SIA Insights

TECHNOLOGY

WINTER 2013–2014

Welcome

Dear Reader,

When we published the first edition of *SIA Technology Insights* in June, we had high hopes but uncertain – though optimistic – expectations. We wanted to fill a niche by providing vendor-neutral information about security technologies that end-users could apply in their enterprises and facilities. As with any new product, though, we weren't sure how it would be received. So we were very happy when the publication was met with rave reviews from members of the industry, various vertical markets and the press.

We are now proud to present the second edition of *SIA Technology Insights,* and we have worked hard to ensure that it matches the high standards that were set by the first one. In these pages, you'll find useful, in-depth articles on a wide range of security topics: video cameras, access control hardware, authentication methods, security solutions for small businesses, manufacturing standards compliance and central station efficiency.

Of course, some of you are not reading these words on physical "pages." For those that are, remember that *SIA Technology Insights* is also available online at www.securityindustry.org/techinsights. The first electronic edition was posted this summer, and the current issue should be available digitally in December.

Finally, as always, we want to thank the many people responsible for producing this edition – the expert and thoughtful writers, the visionary members of the *SIA Technology Insights* Advisory Board and the committed and professional SIA staff. You have once again produced a publication that makes the association proud.

And thank you all for reading. We invite you to share your comments and article suggestions with us by contacting Ron Hawkins, the publication's editor-in-chief, at rhawkins@securityindustry.org.

Sincerely,

Jay Hauhn
Chairman
Security Industry Association
Board of Directors

Don Erickson
CEO
Security Industry Association

How to Navigate Through the Magazine

Navigation Bar

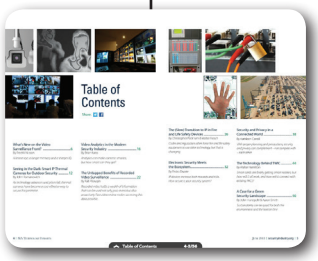
Click the arrows button to expand or contract the navigation bar.

Click the search button to look for keywords.

Click the fullscreen button to view page.

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

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



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

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

Topic Tabs

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

Page Turn

Click the arrow to view next page.

Article

Click the title to go directly to the article.

Page Thumbnails

Scroll to view the next page

Table of Contents

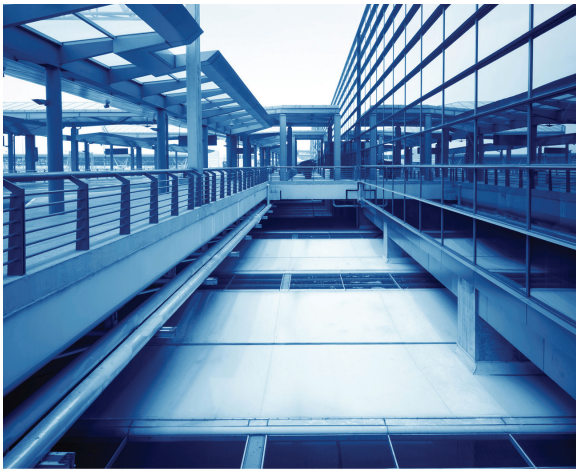
Megapixel Cameras Go Mainstream

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

By **Scott Schafer**,
Executive Vice President
Arecont Vision

Since the birth of video surveillance – known then as closed circuit television (CCTV) – manufacturers and entrepreneurs alike have brought ingenuity to bear on creating better ways for us to watch over people, property and premises. From the original analog systems through the invention and adoption of IP-based systems, technology development has accelerated, with new features and capabilities giving users information at a speed and density previously unthinkable. Now, with the ongoing improvements in megapixel technology, video surveillance systems are capable of vastly more than what could have been imagined in the early days.

