

High Fidelity

The power of audio surveillance

**Security's
3-Legged Stool**

Integrating intrusion with video and access

**Cutting the
Cord**

Wireless fire and life safety devices

SIA
Insights
TECHNOLOGY

**Volume 3, Issue 1
Spring 2015**

Welcome

Dear Reader,

Two years ago, SIA set out to produce a publication that would be unique in the security industry – one that would offer in-depth, commercial-free content to help end users and integrators identify and implement security solutions. Since that time, we've built up quite a library, and, with this fifth edition of *SIA Technology Insights*, we now have published more than 40 articles about a wide range of security technologies.

So we've added something new in this issue. In the back, you'll find a list of all *SIA Technology Insights* articles sorted by subject. We invite you to visit www.securityindustry.org/techinsights to read the ones that most interest you, or even download all editions to keep on your computer as a resource.

Of course, before you get to that list, we hope you'll stop and read some of the great articles that come before it. From integration to fire protection to video surveillance to *audio* surveillance and more, this edition analyzes some of the leading technologies in the security space. And for those of you who work in or with schools, maritime transportation/ports, or transit systems, there are articles that focus on security challenges in those verticals.

We hope you enjoy this edition, and we thank you for reading *SIA Technology Insights*.



V. John Stroia
Chairman, Board of Directors
Security Industry Association

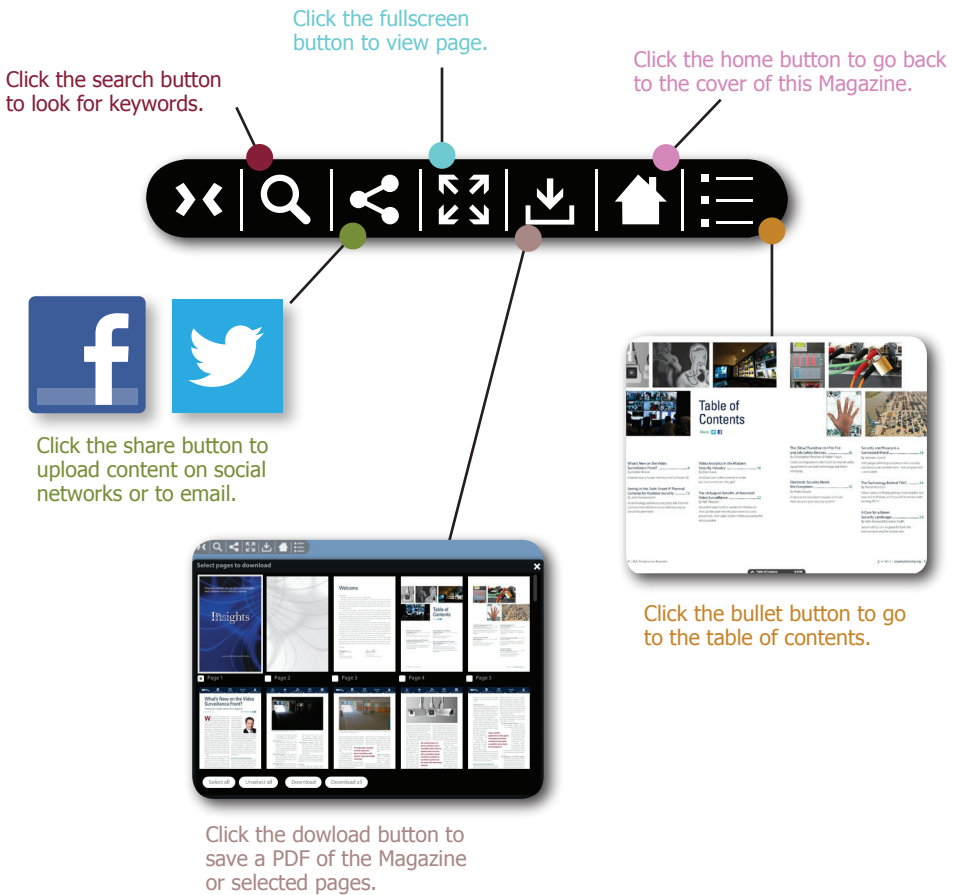


Don Erickson
CEO
Security Industry Association

How to Navigate Through the Magazine

Navigation Bar

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



Topic Tabs

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

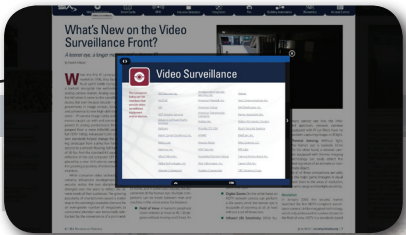


Table of Contents

Share: [Twitter](#) [Facebook](#)

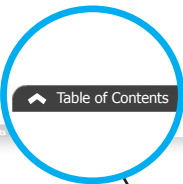
What's New on the Video Surveillance Front? By Fredrik Nilsson	6
A keener eye, a longer memory and a sharper IQ	
Seeing in the Dark: Smart IP Thermal Cameras for Outdoor Security By John Hunepohl & Aaron Smith	22
As technology advances, do cameras become a convenient way to secure the perimeter?	
Analytics in the Modern Security Industry By Rafti Plosof	16
IP devices can make cameras smarter. How smart can they get?	
The Untapped Benefits of Recorded Video Surveillance By Rafti Plosof	22
Recorded video holds a wealth of information that can be used not only post-event but also proactively. Fast video review makes accessing this	

Article

Click the title to go directly to the article.

Page Turn

Click the arrow to view next page.



Page Thumbnails

Scroll to view the next page

Table of Contents



Commanding the Enterprise..... 8

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

By Rob Hile, SureView Systems



**Removing the Barriers:
The Wireless Side of Fire Protection and Life Safety..... 14**

The industry's wireless movement is fueling innovation

By Richard Conner, Fire-Lite Alarms and Silent Knight



Do You Hear What I Hear?..... 22

Audio technology is redefining the surveillance industry and has become an essential component of security systems

By Richard Brent, Louroe Electronics



The Sun Shines on Surveillance 30

Solar power enables wireless video solutions in remote locations

By Dave Tynan, MicroPower Technologies



Integrating Intrusion..... 38

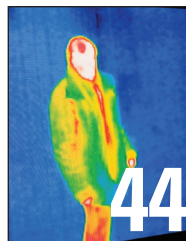
Video and access have converged on the network; the time has come for intrusion detection to join them

By Mark Jarman, Inovonics

Surveillance in the 21st Century 44

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

By Jumbi Edulbehram, Oncam Grandeye



10.7 Billion Security Challenges 52

As transit ridership increases, so must security

By Steve Cruz, Panasonic



Tying It All Together 60

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

By Mitchell Kane, Vanderbilt Industries



The Future of Video Surveillance 68

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

By Alex Asnovich, Hikvision USA



Safe on the Water 74

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

By Kostas Mellos, Interlogix



SIA Technology Insights Article List 79



ECCS helps organizations tackle one of the most common problems – how to integrate and streamline a multitude of different security systems and sensors into one, easy-to-use interface.



Commanding the Enterprise

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

Software platforms that integrate multiple systems and devices – commonly known as physical security information management (PSIM) systems, command-and-control software or situation management solutions – have been successful in addressing the needs of the public sector, especially in the critical infrastructure and transportation markets where government money is often readily available and long purchasing cycles and implementation times are common. But these same platforms have struggled to address the needs of the dynamic large enterprise and commercial space. Typical PSIM products have not been designed to address the stringent needs of customers in these markets and, as a result, successful deployments have been rare.

In the early days of PSIM deployment, critical infrastructure sites needed a way to “unify” multiple

By Rob Hile
SureView Systems



security systems into one platform to simplify system administration and management and correlate data points into one interface. This approach was one way to provide quicker responses to issues that could



disrupt normal business operations. Many enterprise customers looked to deploy similar solutions to gain new levels of situational awareness and risk management, but early attempts failed because most enterprise customers typically consist of multiple facilities spread across a large geographic region, even, in some cases, around the world. But traditional PSIM applications, deployed on old client/server technology, cannot offer the licensing flexibility or scaled architecture needed for the variety of network configurations and communication platforms common within today's enterprise.

Evolving Business Requirements

Enterprises come in all shapes and sizes, but they share a common set of challenges, including risk management, compliance, physical security, IT security and employee safety. As risk management demands widen the scope of security, the security function itself transforms into business security. What does this mean? Business security encompasses people, processes and locations – in short, all of the assets of the business, across the enterprise, are combined to be managed in a cohesive and integrated way.

Acquisitions, mergers, brand

protection strategies, compliance, regulations and strategic investments all create a requirement for technology solutions that accommodate change and offer new levels of flexibility. These needs are far more diverse than what is typically seen in the public sector.

Enterprise customers commonly have

widely distributed facilities that need to be linked and disparate systems that need to be integrated. Consolidated operations among these sites and across existing technology investments is critical to achieving greater levels of

situational awareness. Security and risk leaders also need to ensure a strong return on investment for all capital expenditures to receive continued support and buy-in from senior leadership. All in all, business leaders want streamlined procedures across the enterprise, enforced by consolidated and robust reporting capabilities.

Enterprise customers are unique in that they are typically geographically-diverse organizations that have completely distributed network architecture challenges and, in most cases, operate with many smaller security operations centers in place. However, enterprise customers are not limited to the commercial market. Cities, transportation entities and universities



have many of the same challenges as typical “enterprise” business operations. Many enterprise organizations, though, are for-profit businesses that need a solution that can meet today’s business challenges but can also scale and grow as business needs evolve.

Enter ECCS

Reaching far beyond the capabilities of traditional security software platforms, enterprise command center software (ECCS) is a situational awareness software platform used by businesses, institutions and agencies to monitor security, IT and business systems, and protect critical assets. It is the driving force behind today’s private command center movement and is designed to drive down the cost of monitoring multiple systems across locations while increasing the effectiveness and response time of the security team.

ECCS is designed to address the enterprise space, specifically. Its web-based architecture and ability to support a variety of network topologies

and communication platforms lends itself to the distributed nature of the enterprise market. In fact, the software platform is particularly well suited to global enterprise organizations. This architecture also supports a rapid deployment model and a strong return on investment/total cost of ownership model. Most importantly, it is agile enough to meet the changing dynamics of enterprise businesses.

What makes ECCS different?

ECCS has been designed from the ground up to focus on the four major components critical to delivering security services throughout an enterprise:

- *Architecture.* Completely web-based, it allows customers to map the system to the specific needs of their organization.
- *Open Platform.* Open architecture and integration support for a wide variety of third-party devices supports rapid deployment and minimizes expensive, complex



- *Piecemeal solutions.*
- *Automation.* Allows for the automation of manual processes to streamline the delivery of security services, eliminating the possibility of operator error and nuisance alarms, and ensuring that only actual security events are handled.
- *Agility.* Scalable, highly reliable, secure and flexible.

Enterprise Requirements

The needs of today's enterprise customers are complex and constantly evolving. Business and security leaders need to reduce risk and protect themselves against rapidly changing security threats, including theft, terrorism, brand risk and IT attacks. Business continuity must also be guaranteed across various sites and around the globe. At the same time, leaders must ensure that budgets are met and investments can carry far beyond one function to provide long-term value and usability.

The flexible nature of the ECCS solution enables faster time to market, helping customers drive optimization throughout the organization. Because of its cloud-based architecture, proof-

of-concepts can be up and running in as little as one week. This approach also enables the flexibility to adjust to changing business needs, such as new locations added organically or through acquisition, changing business requirements, and the addition of new technology systems.

ECCS helps organizations tackle one of the most common problems – how to integrate and streamline a multitude of different security systems and sensors into one, easy-to-use interface. It enables enterprises to easily incorporate information from many physical locations into a global security command center to provide an enhanced form of monitoring that streamlines operator requirements.

If something does require attention, the system will automatically pull up any relevant security systems in the area of the alarm, such as surveillance cameras, and provide the operator with directions about what steps to take next.

Easing operator duties is a key benefit of ECCS. Auto-handling ensures operators are paying attention to the most critical security alerts and following best practices. For example, in the past, an email alert would come in to an operator,

who would then have to open it to gauge its potential impact on the organization. With ECCS, email alerts are automatically filtered to enable users to quickly determine which messages need immediate attention. If something does require attention, the



Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance



system will automatically pull up any relevant security systems in the area of the alarm, such as surveillance cameras, and provide the operator with directions about what steps to take next.

Training is also simplified because operators are using a single, unified interface, as opposed to managing interfaces for each of the systems they monitor. The ability to add predetermined steps for operators to follow during various security events also enables users to become more efficient in performing their duties. Overall, ECCS simplifies the management of an organization's entire security technology network and, subsequently, eliminates the need to learn and become proficient on multiple platforms.


The Future of the Enterprise

What differentiates ECCS from a traditional PSIM system is that it provides end users with more than just a vat of converged data. Because of all of its moving parts, a PSIM platform is

What differentiates ECCS from a traditional PSIM system is that it provides end users with more than just a vat of converged data.

nearly impossible to implement to its full potential. ECCS, however, brings multiple areas of a security program together into one solution to not only

provide information but to actually help the user take action. The system is designed with multiple integration points and numerous sensors to help security professionals make a decision as soon as information is available, transforming ECCS from a physical information system into an enhanced monitoring tool. ■ **Back to TOC**

Rob Hile (rob.hile@sureviewsystems.com) is director of strategic accounts for SureView Systems (www.sureviewsystems.com). 



As installers look at new ways to expand fire alarm coverage in areas of limited infrastructure, detection devices that leverage wireless networks have emerged as a valuable new offering.



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

The industry's wireless movement is fueling innovation

This is an exciting and challenging time in the fire alarm and life safety industry. Historically, the sector has seen subtle changes through technological advances, combined with more drastic changes resulting from unfortunate local and global events. Even more profound are the effects that recent innovations in wireless technology have had on fire alarms, from detection to central station communication.

As installers look at new ways to expand fire alarm coverage in areas of limited infrastructure, detection devices that leverage wireless networks have emerged as a valuable new offering. Fire alarm system manufacturers have heavily invested in research to determine what networks work best for life safety applications, where communication methods *must* be highly reliable.

