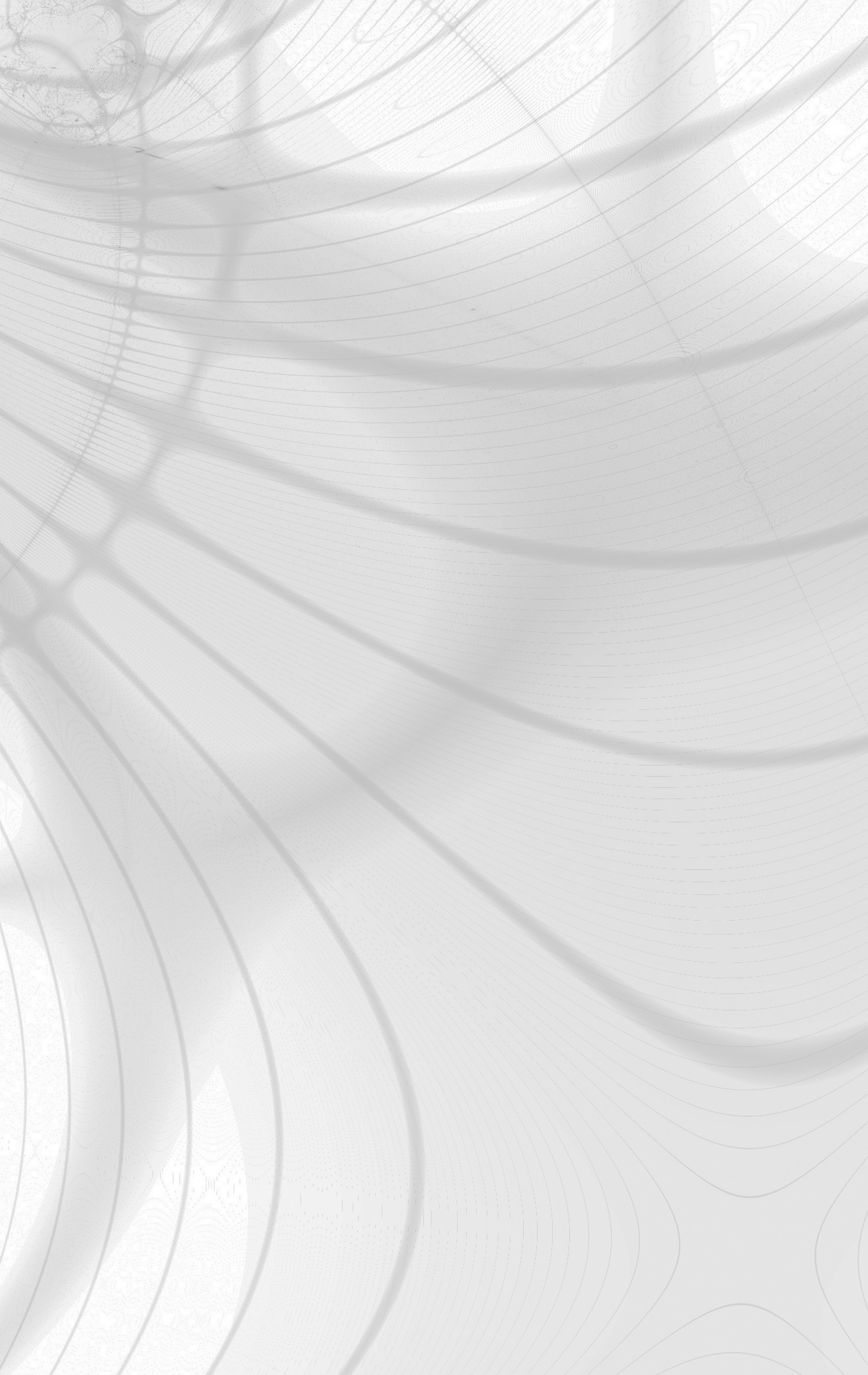
Visionary articles on security technologies and solutions from industry experts

SIA Technology Insights

www.securityindustry.org/techinsights



Welcome

Dear Reader,

Welcome to the first edition of *SIA Technology Insights*.

We have created this semi-annual publication to serve as a resource for security practitioners who are interested in the latest security solutions. The articles that follow are original, in-depth examinations of particular aspects of electronic physical security technology written by experts from SIA member companies. All of the pieces are vendor and product-neutral.

The theme for this edition is the transition to IP within the security industry. More and more security systems are going online, creating new functionality and enhancing effectiveness. This creates new opportunities, as well as new challenges in identifying the appropriate technology for one's facility. This publication will offer an exclusive look at how IP connections are shaping the industry and what this means to the end-user, with related stories on privacy, TWIC and the "greening" of security.

We hope you enjoy reading this publication and that you learn something that you can put to use within your enterprise. We encourage you to use the links and email addresses provided at the end of each article if you want to find out more about any of the topics that are addressed. Also, we would like to request that you take a look at what the Security Industry Association does by visiting www.securityindustry.org. SIA offers many opportunities for participation by end-users, from standards development to educational programs to a school safety and security committee, and we would welcome your involvement.

Finally, we want to offer our thanks to the volunteer members of the *SIA Technology Insights* Advisory Board, who have provided invaluable strategic direction; to the writers who took the time to produce such outstanding articles; to the association staff who put the publication together; and, of course, to you, the reader, for giving all of this work purpose.

Sincerely,

Jay Hauhn
Chairman, Security Industry
Association Board of Directors

Donald R. Erickson
CEO, Security Industry Association

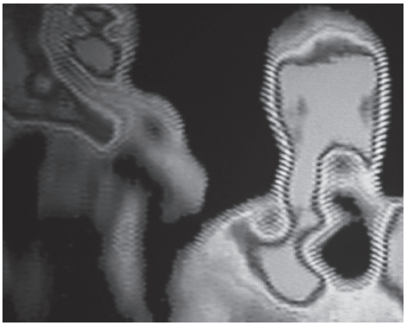
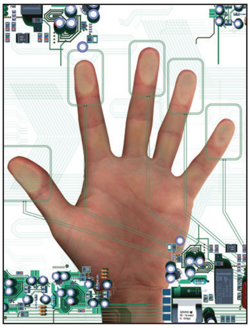


Table of Contents

Share:



What's New on the Video Surveillance Front?

A keener eye, a longer memory and a sharper IQ.

By Fredrik Nilsson

Share this Article:

When the first IP cameras hit the market in 1996, they faced a difficult uphill battle trying to gain a toehold alongside the well-entrenched analog camera market. Analog was king of the hill when it came to the surveillance industry. But over the past decade – with improvements in image sensors, lens quality and adherence to new high-definition standards – IP camera image clarity and performance caught up with and eventually surpassed its analog predecessors. Resolution jumped from a mere 640x480 pixels to a full HDTV 1080p. Advanced H.264 compression standards helped change the streaming landscape from a jerky few frames per second to a smooth-flowing, full-frame rate of 30 fps. And the standard 4:3 aspect ratio reflective of the old computer CRT was replaced by a new 16:9 ratio to complement the growing popularity of widescreen HDTV monitors.

While consumer video technology has certainly influenced development in the security sector, the two disciplines have diverged over the years to reflect the diverse needs of their audiences. The growing popularity of smartphones caused a stutter step in the seemingly insatiable demand for an ever-greater number of megapixels as consumers' attention was temporarily sidetracked by the convenience of a point-and-click, all-in-one device. Though HDTV video eventually arrived on the smartphone, its potential was somewhat stymied by limitations in lens quality and in-camera storage. Meanwhile, the surveillance industry forged ahead in designing camera imaging technology to provide the ever greater detail demanded by electronic surveillance and forensic investigations.

In the past three years, we've seen some amazing advances in IP camera technology that have begun to reshape the way security professionals approach the challenges of electronic surveillance. The main achievements fall into three categories: visual acuity, onboard storage and in-camera intelligence.

Visual Acuity: Seeing is Believing

Visual acuity refers to the IP camera's ability to mimic, and in some cases surpass, the discernment of the human eye. Multiple comparisons can be made between man and machine in the vision arena. For instance:

- **Field of View:** A human's peripheral vision extends at most to 90-120 degrees without moving one's head. An

Inside a parking garage as viewed with the naked eye.

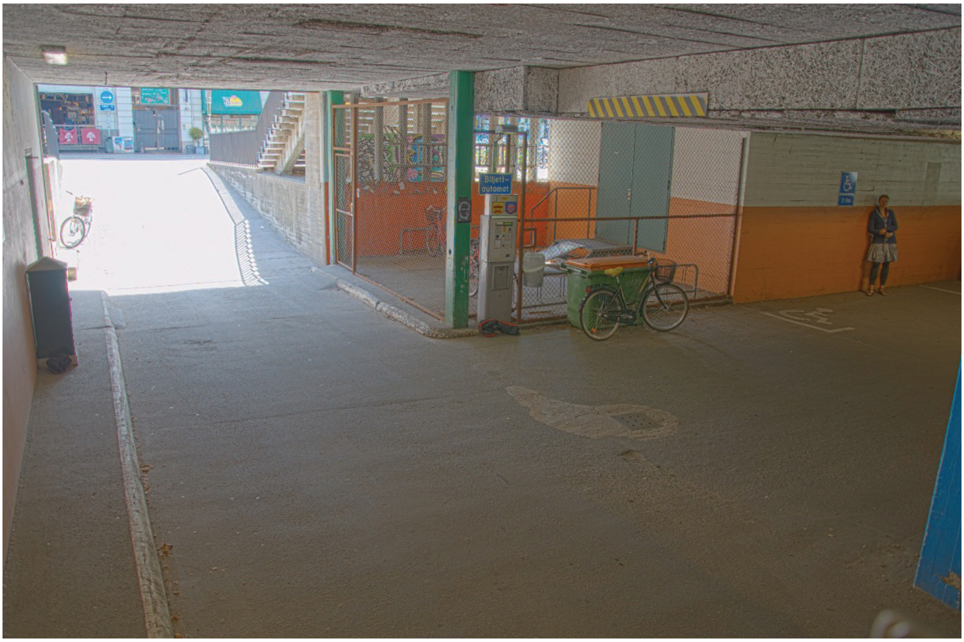
IP camera's field of view can extend to 180 degrees or, in more advanced cameras, nearly a full 360 degrees.

- **Autofocus:** The human eye can switch between foreground and background focus almost instantaneously. On an IP camera, autofocus is a mechanical operation, so the process is a bit slower. But technology is quickly catching up.
- **Pan/Tilt Speed:** A human eye can swivel 900 degrees per second. A typical pan-tilt-zoom (PTZ) camera can only manage 450 degrees in the same time span.
- **Digital Zoom:** On the other hand, an HDTV network camera can perform a 20x zoom, while the human eye is incapable of zooming at all, at least without a set of binoculars.
- **Infrared (IR) Sensitivity:** While humans cannot see into the infrared spectrum, network cameras equipped with IR cut filters have no problem capturing images in IR light.
- **Thermal Sensing:** Without light, the human eye is basically blind. On the other hand, a network camera equipped with thermal imaging technology can easily detect the heat signature of an animate or inanimate object.

While all of these comparisons are valid, I believe the major game-changers in visual acuity have been in the areas of resolution, wide dynamic range and lowlight sensitivity.

Resolution

In January 2009, the security market launched the first HDTV-compliant surveillance camera. Unlike megapixel technology, which only addresses the number of pixels in the field of view, HDTV is a standards-based



The same parking garage depicted through a WDR camera. Notice that the WDR camera clearly shows details both in the well-lit entrance and the dark shadows.

format governed by the Society of Motion Picture and Television Engineers (SMPTE) that not only guarantees resolution (720p, 1080i or 1080p), but also a 16:9 widescreen format, 30 frames per second and full-color fidelity, providing a much better overall video viewing experience.

Today, a large share of IP surveillance cameras sold in North America are HDTV-compliant, giving security professionals the same superior viewing experience and performance from their surveillance systems as they were enjoying on their home entertainment systems.

Great strides have been made in the four years since the initial launch of HDTV-compliant cameras. Today, these IP cameras come in all shapes, sizes and price points. Innovative manufacturers have even turned the aspect ratio on its side, delivering a 9:16 corridor format to provide better coverage of hallways, tunnels and aisles with high-racking shelves without wasting pixels on the sides.

The major game-changers in visual acuity have been in resolution, wide dynamic range and lowlight sensitivity.

Wide Dynamic Range

WDR incorporates techniques for handling a wide range of lighting conditions within a single scene, such as a brightly lit garage with darkly shadowed corners or a backlit situation in which a person is standing in front of a sunlit window. A non-WDR network camera would inevitably produce an image that left objects in the dark areas

barely visible. A network camera equipped with WDR, on the other hand, takes multiple exposures with different exposure times, and then creates one image with nearly uniform visibility across the field of view.