A great deal of what is driving the continued improvements in surveillance technology is related in one way or another to the growth of megapixel camera performance and the capabilities it brings to overall system function. In addition to actual system capabilities, the resulting cost efficiencies drive the adoption, development and deployment of



Megapixel cameras do a far better job of capturing more information than standard-resolution cameras, and that superior performance translates into ROI in several ways.

more advanced video surveillance systems. Basically, the extreme clarity and precise detail of megapixel cameras have provided compelling reasons for customers to migrate to the superior performance of networked systems. Not only that, users are given ample evidence to persuade them to deploy the more advanced video management system (VMS) solutions and video analytics that take advantage of these high-resolution images. These are developments that are simply not possible with analog cameras or even conventional IP cameras. Growth building upon growth, megapixel cameras are being increasingly deployed around the world in mainstream applications and delivering terrific value for end-users and systems integrators alike.

Let's examine in further depth some of the other factors that continue to stimulate even greater demand for megapixel cameras.

Better System Performance

In the real world of video surveillance, one critical and primary objective of a video surveillance system is to enable the user to identify the face of a victim or suspect, to see clearly the key details of an incident or to read a license plate number of a passing vehicle. Megapixel video technology provides clearer images than non-megapixel cameras, images that can be enlarged so the security team can see the details they require. Customers accustomed to accepting the limitations of analog and VGA IP video resolutions are enthusiastically discovering and embracing the greater capabilities of megapixel cameras. Customers who previously relied on pan/tilt/zoom (PTZ) devices to cover larger areas are very aware of their limitations. A PTZ can only point in one direction at a time, which creates a significant risk for missing an important or security-threatening event in another part of the coverage area. The wider views delivered by megapixel cameras provide a much stronger solution. Megapixel cameras provide more complete coverage, and users can take advantage of "virtual" PTZ in live or archived video.

Solutions for Virtually any Application

Once, megapixel cameras offered exceptional resolution but not much else in the way of intelligent or application-specific features. Now, there are more types of megapixel cameras than there ever were analog or even non-megapixel IP cameras. New megapixel imaging technologies

are ideal for virtually every application and facility, including education, health care, utilities, ports and many more. To meet those diverse needs, there are cameras with resolutions ranging from 1.3 to 40 megapixels. There are day/night cameras, compact cameras, multi-sensor day/night camera systems, all-in-one dome cameras, vandal-resistant dome cameras, wide dynamic range (WDR) cameras, and cameras designed to endure difficult environmental challenges. Having the right camera for the application is of critical importance as megapixel video extends its reach into more mainstream uses.

The extreme clarity and precise detail of megapixel cameras have provided compelling reasons for customers to migrate to the superior performance of networked systems.

H.264 Compression is a Game Changer

Managing resources such as network bandwidth and storage is an important consideration when designing IP video surveillance systems. Years ago, the widespread adoption of megapixel technology was held back by the limitations of how much data a user's network could carry. Cameras had to be "tuned back" to very low frame rates, compromising efficiency and the delivery of useful data. H.264 compression technology is a game changer because it enables the use of higher-resolution cameras in networked systems and requires less bandwidth and storage. Compared to motion JPEG, H.264 technology is up to five to 10 times more efficient when it comes to bandwidth and storage. H.264 makes megapixel cameras more economical to use and paves the way for greater use of high-resolution cameras to provide better functionality and greater image clarity. And H.265 will be coming in the near future and will deliver additional benefits.

	Analog				VGA (SD)				Megapixel		
	Qty	Cost	Extended		Qty	Cost	Extended		Qty	MSRP	Extended
Box Cameras 768 x 494	17	$250	$4,250	Box Cameras 640 x 480	17	$500	$8,500	Box Cameras (3MP) 2048 x 1536	2	$850	$1,700
								Panoramic (180°) 6400 x 1200	1	$2,398	$2,398
Lenses	17	$80	$1,360	Lenses	17	$80	$1,360	Lenses	2	$170	$340
Housings	17	$230	$3,910	Housings	17	$230	$3,910	Housings	2	$230	$460
Encoder Channels	17	$200	$3,400								
NVR Licenses	17	$300	$5,100	NVR Licenses	17	$300	$5,100	NVR Licenses	3	$300	$900
Cables	17	$150	$2,550	Cables	17	$100	$1,700	Cables	3	$100	$300
Power Supplies	17	$20	$340								
Labor (2/cam)	34	$95	$3,230	Labor (3/cam)	51	$95	$4,845	Labor (3/cam)	9	$95	$855
30 Days Storage (2TB drives)	1	$1,000	$1,000	30 Days Storage (2TB drives)	1	$1,000	$1,000	30 Days Storage (2TB drives)	2	$1,000	$2,000
System Cost			$25,140	System Cost			$26,415	System Cost			$8,953
Total System Pixels	6.45 MP			Total System Pixels	5.22 MP			Total System Pixels	14 MP		

The difference in resolution (total system pixels) and cost is considerable.