On the side of central

By Richard Conner
Fire-Lite Alarms and Silent Knight



station communications, the telecommunications industry is changing rapidly, as well. Plain old telephone service (POTS) lines are being phased out to support wireless

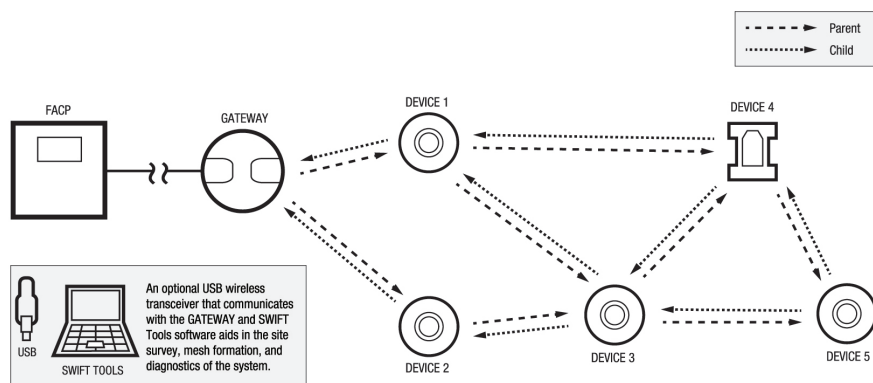
and IP-based alternatives that enable increased communication speed and improved accessibility to data. As a result of this transition, cellular carriers and device makers have changed their focus, offering new technologies and powerful cellular networks to handle consumer demand for increased bandwidth. As the focus on IP and cellular networks grows, the fire alarm market has had to adopt alternative communication methods to ensure network and device communications are reliable and up-to-code.

How can these developments save customers money while ensuring investment protection from future technology changes? How can customers get the best return on investment when migrating to a fully wireless cellular solution? Let's take a closer look at the changing landscape for fire alarm systems and examine how wireless and alternative communications can help installers enhance system reliability and ensure a high level of customer support.

A Wireless World

Wireless devices deliver a new level of reliability and flexibility to the fire alarm market. A variety of networks, including mesh, point-to-point and point-to-multipoint, can be used to transmit information and data wirelessly. These different solutions provide different benefits and value propositions. Let's take a look at each.

Wireless mesh networks allow installers to connect many devices via a network that "blankets" the area, rather than requiring that each device have a direct wireless or wired connection to the termination point. In a Class A mesh network, each smoke detector and monitor module, for example, creates its own communication structure. That means that communication travels from point A to point B through any number of these devices, creating multiple, redundant communication paths. With multiple paths to employ, the system's reliability is maximized. If one device is lost, the remaining devices will immediately find another path for communication. This is known as a self-healing network.





Point-to-point (P2P) technology provides a dedicated link between two devices.

For example, P2P enables communication between two smoke detectors, or between a monitor module and the main controlling element of a fire alarm network. P2P technology is reliable, but it also tends to be more expensive and more time-intensive to install.

Plus, if one device fails, it could affect the entire network.

Point-to-multipoint (P2MP) technology is a hybrid between mesh and P2P wireless networking. With this type of network, central units connect to multiple “subscriber” units. In order to function, all P2MP networks require that all subscriber units be in range of the central unit. If they are not, additional central repeater units are required. For many installations, this makes P2MP networks impractical and prohibitively expensive. In addition, the failure of a central unit or repeater could mean failure for multiple subscriber units.

Therefore, we’ve determined that devices used for fire protection and life safety require a mesh network with bi-directional communication to ensure reliable data transmission. In

fact, we’ve even developed terminology for this approach, calling it a “parent-

child” relationship: every child device has at least two parents to send information through, and every child device may also be a parent to other child devices. That way, inbound and outbound communications can use various paths through the parent and child devices, ensuring that every message is

received, which is obviously vital to the operation of life safety systems.

Today, a more modern central station infrastructure helps installers save on installation and maintenance costs, allows users to reduce ongoing service requirements, and enables authorities to achieve stronger reliability for transmitting fire alarm signals.

Mesh Networks and Fire Alarms

Mesh networks deliver many new benefits to the fire alarm market. Devices that use this communication method provide incredibly reliable fire alarm communication. Frequency hopping prevents system interference, and the network’s infrastructure creates redundant communication paths between each device, so if one device is lost, the others immediately find another path for communication. This is critical in the fire alarm market, where immediate and robust device communication can mean the difference between fire prevention and fire response.

A mesh network also provides



installers with the flexibility to extend a fire alarm system quickly and easily. In addition, it benefits the end user by keeping costs low, while providing self-healing capabilities and the highest level of reliability and protection.

New wireless fire detection solutions are particularly well suited for difficult

or obtrusive applications where running wire is challenging.

Based on a Class

A mesh network, these solutions deliver the same reliability that is expected from a

commercial “wired” fire alarm system. Typical applications for such wireless technologies are parking garages, historic buildings and warehouses. Whether for new installations or retrofits, the fire alarm system can be a combination of wired and the new wireless devices, allowing for easy expansion and additional flexibility.

Central Station Reporting

Fire alarm systems that offer multiple options for central station communications are critical for today’s installations. The growth in new communication networks has pushed central stations to look at the ways in which they can support alternative communication methods and the new fire alarm communicators supporting those networks.

POTS has been used in the fire alarm industry for more than 40 years and

has mainly been viewed as reliable. But communication providers now view the network as archaic and obsolete. In fact, the Federal Communications Commission (FCC) reports that POTS is not sustainable, and the agency is “seeking ways to phase out relics of a bygone industry.” Unfortunately,

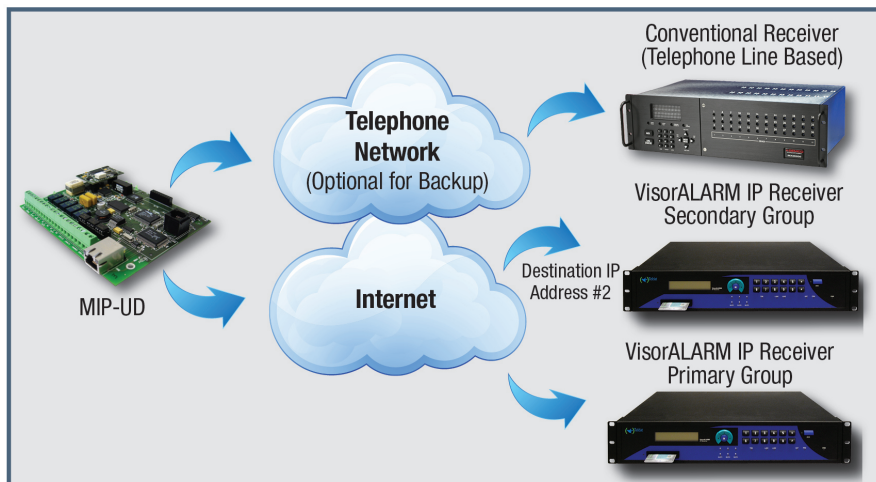
because many fire alarm systems were designed specifically to report to central stations over this legacy network, devices will need to be updated as the use and

support of POTS declines.

For alternative communication options, a variety of cellular formats are available, and all have different effects on cellular monitoring. Compared to POTS, second-generation (2G), third-generation (3G) and fourth-generation (4G) cellular networks offer significantly better speed and coverage. While improved speed is not a requirement in the fire alarm market because the amount of data being transferred is not significant, reliability and longevity are key. A fire alarm control panel needs to be connected and communicating at all times in order to transmit life safety events, and, for the safety and economic benefits of end users, needs to last for many years.

Many jurisdictions today allow alternate means of communication; however, they often vary in acceptance of dual-path (two technologies) or

Devices used for fire protection and life safety require a mesh network with bi-directional communication to ensure reliable data transmission.



single-path (one technology). As an example, dual-path could be IP and GSM (cellular) and single-path could be just one of those technologies. Once you know what is accepted, it is a matter of preference and available communication infrastructure at the protected premises. Additionally, regardless of the chosen technique, technologies that are field-configurable to allow customization to a specific application should be evaluated.

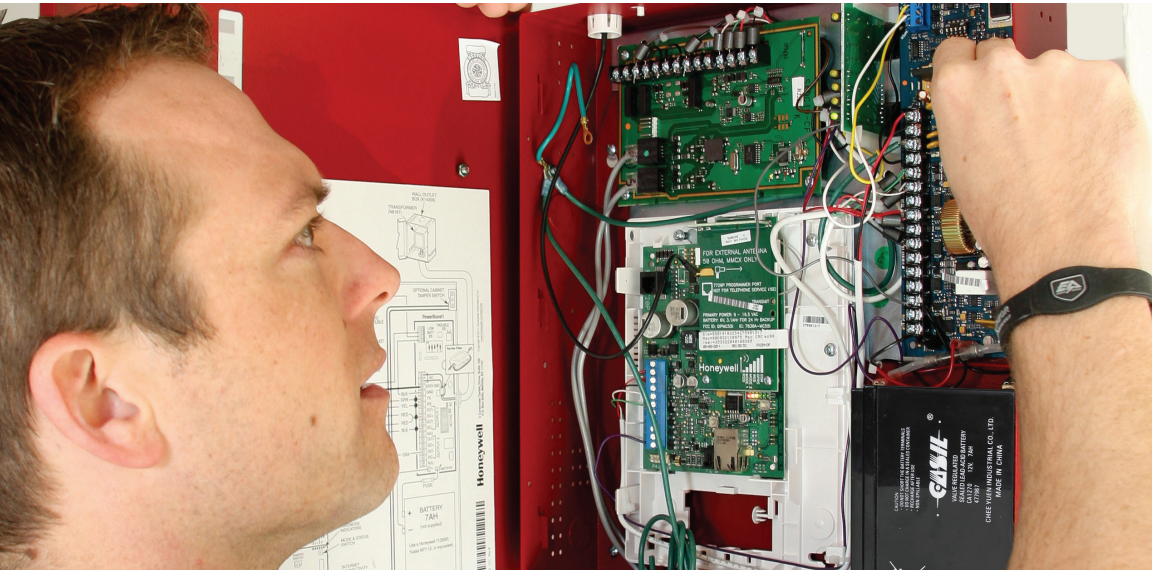
Standards for Alternative Communication

Central stations must comply with new communication standards based on NFPA 72-2013. The new standards describe approved communication methods for central station reporting, as well as options for alternative communication methods not specifically outlined in the published standards. Specified supervision requirements for single-path (cellular only and IP only) and multiple-path (IP

primary with cellular for backup, or IP primary with POTS lines for backup) technologies are also published in this edition. What are the most significant changes in the 2013 standards?

Generally speaking, the NFPA standards change the supervision requirements for single and multiple-path technologies. For single-path communication technology, the central station must annunciate a fault condition within 60 minutes after loss of communication. When using multiple-path communication technologies, the central station must annunciate trouble within six hours after loss of communication.

Chapter 26 of the NFPA 72-2013 standards outlines requirements for communications, and communicators that transmit alarms must comply with its mandates for central station reporting. Furthermore, this section states that it does not limit the use of alternative communication networks, such as cellular or IP, for central



station reporting.

Transmission channel requirements specifically look at the decline of POTS and how central station communications need to be set up to prepare for the sunset. For example, section 26.6.3.2.1.4 of the NFPA code states that, with one exception, a second communication technology must be used when employing a telephone line. The transmission means outlined in the code include a one-way private radio alarm system, a two-way RF multiplex system, or a transmission means complying with section 26.6.3.1. Approval can be given by authorities to use two phone lines in areas of reduced cellular or IP network infrastructure, but if two phone lines are used, each line needs to be tested at alternating six-hour intervals.

These changes in standards are all designed to simplify service and monitoring, while ensuring

comprehensive safety parameters.

Overall, they help reduce unnecessary service calls and enable new technologies in more jurisdictions.

Central stations are free to expand support for new digital technologies to further prepare for changes in network development, and to provide support for new and innovative fire alarm devices. At the same time, delivering support for legacy POTS technology is critical to helping fire alarm installers and customers. Today, a more modern central station infrastructure helps installers save on installation and maintenance costs, allows users to reduce ongoing service requirements, and enables authorities to achieve stronger reliability for transmitting fire alarm signals.

Cellular Communication Standards

When selecting a cellular communicator, it is important to



understand which cellular network is being used and to make sure that the specific coverage required for the communicator is available in the location needed.

It cannot be stressed enough: *Do your research.* Make sure there are no

immediate plans to discontinue the network on which the fire alarm communicator operates. For example, support for 2G service, launched in the United States in 1987, is diminishing at a rapid rate. In

fact, AT&T announced that it expects to completely discontinue their 2G cellular networks by 2017. 3G networks appear to have somewhat more longevity because of the significant research and development that was done to ensure network robustness and a longer lifespan, but rumor has it that major carriers will look to discontinue support in 2020. 4G – designed and launched in 2010 to support the growing demand for data transmission – currently offers the fastest speeds available, and coverage continues to be expanded as companies invest in this technology. There are different 4G formats, such as LTE and HSPA+ that vary by carrier.

Realizing the value of 4G and its long-term viability, manufacturers have designed new cellular communicators to leverage the benefits of 4G technology to ensure the best coverage

and the most longevity possible. For example, the top fire communicators produced today connect to the DACT of any UL-listed fire alarm control panel and communicate over 4G cellular, IP/Ethernet or both. This approach allows customers to save on the costs

of expensive POTS lines, while offering comprehensive and reliable network coverage.