When comparing cameras with WDR, the capabilities are typically given a "dB" rating – often in the 120dB range. But the dB rating does not tell the full story. Two cameras could have the same 120dB rating, but one might be able to cope with 0.4 to 400,000 lux while the other can handle 1.0 to 1,000,000 lux. The first range is much more useful as environments with lighting in the sub 1.0 lux range are quite common. But any range over 150,000 lux is fairly useless as direct sunlight only emits around 100,000 lux.

So how does WDR work? It brings visibility to objects located in the bright and dark areas of the video frame by using several images with different exposure times. It assimilates information from all light levels in the scene at the same time, enabling users to detect and reliably identify people, objects, vehicles and activities that would otherwise be hidden from view. The caveat with using WDR technology, however, is that some lower-performance cameras might experience motion blur, additional noise or "cartooning" in the images.

The transformation of a passive eyewitness into a surveillance device that can evaluate what it sees has had a tremendous impact on both the scalability of surveillance systems and the value of the video being captured.

WDR technology addresses the problems of conducting surveillance in environments with extremely bright sunlight and dark shadows; backlit situations; and locations with a lot of reflected light, such as large picture windows in office buildings and shopping malls, entrances to buildings, tunnels and parking garages that contain wide variations in lighting, and public transit and other environments in which vehicles with bright headlights are driving directly toward the camera.

Lowlight Sensitivity

Poor lighting has always been a challenge in video surveillance applications, and, for the longest time, the best a good camera could achieve was about on par with human vision when it came to seeing any color at night. But, recently, cameras with much better light sensitivity have changed that.

Light sensitivity technology is now available that works in concert with a network camera's advanced image processing capabilities to capture high-quality, life-like color video, even at night. Highly sensitive to low light, this technology effectively allows the camera to "see" in the dark, maintaining sharp focus and accurate color fidelity from dusk to dawn, as well as in full sunlight.

Cameras with this technology are now being used to reveal the identity of ships approaching ports and to help transit authorities monitor subterranean tunnels and long stretches of track across remote terrain. And thieves looking for easy pickings at unmanned construction sites in the dead of night are being recorded in vivid detail as they attempt to steal equipment.

Today, analytics applications run the gamut from people and vehicle counting to license plate recognition and customer line management.

Onboard Storage: Saving the Day

With the price of storage continuing to drop, users are choosing to retain more video for longer periods of time on their centrally located servers. But now there is another option. Many of today's newer network cameras include slots for SD and microSD memory cards that can store from 32GB to 64GB of video, which translates to several days' worth of video recorded at full frame rate in HDTV-standard 720p resolution. As Moore's Law continues to bear fruit, driving down the cost and size of storage devices even further, it will soon be possible to store weeks and, eventually, even months of recorded video in-camera.

Greater storage capacity coupled with increased processing power opens a whole new range of possibilities for the surveillance industry, including:

- *Self-Contained Solutions:* With sufficient capacity to embed the video management system in-camera, users could avoid the cost of external storage while still being able to remotely access the onboard video directly. In outlying areas with limited bandwidth or environments hostile to sensitive computer technology, robust self-contained cameras could provide the eyes, ears and analysis of the scene as well as store any forensic evidence of activity.
- *Redundancy for Network Outages:* With greater storage capacity in-camera, manufacturers will be able to offer a level of fault tolerance for network outages previously unattainable, even for applications that require high resolution and real-time recording rates. Cameras now contain the intelligence to detect an outage and automatically begin storing images in-camera until

the connection is re-established and video can once again be streamed over the network. This is especially valuable in casinos, security lines and airport exits where coverage is mandated by law and any loss of video would incur stiff penalties.

In-Camera Intelligence: Analyzing the Situation in Real-Time

With processing power doubling every 18 months in accordance with Moore's Law and memory capacity continuing to expand, intelligent analytics previously relegated to the video management server are now being performed in-camera. Analysis of video inside a camera (also referred to as "at the edge") enables access to uncompressed video – with all of the image details intact – and allows for more accurate analytics.

The transformation of a passive eyewitness into a surveillance device that can evaluate what it sees has had a tremendous impact on both the scalability of surveillance systems and the value of the video being captured. Shifting more intelligent applications to the edge not only saves bandwidth consumption, storage and central processing costs, but it also allows security professionals to process events and alerts in real-time. This can trigger more immediate searches for suspect activity and increase the likelihood of resolving incidents more quickly, turning electronic surveillance from a reactive to a more proactive operation.

The earliest analytics to migrate to the camera were motion, tampering and cross-line detection. But with many camera manufacturers supporting an open application platform, a number of third-party software developers have added to the in-camera analytics portfolio. Today, analytics applications run the gamut from people and vehicle counting to license plate recognition and customer line management.

With ever-greater processing power being allocated to in-camera applications and the need for proactive surveillance tools increasing, it won't be long before a variety of intelligent applications are developed and downloaded to the edge.

Keeping Responders out of Harm's Way

Advances in image processing, light sensitivity and on-board storage continue to push the boundaries of our surveillance camera expectations. In the past three years alone, we've seen quantum leaps in resolution, performance in low and variable lighting conditions and onboard video storage and intelligence. And all of these achievements have enabled network cameras to take on a more vital role in analyzing, managing and acting on events within their security systems.

But the true importance of this accelerated rate of improvement harkens back to why we deploy video cameras in the first place. The ability to monitor environments from a remote location doesn't just allow security departments to simultaneously cover a broader expanse of territory without expanding foot and vehicle patrols. It actually protects the human element from harm. By providing exceptionally clear situational awareness and analysis, cameras give security professionals and law enforcement the opportunity to formulate an appropriate response rather than going into an incident blind.

Back to TOC

Fredrik Nilsson (fredrik.nilsson@axis.com) is the general manager of Axis Communications in North America (www.axis.com). He serves on the Security Industry Association Board of Directors. He has more than 15 years of experience with IP video systems and is the author of Intelligent Network Video: Understanding Modern Video Surveillance Systems*, published by CRC Press.*

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

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

By John Romanowich

Share this Article:

Smart thermal cameras are increasingly specified and deployed in mainstream network surveillance applications for outdoor security. Outdoor security systems are the first line of defense for the protection of people, facilities and assets, and smart IP thermal cameras provide the awareness around a facility's exterior that is necessary to meet critical security needs. This article will discuss the advantages offered by smart IP thermal cameras and how they have come to be the breakthrough technology solution for securing outdoor assets.

Enhancing Information with Analytics

Thermal cameras have always been a good choice for nighttime surveillance applications because they are able to "see in the dark," protecting areas where lighting was unavailable or too costly to deploy. However, today's smart IP thermal cameras bear little resemblance to solutions of the past. Recent advancements in the sensitivity of thermal imagers, combined with sophisticated image processing have expanded the usefulness of IP thermal cameras from their traditional role as "night vision" cameras to 24-hour security solutions. When combined with video analytics, today's IP thermal cameras offer real-time, pre-emptive security with instant notification over the IT and mobile network about security violations as they occur.

The image quality of smart thermal cameras has also been addressed through increased image processing. Thermal cameras now present a very clear, detailed image, even in low-contrast situations such as fog, rain and humidity, while overcoming "white-out" problems once caused by bright sun. Objects that once blended into the background because of outdoor conditions are now revealed, details are clearer at greater ranges, and the results are particularly striking in hot weather during the daytime. Thermal cameras now provide detail approaching black-and-white video instead of the blurrier images once associated with the technology.

In the past, sophisticated thermal security solutions were typically deployed to protect

large critical infrastructure, where a disruption in operations would have a serious economic impact. However, as smart thermal cameras with on-board video analytics fall to the $5,000 price barrier, the technology now makes sense in both critical and less mission-critical environments. In fact, one of the most fundamental security functions – theft prevention – can now be addressed economically using the same sophisticated thermal camera solutions. Applications include preventing copper theft at electric substations, securing equipment at maintenance yards, protecting car lots, securing the millions of oil and gas wellheads in use, and other areas where theft prevention remains a key objective.

Historically, the approach for these applications has been to use a "blind" sensor such as coax on the fence acting as an intrusion detector, which required augmentation by a camera to determine the cause of the alert. These systems were not fully effective because the sensors would generate many nuisance alerts, and they were costly because they involved the use of two separate systems – a sensor system and a video system. Thermal detection cameras offer a key functional advantage over these traditional solutions because thermal cameras simultaneously detect and "see" an alarm event, providing instantaneous validation for prompt action. The result is a viable, single-technology solution that reduces costs for securing and monitoring assets and facilities around the clock.

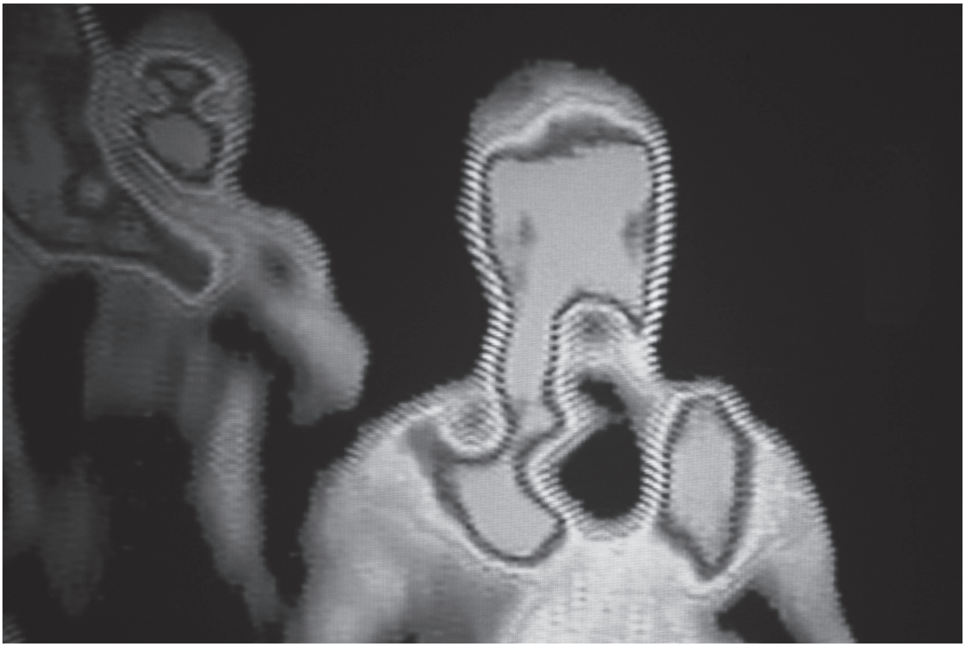
The Role of Image Processing

Placing significant processing power inside the camera itself is the key to overcoming outdoor challenges, making outdoor video detection both accurate and cost-effective and providing true pre-emptive awareness around a secure area. Importantly, this image processing is performed in advance of the analytics, a critical first step for making outdoor video analytics accurate and reliable. For example, the processing first electronically stabilizes the image to eliminate camera motion as a source of nuisance alerts. Objects such as trees and leaves that flap in the breeze can create the appearance of an intrusion, unless properly addressed with image processing. When you add in snow, rain, humidity and dust, such a dynamic environment can create an overwhelming amount of false alerts for thermal detection cameras that lack the image processing to compensate for such conditions.

How Thermal Cameras Work

Thermal cameras operate by "seeing" heat energy from objects. Because thermal cameras see heat rather than reflected light, thermal images look very different than what's seen by a visible camera or the eye. In order to present heat in a format appropriate for human vision, thermal cameras convert the temperature of objects into shades of gray that are darker or lighter than the background. On a cold day, a person stands out as lighter because they are hotter than the background. On a hot day, a person stands out as darker because they are cooler than the background.

Thermal imagery is very rich in data, sensing temperature variations down to 1/20th of a degree. Thermal cameras must convert these fine variations – representing 16,384 shades of gray – into about 250 gray scales to more closely match the capability of our eyes to decipher them. In the past, most thermal cameras converted this data in a simplistic way by mapping gross areas together that are close in temperature. This is why thermal images from cameras that do not use sufficient image processing can often look blurry, lack detail and fail to reveal intruders under some conditions. Such lack of image clarity can reduce security effectiveness. Security personnel who have to view blurry, undefined video can become fatigued and confused by images that are not as informative as they would be with



daylight cameras. New thermal cameras now provide the necessary detail to make security applications reliable and accurate.

Additionally, greater processing can offset the effect on image quality that results from thermal loading, which occurs during the day when darker objects absorb the sun's energy and heat up. Because of thermal loading, as well as humidity, rain and other conditions, targets can become very close in temperature to the background. Image processing enhances contrast to make sure the camera can discriminate the target from the surrounding environments. When using video analytics, this additional contrast avoids miss-detects, which is a bigger problem than nuisance alerts.