Users Can Build a Best-of-Breed System

More and more, both integrators and users are making the choice to build systems that take advantage of the best technologies the market has to offer. It only makes sense. Many, if not most, of the leading providers have a core expertise and build products that are optimized to deliver on that expertise. Top megapixel camera manufacturers and VMS suppliers work closely together to facilitate integration of megapixel images and recording systems. Technology and software collaboration among industry suppliers ensures that megapixel video works with leading VMS systems.

> Technology development has accelerated, with new features and capabilities giving users information at a speed and density previously unthinkable.

Better Return on Investment

The global economy is improving, but a greater focus on cost justification and return on investment (ROI) is here to stay. The mandate to control costs and maximize ROI plays perfectly to the strengths of megapixel cameras.

When customers buy cameras, what they want is the ability to view video that cost-effectively achieves the goals of an application. They need video that can deliver facial recognition and license plate identification, that captures numbers from shipping crates and shows activity at retail stores, bank branches, companies, government facilities, borders, airports, ports and more. They are purchasing the capabilities and functionality that the cameras can provide to solve a specific problem.

Megapixel cameras do a far better job of capturing more information than standard-resolution cameras, and that superior performance translates into ROI in several ways. Based on the measurement of "pixels per meter," a standard for the number of pixels required to depict one meter of a

Class	Resolution	Pixels	Pixels per $1
VGA	640x480	307,200	1,536
HDTV 720p	1280x720	921,600	2,836
1.3 MP	1280x1024	1,310,000	4,039
HDTV 1080p	1920x1080	2,073,000	5,891
3MP	2048x1536	3,145,728	7,149
5MP	2592x1944	5,038,848	10,179
10MP	3648x2752	10,039,296	18,438

Megapixel cameras provide vastly more pixels per dollar than other technologies.

scene for a specific application, a camera with a higher pixel count will provide the user with a larger viewing area. For example, while it could require 10 standard-resolution cameras to cover a single parking lot, the same coverage can be delivered using three or four three-megapixel cameras or even a single megapixel panoramic camera, depending on the application requirements. This reduction in the number of cameras translates into a decrease in installation costs and maintenance costs. Furthermore, the ability to digitally zoom into live scenes and recorded video while maintaining high resolution and wide-area coverage virtually eliminates the need for mechanical PTZ devices. By capturing a detailed, wide-angle view without the PTZ camera requirement of having a person following events in real-time, megapixel cameras can also deliver reduced operating costs by eliminating operations staff.

For these reasons, megapixel video makes it easier for the security professional to demonstrate to management the value of a better-performing system, whether it's being able to solve a criminal case or thwart a personal liability lawsuit. The precise value of the added performance and functionality depends upon each application and is specific to each end-user organization. High-resolution megapixel images provide an easily observable and tangible benefit for networked video surveillance systems. From a systems perspective, using megapixel cameras means fewer cameras are needed, and fewer cameras require fewer software licenses, less support, fewer cables and housings and reduced installation costs.

All of these factors are merging to ensure a healthy future for megapixel cameras in a wide range of uses around the world. As more manufacturers rev up their research and development engines to create myriad types of products that take advantage of megapixel technology – both within and outside the security industry – these factors will continue to lead to excellent opportunities that will firmly establish megapixel video as the new global benchmark of security system performance. **Back to TOC**

Scott Schafer is executive vice president of Arecont Vision (www.arecontvision.com) and secretary of the SIA Board of Directors Executive Committee. He can be reached at sschafer@arecontvision.com.