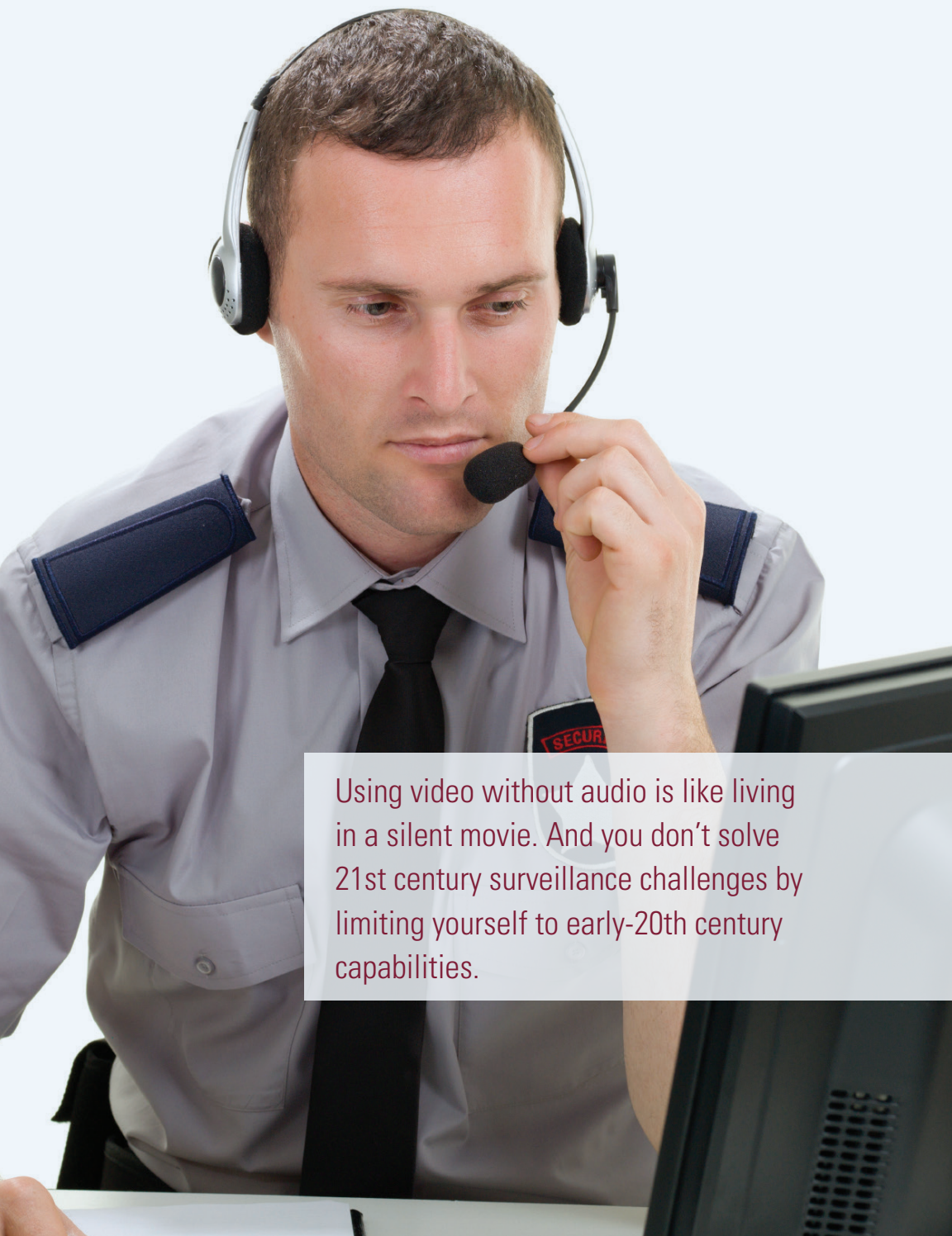
At the same time, new communicators enable increased flexibility by allowing the conversion of fire alarm control panels from POTS

to cellular or IP, with single or dual-path technology for central station communication and the ability to work on 2G, 3G and 4G networks.

Market Evolution

The fire alarm industry has experienced dramatic change over the past few years. As support for POTS further declines, new technologies, including the wireless devices and fire alarm communicators discussed above, are having a significant impact on the market. These new technologies are expanding opportunities for installers and central stations and ensuring a higher-than-ever level of protection for customers. ■ **Back to TOC**

Richard Conner (richard.s.conner@honeywell.com) is director of marketing for Fire-Lite Alarms (www.firelite.com) and Silent Knight (www.silentknight.com). 



Using video without audio is like living in a silent movie. And you don't solve 21st century surveillance challenges by limiting yourself to early-20th century capabilities.



Do You Hear What I Hear?

Audio technology is redefining the surveillance industry and has become an essential component of security systems

We are now a decade and a half into the 21st century, and it is time for a new mode of thinking when it comes to security. Security is on our minds more than ever before, and we need the best tools and strategies at our disposal if we want to construct the most optimal solutions.

While video is arguably the best-known technology in the surveillance and security toolkit, audio technology can and must rise to equal ground in order to form the most effective systems for organizations. The time for audio to take its rightful place next to video as a surveillance requirement has arrived.

One can make an analogy to consumer audio equipment: When you decouple components of your stereo system, you can buy the best of each component separately, then combine them into a system that achieves

By Richard Brent
Louroe Electronics



the optimal sound experience for your home (as opposed to all-in-one, off-the-shelf, one-size-fits-all stereo systems, which never sound as good). In a similar fashion, using the audio



that comes with video surveillance equipment may be better than no audio at all, but it will not perform as well, nor will it achieve the same results, as using a separate, optimized audio solution.

Security and Surveillance: The Demand for a Complete Solution

To get a sense of how important audio is, consider our five senses. Each one is there for a reason and they are all equally valuable. (Evolution is efficient that way). Take one sense away, or ignore multiple senses, and you are at an immediate and significant handicap.

The same holds true in the realm of security and surveillance. Too often, the emphasis is on video alone, to the exclusion of its sister sense, audio. We need to start giving audio the same amount of attention that we give video.

While many may say they agree that

audio and video should be on the same playing field, the present reality is that our industry remains focused on video-only systems. This simply must change if we are to successfully face the demands of 21st century protection.

Bottom line: Using video without audio is like living in a silent movie. And you don't solve 21st century surveillance challenges by limiting yourself to early-20th century capabilities.

How Audio Increases Security

Real-World Evidence

A few years ago, an incident occurred involving a bus monitor and her students that illustrates how audio greatly enhances security.

It was June 2012. The location: Greece, N.Y. Karen Klein was harassed on a school bus by four schoolboys who verbally abused the 68-year-



old bus monitor with violent and graphic threats. While the bus's video surveillance captured footage of the boys pointing at her, it was the recorded *audio* footage (later posted to YouTube) that provided the most potent evidence – the boys' voices lashing out at her. Ultimately, the boys were punished with fines and suspensions because of this evidence of their verbal assault.

Video alone may have hinted at trouble, but only the audio provided enough evidence to prove guilt.

Alarm Verification

A key benefit of audio monitoring is that it assists in capturing a cause for alarm. It also helps combat false alarms by allowing companies to both see and hear what is going on (when combined with video security technology).

Audio monitoring, thus, provides secondary verification when a video system is triggered to an emergency, security threat or other unusual situation. The security system operator can verify to first responders that two sense points were triggered by the incident.

By adding audio monitoring, alarms can be activated based on sounds (above a specified, adjustable decibel

level). For example, in November 2013, police in Evansville, Ind., received a verified audio alarm from a local body shop. When they arrived, two suspects were taken into custody, and each had property from the body shop on them.

In short, a verified alarm can be a godsend to many organizations, as it provides real-time confirmation of an intrusion via visual or audio monitoring.

This technology truly provides companies with an enhanced way of keeping their assets safe.

Deterrence and Prevention

There have been many recent strides toward innovative technology (and applications of such technology) in the audio monitoring field,

including the twin areas of deterrence and prevention. One example of this is in the domain of security personnel and teams. Using a network-based, two-way audio system, along with video, security staff can remotely interact with suspicious persons in real-time, rather than needing to physically send a guard to the area. As a result, guards can monitor multiple zones, restricted areas or commercial locations, better identify threats in progress, and quickly respond with verbal warnings and directions.

Audio monitoring, thus, provides secondary verification when a video system is triggered to an emergency, security threat or other unusual situation. The security system operator can verify to first responders that two sense points were triggered by the incident.



Beyond Security: Other Ways Audio Improves Business Operations

When it comes to an organization's most fundamental security needs, audio is critical. However, there are other ways to use audio to benefit organizations.

- *Monitoring High-Traffic Areas.* Audio may be used to monitor high-traffic areas, in order to help keep people safe. This can be during normal, day-to-day, high-traffic periods, as well as during emergencies or natural disasters.
- *Loss/Vandalism Prevention.* Equipping businesses with audio monitoring can help them in their loss-prevention efforts, ensuring that employees are not stealing resources. Audio also helps strengthen protections against vandalism.
- *Training.* Audio is useful for providing employee training. For example, a fast food chain may want to use audio monitoring to ensure that employees are taking orders correctly.
- *Other Uses of Audio.* Audio technology can prove beneficial by improving operations, enhancing employee-to-employee and employee-to-

customer communications, and simply enabling day-to-day business to be conducted in a more efficient manner.

Challenges for Retail Businesses

Disputes with customers can be significant challenges for businesses. When such disagreements arise, a store manager can often use audio recordings to help resolve the issue. If there is a dispute between an employee and a customer, the manager can download and review the audio file from the store computer and determine what really happened, as well as what action should be taken.

In one case involving a customer and a shipping store, the customer claimed that an employee promised a refund. To resolve the issue, the store manager downloaded the audio file and

listened to it with the customer. The audio verified that the employee did not, in fact, promise a refund. This is just one example of many where audio can verify what really happened in a business setting. Video, by itself, in most cases, simply cannot capture exactly what was said and what interactions took place.

Businesses must deliver a safe, secure and welcome experience for their customers. Store managers face an ongoing need to prevent security

Audio can benefit organizations on many occasions by helping them avoid lawsuits, potentially saving them thousands of dollars.



breaches and property damage; they want to monitor their store's surroundings around the clock. To meet these needs, an optimal surveillance and security system would include multiple cameras and, in many cases, just a single microphone. The cameras would be placed throughout the store, while the microphone could be mounted on the ceiling above the main cash register. All of this gives the business owner and the store manager greatly enhanced peace of mind.

Legal Matters

In cases where an organization must meet certain legal requirements (for example, needing to avoid or achieve certain outcomes), audio can serve as additional verification, over and above any verification that is provided by video or other equipment already installed on-site. Video alone often cannot provide the full picture. Audio can help substantiate what was said by an organization's employees or visitors.

One of the greatest benefits that audio provides is protection against liability. Audio can benefit organizations on many occasions by helping them avoid lawsuits, potentially saving them thousands of dollars. In some cases, it may only take a single incident for audio equipment to pay for itself and for the organization to see a return on its investment.

The most common question that arises from dealers, integrators and end users alike is whether audio monitoring is legal. Title 18 of Section 2510 of the



United States Code defines privacy as communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." Simply put, when there is an expectation of privacy, monitoring is prohibited. By default, the statute also implies that when there is no expectation of privacy, recording is allowed.

For example, if people are walking and talking in a public space such as a town square or mall, there is a strong possibility that they might be overheard. As such, there is no expectation of privacy, and organizations can monitor for security purposes. Moreover, if an organization wants to install a surveillance system in a store or building, one of the tools they can use to remove the

expectation of privacy is signage. A clearly visible sign stating “audio monitoring is taking place on these premises” alerts people that the area is considered public, and, thus, privacy is not guaranteed.

What security professionals need to look out for are state laws on monitoring small groups of people. In order to record, consent must be given from the involved parties. However, each state has different laws regarding how many parties need to give permission. In Virginia, for example, only one of the parties needs to give approval, while in neighboring Maryland, all parties must do so. See

End users are demanding better solutions, and audio simply must be part of the equation.

the chart for more information. For expert legal advice, consult an attorney.

Audio Industry Forecast

Strong growth is anticipated in the adoption of audio monitoring as a security technology. More and more end users are realizing the value of audio when used in combination

with video. This adoption is taking place in both the IP and analog segments, and across verticals, including law enforcement,

retail, education and transportation. Public-facing positions in these verticals are increasingly embracing audio to provide verification of

State Statutes Addressing Audio Monitoring

State	Statute	Party Consent	State	Statute	Party Consent
Alabama	Ala. Code §13A-11-30	1	Missouri	MO Stat §542.402	1
Alaska	§42.20.310	1	Montana	MT Code §45-8-213	ALL
Arizona	Az. Stat §13-3005	1	Nebraska	NE Stat §86-290	1
Arkansas	§5-60-120	1	Nevada	NV Stat §200.620	1/Court Order
California	CA Penal Code §631	ALL	New Hampshire	NH Stat §570-A:2	ALL
Colorado	CO. Stat §18-9-303	1	New Jersey	NJ Stat §2A:156A-3&4	1
Connecticut	CT Stat §52-570d	ALL	New Mexico	NM §30-12-1	1
Delaware	DE Code Title 11, §2402(c)(4)	1	New York	NY Penal Law §250.00, 250.05	1
DC	DC Code §52-541 & §23-542	1	North Carolina	NC Stat §15A-287; §14-155	1
Florida	FL Stat Ch 934.03	ALL	North Dakota	ND Code §12.1-15-02	1
Georgia	GA Code §16-11-62	1	Ohio	OH Code §2933.52	1
Hawaii	HI Stat §803-42	1	Oklahoma	13 Okl. St. §176.2 -4	1
Idaho	ID Code §18-6702	1	Oregon	OR Stat §165.540, 165.543 & §133.005	1
Illinois	720 ILCS 5/14-2	ALL	Pennsylvania	18 PA Stat §5703 to 5704	ALL
Indiana	IN Code §35-33.5-1-5	1	Rhode Island	RI Gen Laws §11-35-21, §12-5.1	1
Iowa	IA Code §727.8	1	South Carolina	SC Code §17-30-20	1
Kansas	KS Stat §21-6101	1	South Dakota	SD Codified Laws §23A-35A-20	1
Kentucky	KY Stat §526.010	1	Tennessee	TN Code §39-13-605	1
Louisiana	LA Stat §15:1303	1	Texas	TX Penal Code §16.02	1
Maine	ME Title 15, §709	1	Utah	UT Code §77-23a-4	1
Maryland	MD Code §10-402	ALL	Vermont	No VT Statutes Address Monitoring	
Massachusetts	MA Ch 272, §99	ALL	Virginia	VA Code §19.2-62	1
Michigan	MI Laws §750.539c	ALL	Washington	WA Code §9.73.030	ALL
Minnesota	MN Stat §626A.02	1	West Virginia	WV Code §62-1D-3	1
Mississippi	MS Code §41-29-501 to 537	1	Wisconsin	WI Stat §988.31	1
			Wyoming	WY Stat §7-3-701	1



events and transactions. Playing back audio allows users to resolve any misunderstandings or disputes about what was said or offered to a customer, visitor or service provider. As the number of security cameras, recorders and software options supporting audio grows, a commensurate increase in the use of audio technology is expected.