Providing More Actionable Information

Smart, cost-effective thermal cameras open up a whole new world of understanding what is happening outdoors beyond security, from early detection scenarios to looking at behavior that increases a company's operational efficiency. For instance, a company could use a thermal camera to determine if there is a leak at a refinery, or if transformers are overheating at a power station, or to monitor storage tank levels. The possibilities for thermal cameras extend to highway safety, measuring parking area occupancy, measuring the volume of vehicle traffic, or automatically determining if a car is driving the wrong way on an on-ramp or road. New return-on-investment scenarios and greater functionality now make smart thermal cameras a perfect technology tool for such applications.

A Cost-Effective Security Solution

Smart IP thermal cameras may seem like a high-tech solution, but the economics of these systems have become very cost-competitive. The economic advantage of newer outdoor thermal imaging really becomes clear if you examine the "per-foot" costs of securing a perimeter. While many manufacturers do not present their pricing in this way, the costs can be calculated, and the results are motivating a wider range of customers to adapt this security approach. Thermal analytic camera systems are now available at an MSRP as low as $10/foot, making the most accurate perimeter security technology comparable in price to traditional visible cameras with analytics, fence sensors, or buried cable systems.

Additional economic advantages are realized through the longer ranges that smart thermal cameras are able to detect, exceeding 600 meters in some cases. Longer-range cameras require fewer poles, power and communications, reducing infrastructure needs proportionally. Consider, too, that a significant manpower advantage is realized when operators become more effective by receiving accurate alerts automatically over the network, allowing system scalability, along with a greatly diminished false alarm/nuisance alarm rate.

Thermal network cameras perfectly complement and complete an outdoor security system, making sure that objects, intruders and incidents are detected 24 hours a day, seven days a week, to keep your people and assets safe.

Back to TOC

John Romanowich (jromanowich@sightlogix.com) is the president, CEO and founder of SightLogix (www.sightlogix.com). He serves on the Security Industry Association Board of Directors and chairs SIA's Perimeter Security Working Group. He is also a member of RTCA, which is focused on airport perimeter security standards.

Video Analytics in the Modern Security Industry

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

By Brian Karas

Share this Article:

We hear a lot about "video analytics" these days. It comes up in vendor pitches. We see references to it on a wide variety of cameras. There are companies that concentrate primarily on building a video analytics product of some sort and other companies that offer video analytics for "free." After the Boston Marathon bombing in April, references to video analytics seemed to be everywhere, yet, in the end, it was acknowledged that few current technologies could offer any real benefit in that situation, or in similar scenarios.

The term "video analytics" is widely used to refer to some sort of computer algorithm or process that attempts to extract information from a data stream of video frames. Most video analytics products work in "real-time," meaning they process video as it happens and look for particular objects, generally people or vehicles, in the field of view. Other products take recorded video and attempt to process it down so that an operator can see only the times when there was relevant activity. This can reduce investigation times, or let an operator spot trends (like a person returning to a given area every two hours) that might not be obvious by just casually watching the live or recorded video.

Much like the term "CCTV," "video analytics" can be interpreted to mean a lot of different things. Phrases like "motion detection" or "advanced motion detection" also come into play and can confuse potential users of the technology. Developments over the last few years have started to provide some more clear differentiators between "analytics" and "motion detection."

Motion detection, or advanced motion detection, is a low-level technology often found for free in a variety of cameras, or sometimes as a software add-on to a video management system platform. Systems based on motion detection will lack a true understanding of the geometry of the scene they are observing. The operator may have some coarse filters like "percentage of movement" or "object size" to try to limit the things that cause the motion detection to trip an alarm or initiate a recording, but, in the end, these devices have very limited applications, especially in outdoor scenes where there is a lot of random motion. Motion detection is not video analytics, though it can be useful for simple tasks, such as reducing recording

detail during times of inactivity in the scene. Also, in a simple indoor camera with an evenly lit scene, motion detection might work well enough for alerting to an intruder, since there would typically be no motion at all in such an environment.

True video analytics devices will have an ability to understand the rough layout and perspective of the scene they are watching. This is usually done by calibrating the system, a process that often involves the installer taking measurements of key areas and then programming those measurements into the system. Some analytics systems have the ability to self-calibrate, which allows them to determine the layout of the scene simply by observing activity. A self-calibrating system is the ideal case, but this level of capability is still somewhat rare to find.

Once the system is calibrated, it understands that a person is going to be 800 pixels tall, for example, in the front-right quadrant of the video, and only 90 pixels tall in the rear-right quadrant. These calibration points allow the algorithms to understand key elements of the scene, like the location of the ground-plane, and any tilt of the horizon. For a manually calibrated system, it may be necessary to check or reset some of the calibration points throughout the year to maintain accuracy.

Real-time analytics are most often used in environments where the user wants to be notified of objects and activities that pose a threat. The most simple example would be a person entering a secured area outside of normal business hours. The ability of a system to differentiate a person from an animal, or from a tree blowing in the wind, is a critical requirement in an application like this in order to keep false alarms to an absolute minimum. Different systems will detect this unauthorized activity in various manners. Some may use a kind of "video trip wire," in which the operator sets a boundary line and the system looks for objects crossing that line. Other systems will have the operator define an "area of interest" and will look for persons within that area after hours. These applications are usually referred to as "perimeter protection" deployments, and are among the most common applications of video analytics. By receiving alerts in real-time, the user has the ability to call the police or send on-site guards to prevent small crimes from becoming large losses. In modern perimeter protection systems, the ability to analyze the scene and spot rule violations is a capability embedded within a camera or encoder device, requiring no external resources (other than a platform to route alert events to). This makes these systems very adaptable to a variety of environments.

Another use of real-time analytics is for business intelligence. In this case, the operator is less concerned about a violation of a specific rule and more concerned about what people (or vehicles) do in a given environment. Retail stores are large users of business intelligence analytics, gathering data on the paths shoppers take through the store, or around which display shoppers have stopped to browse for, say, more than 15 seconds. Many retail chains use video analytics to detect if checkout lines are too long or are moving too slowly, so that backup cashiers can be called to the front of the store. Many times, a business intelligence video analytic will be coupled to data from the point-of-sale system, so that things like the number of shoppers and the average receipt total can be computed. Analytics platforms that concentrate primarily on business intelligence will sometimes also have the ability to identify the gender, approximate age, and even ethnicity of shoppers. For the highest level of accuracy, this requires higher-resolution cameras, placed so that a clear view of the faces of shoppers can be obtained. Though not entirely common yet, there are some companies embedding cameras into store mannequins for this purpose. Business intelligence applications can also include vehicle traffic monitoring. In these cases, municipalities might be interested to know about traffic patterns, times of highest traffic density, or ratio of large trucks to motorcycles in an area. Data gathered from business intelligence analytics is used to better design store layouts, stock popular products, or design new roads and intersections. In most of these systems, the cameras will have the ability to differentiate objects from each other and will report the location and appearance of these objects to a back-end server, which then stores the information and correlates it into various reports (e.g., the number of red trucks traveling south, the number of female shoppers that walked past a display without stopping to look at the items).

In modern perimeter protection systems, the ability to analyze the scene and spot rule violations is a capability embedded within a camera or encoder device. This makes these systems very adaptable to a variety of environments.

Generally speaking, an analytics vendor will usually specialize in either perimeter protection or business intelligence applications. Rarely will one vendor cover both scenarios fully. This is because of the specifics and requirements of each application.

In perimeter protection applications, incidents recorded by the system are usually routed to a guard or property manager. False alarms in these cases can be very costly if they flood the guard with nuisance alarms. For this reason, a good perimeter protection system will be adapted to ensure that only true people or vehicles generate alarms. Also, less effort will be dedicated to the granular counting of objects. Four people entering a secure area is the same basic threat level as three people or five. So resources are spent on ensuring that these moving objects are actually people, and not so much on exactly how many people are present. In a perimeter protection application, a single camera can cover an area of a half-acre or more, and with these fields of view, it is not always possible to see every individual person in a group clearly anyway. For perimeter protection setups, the cameras are usually mounted about 12-15 feet above ground and set up to look down large swaths of fence-line – some systems can cover 1000 feet of fence with a single camera – or across vast areas of property. As you might imagine, a group of four people at a 500-foot distance from the camera might appear such that only two of the four people are clearly distinguishable. Very few users would say, "Two people entering my property after hours is OK, but four is certainly a problem." Rather, *any* person entering after hours is a threat that needs to be evaluated. Thus, determining the specific number of trespassers is a task better served by the guard than by the technology.

An analytics vendor will usually specialize in either perimeter protection or business intelligence applications. Rarely will one vendor cover both scenarios fully.

Business intelligence applications are concerned with specific counts and accuracy of the data gathered. In these applications, the user will typically expect accuracy rates of 90 percent or higher. Counting four people as three or five is a big problem and is generally unacceptable for the purposes of business intelligence. A single camera in a business intelligence application will usually only cover a relatively small area, such as entry/exit doors, or the general area around a store display or a cash register line. In an indoor example, false alarms – or, rather, really wrong classifications, because we are not generating alarms – become a reduced issue. Almost everything moving is going to be a person, so only minimal filtering to exclude nuisance objects (such as shopping carts) is needed. For a business intelligence deployment, cameras are often mounted so that they have a mostly overhead view of the areas they are looking at. This prevents things like store displays from obscuring the camera's view and also allows the greatest opportunity for accurate counting. Four people moving in a small group (like a family shopping together) will still have some amount of spacing between the individuals, and this will be most apparent in an overhead view. The requirement to get clear shots of displays and maintain higher accuracy in counting will limit the size of the area that a single camera can cover. This often works to the benefit of the analytics algorithms, because people will appear relatively large in the field of view, making it easier to set up basic size filters to exclude objects that we don't want to count or analyze.

The ability to look for different actions, or behaviors, can sometimes be a differentiating factor between various vendors. Many systems can, at a minimum, look for:

- Line crossing
- Object present in region
- Object loitering in region
- Object moving in a prohibited direction

The "object" in these cases can usually be a person or a vehicle, or both at the same time. Time-of-day and day-of-week-based rules are standard, and the more advanced systems can analyze multiple regions of the image for behaviors or actions simultaneously.

Because many systems have advanced to the point of being able to differentiate objects accurately in their recommended use cases, the list of "behaviors detected" can sometimes be used, or over-promoted, as a key decision factor. This is where many analytics vendors have earned a bad name, by suggesting that things are possible that are well outside the realm of reality.

By far, one of the most common examples of something that simply isn't possible in a practical sense is determining a "left object." Following the Boston Marathon bombing, discussions of the object-left-behind use case have skyrocketed. Understanding why this isn't feasible requires a little more background regarding what makes video analytics valuable and reliable, and what the limitations of the technology are.

The best analytics systems available today (or in the foreseeable future) are not about the systems' ability to spot things an operator would miss, but, rather, their ability to perform this task tirelessly and consistently. Analytics algorithms are very good at finding objects that fit set appearance patterns. People are a good example of this. Even though 100,000 people in a crowd will likely all have unique appearances, they will also share a lot of common traits. Movement styles, aspect ratios, average heights and so forth will be within a relatively small range across the entire crowd. It becomes somewhat easy to spot a "person" or ignore foliage movement or shadows when the system knows what patterns and key identifiers to look for. A "threatening object," however, could take on almost any appearance. It could be a backpack, a box, a soda bottle tossed aside, or any number of other forms. Trying to look for these objects would not only overwhelm the system, it would require that the camera count be increased by an order of magnitude. In order for any object to be recognized or identified, the analytics algorithm needs to first see the object. You cannot consistently make accurate decisions by having 100 pixels on something that could be either a bomb or a cupcake. If the system cannot make reliable decisions, its value will be eliminated. Generating continuous false alarms, or missing valid threats, is going to cause the operators to lose trust in the system. Also, in most cases, a supposed left object will be obscured by other activity in the scene, further reducing a system's ability to spot it with any reliability.

Analytics are not going to be a wholesale replacement for guards, but they can make those guards much more effective in their duties.

We should not expect analytics to perform tasks that a trained operator could not perform, such as matching blurry faces together, or spotting the one person in a crowd of 10,000 who is acting "suspicious." We can expect analytics to look for high-level things and to do so without pause. Video analytics, in this case, is often referred to as a "force multiplier." It can call certain things to an operator's attention for greater scrutiny, or it can eliminate the need to have operators watch secured areas that should be void of activity, freeing personnel to instead concentrate on looking for the more nuanced things that analytics cannot spot. In other words, analytics are not going to be a wholesale replacement for guards, but they can make those guards much more effective in their duties.