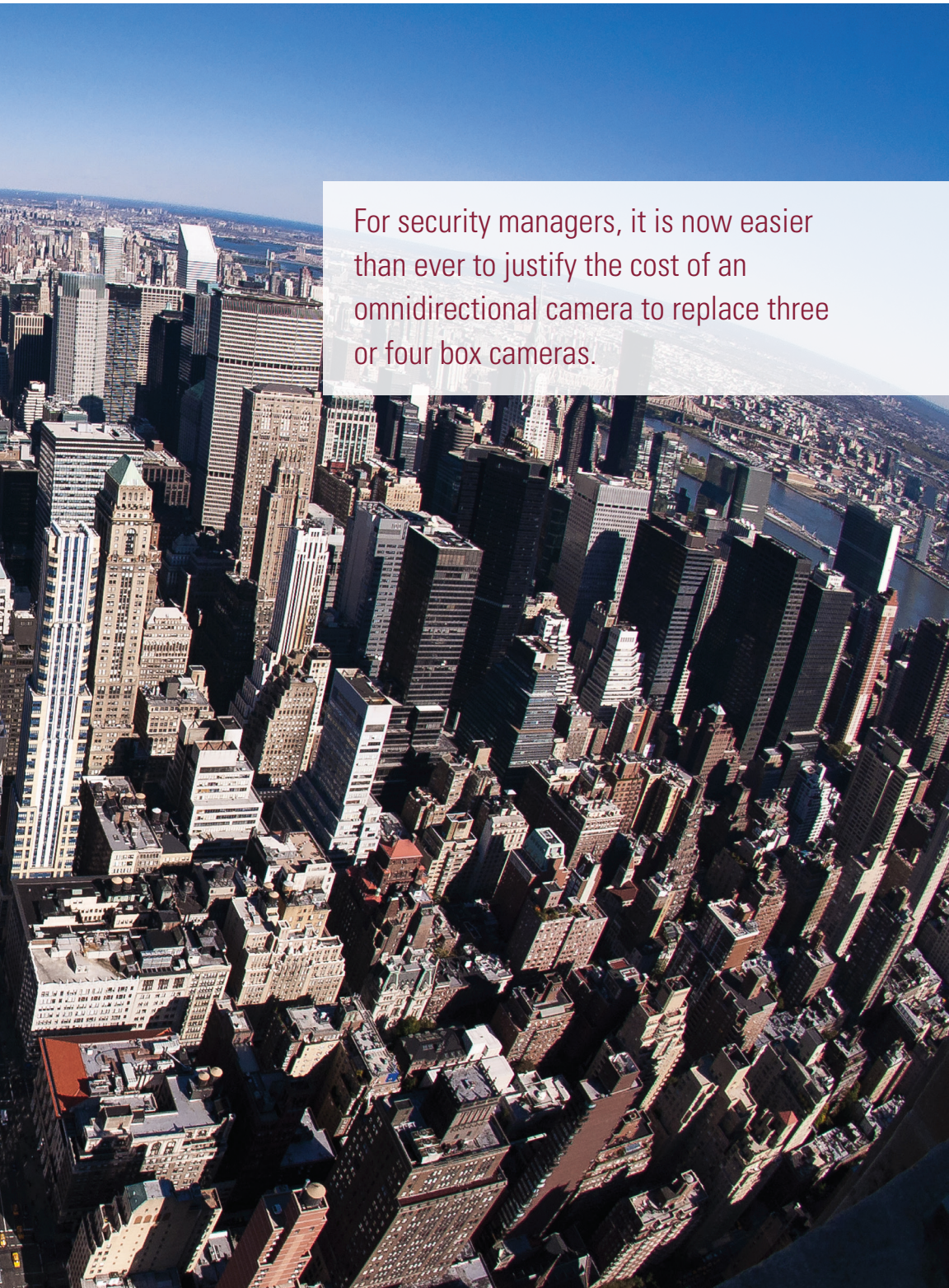
Seeing the Big Picture: 360-Degree Camera Technology

High-resolution panoramic video overcomes the limits of PTZ cameras

By **Steve Malia**,
Vice President of Engineering Services & Marketing
North American Video

Recently, a guest at a casino lost a large sum of cash while walking on property grounds and was convinced he would never see the money again. As it turns out, the money was found by a hotel employee who turned it over to security. By reviewing video footage from one of the casino's 360-degree HD megapixel surveillance cameras, security personnel were able to find an image of the guest who lost the money. The cash was returned to the surprised and elated guest, and the casino won a customer for life.