Conclusion

The trend is clear: An increasing number of major organizations in retail, education, transportation, commercial and many other sectors have begun leveraging the power of audio for their surveillance and security needs.

Incorporating audio into security systems is the only way to ensure

the most optimal solutions for organizations that need to conduct surveillance and maintain security. End users are demanding better solutions, and audio simply must be part of the equation.

In summary, organizations cannot afford to turn a deaf ear toward audio when it comes to deploying a complete, all-around security solution. Combining audio and video is the only way to ensure that the best technologies are being applied to the world's surveillance and security challenges. ■ **Back to TOC**

Richard Brent (rbrent@louroe.com) is CEO of Louroe Electronics (www.louroe.com). 



By expanding surveillance coverage throughout an organization and across its perimeters – and even to remote sites – end users will be able to gain new levels of insight into their security programs while ensuring business efficiency and productivity is maximized.



The Sun Shines on Surveillance

Solar power enables wireless video solutions in remote locations

At some point, security professionals in nearly every organization must determine how to secure a perimeter or remote location. But adding surveillance cameras to monitor outdoor areas often comes with a hefty price tag. Traditional video security cameras are limited because they rely on cabling for power and network access, making surveillance difficult to add in areas of limited infrastructure.

A growing number of end users are seeking flexible surveillance technology that enables their organizations to gain a more comprehensive understanding of their security risks and operational efficiencies. Today's customers recognize the value of video surveillance solutions to protect the perimeter of their facilities, respond to emergencies and, in many cases, prevent incidents before they occur.

By Dave Tynan
MicroPower Technologies



Various new surveillance technologies have been designed with flexibility, cost savings and reliability in mind. Product developers are incorporating proven technologies,

such as wireless and solar, into robust surveillance platforms. These technologies are still fairly new to the security industry, but they deliver significant benefits to customers looking to secure outdoor and remote sites. Let's take a closer look at how these solutions provide an effective and flexible solution for remote facilities, critical infrastructure, perimeter security and more.

Wireless vs. 'Wireless'

Wireless cameras are an attractive option to meet perimeter or outdoor security and surveillance needs. A recent Google search on the phrase "wireless IP security camera" resulted in more than 2 million hits. But are all of these systems truly wireless? Wireless surveillance cameras promise to eliminate high installation costs by reducing cabling needs. Some models offer the choice of either a wireless or a wired connection to the network, but these cameras still require one outlet for power and network. Therefore, they are not truly wireless.

The challenge of routing a power source to a camera remains a major obstacle to the broad adoption of wireless cameras. Other common problems include dropped connections, interference from other wireless devices, poor video quality,

and even security inefficiencies related to the transmission of data. Such issues have a direct impact on the market's perceived reliability – and, hence, adoption – of wireless technologies. But today's next-generation wireless providers have made significant strides in the development of more robust solutions that "play nice" with other wireless devices and offer the same level of robust transmission protocols commonly seen within the consumer market.

In the mission-critical game of surveillance, where critical infrastructure and other facilities must remain operational and where failure

is not an option, organizations are not interested in a technology that provides anything less than 100 percent integrity. Surveillance systems that are protecting an electrical grid

or a hospital, for instance, require technology that can automatically fix any transmission or signal problems. Advanced line-of-sight technology is essential for facilities to ensure optimal system performance and up time.

Wireless surveillance systems based on open infrastructures can be easily integrated with existing investments, such as video management systems or additional cameras. The ability to integrate with third-party systems is

Wireless, solar-powered solutions can be deployed at unmanned or remote substations for less than half the cost of a traditional surveillance system.



absolutely imperative. Today, many end users strive to achieve a fully integrated security system to boost the efficiency of their security program and enhance response.

To effectively speed up response, communication with outdoor facilities and remote sites is critical. This is especially true for isolated sites, such as unmanned substations, that are situated miles from the nearest city. Additionally, network security is a top priority. Therefore, wireless systems need to be highly reliable and secure. Various emerging wireless solutions incorporate robust security protocols to maintain secure and reliable data transmission. No matter what, security and operational application monitoring relies on secure, live video data 24x7 to allow users to address

potential security threats efficiently and effectively.

Wireless cameras – those that *do not* require wires for cabling or data transmissions – eliminate the need for trenching, and can be installed quickly and efficiently, saving end users thousands in initial infrastructure costs. For example, wireless, solar-powered solutions can be deployed at unmanned or remote substations for less than half the cost of a traditional surveillance system.

Solar Energy

Alternative energy sources are emerging as highly reliable alternatives to traditional power. Consider solar energy. Solar technology is evolving at a breakneck speed, with incredible new innovations emerging every year. More

consumers and businesses are turning to solar energy to power their homes, office buildings, vehicles and more.

It is, arguably, one of the most exciting times the solar technology industry has ever seen.

But solar technology – like wireless – has had a long and, at times, difficult journey. Although solar power is now a mainstream energy source, it was once regarded as a niche technology, even though it has been used for hundreds of years. In 1767, the first solar collector was created by a Swiss scientist. This insulated glass box could reach temperatures of 230 degrees Fahrenheit. Almost 200 years

The incorporation of solar into security technologies enables organizations to realize cost and power savings. It also allows the security department – once only seen as a cost center – to contribute to sustainability initiatives and deliver new levels of cost efficiencies.

later, solar technology traveled to space, as the Soyuz 1 became the first manned spacecraft to be powered by solar cells.

Since that time, more efficient solar cells have been developed, reaching a photovoltaic efficiency of 36 percent. Improved solar power efficiency, combined with accelerating acceptance, innovation, and residential and corporate incentives, has helped push

global photovoltaic production to 1 gigawatt. In 2012, residential solar sales reached record numbers, as enormous investment in utility-scale solar plants continued. In 2014, total global solar power output surpassed 150 gigawatts.

Alternative energy sources gain more and more interest each year as organizations look to achieve corporate and environmental sustainability initiatives while maintaining the innovative level of technological advancement that is required to remain successful. Green policies give companies a better reputation when it comes to being a responsible corporate citizen, and they also produce benefits for an organization's bottom line. Sustainability efforts have taken off in many business sectors,





but the security industry remains one of the final frontiers for the adoption of eco-friendly solutions, mainly because those solutions have not been sufficiently cost-driven or practical.

Solar energy is not a new concept, but using it as a key component of a security system is. Solar power enables the development of technologies that are environmentally sustainable, consuming much less power than traditional systems. The incorporation of solar into security technologies enables organizations to realize cost and power savings. It also allows the security department – once only seen as a cost center – to contribute to sustainability initiatives and deliver new levels of cost efficiencies.



Added Operational Value

Organizations have found new uses for outdoor surveillance technologies, specifically for operations at isolated locations, which are common in the oil, gas and utility markets. Often, these sites are unmanned and need to be monitored to ensure safety and continued operations. The power and cabling requirements of traditional products often limit the use of video in such facilities, which face a wide variety of risks, such as terrorism, vandalism and crime, including copper

theft. Because wireless, solar-powered video solutions can be quickly set up without a complex installation process, the system is a good fit for these types of applications.

By leveraging surveillance systems for uses beyond security, various departments across an organization can review tasks, boost productivity and potentially cut costs.

End users in a variety of markets have begun leveraging the power of surveillance for uses beyond traditional security applications, enabling their organizations

to shift from situational awareness to situational assessment. For example, an operator not only sees that an emergency is unfolding, but also has enough information at his fingertips to

quickly decide whether the situation requires first responders or simply a maintenance crew.

In particular, oil, gas and utility providers have looked to cost-effective technology options to ensure a safe workplace and reliable operations. When users can optimize and monitor operations within their businesses – for example, employee adherence to company policies – using video surveillance investments, they gain a better-rounded picture of the organization's security status at any given time. This also helps spread the cost of a video surveillance investment across multiple departments and creates value throughout an organization.

Committed to remaining fiscally responsible and financially successful, end users continually look for ways to enhance customer service, boost operational efficiencies and reduce costs. Today's wireless solutions help these customers take steps to better protect corporate assets while remaining cost-conscious. Not only

does this allow organizations to save significantly on operational costs, it also enables users to remotely monitor operations to make more informed decisions about business processes and to respond to changing system demands, as needed. By leveraging surveillance systems for uses beyond security, various departments across an organization can review tasks, boost productivity and potentially cut costs.

The Future of Surveillance

No matter what kind of market users operate in – oil, gas or utility environments, educational facilities, or transportation sites – most require each new system to integrate with existing systems, including physical security information management (PSIM) platforms, passive infrared (PIR) sensors, video analytics, fence sensing, access control, and gunfire detection systems, to ensure a complete, end-to-end security solution. As companies look to add new solutions, they must make sure each system can integrate with existing investments. This will





allow information to be consolidated between various devices and help improve response times in the event of an incident, providing operators with an additional layer of situational awareness.

The future of the surveillance market will focus on systems integration and consolidation. Users continually look to get more out of their investments and increasingly demand the ability to tie multiple data points together. By expanding surveillance coverage throughout an organization and across its perimeters – and even to remote sites – end users will be able to gain new levels of insight into their security programs while ensuring business efficiency and productivity is maximized.

For companies today, the safety of their surrounding community, brand,

customers and employees comes first. Outdoor and perimeter areas cannot be ignored. Wireless, solar-powered solutions can be installed in high-risk, remote areas and then easily redeployed to other security hot spots for more targeted and fuller coverage. Technologies that enable users to better secure remote locations, while ensuring employee health and safety compliance, allow security professionals to remain focused on providing affordable, innovative, reliable security programs that contribute to a business's overall value. ■ **Back to TOC**

Dave Tynan (dave.tynan@micropower.com) is vice president, global marketing and sales, at MicroPower Technologies (www.micropower.com). 



The fit to IP seems to feel like hitching a locomotive engine to a shopping cart. It's just overkill, unless you recognize the added value associated with the convergence of intrusion with video and access control.



Integrating Intrusion

Video and access have converged on the network; the time has come for intrusion detection to join them

By any measure, IP communication is the most important trend in electronic physical security in decades. Although IP entered security technology as a solution to managing large amounts of video data generated by digital cameras, it now facilitates communication between disparate security systems so that each can leverage and incorporate the other's subsystem domain knowledge and features. This communication between devices is commonly referred to as IP convergence. It results in a system that promises better overarching functionality and, ultimately, a more intelligent and more complete threat response. Good systems integration adds value to the total system, enabling capabilities and benefits through interaction, and sharing, between the subsystems.

We are only in the beginning stages of true convergence between the two

By Mark Jarman
Inovonics



historically separate electronic security disciplines of video and access control. However, the trend is clear, and it will ultimately include the third discipline of intrusion detection.

The Rise of IP in Commercial Security

Video was the first security technology to move toward IP enablement, which granted a whole host of new benefits by making images digital and using IT equipment and methods to move data, analyze it, and store it most efficiently. And the marketplace responded: According to IHS, sales of IP video equipment surpassed sales of traditional analog video equipment in the United States in 2013.

The success of IP video has led to a similar move toward IP-enabled access control. Traditionally, access control was connected to a dedicated host computer using the serial RS-485 protocol. Now, a growing number

of access control systems are taking advantage of IP controllers. As a result, the video versus access rivalry has strengthened, but so has their combined value proposition. Before convergence, these two systems could only be made to communicate with one another through customized software and/or hardware, usually deployed and maintained by leading integrators or professional IT departments/firms. Now, when IP-enabled, they communicate using the same language, share similar data and execute decisions based on the sharing of inputs.

The benefits are greater scalability, the flexibility to expand the number of doors and cameras one at a time, and the connecting of features and functions in a way that enhances





each technology's value. All events are logged in the same way at the same time, providing a more coherent picture of a given situation.

Why Should Intrusion Be Part of the IP Party?

Why is intrusion a good candidate for IP convergence? Intrusion detection systems consist of multiple strategically-placed sensors that communicate a change-of-state

from normal conditions, indicating a security event, at a relatively low cost with high performance.

In other words, intrusion detection is a good value.

For example, a door is either open or closed, motion is either detected or not, infrared beam interruption or glass break detection occurs or does not. Typically,

these sensors connect to a control panel, which interprets the results and sends them to a central station to further investigate or initiate a response.

Intrusion devices are perfectly situated for the same kind of IP-enablement seen in the access control and video sectors. This would provide additional benefits, and at a value, on top of what has already been realized by the IP convergence of access and video.

Good systems integration adds value to the total system, enabling capabilities and benefits through interaction, and sharing, between the subsystems.

An IP-enabled motion sensor, for example, can trigger an IP-enabled camera to increase its frame rate before a subject enters the field of view, increasing the

likelihood that the images needed for identification will be captured. Sure, you can add another camera, but is the system's performance enhancement



worth the additional camera drop, or is the value offered by the convergence of intrusion with access and video greater with the addition of a relatively low-cost sensor?

Taking another step in this concept development, an IP-enabled access control system that includes IP-integrated sensors could conceivably respond to an unknown intruder detected at the perimeter of a facility with a lockdown before

entry is even attempted. With proper system design, the end user achieves tremendous advantages by using video, access control and intrusion sensors all integrated into a single solution.

So why are only two of the three security technologies being leveraged in this way? Why isn't there more of a push to include the IP communications integration of intrusion sensors in commercial security systems?

For starters, cameras generate a lot of data, and higher-quality images can be handled more efficiently over a high-speed communications bus, so IP-enabling here makes perfect sense. Access control databases, meanwhile, are well handled by servers and are similarly architected to IT networks, with intelligence distributed at the controllers of the doors themselves, so IP-enabling makes sense here, as well.

In contrast, intrusion sensors do not create much data and, therefore, do not require a high-speed network or massive storage. The fit to IP seems to feel like hitching a locomotive engine to a shopping cart. It's just overkill, unless you recognize the added value associated with the convergence of intrusion with video and access control.

For even greater value, commercial-grade wireless networks make the installation of intrusion sensors much easier and more cost-effective than before. There are few or no conduit runs, and devices are constantly monitored for their state-of-health. Outdoor trenching is often avoidable, perimeter detection can be far more cost-effectively established, and there is less overall business disruption with a wireless installation.

An IP-enabled access control system that includes IP-integrated sensors could conceivably respond to an unknown intruder detected at the perimeter of a facility with a lockdown before entry is even attempted.