In regard to non-real-time applications, there are a number of products that can "distill" video down to just the most interesting events. Again, like real-time analytics, there are simple systems, which just look for motion, and true analytics systems, which have the ability to model the scene to determine the background from the foreground. A post-processing analytics application will almost always run as a server application-style deployment. It will often do some analysis in real-time, "tagging" certain objects and events to make future post-processing easier. When called into action, the operator feeds recorded video to the system, either by allowing it direct access to stored video, or by extracting/exporting video from a storage appliance and then uploading it to a location where the software can access it. This selected video is then processed so that the background (essentially any static objects or areas in the scene) can be modeled, and then activity within the scene is pulled out separately. The activity can be played back in a layered fashion, allowing the operator to adjust things like time compression (e.g., one minute of video playback might represent one hour of real time) and object density within the scene (how many objects appear at a time, or, in some cases, what kinds of objects are displayed). These analytics platforms can be very helpful when operators need to review video of an incident or of a time period leading up to an incident. The rapid playback and ability to adjust what is flagged in the scene massively reduces the time spent scouring through recorded video. In most cases, these types of analytics applications are not trying to spot any particular activity or action; they just make it easier for human operators to review lots of video without missing critical events.

Choosing the right technology and approach for a given application hinges on understanding what is expected of the system.

In many cases, analytics-based deployments will require a certain amount of pre-planning on the installer's part.

In many cases, analytics-based deployments will require a certain amount of pre-planning on the installer's part. If a direction of travel type of alert is going to be utilized (to track people trying to enter a building through an exit gate, for example), it would be most effective to position the cameras so that the people move perpendicular to the camera's alignment, that is, walking right to left or left to right, instead of directly toward or away from the camera. This makes the movement more apparent and allows the system to react faster. A fully effective analytics-based system is going to be highly dependent on the quality of the system design and installation, as the algorithms can only process what they "see," and better quality video input will tend to lead to better quality, and more accurate, data output.

Back to TOC

Brian Karas (bkaras@videoiq.com) is the vice president of global sales and support for VideoIQ (www.videoiq.com).

The Untapped Benefits of Recorded Video Surveillance

Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing this data possible.

By Rafi Pilosoph

Share this Article:

Gregson: *If you're right, that means every guest that she ever blackmailed is a potential suspect in her murder.*

Holmes: *Correct.*

Gregson: *Said you found a couple of thousand hours of footage?*

Holmes: *The cameras were on 24/7. Unfortunately, there were no time-stamps or references on the videos.*

Gregson: *Which means it will probably take forever to identify the guests who performed blackmail-worthy acts on tape. [Sighs] I'm going to need teams working on shifts to get through it all. It's going to take days.*

Holmes: *Not necessarily.*

Scene from the CBS show* Elementary, *Season 1, Episode 11

On television, ace detective Sherlock Holmes stays up all night to watch the endless hours of video bemoaned by Capt. Tobias "Toby" Gregson of the New York City Police Department. In reality, only a fictional genius like Holmes would have the powers of concentration required to accomplish this feat. In real life, most recorded video isn't watched at all. This fact raises questions about the value and effectiveness of CCTV. Questions such as: What's the point of video recordings if there aren't enough eyes to review it?

The Challenge

Let's analyze some hard facts facing security professionals by taking a look at the city of Chicago, where more than 10,000 surveillance cameras are deployed around the city and in the schools, according to published reports, with the goal of increasing the safety and security of its citizens.

"People want these cameras in their neighborhoods," former Chicago mayor Richard M. Daley told *The Wall Street Journal* in 2009. "We can't afford to have a police officer on every corner, but cameras are the next best thing."

While this may be true, just installing these cameras and recording video isn't enough to do the job. Someone needs to watch the video, either in real-time or following a reported event.

Those 10,000 surveillance cameras operating 24/7 will generate nearly a quarter-million hours of video every day. While some of this footage may be reduced by using solutions such as motion detection, this amount of video is still too vast for real-time monitoring. "But each time a citizen makes an emergency call," *The Wall Street Journal* reported in that 2009 article, "which happens about 15,000 times a day, the system identifies the caller's location and instantly puts a video feed from the nearest camera up on a screen to the left of the emergency operator's main terminal."

Nevertheless, the task of investigating those cases after they happen and preparing court cases is monumental. On average, each one of those 15,000 daily cases will contain 16 hours of video that will need to be reviewed. Even if only 1 percent of the received calls require review of video, that's still 2,400 hours to examine, requiring 300 video investigators working full time, not to mention the additional five to six hours required, on average, to prepare a court case. So this approach would be impractical. Unless you have a Sherlock Holmes on staff, the cases begin to pile up and the backlog of investigations requires, to paraphrase Capt. Gregson, teams working for days.

As Holmes indicated, though, there may be another, better way.

The Solution

Video content analytics can be a practical solution for detecting pre-defined unusual behaviors or facilitating video search in post-event investigations. However, there are many behavior patterns, both innocuous and suspicious, that defy definition by algorithm. Police video investigators very often cannot describe what it is that they are looking for. They will tell you, "I'll know when I see it."

Another solution, video synopsis, has a different approach. Instead of filtering out events, it presents all of them to the viewer, but in an extremely efficient way. The award-winning innovation, which was invented at the Hebrew University of Jerusalem, is based on a sophisticated algorithm, which allows operators to "browse hours in minutes" by creating a summary of the original video for rapid review that is indexed back to the original.

Using video synopsis, review time is reduced to an average of 1/60th of the original, meaning that one hour of video can be viewed in one minute, but all of the events from the original video are retained, and access to the original itself can be executed in a single click. When the reviewer decides to focus on a certain area (or areas) in the frame, those areas can be marked by defining an "area of interest" (AOI), further reducing the review time to as little as 1/300. Going back to the Chicago example, the amount of video to be reviewed can be reduced from 2,400 hours to 40 hours, a task easily completed by five investigators.

How Does It Work?

Video synopsis tracks and analyzes moving objects and converts video streams into a database of objects and activities. When a video summary is needed, all objects from the requested period are collected and are shifted in time to create a much shorter synopsis video showing maximum activity. A synopsis video clip is generated, in real-time, in which objects and activities that originally occurred in different times are displayed simultaneously on the same video frame, while maintaining the sequence of events so the reviewer can follow the actions in the scene.

The Technology

Video synopsis technology combines a visual summary of stored video with an indexing mechanism. It enables substantial shortening of surveillance video through the simultaneous display of events that occurred at different times.

The process begins by applying a motion detection algorithm to detect and track all objects in the video. Each object is represented as a "tube" in the "space-time" of all the video frames in which it appears. All objects are then stored in a database in approximately real-time.

Following a request to summarize a time period, all objects from the selected time are extracted from the database and are shifted in time to create a much shorter summary video containing maximum activity.

Real-time rendering is used to generate the summary video after object re-timing. This allows end-user control of the number of objects/events in a frame (event density) and the speed at which they appear. The user can choose to focus on a specific area in the frame, such as an entrance to a building. This is done by defining an AOI, which, in turn, generates a newly rendered synopsis in real-time that ignores all of the objects outside that area. The result is an even shorter synopsis that can squeeze an hour of video into a synopsis of a few seconds.

Different Users, Different Solutions

Not all users are the same, of course. Some need to review video rapidly in order to take action quickly. Others conduct thorough post-event investigations, searching for evidence for days, weeks and even months after the fact.

Identifying various use patterns and differentiating between the needs of the security officer monitoring the video screen in real-time for the purposes of immediate incident response and the post-event investigator conducting an in-depth analysis has resulted in several solutions that can provide video synopsis functionality to all user types.

By using an "on-demand" mode, security officers can immediately receive synopses of the last few minutes from any selected cameras. Within seconds, they are able to locate the event of interest, index back to the original video and respond to the incident in real-time.

Post-event investigators can use video synopsis not only for reviewing forensic video but also as a proactive tool to look for potentially related incidents. The time to conduct post-event investigation, court case preparation and other examinations is cut considerably. The solution also maximizes the return on the investment in cameras and video recording systems.

Real-World Examples

How is this technology being implemented in the field? Here are a few examples:

- **On-Demand Investigation:** On-site investigations often require reviewing hours of video to determine the exact location of events. Using video synopsis, activity patterns can be revealed on the spot. For example, a police investigative unit could use the technology to quickly review crime scene videos in order to determine the best places to dust for fingerprints.
- **Post-Event Investigation:** A computer was reported stolen from a booth at the ASIS 2010 security trade show in Dallas, Texas. Using video synopsis, security officers were able to review 10 hours of video from the previous night in minutes. The culprits – a ring of thieves within the night cleaning crew – were spotted on tape and questioned that same evening. The suspects confessed not only to one crime but to a series of thefts from previous trade shows.
- **Risk Management:** A store customer filed an accident claim, stating that she had bumped her head on a fixture that had been hung too low. Ordinarily, the store would have simply paid her damages rather than risk a lawsuit or spend hours of valuable time on video review. In this case, though, security officers used video synopsis technology to review hours of video in minutes, locate the alleged accident and prove, without a doubt, that the woman had inflicted the wound on herself. The claim was withdrawn.

The Benefit and the Payoff

So this article's original question of "Why record video if it goes unwatched?" no longer has to be asked. The information obtained from the process of proactive "total video review" that is now possible enables security personnel not only to review unusual events and investigate after the fact, but also to use surveillance video in a preventive capacity, something that, up until now, was completely impractical. This will release the untapped power of video, exploit the investment in cameras and recorders, and turn video into the powerful tool that it was intended to be.

Back to TOC

Rafi Pilosoph (rafi.pilosoph@briefcam.com) is the vice president of marketing and business development for BriefCam (www.briefcam.com).

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

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

By Christopher Peckham & Walter Frasch

Share this Article:

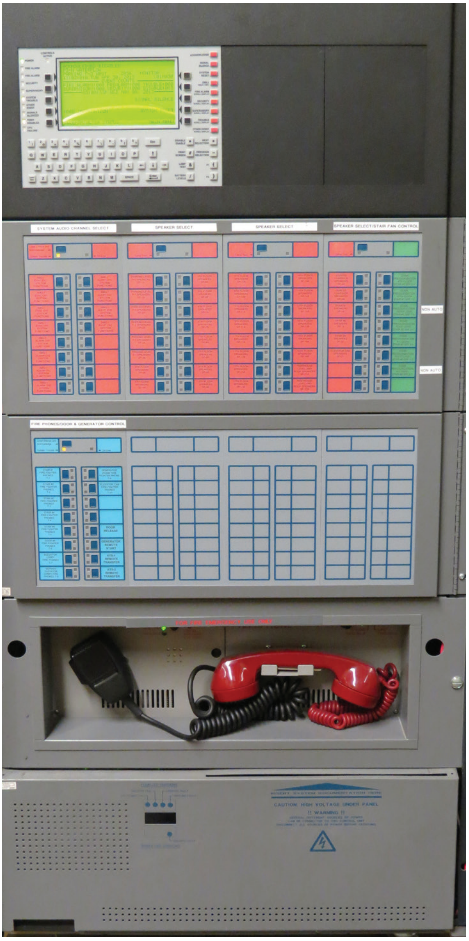
As network-based solutions have become more prevalent across the business landscape, many markets have experienced a shift toward more IP-based products. The fire and life safety market is not exempt from these changes. Since these systems affect life safety, however, they are regulated in a way that other systems in building automation and physical security are not. These regulations are currently preventing the deployment of fully IP-based fire and life safety systems. But some changes occurring in the telephone industry are forcing a more modern approach to connectivity for these systems. Emergency communication systems, which include both in-building and wide-area mass notification systems, are being developed and deployed using digital techniques and IP networks. These systems are integrated with fire alarm systems that may have fire emergency/voice alarm communication systems installed to allow announcements to be made across an organization when appropriate. As additional IP-based systems become part of the normal deployment of fire and life safety systems, changes to the codes and regulations will be made.

Christopher Peckham (left) and Walter Frasch

Physically Separate Parts

Fire alarm systems do not need to stand alone within a facility and can be integrated with other systems in a specific manner. Since these systems directly affect life safety, they are regulated by codes and standards such as NFPA 70, NFPA 72 and UL864. As defined in "NFPA 72: National Fire Alarm and Signaling Code," a fire alarm system has three physically separate parts: an initiating device, a fire alarm control unit, and output functions. The initiating device is a component such as a smoke detector, fire alarm pull station or sprinkler system monitoring device. The control unit that receives signals from initiating devices or other control units is known as a fire alarm control unit (FACU). Based on the various inputs received by the FACU, a decision is made regarding which of the fire alarm output functions should be activated. The output functions include notification appliances (e.g., horns, strobes, speakers transmitting automated messages), fire suppression system activation (e.g., clean agent systems, pre-action or deluge sprinkler systems), security and fire door release, elevator control, stair pressurization, smoke control systems, and transmission of signals to a supervising station.

Multiple telephone providers are planning to eliminate POTS service. As this occurs, a replacement communication method will need to be deployed.



An intelligent addressable fire alarm control panel (FACP) or FACU is one type of fire alarm system that is in wide use today and is the main control unit of a fire system. It is used to integrate the elements of that system with other building systems. The input and output devices are connected with a signal pair of wires in a configuration known as a signaling line circuit (SLC). With an intelligent addressable system, each input and output device has a unique identifier, and the system can be configured to respond to and control each device individually. Many of these intelligent addressable systems use software algorithms to respond to varying conditions that are reported to the system by detectors in the building. Based on these conditions, the system can make decisions as to what might be causing changes to the status of the detector (e.g., an actual smoke condition or a buildup of dirt in the detector over time). Addressable devices also enable staff to quickly identify the location of an alarm or other event and respond accordingly.