This is just one of many incidents that clearly depict the benefits that high-resolution panoramic video surveillance cameras deliver. Unlike conventional cameras, panoramic image recording and viewing offers complete situation coverage with the added advantage of forensic pan/tilt/zoom (PTZ) functionality and the ability to view complete scenes in panoramic or multi-view mode. In almost any mainstream application, a high-performance 360-degree camera can cost-effectively complement the overall video surveillance system



For security managers, it is now easier than ever to justify the cost of an omnidirectional camera to replace three or four box cameras.

Fisheye lenses provide wide fields of view but produce distorted images.

by virtually eliminating potentially susceptible weak areas or blind spots.

Early Solutions for Omnidirectional Viewing

From very early on, panoramic image capture has been a goal of both camera manufacturers and end-users. Wide-angle and fisheye lenses were originally used to capture and create panoramic-type video images, but the distorted, spherical views in the curved, outer corners of the image were often unacceptable for observation or identification purposes. Think of a peephole in a door that lets you see a wider viewing angle but with distortion at the edges. In scenes that contain motion, the video images were even less acceptable.

Another solution developed for the purpose of wide-area surveillance coverage is remotely controlled mechanical PTZ cameras. Using either manual control or programmed PTZ tour capabilities, these cameras can cover wider areas than fixed cameras and accomplish much of the requirement for extended surveillance coverage. PTZ devices have drawbacks however, including the potential to miss important activities because of pan speed or tilt angle or, more simply, because the camera is pointed in the wrong direction at the time an incident occurs. Latency, which is defined as the time lag between when a user sends a PTZ control command and when that action is displayed on the screen, is also an issue. Latency often leads to over-panning when a user stops at a desired position but the camera continues to pan for the latency time. This side effect can be particularly noticeable or detrimental to image accuracy when viewing objects or movement at long distances.

Everything gets recorded, and there is no need for manual camera manipulation that could possibly miss important scene action.

Repair and maintenance of moving parts on mechanical PTZ units can also be difficult and costly. In outdoor applications, such as on bridges or freeways, PTZ cameras

are installed in bulky weather-proof housings. Repairing or replacing those devices, as well as getting access to them in hard-to-reach locations, adds to the cost and inconvenience of conventional PTZ cameras.

In these and other applications in which PTZ devices are included in the video surveillance system, the video is simply recorded to a DVR or NVR. Any events or incidents triggered by an alarm can be viewed live, but, more often, they will be reviewed after the fact. Today's DVR/NVR will, in these cases, allow a certain amount of digital zoom and pan/tilt capability within the recorded video. However, unless the action is live, an operator cannot take advantage of the full zoom and/or pan/tilt capability of a camera to look around a scene, to find and follow an individual across a parking lot, for example. In an automated system, video from a PTZ camera may be captured, but it may not be the video that is needed and, consequently, it may be of little or no value for forensic analysis or as evidence in court.

> Use of these cameras in a video surveillance system helps to ensure that captured images are the ones needed and are not just multiple frames of unusable data.

360-Degree Technology and Its Advantages

The proliferation of CMOS image sensors in video surveillance cameras, megapixel resolution, and improved compression technologies have all paved the way for the introduction and

use of high-performance, high-quality 360-degree cameras. Bringing it all together and enabling omnidirectional capability is the use of advanced software.

The software behind 360-degree images varies from manufacturer to manufacturer and may include re-mapping that seams the images from a single camera into one or video stitching that weaves images from multiple cameras together to form one seamless picture with independent perspective-corrected views for each camera. Technology shared by all 360-degree cameras are megapixel chips for high-resolution images and IP-based operation for system convenience and integration. Many camera vendors have also added Power over Ethernet (PoE) functionality in addition to traditional features such as alarm inputs.

The advantages of designing 360-degree cameras into a video surveillance system are many but can easily be categorized into three main areas: situational awareness, forensic and live analytics, and total cost of ownership.