Open Standards Development Needed for Video, Access and Intrusion

Let's say you are convinced that it makes sense to put all three pillars of security on an interoperable, IP-based platform. It's a beautiful vision, but it can be difficult to realize. Why? There are a wide variety of very technical packet, document and object-oriented communication protocol options within the IP-protocol environment. The video,

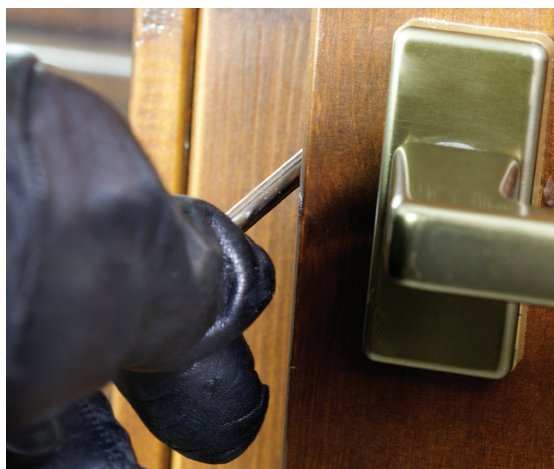


access and intrusion subsystems have different device types, and each has a different definition, behavior, expected output, and status or fault condition. Just talking IP does not solve the tough integration problems. There must be broadly developed and accepted open standards for communication between and among the subsystems. Only then can end users, installers and integrators enjoy cost-effective, reliable, fully-functioning, and scalable systems that operate as a coordinated and coherent whole.

Industry standards are one way the security industry can achieve this, but it cannot be done without the support and involvement of end users. Great effort has been exerted among manufacturers to create open standards that will provide a universal connectivity schema. Take, for example, the Physical Security

Interoperability Alliance (PSIA) and the Open Network Video Interface Forum (ONVIF). Each has been in existence for some time now, but neither has the full support of a majority of the industry. If the metric is end user demand and adoption, the efforts, as well intended as they are, are fragmented at best. Neither of these organizations provides comprehensive attention or appropriate weighting for all three disciplines. This creates an imbalance in the marketplace

Just talking IP does not solve the tough integration problems. There must be broadly developed and accepted open standards for communication between and among the subsystems.



that, unfortunately, end users are left to sort through to decide if and where there is additional value. Thus far, they have

demonstrated an unwillingness to do so because wide-scale adoption just is not there.

Now that intrusion has been entered into the IP convergence discussion and will gain inclusion into the lexicon of

open standards and trends, the security industry needs to broaden its view of what it means to focus on end user satisfaction. Higher performance and lower costs are very good places to start and are certainly within our technical grasp today. ■ **Back to TOC**

Mark Jarman (mjarman@inovonics.com) is president of Inovonics (www.inovonics.com). Ben Whitmer and Don Commare, both staff members at Inovonics, contributed to this article. ✉

A thermal image of a person standing against a blue background. The person's head, torso, and arms are visible, with colors ranging from yellow to red, indicating heat. The image is slightly blurred.

Cameras with increasingly higher resolution and higher frame rates have flooded the market. However, improvements in resolutions and frame rates are not the only technology trends that will influence the future of IP camera technology.



Surveillance in the 21st Century

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

The constantly evolving security industry has experienced some significant shifts in technology offerings in the last decade – from server-driven storage to cloud-based solutions, from analog to IP, and much more – and these advances often lead to the question, what's next?

End user organizations are leveraging technology to address issues in numerous vertical markets where security is paramount, including critical infrastructure, transportation, health care, government, education, retail and manufacturing. As more and more businesses and organizations identify the risks posed by outside threats, they seek out the latest and greatest technologies to help mitigate the danger.

Cameras with increasingly higher resolution and higher frame rates have flooded the market. However, improvements in resolutions and frame

By Jumbi Edulbehram
Oncam Grandeye



rates are not the only technology trends that will influence the future of IP camera technology.



Camera as a System

IP cameras with the capability to run a video management system (VMS) are making their way to the marketplace, delivering powerful features to customers.

Processing power in the cameras is increasing dramatically, and only a small percentage of the total processing power available is necessary to support video capture and transmission.

Therefore, companies are finding other ways to fully utilize this power, which results in new levels of intelligence and feature sets. Processing power will increase

functionality – not only for video management features but also for system management and administration.

The ability of cameras to store large amounts of high-resolution video on-board and only transmit video of interesting incidents will have a significant impact on the design and use of video surveillance systems.

Running a video system directly on the IP camera or a network of these cameras reduces the need for additional servers and software. All of the features present in a VMS – networking, communications, analytics, etc. – will live in the camera, allowing for cost-effectiveness and ease of use. An

example of an advanced application running in the camera is people-tracking – two separate cameras in a network could track a single person





transiting from one field of view to the next, and the cameras would have the ability to communicate and make intelligent decisions without having to run through a separate VMS.

Higher Resolution and Storage

There is no question that sensors, processors and storage are becoming more affordable as technology advances. The security industry is seeing increases in camera resolution. At the same time, as a result of more affordable storage options, businesses and other organizations have the opportunity to maximize their ability to collect and store video data, while addressing one of the major concerns in collecting this data.

While top-of-the-line resolution in security is approximately 30 megapixels, there are now cameras that are capable of gigapixel (yes, that's a billion pixels) resolution. Certain sectors will drive the adoption of these higher-resolution IP cameras, but as they become more affordable, other vertical markets will take notice and invest in them, as well. For example, there are already cameras capable of capturing detailed images of flying planes from the earth.

With higher-resolution video, the cost of storage will continue to be a major consideration, given that storage is one of the most expensive parts of a video surveillance deployment. One of the most significant trends today



is the increasing amount of on-board storage, which reduces the need for external storage. SD/SDXC cards of up to 256MB are currently supported, and preliminary testing is even being conducted with 2TB cards. The ability of cameras to store large amounts of high-resolution video on-board and only transmit video of interesting incidents will have a significant impact on the design and use of video surveillance systems.

Increasing Frame Rates

Most security industry professionals only see frame rates going as high as 120 frames per second (fps), but experimental cameras capable of producing 1 trillion fps – yes, 1 *trillion* – have already been developed in research labs. For the security world, only some applications, such as license plate recognition or gaming, currently require high-frame-rate cameras. However, there could be broad implications for such cameras in the transportation sector and in law enforcement. In the future, law enforcement may use ultra-high-frame-rate camera technology to determine the trajectory of a bullet during an investigation.

Better Compression

Not only are resolutions and frame rates continuing to increase, but larger amounts of data are also being collected from video surveillance

cameras, increasing the need for better compression. Currently, the state-of-the-art codec for compression is H.264, but H.265 is on the horizon, which will produce up to 50 percent better compression.

There also is a trend toward applying intelligence to compression techniques, so that interesting objects within a field of view have greater resolution than the rest of the image. For example, faces in a video could be captured at higher resolution, while the rest of the image could be in lower resolution, depending on bandwidth and storage constraints.

IT Security

Late last year, the world watched helplessly as hackers broadcast hundreds of thousands of video streams from security cameras on a public website, inciting widespread panic about the security of camera networks.

Moving forward, IP cameras and networks will need to incorporate or adopt higher levels of network security.

As we have seen in the past few years, data breaches and IT security have become major issues for

businesses and organizations that are entrusted with keeping personal information secure. As it stands today, not many IP cameras and camera networks are very secure, either in terms of penetrability or data integrity. Moving forward, IP cameras and networks will need to incorporate or adopt higher levels of network



security, such as virus protection, intrusion detection, prevention of denial of service attacks, etc., as well as encryption of video and data in transit and storage.

Light Sensitivity and Day/Night Capability

IP cameras on the market today have the ability to “see” in the dark using infrared (IR) or thermal detection technology. With these methods, images lose critical information such as color and may even lose significant resolution, making it difficult to distinguish facial features or other identifying characteristics that would help in an investigation.

Some IP camera manufacturers are spending time and resources developing more light-sensitive

sensors that will allow normal color images to be collected in much lower light. Additionally, there is now technology available that can add color information to IR images so that they appear the same at night as they do during the day.

Video Analytics

Not only do certain cameras now offer VMS capabilities, some contain a large number of applications that can be run inside the camera so that interesting events and data can be extracted and analyzed. There are a host of basic pixel-based analytics, as well as relatively sophisticated object-based analytics, that can be run inside the camera, which means additional analytics software does not have to be installed.



Businesses and organizations can look forward to analytics in cameras that include behavioral and predictive analysis, learning systems, and multi-camera intelligence. With these capabilities, video becomes a management tool to optimize business solutions. This intelligence capability inside an IP camera adds value to organizations by allowing video to take on multiple roles – for example, tracking employees and staffing levels inside a retail store, analyzing traffic flow patterns, noting how long people dwell at a certain location, and much more.

Omnidirectional Cameras

More and more omnidirectional, or 360-degree, cameras are making their way to the market, and, as the technology improves, they are becoming more affordable. These 360-degree cameras provide much more coverage than narrow field-of-view cameras. Single-lens fisheye cameras get a full 360-degree image that then needs to be “dewarped.” Multi-lens 360-degree cameras contain multiple lenses in one unit whose images are stitched together to create a full, inclusive image. With higher resolutions and more efficient dewarping/stitching technologies,

these omnidirectional cameras will soon replace the standard pan-tilt-zoom (PTZ) cameras widely used today.

Higher resolution also will allow these multi-directional cameras to deliver superior images and give

Businesses and organizations can look forward to analytics in cameras that include behavioral and predictive analysis, learning systems, and multi-camera intelligence.

businesses more value. With current PTZ technology, the video stored is only what the camera sees, but with 360-degree cameras, multiple areas are monitored at the same time for full situational awareness. Even

if the operator is only interested in a certain area, the stored video features the full 360-degree view.

Wireless Connectivity

Today, Wi-Fi is being used for wireless connectivity in IP cameras. As greater 4G data bandwidth becomes available and costs decrease, cameras will have the ability to connect directly via cell phone networks. Further in the future, as satellite bandwidth becomes cheaper, cameras may even be able to communicate via satellite.

3-D Cameras

We view the world in 3-D, so it is only natural that cameras with 3-D capabilities would deliver a big advantage for security systems. These 3-D images provide more valuable information and are much



more intuitive for the human eye to process. For example, today's cameras might see two people enter a door, but the camera cannot distinguish between the two different objects. With a 3-D camera, the two people are viewed as separate and, as a result, more accurate analytics readings can be taken. Similarly, a camera placed overhead today for people counting cannot distinguish between an adult and a child; 3-D cameras, however, provide the additional "depth perception" that allows this distinction to be made.

Light-Field Cameras

Another interesting development concerns light-field, or "plenoptic," cameras that can be focused after the fact – that is, an operator can refocus an image on a computer after the picture has been taken. Right now, this

technology is too expensive for use in security cameras, but, as the technology becomes more affordable, the capability will enable security personnel to focus on objects of interest in recorded video. Additionally, integrators will not need to focus cameras on installation, allowing for quicker and cheaper installations.

The Future is Bright

The future of IP camera technology is an exciting part of an ever-changing industry. Improvements in storage, resolution and processing capabilities are at the core of this shift, and as organizations begin to invest in this advancing technology, they will benefit from the safety and security that comes with it. ■ **Back to TOC**

*Jumbi Edulbehram
(jedulbehram@oncamgrandeye.com) is
regional president, Americas, at Oncam
Grandeye (www.oncamgrandeye.com). ✉*



As transit infrastructure continues to develop and ridership increases, so do its safety and security challenges, especially in urban and densely populated areas.



10.7 Billion Security Challenges

As transit ridership increases, so must security

Transit plays an important role in the American Dream. Not only do bus and rail infrastructures across the country offer transportation to millions of commuters and deliver goods and services, but these operations provide a significant amount of jobs that help the American economy grow. Transit security falls under the auspices of the Department of Homeland Security (DHS), and the sector is classified as critical infrastructure. According to DHS, critical infrastructure is defined as the “assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

Transit infrastructure continues to grow today, fueled in part by volatile

By Steve Cruz
Panasonic



gas prices and the desire by many to move into urban areas. According to the American Public Transportation Association, Americans took 10.7 billion trips on public transportation in 2013.



Other statistics confirm the vitality of this vertical:

- Since 1995, public transit ridership has increased 37.2 percent, outpacing population growth (up 20.3 percent) and vehicle miles traveled (up 22.7 percent).
- People board public transportation 35 million times each weekday.
- Public transportation is a \$57 billion industry that employs more than 400,000 people.
- More than 7,200 organizations provide public transportation in the United States.

With increasing ridership, the sector continues to upgrade and build out infrastructure. In February 2015, \$3.2 billion in new initiatives were announced by U.S. Transportation Secretary Anthony Foxx to advance the construction or completion of 25 rail, bus rapid transit (BRT), and streetcar projects in 13 states. These projects, competitively funded through the Federal Transit Administration's Capital Investment Grant Program, would

create thousands of construction and operations-related jobs and help communities expand transportation choices that offer "new ladders of opportunity for residents," according to the FTA.

The federal budget outlines funding recommendations for 11 new transit projects to connect thousands of residents in cities and communities across the country with jobs and other opportunities. A few of these projects include:

- The Cleveland Avenue BRT line in Columbus, Ohio, which will reduce overcrowding and shorten travel times on the Central Ohio Transit Authority's second-busiest bus route and improve connections to downtown Columbus's employment, education and health destinations for thousands of residents who live along the corridor.
- The Mid-Coast Corridor Project in San Diego, Calif., which will extend light rail service to the northern community of



University City, significantly improving access to educational institutions and the Veterans Affairs medical facility in north San Diego, and connecting residents to existing light rail service in downtown San Diego.

- The Provo-Orem BRT line in Utah County, Utah, which will provide more frequent, reliable bus service connecting the Brigham Young University and Utah Valley University campuses to Provo and Orem, as well as employment centers within the corridor.

With this growth spike, transit agencies with antiquated security and analog infrastructures will likely look to upgrade to the latest technologies in perimeter security, intrusion detection, video surveillance, mobile and wireless connectivity, and access control – with everything connected and networked via IP.