Depending on the information being received from detectors or other contact-type input devices, the FACU is configured to send commands to output devices such as alarm notification appliances, fire and security door-releasing equipment, and other output devices in the system. While intelligent addressable systems are more expensive to install, they can have lower maintenance costs. Initiating devices are in contact with the panel on a regular basis, updating their status. If there is a problem with a unit in the field that requires maintenance, the unit with the problem is reported to the panel and can be addressed as necessary.

The connectivity between initiating devices and the FACU is not performed using an IP network. Currently, the NFPA does not allow IP connectivity to be used in this manner. However, some manufacturers do use IP connectivity to connect between distributed control panels and display systems. Other vendors have IP connectivity to the FACU to allow for monitoring and integration with other software systems.

Connectivity to the Central Station

In the past, the fire alarm industry has used the Public Switched Telephone Network (PSTN) that provides Plain Old Telephone Service (POTS) lines as the primary connectivity between a protected premise and the remote monitoring stations. However, multiple telephone providers are planning to eliminate POTS service. As this occurs, a replacement communication method will need to be deployed.

While IP communications meet NFPA code, some authorities are resistant to supporting their implementation.

Many fire systems being deployed today are using Voice over IP (VoIP) or are connected directly to the central station using TCP/IP. IP networks are very mature and have been proven to be robust and reliable. They are used across a large variety of applications, from bank transactions to military networks. Using an IP system, enhanced supervision of an alarm connection is possible. Lines can be supervised as often as desired at no additional cost for the circuit. The use of IP connectivity also saves money as it is priced at a flat-rate versus the cost of a toll-free telephone number which was used for alarms in the past. When using IP, there is also no cost associated with a dedicated telephone line for alarm monitoring. One disadvantage of using IP, however, is that the systems require an uninterruptible power supply or battery backup to operate in the event of a power outage. POTS lines operate during power outages as the power is supplied across the line.

An IP-based communication device can be connected to the primary and secondary communication ports of the FACP's digital alarm communicator transmitter (DACT). Multi-mode communication products have been developed that include connectivity options for IP-only, GSM (Global System for Mobile) or cellular-only, or IP primary/cellular backup, where the cellular connection is used if an Internet connection goes out of service. Some communicators can be configured to use multiple IP devices, with one address set to the primary central station receiver, the second set to a backup or another location for disaster recovery purposes, and the third set up as an address where maintenance events can be reported.

Installed at the central station, an IP-based receiver can emulate a conventional phone receiver and support thousands of accounts. These units also supervise the IP link of each registered account. The 2010 version of NFPA 72 specifies that if any single method of communication device is used, failures need to be annunciated at the supervising station within five minutes of the failure. This five-minute test is verified by the use of a test signal or "heartbeat." IP-based systems will perform this task every 90 seconds in place of testing once every 24 hours, as is done when using traditional phone lines. At the protected premises, an error will cause a "trouble" indication in 60 seconds or less. While IP communications meet NFPA code, some authorities are resistant to supporting their implementation.

Emergency Communications Systems

Fire alarms and emergency/voice communications systems have been integrated with one another for many years. The 2010 version of NFPA 72 requires that the emergency communications system (ECS) can be programmed to supersede the fire alarm. The ECS can be used to announce fire alarms, as well as other events such as bomb threats, storms and active shooter incidents. It can also be used by public safety operators to provide additional information or change the egress path during an event. The installation of an ECS is not mandated by the NFPA at this time. However, it is mandated by the U.S. Department of Defense in its facilities and buildings.

Voice evacuation messages are also being improved by the use of digital techniques. Analog signals are susceptible to noise when they are transmitted across a distance. Digital signals are not affected in the same manner when being stored or transmitted. Digital messages can also be sent to and stored on remote panels for use when a message cannot be obtained from a main panel during an event. The sound level of alert tones compared to other parts of a message is also easier to control without causing distortion when using a digital system.

An IP-based ECS allows network-based PCs to be used as a console device for system control. These systems can also leverage the existing network infrastructure, providing for reduced installation costs. Zones can be targeted for geo-location specific notifications. These zones would also allow for the selection of voice-enabled fire alarm systems, outdoor speakers, emergency call stations, and messaging signs. Finally, smartphones and other mobile devices can be sent messages in the event of an alert. These systems can be used to warn or direct people across the facility with specific or general messages depending on the type of event.

An IP-based ECS allows network-based PCs to be used as a console device for system control. These systems can also leverage the existing network infrastructure, providing for reduced installation costs.

Full Integration

With the selection of the proper technology platform, an IP-enabled system can assist in managing a large number of fire and life safety systems in an efficient manner. The deployment of such a system can provide effective incident management and response. The ECS should also be integrated as part of the overall life safety system. Software systems are available that can provide a total solution for the operation of a facility that includes HVAC, fire and life safety, video, access control, and emergency communications. These systems provide monitoring and integration

Integrated IP-Enabled Systems

Integrated IP-enabled systems can react to events in one system and trigger events in another. One scenario would be:

- A person activates a fire alarm pull station.
- The system would display video in the command display and initiate archival of video of the pull station before it was activated.
- It would unlock doors to allow safe egress while presenting live video of egress points to maintain the security of the facility.
- It would automatically instruct the HVAC system to activate smoke control system functions.
- It would present the SOPs containing instructions and additional information to control operators to help them manage risk and follow proper emergency procedures. Various steps could be acknowledged by the operator as they were performed for future reference.

This interaction is possible through integration and the leveraging of the IP connectivity between systems and devices.

between the applications and sub-systems to reduce risk within the facility and provide for a high level of operator productivity. This integration can also provide a means to report on the location of employees during an evacuation event. A deployment of this type is the fire and life safety system equivalent of a physical security information management (PSIM) system. These systems allow both routine and emergency situations to be handled efficiently by providing the information required to make a decision as defined by the organization's standard operating procedures (SOPs).

Final Thoughts

The parts that create a fully connected building system are independently deployed and controlled. Some of these systems do not use a common communications protocol, and system integration may be very simplistic. There are many areas of building management and physical security systems that already fully embrace IP technologies. POTS lines are being replaced by IP connections, and the resulting service levels exceed those of the more traditional central station reporting systems used in fire and life safety systems.

There is already some integration between ECS/mass notification systems and fire alarm systems. The use of IP in this area will expand. In the future, existing or modified sensors in buildings could be used to provide detailed information, such as tracking smoke or heat movement, during an event if they were connected using IP. Fire and life safety systems are currently limited in their use of IP by national and local codes. Changes to how fire and life safety systems are deployed will be driven by technology changes, market trends and updated regulations. As additional IP-based systems become part of the normal deployment of fire and life safety systems, changes to the codes and regulations will need to be evaluated. Back to TOC

Christopher Peckham (chris.peckham@kratospss.com) is the senior vice president and chief technology officer, special projects, for Kratos Public Safety and Security Solutions (www.kratosdefense.com). Walter Frasch (walt.frasch@kratospss.com) is the technical representative for Kratos.

Electronic Security Meets the Ecosystem

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

By Pedro Duarte

Share this Article:

Every year, we see a certain collection of "buzzwords" enter the mainstream. This year, the phrase "security ecosystem" emerged to describe everything that runs together and around any security solution, complementing and justifying its existence and success. Naturally, as with any ecosystem, the security ecosystem is fragile, and it demands a full understanding of all of its implications if strategic business plans are to be effective.

For most manufacturers, and those in the security industry are not exceptions, the IP world has become a reality (albeit a sometimes painful one). The migration of analog security systems to IP, and the fast speed at which it is happening worldwide, has created a race to see who will better survive with this new technology. Everything is going IP – I even have a new thermostat that talks to my Wi-Fi at home, and it works like a breeze – and all manufacturers are trying to find the formula that will lead to success.

After a relatively short period of time in which some big companies tried to convince the market that they could provide a "Total Security Solution" of their own exclusive manufacturing, the reality of the market dispelled this notion, and most companies failed or gave up this value proposition.

The problem is that each "Total Security Solution" is as different as each one of us, and companies had to accept the fact that they needed to adapt their solution from one-size-fits-all to a custom-made approach that fulfilled the requirements and wishes of each customer. Few customers are willing to simply dispose of all of the equipment and systems that they have installed. Instead, they want to make their personal "orchestra" continuing to play in tune regardless of what feature they add to the system.

In this way, each customer wants to maintain the freedom to select the parts of the system that they are comfortable with, integrating it with other parts of the "ecosystem" (access control, video management system software, wireless transmission, intrusion detection, fire detection, building automation, etc.).

So manufacturers had to reconvene their troops and face the reality that they had to implement a self-driven, reliable and dynamic integration process. This needed to go beyond the existing processes and standards, considering that the latter is almost always delayed relative to both customer needs and the innovations and features introduced in the market.

At the same time, the entrance of IP technology brought a lot of "complication factors" related to the security and integrity of data. So now we are forced not only to be compatible and interface with each manufacturer that is using the same network, but we also must keep a sharp eye on how to protect the data and connections.

Therefore, it gets better and more complex: It is not enough to make every system connect to each other. Now, since all systems will be running over IP and sharing the same network, we also need to implement a set of solid cybersecurity processes to protect this new breed of toddlers walking in the IP alley.

That is a great challenge. It is not enough, as an example, to make a CCTV system capable of interfacing with several manufacturers of different products; we also must ensure that the whole system will be protected against cyber attacks.

An important difference between traditional analog CCTV and new IP-based cameras is that the former normally did not allow images to leave the protective confines of the building where the system was connected with coaxial cables. With an IP system, however, these videos can go beyond the gate and be transmitted anywhere on the Internet if an unsecured IP-based camera is used.

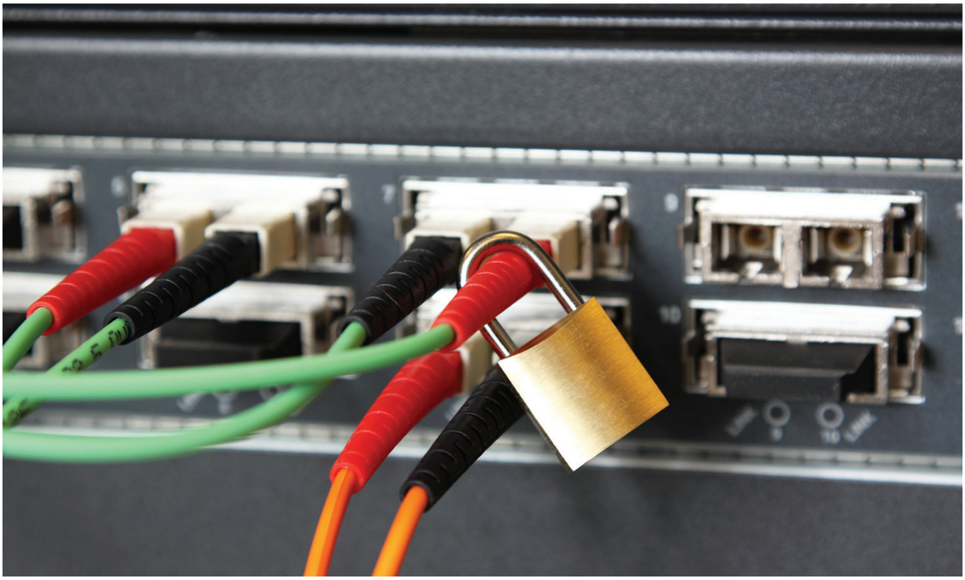
It is easy to lose sight of the dangers posed by unsecured IP-based cameras, especially amidst all the promotional fanfare surrounding the latest IP surveillance systems. However, it is clear that there are very real threats to using unsecured IP cameras. Whether they are connected to other systems or not, they can be exploited by criminals.

One thing we can be sure about is that IP surveillance networks will have all of the vulnerabilities that any other data network has. The problems arise when those who install the cameras are unaware of networking and security best practices. Secure protocols are not always being sold with IP surveillance systems, and the data transmission setup can affect the level of security.

Choosing an IP-based camera that offers the best security features is an excellent first step. The next critical step is to have it installed by someone who is cognizant of those features and how they should be implemented within the system.

A big weak-spot in IP-based cameras is that many run internal web servers with http instead of https for administrative log-ins. Only https will allow for an encrypted session, while http enables unencrypted data, such as content, user names and passwords, to be transmitted across the network and reach points in the outside world.