Situational Awareness

When the goal of video surveillance is to monitor areas and events, the challenge is to ensure that all information is captured, and this is where 360-degree cameras excel. Use of these cameras in a video surveillance system helps to ensure that captured images are the ones needed and are not just multiple frames of unusable data. Blind spots are eliminated, and the increased visibility can prompt faster reaction times, which, in turn, can enhance the safety and security of people, assets and premises. While the oval image provides a 360-degree field of view, most products also provide multiple separate images that can be viewed simultaneously, providing up to four (or more, depending on the product) flat-screen digital video feeds that can be viewed and recorded separately. Images can

be recorded at up to 30 frames per second and megapixel resolution ensures high-quality, detail-rich video. These 360-degree cameras are ideal for a wide range of applications, both indoors and outdoors, including retail, casinos, schools, warehouses, military and airports, to name just a few.

Analytics

One of the primary reasons for installing a video surveillance system is to provide images that have sharp and defined details and that can be used in investigating incidents and prosecuting individuals accused of criminal activity. The 360-degree megapixel cameras are both high-resolution and feature-rich, with forensic and monitoring capabilities. These might include digital PTZ for forensic viewing of panoramic images; detection zones that will provide alerts if an area is breached; tagging and following of targets with automatic panning and tilting as needed; and a separate flat screen for PTZ views. Everything gets recorded, and there is no need for manual camera manipulation that could possibly miss important scene action. Panoramic cameras also provide an added benefit in the reduction of investigation time because it's easier for security management to view one panoramic video image than to have to watch several images from several cameras and try to visually sew them together.

Total Cost of Ownership

As the features and benefits of 360-degree megapixel cameras increase, the costs of the cameras continue to decrease. For security managers, it is now easier than ever to justify the cost of an omnidirectional camera to replace three or four box cameras. Costs are also saved in labor, cabling and infrastructure installation, recorded video storage, and maintenance, as there are fewer moving parts to wear out or fail. Of course, if several 360-degree cameras or other megapixel cameras are planned for installation, a separate Ethernet network dedicated to video surveillance transport is best, which may affect the initial cost of ownership. Panoramic cameras are easily integrated with other security systems, and because most leading video management systems (VMSs) and NVRs charge only one license fee for all camera sensors, it is an additional value that can be measured.

The Big Picture

The practical requirements of an application need to be the leading factors in the evaluation and implementation of 360-degree megapixel camera technology. While panoramic megapixel cameras offer overall performance benefits and cost efficiencies that make them appropriate for a wide range of mainstream video surveillance applications, the expertise of an integrator with regard to market offerings and technical capabilities is a key element in helping the user select the best options. **Back to TOC**

Steve Malia is vice president of engineering services & marketing for North American Video (www.navcctv.com). He can be reached at smalia@navcctv.com.