Challenges and Issues in the Transit Environment

As transit infrastructure continues to develop and ridership increases, so do its safety and security challenges, especially in urban and densely populated areas where the majority of the agencies charged with operating these entities reside. But criminal activity at bus, light rail and heavy rail facilities has actually decreased over the past two years, perhaps as a result of the ongoing installation of video surveillance cameras. The city of Chicago has been at the forefront of this activity, installing more than 3,600

With this growth spike, transit agencies with antiquated security and analog infrastructures will likely look to upgrade to the latest technologies in perimeter security, intrusion detection, video surveillance, mobile and wireless connectivity, and access control – with everything connected and networked via IP.

cameras at its Chicago Transit Authority stations, as well as high-definition cameras in 850 rail cars.

While reducing crime remains a challenge, there are also concerns about an uptick in liability claims, fraudulent activity, safety violations and non-compliance by operators and other transit personnel. And technology, especially solutions that are seamless and easily accessible, can be used to efficiently mitigate those concerns.

The Vast Transit Landscape

Transit agencies and their facilities need comprehensive, integrated solutions to address their wide array of challenges. Security technology not only needs to address assaults, weapons violations and even homicides, but also



slip-and-falls and unsafe operations. Agencies not only need to make vehicles, rolling stock and station facilities safer, but also take advantage of networked surveillance and high-definition video that can be used to educate operators about correct

procedures, or the dos and don'ts of safe train or bus operations. In addition, issues such as fare evasion, revenue theft by employees, and crimes against transit property, such as vandalism and graffiti, need to be addressed on a daily basis. The threat of terrorism is also a

Case Study:

Denver Regional Transportation District

Mobility is a definite advantage of using IP-based solutions as opposed to analog devices, and this is critical to transit systems – which are literally on the go. A recent deployment at the Denver Regional Transportation District (RTD) Transit Police Division is a prime example of how mobility assists transit security.

One of the largest public transportation systems in the nation, the RTD has worked extensively over the last several years to conceptualize and deploy a comprehensive mobile video surveillance system to meet the expectations of riders, employees and other stakeholders. Using LTE cellular broadband, RTD officials can access live video streams from trains and buses on their IP-enabled devices anywhere, anytime, whether at a command and control center or in the field with smartphones or tablets. In the event of an emergency, law enforcement can access transit vehicle video feeds from patrol cars, using laptops and tablets to gain

better situational awareness prior to responding.

Leveraging the existing IP network infrastructure, integrated security solutions also offer transit security officials the ability to automatically offload video recordings. Instead of relying on drivers or maintenance crews to manually remove hard drives from buses, then spending countless hours reviewing videos to investigate an incident, as was the case with analog DVRs, administrators use wireless connectivity to retrieve video recordings without putting the equipment at risk. This enables them to reduce the time and costs associated with system maintenance and streamline the video transfer process.

Recognizing the challenges of mobile video surveillance, the RTD has installed rugged, vandal-resistant, IP66-rated cameras that are specially engineered to withstand vibration, shocks and impacts. Each of the new cameras is equipped with anti-



consideration, especially in densely populated areas marked by DHS as being potential targets of terrorist attack.

Compounding the need to provide comprehensive security, safety and accountability is the vast and

varied transit landscape. This critical infrastructure can include structures in isolated facilities, parking lots, and a host of other remote and in-city sites. As such, they may require security lighting, fences and anti-vehicle barriers coupled with other system solutions.

vibration mounts to ensure long-term performance, while cameras on bus exteriors are secured in purpose-built shroud housings for added protection against impacts and extreme temperatures.

IP-enabled mobile video surveillance solutions also offer the high-definition video quality needed to maximize situational awareness within public transportation systems. Using full HD 1080p and HD 720p

network cameras inside and outside of each bus, RTD administrators have integrated their new IP-based system with other hardware and software components to create an end-to-end mobile security solution.

In the past, RTD investigators had to search through surveillance recordings to investigate every incident. The new system leverages video management software with

time-stamping capabilities to view and manage video files. It also integrates with various other video and audio sources and case files, creating a unified event timeline, no

matter where in the district the incident occurred. These capabilities dramatically reduce the amount of time spent investigating incidents and ensure the availability of high-quality video evidence when it

is needed.

The city of Denver is embarking on an independent study to determine the effectiveness of its new solution. However, the Denver Police Department has already used the system as an investigative resource to solve a crime. The police were able to use video from several stations to identify the person responsible for a sexual assault.

Using LTE cellular broadband, RTD officials can access live video streams from trains and buses on their IP-enabled devices anywhere, anytime, whether at a command and control center or in the field with smartphones or tablets.



Consultative Approach

As with any other security system deployment, each transit agency requires the solution provider to conduct an in-depth site survey and comprehensive evaluation of current and future needs, threats and challenges. Legacy technologies and their effectiveness should be part of the consultation. Although many transit agencies have been upgrading from analog to IP-based video surveillance as they revamp or rebuild their facilities and replace their buses and rail cars, some still rely on analog, making attainable migration paths to digital a necessity in overall planning.

Video surveillance and IP installations play a significant role in addressing the ever-changing and varied needs of the transit market. In recent years, the shift from analog to IP has paved the way for integrated, IP-based, mobile video surveillance solutions. Mobile DVRs with hard drives operating alongside analog cameras have moved to mobile NVRs with network connectivity. This provides ease of use, reliability and greater accessibility to recorded video.

In addition, driven by increasing demand for advanced technologies such as high-definition video, thermal imaging and video analytics, the security industry has been working to develop cutting-edge systems for the transit market to update their infrastructure with additional solutions that quantify

security and safety and gather intelligence and other operational data from network-connected systems.

Safety and Operations Compliance

As many transit administrators know, the most critical area of any transit vehicle – whether it is a train, bus or railway car – is the driver's seat. By installing audio recording security devices in the driver's booth, public transportation officials are able to better

protect staff and ensure activity within the vehicle complies with all laws and codes of conduct. These next-generation devices can even be used to help train

new employees or resolve fraudulent injury claims. IP mobility also promotes additional safety for drivers, with the ability to deploy two-way audio and duress or panic devices in the train operator's cab or near the bus driver's seat.

The examples of transit organizations deploying security technology continue to multiply. For heavy rail, the Long Island Railroad has put in a new mobile surveillance system that will assist with security concerns in their rolling stock, while also addressing potential terrorist threats. In Boston, the Massachusetts Bay Transportation Authority is in the process of retrofitting more than 200 buses in its fleet with new high-tech cameras that show the insides of the vehicles from multiple angles. This gives

Security technology not only needs to address assaults, weapons violations and even homicides, but also slip-and-falls and unsafe operations.



the agency a good look at who is riding the bus, with each installation including a quad-matrix monitor at the front of the vehicles, so riders, too, can see what is happening. In total, some 235 vehicles are expected to eventually have the technology, which will allow transit police to download footage wirelessly. The security system is being funded by a \$7 million grant from DHS.

Integrated IP security solutions and network connectivity provide the mobility the transit market needs. Now, transit authorities can leverage high-speed Wi-Fi, 3G and 4G wireless, and even mesh radio signaling to provide a comprehensive solution to keep passengers and personnel safer. Being able to access live video streams on the fly enables administrators to improve safety for passengers and

transit workers, protect physical assets and aid the investigation of accidents or liability claims. Recorded video of

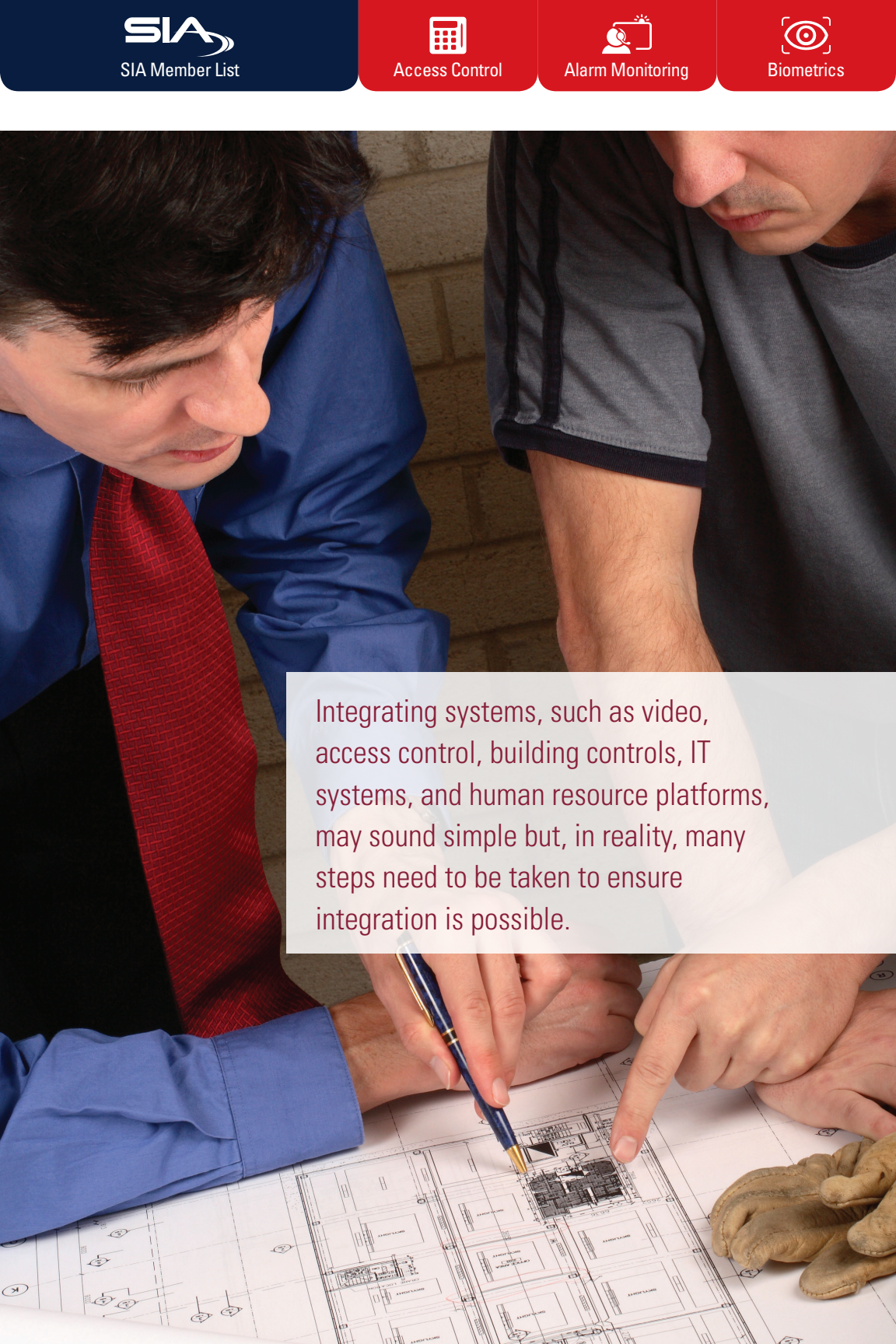
Video surveillance and IP installations play a significant role in addressing the ever-changing and varied needs of the transit market.

drivers and train operators provides a much-needed learning resource, recording actions as they happen so necessary corrections can be made before

a safety incident occurs.

The transit market is rapidly changing, upgrading its infrastructure to keep up with a growing population of riders. The security industry has all the technology it needs, and the forward-thinking attitude to apply it correctly, making the American Dream a safer reality. ■ **Back to TOC**

Steve Cruz (steven.cruz@us.panasonic.com) is strategic solutions manager for transit at Panasonic System Communications Company of North America (www.panasonic.com/business-solutions). 

A photograph showing two men, one in a blue shirt and red tie and the other in a grey t-shirt, leaning over a table and looking at architectural blueprints. One man is pointing at a specific area on the plan with a blue pen, while the other points with his finger. A pair of work gloves is visible on the right side of the table.

Integrating systems, such as video, access control, building controls, IT systems, and human resource platforms, may sound simple but, in reality, many steps need to be taken to ensure integration is possible.



Tying It All Together

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

Faced with a growing number of threats, it is up to security professionals to safeguard their facilities, assets and employees with an effective blend of technologies and policies. Access control solutions often are the first line of defense, but users increasingly look to add layers of protection to their organizations. Such additions may include video surveillance, biometrics and video analytics, among other solutions.

Today's end users want more. They want more video, more access control functionality, more security data and more situational awareness. All of these wants, which often turn into needs, are a direct result of the desire to integrate multiple networked systems together. Integrating systems, such as video, access control, building controls, IT systems, and human resource platforms, may sound simple, but, in reality, many steps need to be taken to ensure integration is possible.

By Mitchell Kane
Vanderbilt Industries



Ensuring Safety

Organizations of all sizes in all markets must be diligent in ensuring the safety and welfare of their employees and visitors, while



protecting infrastructure and trade secrets. No business is immune from threats of crime, violence and other disruptive behaviors. End users continually seek new ways to innovate, and technology investments are a significant part of this initiative.

Security systems are absolutely critical to helping ensure a high level of security and compliance with various safety processes and security regulations. Access control is the backbone of any strong security solution. These systems limit where individuals can go within a facility and ensure that visitors are registered and monitored.

IP video surveillance cameras help users keep an eye on security processes and business operations. Cameras are extremely valuable, but any comprehensive security installation has to start with access

control. Once both systems are running in conjunction with each other, the access control system lets users know whom they are seeing on the video. Without access control, this level of

information is not delivered. A comprehensive safety and security program that integrates video and access into

one combined solution effectively provides new levels of awareness while ensuring a high level of security.

By far, integration between access control and video surveillance systems is what end users most demand.

Intelligent Integration

By far, integration between access control and video surveillance systems is what end users most demand. Video is a more valuable tool when combined with access control data – it provides visual verification of alarms and a variety of access control events. For example, security personnel can view the video associated with a door opening. This can help them determine





Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance



whether an approved individual entered the facility or a card was stolen. The correlation of the data from these two systems also allows for an additional level of situational awareness. Video playback can provide security personnel or first responders with a better understanding of a security or life safety event before responding.