Another problem is that these unsecured cameras run file transfer protocol (FTP) sessions instead of the more secure SFTP session that encrypts content, user names and passwords during the image transfer to a server or client. Because these server connections enable unencrypted data to be sent across a LAN, WAN or both, unauthorized users can gain



access to critical information that they can then use to attack the network system. This could potentially give them access to not only the CCTV network, but also, if it is connected with other devices in the "ecosystem," the entire security system.

All IP cameras have built-in password protection; however, some of the more expensive models also offer other security features, such as encryption. It is essential for an enterprise's decision-makers to research the security features of various models and choose the one that best fits their security needs. Choosing an IP-based camera that offers the best security features is an excellent first step. The next critical step is to have it installed by someone who is cognizant of those features and how they should be implemented within the system. This includes a solid knowledge of how the system will interface with other systems (access control, intrusion detection, fire detection, etc.), and what kind of cybersecurity will be implemented based on sound policies and procedures.

In the case of accessing a remote or private network, there are many options, whether using an IP security (IPSEC) or SSL virtual private network (VPN). VPNs are the first solution to guarantee to secure access to an IP-based camera through a firewall. A VPN prohibits unauthorized access from the Internet via several means. Importantly, it encrypts all the data that passes down the tunnel so that it is indecipherable to hackers. Also, a VPN authenticates via user name and password, making it unlikely that a hacker would even gain access to the encrypted data. However, if the data were compromised in any way, the VPN device would drop the data packets and end the session.

Video data storage is also crucial in order to have long-term data storage and rapid recovery of relevant information. This is particularly true in the case of video images captured from IP-based cameras. These images need to be retained for a specified length of time and be easily retrievable so that illegal activity on a given day can be thoroughly investigated.

A problem with data storage is that it inundates network servers and slows down network functions. For this reason, storage security appliances are now being used. Along with on-site storage, disaster recovery plans typically also involve the use of the cloud or another type of off-site storage so that, in the event of an on-site disaster, information will be safe.

Making sure that data is safe from physical damage is crucial, but it is equally important to ensure the integrity of the data. As mentioned earlier, hackers and cyber spies are constantly seeking new ways to access private information. Video captured from IP cameras often includes private images (e.g., some retail stores have cameras in their changing rooms). Every enterprise has a responsibility to protect this stored data from unauthorized access, and data encryption is becoming a key strategy.

Constantly monitoring for intrusion is also critical. Ultimately, the responsibility for security lies not in the hands of the manufacturers who produce IP-based cameras or data storage solutions, but in the hands of those who deploy and use these devices.

Ultimately, the responsibility for security lies not in the hands of the manufacturers who produce IP-based cameras or data storage solutions, but in the hands of those who deploy and use these devices.

Well-trained security personnel will remain abreast of the latest network intrusion strategies in order to be able to block entry at every turn. However, despite best efforts, network intrusion can and does occur. It is important to ensure that security staff is properly trained to handle a security breach. What are the policies and procedures that they will follow? Practices outlined by the Scientific Working Group on Digital Evidence and Image Technology will help an enterprise implement effective strategies to prevent intrusion and to deal with it when it occurs.

Unintentional ethics violations also must be avoided. Security personnel may have sound technical knowledge, but they lack training in ethics protocols. State laws vary regarding video surveillance, so security personnel need to be aware of the regulations governing their state. For example, 13 states expressly prohibit the unauthorized use of cameras in private places, such as changing rooms, restrooms and locker rooms.

Video surveillance cannot be entered into lightly. It is essential for enterprises to protect the constitutional rights of employees and patrons.

As we can see, IP video has come a long way since the first IP camera was manufactured back in 1996. Mostly in the government and financial applications world, there is a higher threat level, requiring a very high frame rate and the installation of additional security measures, such as PKI encryption and certificates in order to meet the standards of the government's Defense Information Assurance Certification and Accreditation Process certificate.

We've all seen movies like *Mission Impossible* in which somebody does a contortionist exercise to tap a surveillance system. In most of the movies, there is a set of security cameras, ineptly monitored by one or more security guards. And, naturally, the intruder

always manages to avoid detection, hack into the video signal and disable it or inject a decoy image before escaping at the last second.

With today's secure video management technology, is any of this really possible? How protected are the cameras and video streams at the edge of the network? As Steve Surfaro, a veteran security industry professional, has explained, in most of the movies in which somebody is trying to tap into a camera feed, the systems are analog. Digital video is far superior, because it can be locked down, whereas analog video has a physical component that can be compromised. With a properly secured IP video system, those guys would not easily be able to tap into or hijack a digital video stream.

The greatest system-wide concerns, however, are adaptive, or mixed, denial-of-service attacks, in which a hacker gains access to an internal network and wreaks havoc by clogging the network, consuming all of the resources, and rendering some or all of the video unavailable and basically shutting down the system. The best preventative measure in this situation is credentialing.

Today's advanced endpoint security can authenticate both the video source and the consumer of video in accordance with a credentialing authority, such as FICAM (Federal Identity, Credential, and Access Management). This is often used for smart card deployments, physical access control and logical access control.

There's a new framework in place that a number of companies are adopting to secure devices known as non-person entities, or NPEs. An NPE can be a network camera, a physical access control measure, or a VoIP device. A software application, recording video server or mobile user can gain access to a video stream only when the credentialing hierarchy authenticates the consuming device. This means you don't have to rely on a static password system to establish a password for every single camera, and you don't have to use static encryption keys or dynamic encryption keys associated with regions of cameras.

Another troublesome network risk is a rogue application installed by a hacker on a video management system that transmits log-in information periodically, without a person even being there. A hacker can set up a remote download to a server and install an application that records keystrokes and forwards them as images, enabling log-ins as a remote user. The way to safeguard against this is to keep anti-virus and anti-spyware systems always on and up-to-date.

The greatest system-wide concerns are denial-of-service attacks, in which a hacker gains access to an internal network and wreaks havoc by clogging the network, consuming all of the resources, and rendering some or all of the video unavailable and basically shutting down the system. The best preventative measure in this situation is credentialing.

A key point that has been emphasized by Surfaro is that NPEs, such as network cameras, should always be authenticated in accordance with a credentialing hierarchy. This is the most effective way of protecting an IP network that carries video surveillance traffic. A properly secured network video camera won't usually become a victim. If users employ the appropriate credentialing authorities, the camera won't stream video to a hacker, because the credentialing system prevents them from joining the pool of authorized consumers.

If a hacker successfully attacks a video management system, he could conceivably provision the camera to stream to him. He could sit on a network, quietly listening, sniffing traffic, analyzing and gaining trust with a web server, until an opportunity arises to hack the network. How do you guard against this? The easiest way, Surfaro has said, is to authenticate every user as they come onto the network. A third-party credentialing service can do this, and what's really nice about using an external service for authentication is that it often is inexpensive for a small number of users – as low as $15 per device per month. Many organizations don't realize they can use outside services to provide credentialing and authentication. With this kind of service, you always know who is on your network because they always have the appropriate keys. And to secure your video, you should always deploy cameras that have the capability of running encrypted algorithms.

Complicated? It may seem to be, but it is a small price to pay to evolve technologically. The ability to reliably monitor your security system – including accessing it from a smartphone or tablet – with total security is worth the pain. Back to TOC

Pedro Duarte (duarte.pedro@samsung.com) is the vice president, Latin America, for Samsung Techwin (www.samsungtechwin.com).

Security and Privacy in a Connected World

With proper planning and precautions, security and privacy can complement – not compete with – each other.

By Kathleen Carroll

Share this Article:

Providers of security products and services are facing a brave new world as security technology solutions are increasingly connected to networks. This makes security systems vulnerable to privacy and security threats unseen and unrealized in the offline world.

Add to this the increasing use of new technologies, such as biometrics, mobile devices and the cloud, and the complexity of addressing privacy and security concerns increases exponentially. The issues raised are new and unfamiliar territory for many in the security industry, from manufacturers to integrators to installers to, ultimately, the customer.

Unfortunately, public policy and statutes have not kept pace with the rapid innovation occurring in the industry. Even worse, the public discourse about security technologies such as RFID, biometrics and video surveillance has been dominated by privacy advocates, legislators and media outlets who lack a thorough understanding of how such technologies can be used and, yes, abused.

For example, a recent episode of *Person of Interest*, a CBS series that features technology as a problem solver, inaccurately depicted how RFID employee badges could be used. One of the main characters, a nerdy sort, is shown sitting in front of a computer monitor, which shows little blue dots indicating where every person in the office is sitting. Most of us know that RFID badges used in the employment context cannot be tracked this way. At best, we would know who was in the building but unless there were a reader at every desk, we wouldn't know exactly where employees were located.

Facial recognition technologies suffer the same fate, being depicted in movies as being able to pick faces out of a crowd, when, in fact, it is much more difficult to actually identify someone in a crowd.

According to an NBC News report, New York state officials have had significant success in solving identity theft cases using facial recognition software. But that's because its Department of Motor Vehicles (DMV) uses the software for driver's licenses and the pictures are full-face shots of individuals. Using the software, New York's DMV has investigated 13,000 cases of potential identity fraud and made 2,500 arrests.

The point is that the media often overstate how technology can be used to solve crimes. Yes, identifying folks in a crowd using facial recognition software has privacy implications and could chill free speech by making people more hesitant to appear in public. But video cameras in public places have also helped law enforcement solve heinous terrorist attacks as in the 2005 London subway bombings. And in April, of course, cameras helped identify the suspects in the Boston Marathon bombings when authorities were able to use surveillance video from a store, restaurants and other sites near the incident.

Beyond video surveillance and facial recognition, there are global positioning systems that can pinpoint location. Add to that the millions of mobile phones and tablets with cameras in the hands of consumers, and we truly are living in a "surveillance society."

That can be both a good thing – we can identify perpetrators of crimes more quickly and accurately – and a bad thing – personal privacy in public spaces is going the way of the dodo. Privacy advocates are often most concerned about the enormous amount of data being gathered on each and every one of us on a daily basis.

And they raise some very important questions. Who has access to that data? Where is the data stored? How long is the data retained? How secure is the data from accidental breaches or deliberate hacks? These are questions that the security industry should be asking as well. It is our technology – RFID, video surveillance, biometrics – that allows for the capture of much of this data.

In the past, the big question was always how to balance privacy and security. But the better question – and the challenge for the security industry – is how to provide security and, at the same time, protect privacy. Public policy and law isn't much help as it hasn't kept pace with rapid technological innovations.

Beyond video surveillance and facial recognition, there are global positioning systems that can pinpoint location. Add to that the millions of mobile phones and tablets with cameras in the hands of consumers, and we truly are living in a "surveillance society."

What is Privacy?

I was recently asked for a definition of privacy and the question gave me pause because privacy means different things to different people. Data privacy and location privacy have garnered most of the attention in the policy world. Data privacy gained prominence with the advent of computer collection and storage of data in the last half of the 20th century, and it continues to raise alarms with the advent of the cloud and big data. Location privacy has emerged as a top concern with the proliferation of mobile technologies and applications.

Security systems often capture vast amounts of data such as dates and times of entry into secure locations, and video footage of individuals coming and going in areas covered by surveillance cameras. That data can also include the location of individuals at a specific point in time. Is this personal data, deserving of privacy protection? What steps are policymakers taking to ensure that such data is kept private?

Federal Privacy Policy and Law

There are no clear guidelines in federal law regarding how to deploy security technology in a privacy-protective manner. In fact, U.S. courts have often ruled on the side of private entities that have deployed such technologies to protect their customers, employees and property.

Privacy policy in the United States has been a combination of sectoral law (e.g., Health Insurance Portability and Accountability Act (HIPAA) for personal health information, the Gramm-Leach-Bliley Act for financial information), market forces (reputation) and self-regulation.

Both the Federal Trade Commission and the Department of Commerce have looked at the use of RFID, CCTV cameras and mobile technologies in the government and private sectors. Thus far, they have favored a self-regulatory approach, saying that this protects privacy in a more flexible and cost-effective manner without slowing the pace of technological innovation.

This approach may change as concerns about the effectiveness of self-regulatory schemes increase. In particular, the proliferation of data breaches and the emergence of new technologies that gather new kinds of data, such as location, raise additional concerns. From a privacy perspective, dramatic technological change may require a legislative solution, as it did with the advent of wiretapping, which led to anti-wiretapping statutes.

There have been many bills introduced in Congress to address privacy, but aside from the sectoral legislation mentioned above, an overarching privacy bill has not been passed. Several privacy bills are now under consideration, including H.R. 983, the "Online Communications and Geolocation Protection Act." The bill defines geolocation information as information generated or derived from the operation of a wireless communication or tracking device that could be used to determine or infer the present, prospective or historical location of an individual. It would prohibit the government from intentionally intercepting geolocation information pertaining to an individual, though there are emergency exemptions and an exemption for parental consent. While this bill would apply only to government entities, other proposed privacy legislation focuses on the private sector. For example, federal data breach legislation is directed at commercial entities and has been supported by some in the private sector.

