies that are becoming more complex
- A short-term focus that is hurting integrators more than they know

These dynamics are what is bringing the security industry to a seminal moment in its history: either a breaking point or a paradigm shift. Attempting to hang on to the old assumptions – the "us vs. them" mentality and the silos that prevent sharing – is unsustainable.

Fractured Customer Care Ecosystem

The amount of time that integrators spend contacting manufacturers to fix end users' problems is increasing. At the same time, manufacturers are kept on the fringe of the customer care ecosystem.

It may surprise some end users to know that customer care is not a commonly shared activity between integrators and manufacturers. End users may think they have unlimited support from the manufacturer of their security system, but they typically do not – unless they have a maintenance contract or pay for factory support as they go.

Historical data has shown that many integrators cannot or will not sell manufacturers' maintenance contracts to end users. The current customer care ecosystem remains built on the old assumption that services cannot be delivered jointly by the integrator and the manufacturer. The outcome is widespread complacency with less-than-ideal customer support practices that reflect poorly on integrators' reputations and perceived value.

> Integrators are drawing from a tighter pool of qualified candidates, creating more friction with the demands of end users to receive more complete customer support.

Lack of Qualified Personnel

It is no secret that the security industry is suffering from a lack of

qualified technical personnel. It is becoming harder and harder to find skillful techs who have the know-how to set up and troubleshoot access control, managed power, and security video management.

Integrators, as a result, are drawing from a tighter pool of qualified candidates, creating more friction with the demands of end users to receive more complete customer support. It also makes it more difficult for integrators to hold on to top talent. Often, a technical person joins the company, gets trained, learns from mistakes, and becomes a valuable technical support resource. Then another integrator or a manufacturer convinces the newly-minted expert to join them, leaving the integrator that trained him without his skills and talents.

Many end users are not only saying they *want* to have direct access to manufacturers alongside the integrator, but increasingly they are *demanding* it.

Consequently, the end user gets inconsistent technical support because of the stress on the customer care ecosystem and the failure to have maintenance agreements in place with manufacturers, who could supplement integrators' service offerings with product-specific support. Not every technical support person is going to be trained on every technology – the training costs are simply too high, no matter the size of the integration

business – so having access to manufacturers' resources and expertise is essential for end users.

More Training Is Needed

A solution to the lack of qualified technical personnel is more training. Organizations that provide training are creating opportunities for integrators to expand their capabilities to service customers, but a disturbing trend has emerged.

Integrators are too often reluctant to invest in training their people. Understandably, they would rather have employees out on the road generating billable hours. The de facto practice has technical personnel learn on the job by calling the help line of a manufacturer while at the customer site. But every time an integrator's technician calls the manufacturer for an end user who does not have a maintenance contract, the manufacturer and the integrator stand to lose money, potentially a significant amount.

Outdated Financial Model for Customer Support

The existing financial model for customer support is based on 20th century assumptions about integrators continuing to be the frontline service and support provider for end users. But manufacturers cannot be expected to provide full technical support when there is no sharing of revenue to cover the cost of such a value-added service.

Most end users are willing to pay for value and, as noted, they are increasingly demanding to have direct contact with manufacturers in addition to integrators. This should translate into maintenance agreements between end users and manufacturers. The

manufacturer must be allowed to sell its expertise and, in turn, share that revenue with the integrator.

End User Expectations Are Fundamentally Changing

One of the most important things that end users are increasingly demanding is the best tech support possible from the most qualified source for fixing software and hardware. Put more bluntly: End users want to talk to the factory. They may love and need their integrator, but when it comes to a problem with the product, they want to talk to the manufacturer who knows the product best.

This shift has been a long time coming and is the real fallout of the famed IT convergence. It requires bringing the most appropriate people into the customer care equation, whether from the integrator or the manufacturer. This approach to care would demonstrate true customer-centricity.

How valuable are the extra layers of support that the manufacturer of a security product can provide? Many end users are not only saying they *want* to have direct access to manufacturers alongside the integrator, but increasingly they are *demanding* it.

Technologies Continue to Become More Complex

A new level of cooperation is needed between integrators and manufacturers because of the complexities of newer technologies. Providing tech support to end users is not what it was like 20 years ago, 10 years ago, or even five years ago. The intricacies have become numerous, which is why a new customer support model is needed.

Integrators should not be expected to know everything about everything. That does not mean that they do not bring value, but when there is a problem with a product and the integrator cannot fix it, then it is time

for the maintenance arrangement to kick in. It is only fair to manufacturers, integrators and, ultimately, end users, who will be able to get the support they need from the right people at the right time.

Providing tech support to end users is not what it was like 20 years ago, 10 years ago, or even five years ago.

Short-Term Focus Hurts Integrators

Integrators may be afraid of having the manufacturer onsite because they fear that the end user's perception of the value of their services will be diminished. They are afraid that the end user will simply cut them out and just work with the manufacturer.

One of the ways that some integrators, driven by this fear, are reacting is by presenting inflated prices of manufacturers' support contracts to end users, because they do not really want the manufacturer involved. Integrators who practice this method of pricing are shooting themselves in the foot. The lack of sharing is hurting the entire industry.

Time to Share

The good news is that a solution to this problem exists, and both integrators and manufacturers can adopt and use it to the benefit of all. The solution is a shared customer care experience, which will reshape the economics of the security industry by eliminating the fractured ecosystem that operates all too commonly today.

The new shared model does not eliminate or diminish the role of integrators. Instead, it adds extra layers of support that align with the current technological realities and the expectations of end users. It is a model that fairly compensates manufacturers who provide technical troubleshooting remotely or onsite on behalf of and in conjunction with integrators.

The solution is a shared customer care experience, which will reshape the economics of the security industry by eliminating the fractured ecosystem that operates all too commonly today.

Trust is key. For the security industry to thrive over the next decade and beyond, it needs to cultivate maximum trust between integrators and manufacturers. It also needs to cultivate fairness and end user-centricity. If manufacturers and integrators are to share in the care, they must also share in the fare. ■ **Back to TOC**

Steve Wagner (swagner@ooaccess.com) is president of Open Options (www.ooaccess.com).

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

www.securityindustry.org

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