Integration reaches far beyond video and access control, though. Today's end users

The ability to change the environmental or power profile of a building based upon information gathered by the access control system is highly valuable and helps end users reduce costs while securely controlling access points.

require that the security systems they invest in be able to integrate with other network-enabled platforms,

such as building management systems. With this integration, swiping a card can, for example, communicate to the building management system to turn on lights in a certain part of a building. Advanced access control software solutions support

this type of action and also can enable the building management



platform to implement a security profile based on specific, pre-defined actions. Overall, the ability to change the environmental or power profile of a building based upon information gathered by the access control system is highly valuable and helps end users reduce costs while securely controlling access points.

Training is necessary to gain the knowledge needed to integrate various systems. Integrators need to allocate time to participate in manufacturer training or certification courses to learn how to best link technologies together. There are many instances in which a facility manager manages a building's security, while a tenant manages the

Case Study: Crider Foods

Crider Foods is a provider of shelf stable and fully-cooked products for customers around the world. The company recently invested in a state-of-the-art plant for frozen fully-cooked products, and it expanded its canning operation and warehousing.

After building new facilities in Georgia, Crider looked to further enhance its technological capabilities by deploying a comprehensive security system. The company deployed a system that manages access for more than 500 employees and contractors at approximately 150 contact points at 11 locations on the campus. Locations include the cook plant, headquarters, visitor's lodge, canning plant, cooler building, transportation building, warehouses and other sites.

"Our security system is absolutely critical to helping ensure compliance with all the health and safety rules and regulations we have in the food production industry," said Crider IT Director Ron Sasser,

who also oversees security. "We are committed to an extremely high level of access control management to prevent any cross contamination of our products."

Crider also uses its access control system to verify time and attendance information. If an employee does not punch in, Sasser and staff can use the system to verify if and when the employee entered the property. In addition to controlling access to buildings and within buildings, Crider employs guards at the facility's road entrances to verify all vehicles coming onto the property.

"Our priority is to limit access for all our employees as to where they can go in the facility," Sasser said. "The [access control] system enables us to manage employees so that they can access only the areas where they have been scheduled to work, when they are scheduled to work. We also have the flexibility to easily change those access privileges as needed, at any time."



tenant's security. This can lead to the installation of multiple systems. If a systems integrator can speak both languages and bring these multiple stakeholders to the table to have a conversation about the integration of systems beforehand, the investment will be much more valuable to all parties.

On-Demand Intelligence

Many of the current demands from users center on a desire for improved data accessibility, driven by the proliferation of intelligent devices. They want to have access to their systems from anywhere. That is why we see, among other things, expanded mobile applications, offline and

Crider Foods' top priority is achieving full compliance with food and safety regulations in order to reach the highest level of Safe Quality Food (SQF) certification. Crider has

succeeded in attaining SQF Level 3, which requires "a comprehensive implementation of safety and quality management systems," and which only a few companies achieve. "To reach such a certification level,

we carefully control the movement of all individuals within the complex, and this means, for example, restricting access to chemicals and to the roofs of our buildings, among other sensitive areas," Sasser said.

Crider also deployed 100 IP video surveillance cameras to keep an eye on operations.

"Cameras are helpful, but you have to start with access," Sasser said. "My access control system tells me who I'm seeing on the video. Now I know who someone is, because the

access control system puts them in that location."

The system provides layered levels of security, starting from the minute a person steps onto the Crider property. It supplements time and attendance

data and provides documentation for Occupational Safety and Health Administration (OSHA) reporting. Overall, Crider's security management platform provides company managers with the tools they need to maintain one of the highest SQF certification levels in the industry.

"Our security system is absolutely critical to helping ensure compliance with all the health and safety rules and regulations we have in the food production industry."

**—Crider IT Director
Ron Sasser**



online smart locking systems, and smartphone Bluetooth credentials.

There is significant interest in mobile applications. Users of all sizes, whether they are enterprise customers or small and medium-sized businesses, want to be able to manage their security infrastructure from anywhere in the world. As the technology continues to advance, mobile applications and functionality will become more adopted.

Additionally, with the ever-expanding Internet of Things, greater interoperability will be paramount to ensuring disparate systems are linked to create a cohesive solution.

Delivering the best solutions will necessitate embracing new technologies and supporting the

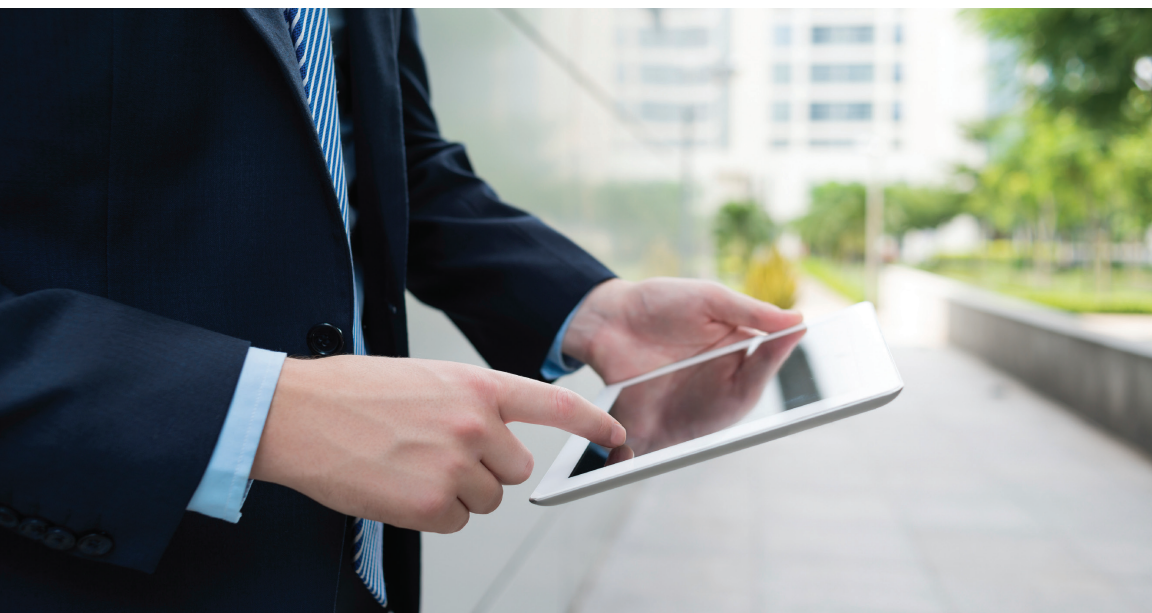
expanded functionalities that these new technologies offer. From an end user's perspective, this means keeping the programming of disparate devices constant with core products. The only real distinction should be how and when data is updated. The trend of co-

existence between traditional mechanical access control and emerging electronic and wireless access control is all about consistency among these technologies,

allowing users to streamline installation, service and maintenance, and to easily expand their access control network when needed.

The functionality of these technological advancements is taking hold of the market, albeit slowly. Although near-field communication

Many of the current demands from users center on a desire for improved data accessibility, driven by the proliferation of intelligent devices.





Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance



(NFC) hit the market first with many trial installations, the jury is still out

on its use for access control, and Bluetooth seems to be surpassing NFC as the preferred technology. Many vertical markets can look forward to expanded mobile capabilities,

including access control using mobile credentials. Additionally, with the growing need for mobile data management, close integration

between multiple systems, and a drive for new levels of situational awareness,

Users of all sizes, whether they are enterprise customers or small and medium-sized businesses, want to be able to manage their security infrastructure from anywhere in the world.

we can expect a greater amount of interoperability between disparate products. This will only help users gain new levels of security, mobility and operational efficiency.

■ **Back to TOC**

*Mitchell Kane
(mitchellkane@vanderbiltindustries.com)
is president of Vanderbilt Industries
(www.vanderbiltindustries.com). [envelope icon]*



Video surveillance is becoming both more commonplace and more cutting edge. One of the most exciting elements in the security industry is how quickly technology is evolving to meet the needs of a diverse set of markets.



The Future of Video Surveillance

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

The global video surveillance industry is expected to grow by 10 percent this year, according to IHS. Public safety is a big concern, given national and global events, and this correlates to notable growth in the education and safe cities verticals. Municipalities are discovering the benefits of video surveillance in public areas, not only for security, but as a way for law enforcement to get a better picture than can be seen with human resources alone. Other markets that have been historically strong, such as finance and retail, are continuing to grow.

North America has been incredibly responsive to video surveillance solutions, both with enterprise and small and medium-sized business (SMB) clients. As the economy improves, businesses in all industries are able to allocate more resources to security, and they are also making video

By Alex Asnovich
Hikvision USA



surveillance an important part of their budgets, rather than an afterthought. Manufacturers who seek to address these needs must place emphasis on localized customer service, as well as



provide technologies that help bring video surveillance to a broader range of end users.

In terms of greenfield installations, video surveillance is increasingly being implemented at the architecture and engineering level. Building information modeling (BIM) is one exciting technology that is helping surveillance grow. Security products

available on software give engineers the ability to incorporate video surveillance into the earliest stages of architectural planning. Camera models can be dropped into a building design and manipulated to determine what the best field of view would be from

The presence of surveillance products in BIM demonstrates how security is becoming a primary element of building infrastructure, rather than being added piecemeal if and when the need to bolster security suddenly becomes critical.

a given location. Cabling and power supply for the security system are then embedded into the structure

of the building in the same way plumbing or HVAC would be. The presence of surveillance products in BIM demonstrates how security is becoming a primary element of building infrastructure, rather than being added piecemeal if and when the

need to bolster security suddenly becomes critical.

When discussing new trends in video surveillance technology, the conversation usually centers on IP. The capabilities of IP video are increasing, in terms of analytical features, resolution





and compression. 4K and H.265 are appearing on the horizon, delivering, respectively, ultra high-resolution video and the ability to efficiently compress it. This combination will support the clearest, crispest images ever seen in video surveillance, and the potential for enterprise applications is endless.

The hefty price tag that traditionally accompanies state-of-the-art IP products can be a challenge for integrators. Those who look at the big picture will understand that the added functionality of IP gives them the ability to be more proactive. They can reach out to end users the moment

they notice that something is awry. For example, most IP cameras and recorders now have the built-in capability to send a signal when something is not functioning properly – such as if a

camera is not operating or a hard drive is failing. Another simple way to monitor equipment is via DDNS, which provides “online status” indicators. This gives a quick snapshot of devices that have gone offline. These tools are used over the existing IP

connection, allowing integrators to offer status monitoring as a service without accruing overhead costs for themselves or for the end user.

It is also important to consider that,

It is also important to consider that, as the high end of video surveillance becomes more technologically advanced – and more expensive – the low end is becoming increasingly more affordable and user friendly.



as the high end of video surveillance becomes more technologically advanced – and more expensive – the low end is becoming increasingly more affordable and user friendly. High quality plug-and-play IP solutions and high-definition analog products are more cost-effective than ever before. The time needed to install and configure these products is minimized, enabling significant cost reductions.

High-definition analog solutions such as HDTVI have proven to be popular because they allow for better performance from analog systems and make the most of investments in original infrastructure. By

sending uncompressed, high-resolution video over existing coaxial cable, HDTVI bridges the technology gap. It supports up to 1080p at distances of more than 1,500 feet, and includes the functionality of bi-directional signaling. The migration from analog to IP becomes seamless with “tribrid” recorders that can simultaneously save data from standard definition analog cameras, IP cameras and HDTVI cameras. There are innumerable legacy analog installations in widespread use, and end users without the budget for a full IP upgrade can turn to cost-efficient high-definition

analog for an interim solution.

Another factor that is conducive to growth in the industry is the increasing ability to integrate other technologies with video surveillance. Cloud-based video surveillance is a growing market that provides great benefits to the user. It eliminates the need for onsite storage and investment in hardware. It is especially well-suited for mobile

solutions, and its widespread use is seen across multiple sectors, including public transportation, education and law enforcement. Another notable element of cloud surveillance is that it enables the user to pay for only the amount of storage needed, and it is extremely flexible

While cloud technology is becoming easier and easier to incorporate, there seems to be a lingering misconception in the marketplace that the cloud is not secure. In truth, the cloud has the potential to be just as secure as any other network solution.

as those needs change from month to month or year to year. In addition, it allows for the delivery of services via the cloud, whether monitoring, storing or serving video for live or recorded view, which is commonly known as video surveillance as a service (VSaaS).

While cloud technology is becoming easier and easier to incorporate, there seems to be a lingering misconception in the marketplace that the cloud is not secure. In truth, the cloud has the potential to be just as secure as any other network solution. Encryption is an established technology that is



becoming simpler to deploy, and end users who choose to keep encryption keys in-house will benefit from an added layer of protection.

It is crucial for manufacturers to educate integrators regarding best practices for a secure video surveillance solution, and for integrators to pass this knowledge along to end users. People take security personally, as they should: Surveillance systems are deployed to protect the most important things in their lives. Manufacturers who cultivate a personal relationship with their integrators and end users will win trust and well-deserved loyalty.

This brings us to another trend in the marketplace today, do-it-yourself (DIY) video surveillance. IHS reported that the DIY video market exceeded \$1 billion in 2014. That is obviously a figure that cannot be ignored, but neither should professional integrators and installers be fearful of it. Instead, it shows that consumers are becoming increasingly interested in video surveillance. New technology has improved the quality of the video offered by DIY systems, while also making the product easier to install.