A Privacy Bill of Rights

In 2012, the White House issued a Privacy Bill of Rights that focused on how private-sector entities handle personal data in commercial settings. The Privacy Bill of Rights emphasizes many of the core tenets of privacy including:

1. **Individual Control:** Control over what personal data is collected and how it is used.
2. **Transparency:** A right to information about the privacy and security practices undertaken by companies collecting, using and storing personally identifiable information (PII).
3. **Contextual Privacy:** Assurance that PII will be collected, used and disclosed consistent with context in which it was collected.
4. **Security:** Assurance that PII will be protected.
5. **Access and Accuracy:** A right to access and assess the accuracy of PII.
6. **Collection Limitation:** Collect only that data that is absolutely necessary.
7. **Accountability:** Requirement that companies handle data and implement appropriate security and privacy measures to protect data.

State Privacy Law

At the state level, legislation relating to both RFID and video cameras has mostly attempted to restrict their use because of privacy concerns. While this legislation has been mostly unsuccessful to date, state lawmakers continue to introduce such bills every year.

Imagine if a bill passed years ago that would have restricted the uses of RFID technologies. Would companies have continued to innovate, delivering solutions such as E-ZPass for toll roads, a technology that many of us take for granted and would not give up? Have there been privacy concerns? Yes, and, in most cases, those concerns have been addressed by legislation that does not attack the technology itself. For example, the data generated by automated toll collection systems can be accessed only by court order in many states.

International Privacy Approaches

Many security companies today operate internationally and should understand that virtually every country has a privacy law that could affect how security technologies are deployed and used. This is especially true in Europe, where some countries restrict the use of video surveillance and access control systems in the workplace. In addition, there has been a significant focus on the use of RFID in any type of application.

In 2011, the European Commission adopted an RFID Privacy Impact Assessment (PIA) Framework that recommended that companies implementing any RFID-based system conduct a PIA. PIAs usually follow a risk assessment methodology and look at where in an RFID system personal data may be collected and stored. The goal is to identify and take steps to protect such data before an RFID system is deployed. Currently a voluntary initiative, the framework could become mandatory if companies fail to deploy RFID systems in a privacy-protective manner.

The Security Industry and Privacy

The Security Industry Association (SIA) has taken the first step to a self-regulatory privacy regime with the introduction of a Privacy Framework. This framework, though not comprehensive, provides a starting point for security companies that want to implement privacy protections.

For integrators and installers of security solutions, the framework recommends conducting a PIA for new deployments of security technology. It is essential to look at specific and actual risks and identify what kind of data could lead to harm if mishandled.

SIA's Privacy Framework takes on new complexity as more and more security products and solutions are connected to the network and may even have their own IP addresses. Typically focused on physical security, SIA members are seeing the line between the physical and cyber worlds blur.

This complexity increases further for those companies operating internationally. As a best business practice, conducting a PIA could help security companies and their customers avoid running afoul of the law. At worst, failing to take steps to protect privacy may cause substantial problems for a company if there is a breach. Privacy breaches have the potential to inflict reputational harm and lead to costly litigation.

As a best business practice, conducting a PIA could help security companies and their customers avoid running afoul of the law. At worst, failing to take steps to protect privacy may cause substantial problems for a company if there is a breach.

Privacy-by-Design

Privacy-by-design, a concept first introduced in Canada, can also help the security industry address privacy concerns. Organizations must make privacy an essential design feature that figures prominently in the very architecture of the system being contemplated, according to Anne Cavoukian, the information and privacy commissioner for Ontario, Canada.

The basic premise of privacy-by-design is to embed privacy into the design, operation and management of information technologies and systems across the entire information life cycle. The same principles could be applied to security systems, as those systems increasingly cross paths with information systems in many organizations. And, as noted earlier, security systems capture a significant amount of data that may deserve privacy protection.

Security product manufacturers can also apply privacy-by-design principles to the development of new hardware and software solutions. By building in privacy-enhancing technologies at the start of the product life cycle, manufacturers could gain a competitive edge in the marketplace, ultimately helping customers achieve their privacy goals more efficiently and cost-effectively.

Where Do We Go From Here?

The security industry is making meaningful progress toward providing security solutions that protect privacy. PIAs and privacy-by-design are first steps. We must also challenge the idea that security harms privacy by correcting misperceptions about technology solutions.

We can also work with privacy advocates and lawmakers to ensure that whatever policies and laws are adopted protect privacy without harming security or slowing innovation that could ultimately lead to greater security *and* privacy. ▨ **Back to TOC**

Kathleen Carroll (kcarroll@hidglobal.com) is the director of government relations for HID Global (www.hidglobal.com). She chairs the Security Industry Association's Government Relations Committee.

The Technology Behind TWIC

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

By Walter Hamilton

Share this Article:

The Maritime Transportation Security Act of 2002 required that the U.S. Department of Homeland Security issue a biometric transportation security card to all civilian maritime workers that require unescorted access to secure areas of regulated maritime facilities and vessels. In this legislation, Congress concluded that biometric identification procedures for individuals having access to secure areas in port facilities are important tools to deter and prevent port cargo crimes, smuggling and terrorist actions. The Transportation Worker Identification Credential (TWIC) program has issued more than 2.2 million tamper-resistant and biometrically-enabled smart cards to merchant mariners, stevedores, longshoremen, truck drivers and other workers in the U.S. civilian maritime sector.

The goal of the TWIC program is to facilitate positive worker identification in secure areas of regulated maritime facilities and vessels. The process of applying for a TWIC includes a background check and security threat assessment.

The TWIC program is fee-based and is jointly managed by the Transportation Security Administration (TSA) and the U.S. Coast Guard. TSA is responsible for enrolling individuals and issuing TWIC cards, conducting background checks, and managing the five-year life cycle of the card. The Coast Guard is responsible for enforcement, access control requirements and regulations related to the use of the card.

Maritime workers enroll in the TWIC program by visiting one of the more than 130 enrollment centers that are located throughout the United States. The enrollment process provides TSA with the information needed to conduct a security threat assessment and background check of the applicant. Applicants may optionally pre-enroll online by providing their personal information (name, date of birth, country of birth, citizenship) ahead of time. At the time of enrollment, the applicant will present the necessary documents to verify his or her identity, pay an enrollment fee, sit for a digital photo and have his or her fingerprints electronically scanned.

The entire enrollment process usually takes about 10 minutes (15 minutes if not pre-enrolled). Following enrollment and successful completion of the background check, the applicant is notified when the TWIC card is available for pick up. The applicant will return to the enrollment center to pick up and activate the card. At that time, the applicant's fingerprints are verified to ensure that the person that originally enrolled is the same person that is receiving the activated TWIC card. Applicants will then select a personal identification number (PIN) and receive instructions on proper handling of the card. Once the card has been issued, the worker can present it to an employer or maritime operator and request authorization for unescorted access.

Activated TWIC cards are entered into a central identity management system that is operated by TSA. This central system manages the life cycle of the card and maintains a list of all cards that have been revoked by TSA.

Two of the key technology components that enable the TWIC program are the TWIC card itself and the devices that read and process data from the card. The technical specifications for these two components are described in the *TWIC Reader Hardware and Card Application Specification*, published by TSA. The specification can be downloaded from the TSA website at www.tsa.gov/twic/reader.

The TWIC card is an interoperable, standards-based, dual-interface smart card that supports both contact and contactless (radio frequency) data interfaces. The front of the card includes a printed photo, name and expiration date. The card also incorporates embedded physical security features such as holograms, color shifting ink and micro-printing to deter counterfeiting or copying. The back of the card includes a magnetic stripe and a bar code.

There is a single integrated circuit (IC) microprocessor chip that supports both contact and contactless interfaces and provides logic for on-board card processing functions and secure data storage. The contactless interface uses a radio frequency antenna that is embedded in the card body and operates at a frequency of 13.56 MHz in very close proximity to the reader.

One of the key differences between the TWIC and PIV smart cards is that the TWIC card permits reading the biometric templates over either the contact or contactless interfaces without entering a PIN.

Data stored on the IC chip includes name, expiration date, digital facial photo, card holder unique identifier (CHUID), PIN and two standardized fingerprint templates. The fingerprint templates are digital representations of certain features that were extracted from the bitmap images of the fingerprints during the enrollment process. These templates conform to an interoperable data interchange standard that is supported by a wide range of suppliers of fingerprint sensor hardware and matching algorithms. The fingerprint templates are stored on the IC chip in an encrypted form to protect the cardholder's privacy during contactless read transactions.

Also stored on each TWIC card is a diversified key for decrypting the fingerprint templates. This key is called the TWIC Privacy Key, or TPK. The TPK is not accessible through the contactless interface, but it can be read through the contact interface or by reading the magnetic stripe.

The TWIC card is based on the same FIPS 201 smart card standard issued by the National Institute of Standards and Technology (NIST) in support of the Personal Identity Verification (PIV) ID card that has been issued to about 8 million U.S. federal workers and contractors. However, there are some differences between the PIV card and the TWIC card that enable the TWIC card to satisfy the unique requirements of the maritime industry.

One of the key differences between the TWIC and PIV smart cards is that the TWIC card permits reading the biometric templates over either the contact or contactless interfaces without entering a PIN. The PIV card requires a PIN to access the biometric data objects. While the TWIC card does support PIN functions, it is intended for use without requiring the maritime worker to use or remember a PIN. Support of biometrics over the contactless interface was a key maritime industry requirement because of the extreme harsh environments in whic many TWIC readers will be installed. Contactless readers can be sealed to protect the electronic components from airborne intrusion of contaminants such as dust or moisture. Also, the maritime industry wanted to avoid the challenge of asking workers to remember yet another PIN or password.

TWIC card readers are not furnished by the government but are, instead, purchased by maritime operators. The readers can be either portable or fixed-mounted access control devices that can directly interface with a maritime operator's physical access control system (PACS) or can stand alone. The interface between a TWIC reader and a PACS can be based on Wiegand, RS 485, TCP/IP or other communication protocols. Portable readers will typically include a wireless interface to an external PACS, host computer or the Internet.

TWIC readers are smart devices that include an on-board processor and memory and may support one or more interfaces for communication with a TWIC card. These can include a contact or contactless interface or a magnetic stripe reader. Readers will also provide visual prompts and/or text displays when communicating the status of a transaction to the cardholder or operator. TWIC readers may also incorporate a numerical pad for PIN entry. A TWIC reader will typically include a fingerprint sensor to collect an

image of the cardholder's fingerprint and convert the image to a digital template format to be used for matching against either of the two fingerprint templates read from the TWIC card.

Fixed readers are typically located at pedestrian or vehicle gates and are often mounted in secure housings to protect against vandalism, weather or impacts caused by vehicles. In the case of vehicle gates, it is also possible that two readers will be mounted at the same gate, but at different levels, to accommodate both automobiles and trucks that have a higher driver position.

Portable TWIC readers are battery-operated handheld devices that are operated by security personnel. They can be used at pedestrian entry points, vehicle gates or inside the secure perimeter to perform random "spot checks" of workers. Portable TWIC readers must be rugged and able to withstand rough handling.

All TWIC readers are capable of reading TWIC cards and should be able to perform all of the following electronic security functions in less than six seconds:

- Confirm that the TWIC card is authentic. In card authentication mode, a TWIC reader will execute a challenge/response function using the card authentication certificate and the card authentication private key on the card.
- Check the integrity of the data objects on the card to ensure that they have not been altered or replaced by validating the digital signing certificates.
- Check the expiration date on the card to make sure that it is still valid for use.

- Confirm the identity of the cardholder by performing a match of the person's presented fingerprint to the fingerprint template(s) stored on the card.
- Check that the card has not been reported as lost, stolen or damaged and has not been revoked for cause by TSA by checking the card's unique identifier against a published cancelled card list that can be downloaded from the TSA website or by checking the card's digital certificates against a certificate revocation list.

When all of the above functions are successfully performed, the maritime operator has a very high level of assurance in the identity of the cardholder.

While a TWIC card is required for unescorted access to regulated maritime facilities and vessels, mere possession of a valid TWIC does not necessarily authorize entry. It is typical for a maritime operator to maintain a "white list" of registered TWIC cardholders that have permission to enter. This access control list can be stored in the control panel of the PACS or in the TWIC reader itself. Employees and frequent visitors will typically be "registered" into the PACS. This registration procedure is usually performed in the maritime operator's security office where the TWIC card is read and validated and the cardholder's fingerprint biometrics are verified. This is also a good time to collect and store the TPK fingerprint decryption key for storage in the PACS. This will enable the use of contactless readers at the entry points since the TPK is now stored in the PACS and can be used for decrypting the fingerprint templates read from the TWIC card. Once the registration process is complete, the cardholder can be added to the access control list.

TWIC readers, or the systems to which they are connected, are also capable of producing a log of entry transactions for auditing purposes. Based on pending Coast Guard regulations, maritime operators will be required to maintain records of TWIC reader entry transactions for up to two years.