Achieving IP Video Management System Scalability through Aggregation

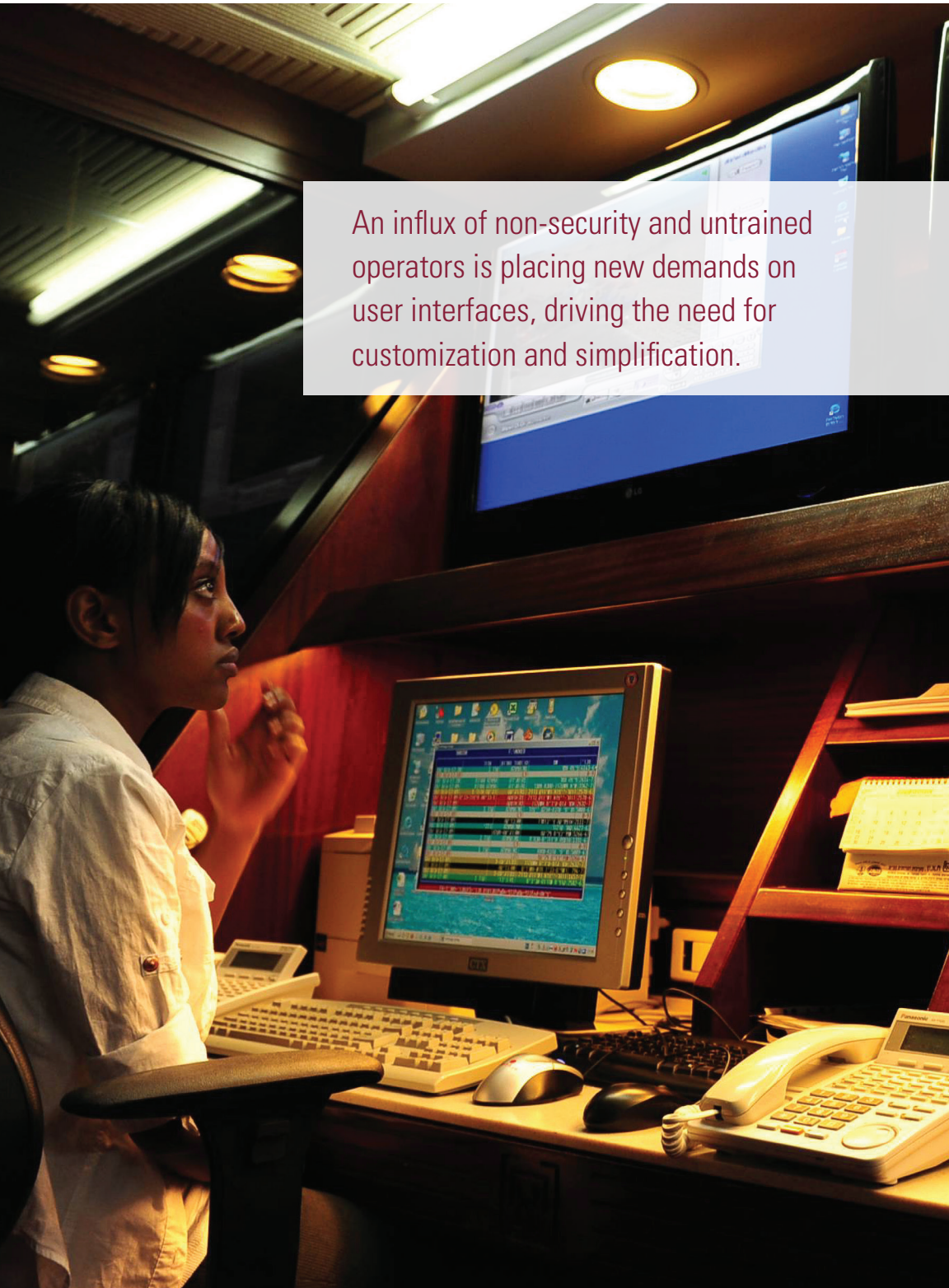
Video isn't just about security anymore

By **Jonathan Lewit**,
Senior Product Manager
Pelco by Schneider Electric

IP video management systems (VMSs) used in security today need to deliver new services and features to a large and ever-growing class of users. And these users' roles go beyond the traditional security mission.

Providing these new services and features becomes more complicated when multiple independent systems are involved. Some IP VMS solutions rely on system federation to connect multiple systems. However, a different approach – aggregation – offers improved ease of administration and better overall system performance.

Previously focused exclusively on security and surveillance, the camera and data feeds monitored by a traditional VMS are now being used to manage day-to-day operations, ensure policies are being followed, and, ultimately, make organizations run more efficiently. Recognizing video system data more broadly as information that can inform all kinds of decisions has led to growth in the base of VMS users. Growing businesses are hungry to consolidate and put this information to good



An influx of non-security and untrained operators is placing new demands on user interfaces, driving the need for customization and simplification.

use, driving optimization across their organizations.

The Problem

New user types are being added to the traditional VMS user base, beyond the standard security officer, supervisor or operator. Demands are being made from marketing, operations, facilities and more to leverage the information captured by the security deployment.

Additionally, an increased expectation of connectivity, driven largely by expanding networks and the proliferation of mobile technology, is placing new demands on systems that previously could have been close-looped. Users need access to pertinent information, often from multiple systems, whenever and wherever they happen to be.

Administrators need to ensure that the right people have access to the right information at the right time across these global distributions. An influx of non-security and untrained operators is placing new demands on user interfaces, driving the need for customization and simplification to ensure that the data a given user needs is what is made available to that user.