Overall, DIY should not have much impact on the professional market. Most consumers do not have the time and/or the skillset to install and maintain a system on the level that a professional installer can. There will come a time when their security needs exceed the capabilities of their DIY system, and they will turn to professionals to handle the upgrade. In addition, a greater understanding of video surveillance could boost overall sales of video



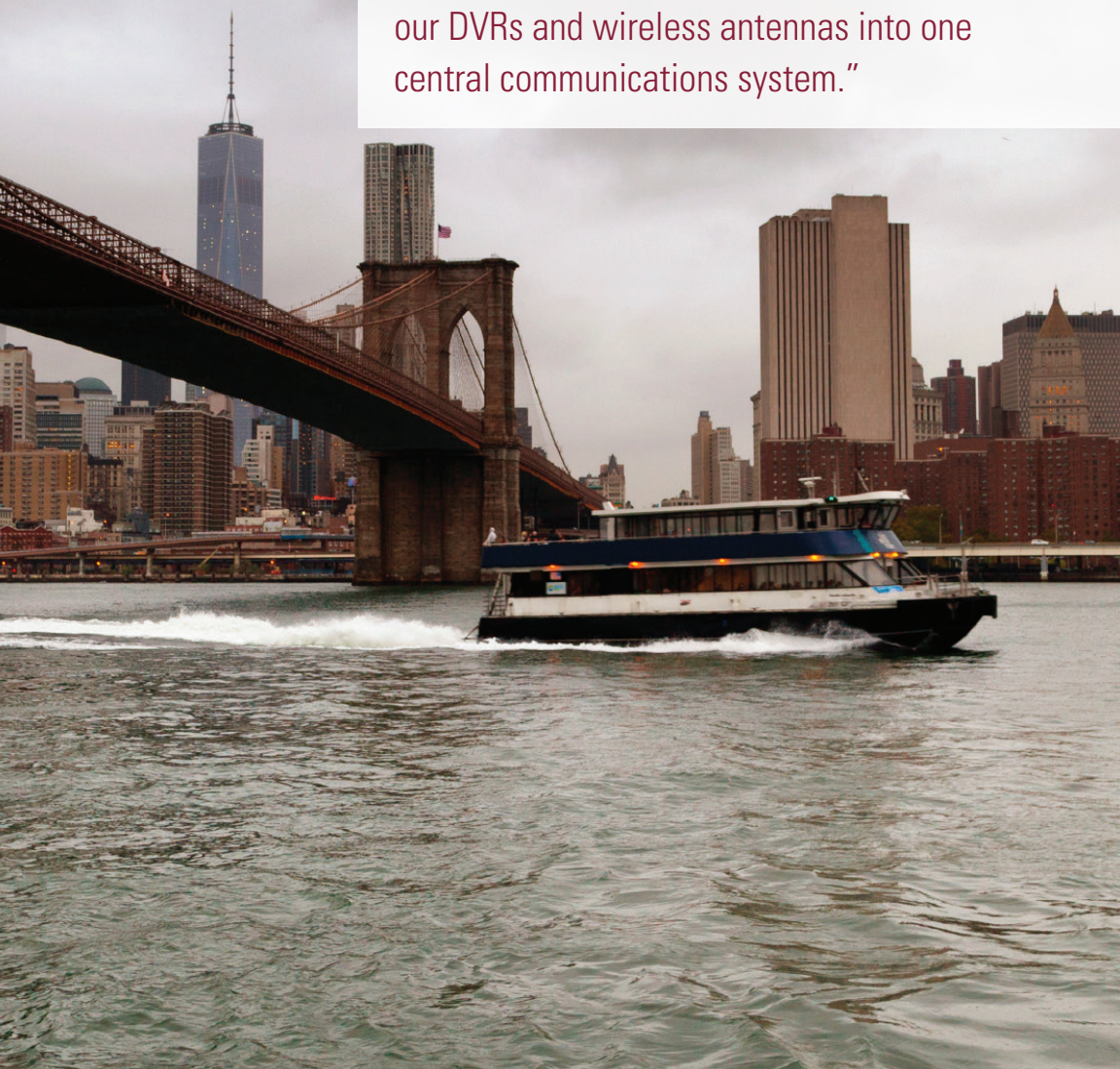
equipment at the SMB level, and maybe even at the enterprise level. Those are sectors that still require the expertise of a professional.

It is clear that video surveillance is becoming both more commonplace and more cutting edge. One of the most exciting elements in the security industry is how quickly technology is evolving to meet the needs of a diverse set of markets. Manufacturers and integrators must keep abreast of the latest trends and seek creative ways to serve end users, in order to provide the benefits of comprehensive security solutions for years to come. ■ **Back to TOC**

Alex Asnovich (alex.asnovich@hikvision.com) is director of marketing at Hikvision USA (www.hikvision.com). ✉



“That’s where [the equipment manufacturers] were able to enhance our security – by integrating our cameras, our DVRs and wireless antennas into one central communications system.”





Safe on the Water

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

To many New York and New Jersey residents, NY Waterway is much more than simply a means to commute between home and work. Time and again, the nation's largest independently owned commuter ferry operator and its employees have been there during an emergency.

- On Sept. 11, 2001, NY Waterway ferries helped evacuate people from lower Manhattan after terrorist attacks on the World Trade Center left the city's mass transit in shambles.
- When a U.S. Airways jet ran into a flock of geese shortly after takeoff on Jan. 15, 2009, the pilot was forced to land in the Hudson River. NY Waterway was there to help rescue many of the 155 crewmembers and passengers.
- In late October 2012, Hurricane Sandy struck the region with

By Kostas Mellos
Interlogix



tremendous winds, rain and high tides that closed subways and major automobile tunnels and bridges for days. NY Waterway resumed its regular



service as much as a week before other transportation alternatives.

- NY Waterway has been a vital transportation option during many other marine incidents, and even during a massive multi-state blackout.

Since beginning service with a single ferry route in 1986, NY Waterway and its associate, Billybey Ferry, now operate 35 vessels covering about 100 miles of the Hudson and East rivers and Upper New York Bay. The company annually serves about 8 million commuters and tourists.

Now, with the help of a grant from the U.S. Department of Homeland Security, those passengers ride in greater safety under the watchful eyes of a sophisticated video surveillance system that provides real-time monitoring of the ferries, landings and terminals. Transmission of video from ferry-based cameras to a land-based security command center is made possible by use of a high-tech wireless mesh network.

Getting the system in place was a major challenge that required equipment manufacturers and an integrator to cooperate closely. The video equipment needed to be

standards-based, able to operate day and night, and durable enough to handle the salt air and water and extreme temperatures.

The transmission solution had to deal with ferries traveling at speeds of up to 45 miles per hour in one of the world's most challenging radio frequency environments, which includes three nearby international airports, and ever-changing sight lines.

Jonathan Figueroa, director of

facilities for Billybey Ferry, which operates about half of the NY Waterway routes, said that the system had to work reliably virtually around the clock.

"That's where [the equipment manufacturers] were able to enhance our security – by

integrating our cameras, our DVRs and wireless antennas into one central communications system," Figueroa said. "And it also gives us the ability to stay onboard and see what is going on in real-time on our vessels."

A multiple protocol label switching (MPLS)-based wireless mesh network was deployed. The network was designed and installed to span the entire 100-mile NY Waterway service area. The MPLS-based protocol establishes virtual pipes ahead of time so no packet routing is needed.

The dashboard allows the ferry operator's security team to monitor the entire network or a single location. The security team can take action on highlighted emergencies and threats and easily collaborate with other agencies.



Cyber/Data Security



EAS



Fire & Life Safety



Intrusion Detection



Video Surveillance



All video is sent to a land-based command center where NY Waterway security personnel

can review it.

The wireless

connection

allows for real-time sharing of

video with the NY

Waterway's port

partners – the

New York Police

Department,

the New Jersey

State Police and

several federal

agencies. The system can connect with

an onboard radio moving up to 220

miles per hour – far faster than the NY

Waterway ferries travel.

Network security is a priority for the

system. With a proprietary protocol and use of the Advanced Encryption

Standard, the

infrastructure is

designed to keep

hackers out of the

network.

The cameras

in the ferries

and terminals

are weather and

vandal-proof

day/night dome

models. A built-

in IR illuminator

provides details

within the field of view even when

no other illumination is applied. The

cameras have proven to be well suited

for the harsh marine environment,

where they are subjected to water

“We are now very confident that we can have constant communications between our boats and terminals, marine operations personnel and our other port partners – anyone we need to coordinate with.”



spray, wide temperature variations and adverse lighting conditions.

The project integrator noted that, even after Hurricane Sandy left many of the cameras underwater for two days, “We took them out, put them back up, and they worked.”

The DVRs and NVRs in the system provide a platform that complies with standards set by the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA). In general, the cameras onboard the ferries are analog connected to DVRs, while the cameras located in the terminals are megapixel connected to NVRs.

Maps and graphical user interfaces show the placement of cameras on each vessel and in NY Waterway’s onshore facilities. The dashboard allows the ferry operator’s security team to monitor the entire network or a single location. The security team can take action on highlighted emergencies and threats and easily collaborate with other agencies. The dashboard can also be used remotely by authorized personnel through any mobile device with a web browser.

According to Robert Matticola, director of homeland security for NY Waterway, the entire system has made his company better prepared than ever to respond to any type of crisis.

“We are now very confident that we can have constant communications between our boats and terminals, marine operations personnel and our other port partners – anyone we need to coordinate with,” Matticola said. “We can now share information quickly and accurately in real-time, which is really the key to an effective emergency response and mitigating the crisis afterwards.”

Billybey Ferry Senior Vice President Donald Liloia said security has always been a high priority for the ferry operators and their passengers.

“Year after year, when we survey our customers, [their top concern] is about safety,” Liloia said. “They feel safe on our vessels. Once they get to our terminals, they consider themselves home.” ■ **Back to TOC**

*Kostas Mellos (kostas.mellos@interlogix.com)
is sales leader for video and transmission at
Interlogix (www.interlogix.com). *



SIA Technology Insights Article List

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

S15: Spring 2015

W14: Winter 2014-15

S14: Spring 2014

W13: Winter 2013-14

J13: June 2013

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

Access Control/Identity Management

Get Up and Bar the Door (W14)

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

By April Dalton-Noblitt, Allegion

Who Is Entering Your Facility? (W14)

Verifying identities is challenging; partnerships can help

By Daniel Krantz, Real-Time Technology Group

Say Hello to Social Spaces (S14)

Social Applications will transform the security experience

By Steve Van Till, Brivo Systems

Fingerprint Biometrics for Secure Access Control (S14)

Moving beyond passwords and tokens can enhance security while decreasing costs

By Consuelo Bangs, MorphoTrak

Integrating Card Access with Interlocking Door Controls (S14)

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

By Bryan Sanderford, Dortronics Systems

Frictionless Access Control: A Look over the Horizon (S14)*New uses of biometric and RFID technologies could make access badges obsolete*

By Henry Hoyne, Northland Controls

More Security, From Bottom to Top (S14)*Buildings are increasing entrance controls on the main floor and upstairs*

By Tracie Thomas, Boon Edam

Hardware Security, Today and Tomorrow (W13)*Advances in door technology are enhancing both safety and convenience*

By Will VandeWiel, DORMA Americas

Secure Authentication without the Cost and Complexity (W13)*New technologies are narrowing the gap between passwords and stronger authentication solutions*

By Ken Kotowich, It's Me! Security

From Access Control to Building Control to Total Control (W13)*How innovation drives the need to update product standards – and ways of thinking*

By Michael Kremer, Intertek

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

By Walter Hamilton, Identification Technology Partners

Cybersecurity**Target, eBay ... and You? (W14)***Cybersecurity threats are real, even for small businesses*

By Hank Goldberg, Secure Global Solutions

Electronic Security Meets the Ecosystem (J13)*IP devices increase both rewards and risks. How secure is your system?*

By Pedro Duarte, Samsung Techwin



Fire and Life Safety

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

The industry's wireless movement is fueling innovation

By Richard Conner, Fire-Lite Alarms and Silent Knight

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

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

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

Integration

Commanding the Enterprise (S15)

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

By Rob Hile, SureView Systems

Tying It All Together (S15)

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

By Mitchell Kane, Vanderbilt Industries

Safe on the Water (S15)

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

By Kostas Mellos, Interlogix

Broken Promises: The Current State of PSIM (W14)

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

By David Daxenbichler, Network Harbor

Enhancing Continuity Planning through Improved Security (W14)

Web-based systems can tie everything together

By Kim Rahfaldt, AMAG Technology

Technology-Enabled Collaboration Builds Safe Cities (S14)

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

By Itai Elata, Verint Systems



Solving a Big Problem for Small Businesses (W13)

New security technologies offer integrated solutions for small and medium enterprises

By Scott McNulty, Kantech

Intrusion Detection/Alarms

Integrating Intrusion (S15)

Video and access have converged on the network; the time has come for intrusion detection to join them

By Mark Jarman, Inovonics

Integrating Technology with Telephone Service at Central Stations (W13)

IVR implementation can be challenging, but when done well, it can significantly increase capacity and customer satisfaction

By Jens Kolind, Innovative Business Software

Related Issues

Do You Hear What I Hear? (S15)

Audio technology is redefining the surveillance industry and has become an essential component of security systems

By Richard Brent, Louroe Electronics

Enabling Safe Learning Environments (W14)

Securing schools demands a layered approach

By Neil Lakomiak, UL

From Horse-Drawn Wagon to Moving Truck (W14)

Nearly a century after the first VBIED was detonated in the U.S., what can be done to mitigate the risk of car bombs?

By Laurie Aaron, Building Intelligence

What Is in Store for the Physical Security Community (S14)

New technologies will open up great opportunities for the industry

By Bill Bozeman, PSA Security Network



Security and Privacy in a Connected World (J13)

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

By Kathleen Carroll, HID Global

A Case for a Green Security Landscape (J13)

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

By John Hunepohl & Aaron Smith, ASSA ABLOY

Video Surveillance

The Sun Shines on Surveillance (S15)

Solar power enables wireless video solutions in remote locations

By Dave Tynan, MicroPower Technologies

Surveillance in the 21st Century (S15)

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

By Jumbi Edulbehram, Oncam Grandeye

10.7 Billion Security Challenges (S15)

As transit ridership increases, so must security

By Steve Cruz, Panasonic

The Future of Video Surveillance (S15)

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

By Alex Asnovich, Hikvision USA

Making Campuses Safer with Innovative IP Technologies (S14)

Networked systems mean more information, more collaboration and more security

By Kim Loy, DVTEL

Harnessing the Increasing Power of Video (S14)

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

Megapixel Cameras Go Mainstream (W13)

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

By Scott Schafer, Arecont Vision

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

High-resolution panoramic video overcomes the limits of PTZ cameras

By Steve Malia, North American Video

Achieving IP Video Management System Scalability through Aggregation (W13)

Video isn't just about security anymore

By Jonathan Lewit, Pelco by Schneider Electric

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

A keener eye, a longer memory and a sharper IQ

By Fredrik Nilsson, Axis Communications

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

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

By John Romanowich, SightLogix

Video Analytics in the Modern Security Industry (J13)

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

By Brian Karas, VideoIQ

The Untapped Benefits of Recorded Video Surveillance (J13)

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

By Rafi Pilosoph, BriefCam

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



securityindustry.org/techinsights

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