For readers that are intended for outdoor use, there are stringent environmental requirements for temperature, humidity, shock, vibration and UV radiation. Also, some TWIC readers may be required to operate in environments where explosive vapors may be present in the atmosphere. This requires special design certifications to ensure that there are no electrical sparks that could cause an explosion.

The U.S. Coast Guard recently issued proposed regulations that will require maritime operators that are placed in a high-risk category to implement TWIC readers to strengthen the security of worker access to their facilities or vessels.

TSA has launched a new program to test TWIC readers to ensure that they conform to the *TWIC Reader Hardware and Card Application Specification*. Readers that are successfully tested will be added to a TWIC Reader Qualified Technology List (QTL) that will be published by TSA on its website. Several independent testing laboratories have already been assessed and approved as TWIC Reader QTL labs by TSA. Each of these laboratories has also been previously accredited under the National Voluntary Laboratory Accreditation Program, which is administered by NIST.

When fully implemented, the TWIC Reader QTL testing program will support the procurement of TWIC readers by maritime operators by providing them with the confidence that any reader listed on the TSA QTL has been rigorously tested and reviewed by a competent independent laboratory and has been proven to conform to the TWIC specification. Information about the new testing program is available at www.tsa.gov/twic/reader.

The U.S. Coast Guard recently issued proposed regulations that will require maritime operators that are placed in a high-risk category to implement TWIC readers to strengthen the security of worker access to their facilities or vessels. Currently, the TWIC card is only subject to visual inspection at access points. The new reader regulations should become final sometime in 2014.

2013 will be a pivotal year for the TWIC program, with the proposed regulations related to the use of readers the most important development. In addition, TSA is revamping TWIC enrollment centers to improve stakeholder service and convenience, and the agency is looking at other ways to enhance the overall effectiveness of the program. ▨

Back to TOC

Walter Hamilton (whamilton@idtp.com) is a senior consultant at Identification Technology Partners (www.idtp.com) and is the vice chairman of the International Biometrics & Identification Association (www.ibia.org). He has been an active participant in the TWIC program since its inception in 2005.

A Case for a Green Security Landscape

Sustainability can be good for both the environment and the bottom line.

By John Hunepohl & Aaron Smith

Share this Article:

"Attention all security professionals and security equipment manufacturers – a new conservation of energy and natural resources law requires that all security systems and security personnel must go into a 'sleep' mode after the first hour on duty if no suspicious activity is observed."

OK, don't panic – that's a hypothetical law, but it's not much of a stretch. For a short time after December 2007, that potential situation existed when the 311-page "Energy Independence and Security Act (EISA) of 2007" was signed into law. While we're on the subject of security regulations, let's take a look at the Uniform Code of Military Justice Article 113:

"Any sentinel or look-out who is found drunk or sleeping upon his post, or leaves it before he is regularly relieved, shall be punished, if the offense is committed in time of war, by death or such other punishment as a court-martial may direct, but if the offense is committed at any other time, by such punishment other than death as a court-martial may direct."

For those of us who have ever served in the military, it was clear that falling asleep while on watch was a gross dereliction of duty. But staying awake and alert consumes more energy and requires more rations, so why not rewrite Article 113 to *require* all sentinels to go to sleep if after the first hour of the watch, "you don't see any threat or suspicious behavior." Now would that make sense to you?

John Hunepohl (left) and Aaron Smith

Well it made sense to the U.S. Congress when it passed EISA. Even though security systems and their devices must remain vigilant and alert at all times, the law unintentionally required every security system to go to sleep on guard duty because those systems consume power for LEDs, sensors and any number of attached devices.

In fairness, the law was well intentioned. Think of all the home appliances that needlessly consume power in a standby or nonoperational mode. Millions of incandescent bulbs turned on for no good reason or a DVR or TV ready to fire up in seconds versus minutes. Personally, I can wait three or four minutes for my TV to "wake up" when I get home. But I don't want my security system to wait even one second and neither does anybody else.

Fortunately, our industry became aware of this flaw in the legislation and, thanks to the efforts of the Security Industry Association (SIA) and a coalition that contained both industry and environmental groups – including the Natural Resources Defense Council (NRDC) – we were able to get Congress to amend EISA. President Obama in January 2011 signed into law H.R. 5470, sponsored by Rep. Frank Pallone, D-N.J., and Rep. Roy Blunt, R-Mo., which provides an exemption from the "no-load" requirements of EISA for security and life safety products.

Security system providers can make sustainability requirements work in their favor by calculating the cost savings an end-user will achieve by installing newer access control technologies, such as Power over Ethernet (PoE) systems and components.

Change: The Process of Becoming Different

It is safe to say that electronic security changes, whether because of needs, technology, codes, standards or regulations. From time to time, a rapid change occurs, but, by and large, change comes slowly in our industry – think of how long we've been using metal keys and pin-tumbler locks. Sometimes change is mandated by codes, standards or regulations. This is the case for cards and readers because of Homeland Security Presidential Directive 12 (HSPD-12), signed into law by President George W. Bush on August 12, 2004.

HSPD-12 created a mandatory, government-wide standard for secure and reliable forms of ID issued by the federal government to its employees and employees of federal contractors for access to certain federally-controlled facilities and networks. The supporting technical criteria – Federal Information Processing Standards Publication 201 (FIPS-201) – was developed by the National Institute for Standards and Technology (NIST), setting minimum requirements for a federal personal identity verification (PIV) system.

Codes, Laws and Common Sense

Now we have the "National Energy Efficiency Enhancement Act of 2010" to keep us up at night, worrying once again about how our security systems will meet a new set of standards. Fortunately, the industry has SIA to look out for these issues and bring a collective voice of reason into the standard, code and law development process.

Though we may cringe at the introduction of new standards and regulations, there are some issues that are unavoidable, and sustainability is one of them.

It behooves us to stay up-to-date on issues that will affect security systems integrators and practitioners. SIA is committed to working to that end, as in the case of the "National Energy Efficiency Enhancement Act of 2010.

Sustainability: The Capacity to Endure

Sustainability, commonly referred to as being "green," has the security industry in its sights. The demand to consume less and less energy and to reduce carbon emissions is upon us. How will that affect security? First, let's look at the typical power consumption of a single electronic-controlled access door. Given a card reader, door position switch, request-to-exit, fail-safe lock or strike, control panel, and power supply, you're looking at consuming 21 watts of power per year in standby mode. What if we could perform the same security function at that door but only consume 2.85 watts of power per year? Do you think Congress would get wind of this and contemplate a law requiring the use of the 2.85-watt device?

> **PoE systems are energy efficient and completely eliminate the need for batteries. When the total life cycle analysis of Wi-Fi and PoE systems is considered, the result is not only less energy consumed, but also less material used during construction.**

Power over Ethernet (PoE) Saves Energy and Money

Security system providers can make sustainability requirements work in their favor by calculating the cost savings an end-user will achieve by installing newer access control technologies, such as Power over Ethernet (PoE) systems and components.

Compared to an "around-the-door" solution, you can document annual savings of $18 per door. In a system of 100 readers, this translates to a savings of $1,800 per year for the customer. If that dollar amount seems unimpressive, think of the "carbon footprint" impact.

Green Standards for Health Care and Other Facilities

Security systems integrators must look at the U.S. Green Building Council requirements and its adoption of ASHRAE 189.1, plus the International Green Construction Code for health care facilities:

"Green building features might once have seemed like a fad, or a meaningless design addition that had no effect on energy footprint. But green building has caught on, becoming a booming business and fostering innovative ideas about how to construct homes, offices, and skyscrapers that use as few resources as possible. By 2015, the amount spent on green building is going to more than double, to $163 billion from $71 billion today."

But it's not just health care facilities that have embraced sustainability; buildings of all types are riding the green wave. The new football stadium for the San Francisco 49ers, for example, "incorporates photovoltaic panels, a green roof, excellent public transit access, convenient bicycle parking, walking path access from the San Tomas Creek Trail, water-conserving plumbing fixtures, sophisticated building control systems, recycled materials, and a long list of other sustainable design concepts."

PoE locks fit nicely into these projects. Leveraging existing PoE infrastructure allows you to streamline the installation process, reduce costs and components, and minimize power consumption. PoE cameras and telephones are already commonplace in buildings. Electronic access control (EAC) and CCTV systems are moving in that direction.

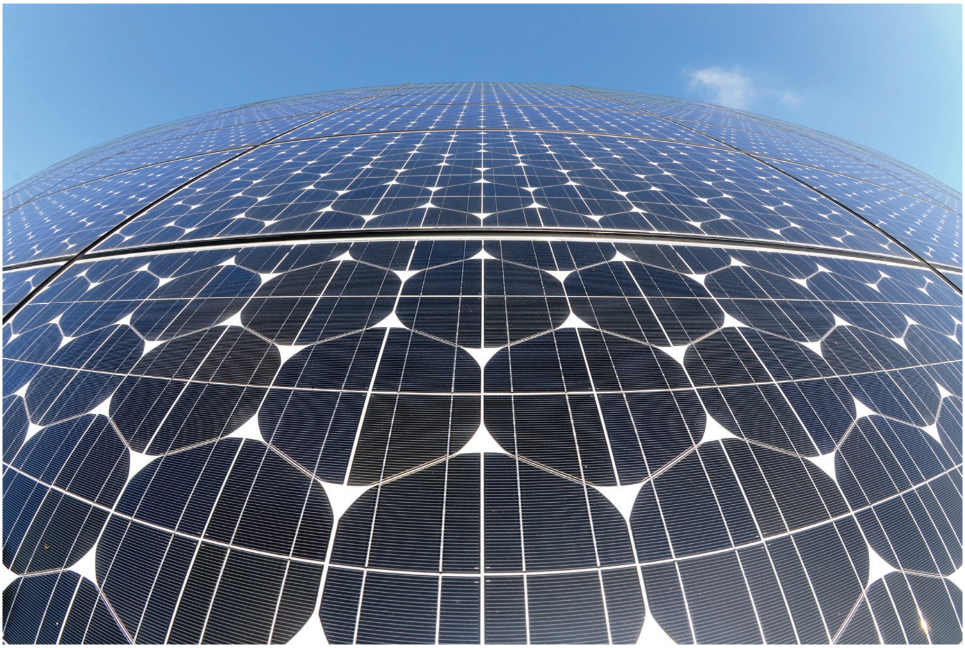
Most facilities now incorporate EAC to provide convenient access with effective security to their buildings. These traditional access control systems typically include several different components in and around the door, including a door position switch, electrified strike, card reader and lock. These components are all connected to an access control panel and require a low voltage power supply. Many of those components require a significant amount of power to operate, which leads us to a second strategy for energy savings.

Today, thanks to the development of newer technology, performance of an EAC system can be significantly improved by consolidating all of these disparate components into one integrated lockset. This solution uses existing network cabling for both power and data and connects to the access control panel, consuming a mere 2.85 watts of power.

PoE systems are energy efficient and completely eliminate the need for batteries. When the total life cycle analysis of Wi-Fi and PoE systems is considered, the result is not only less energy consumed, but also less material used during construction, which helps the bottom line while decreasing the impact of manufacturing, shipping and installation processes.

Learning a New Language

Understanding sustainability requires us to learn a new language. The security industry has faced this challenge before, such as when we had to learn IT terms and acronyms, and we've prevailed. So here are a few questions that security system manufacturers and integrators might hear from their customers:



- How does your security solution help to meet our "net-zero" energy efficiency goal?
- What is your "end-of-life" recycling program?
- Does your security PoE solution provide for Leadership in Energy and Environmental Design (LEED) credits?
- We need to improve security by converting to electrified latch retraction on our egress doors. How will your proposed product help us meet our energy reduction goals?
- Does the security system you propose provide me with one point under MR Credit 5?
- How much "recycled" content is in your product/packaging?
- What is the distance from the product manufacturer's location to the job site?
- What can you provide with your EAC system to help me meet IEQ Credit 10?
- What climate zone is this project in?
- Will your EAC system affect the required U-Value of my openings, as required by ASTM C1363?
- Will your modification of the opening affect my IEQ Credit 2 for acoustics?
- We want to achieve the second point in Energy and Atmosphere Credit 3 – Enhanced Commissioning. Will your system affect our ability to do that?

Just as a seat at most project tables is now occupied by an IT person, a new person may show up – the "Green Guru" whose job it is to make sure a facility meets sustainability and LEED requirements for going green. Security systems integrators must become knowledgeable about these matters to improve their chances of winning contracts and enhance their service to end-users.

Back to TOC

John Hunepohl (jhunepohl@assaabloydss.com) is the director of education for Assa Abloy (www.assaabloy.com). He serves on the Security Industry Association Board of Directors and chairs SIA's Education Committee. Aaron Smith (asmith@assaabloydss.com) is the director of sustainable building solutions for Assa Abloy.

securityindustry.org

8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700