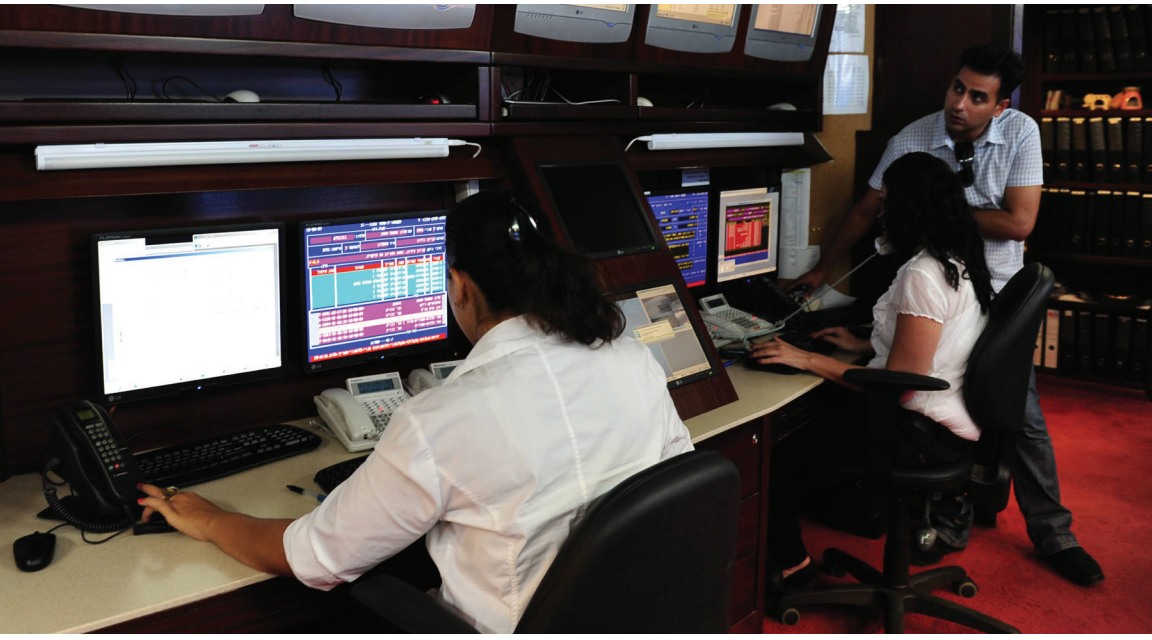
Traditional VMSs were optimized

An Expanded Mission for IP Video Systems

In a broad sense, business owners, security administrators and their responsible delegates are looking to maintain some level of oversight across their organizations. More and more, this oversight is extending beyond traditional security considerations and into operational ones.

- The regional manager of a retail chain wants to ensure that a promotion is set up correctly without driving to each store.
- A facilities representative at home wants to validate that an off-hours alarm was set off by a credible threat before dispatching local law enforcement, avoiding potential fees for nuisance alarm responses.
- A factory manager utilizes security camera feeds to ensure conveyor belts are running as expected, potentially detecting belt failures prior to breakages, minimizing risk to employees and factory downtime.
- An airport uses analytics built into security cameras to calculate wait times at security check-in locations and updates signs directing passengers to shorter lines, improving customer satisfaction.

These new uses for what was previously security-specific data require more effective ways to manage and distribute access.



for the security and surveillance user – cameras were called up by camera number or selected from a lengthy list; sophisticated search queries were used to find and retrieve recorded video; complicated export processes were in place to ensure the authenticity of evidence. While these systems continue to evolve to further meet the needs of security professionals, the resulting interfaces and architectures are becoming unbearable for non-security operators.

Finding and displaying a megapixel camera feed on a monitor in the security operations room is one problem. Serving up a view from that camera and all related cameras at 20 different stores for the regional produce manager of a grocery chain working on a laptop from his hotel room is quite a different problem, indeed.

A new architecture approach – system aggregation – can meet these system needs by using proven, standards-based technologies to provide the necessary structure to

System aggregation can meet these system needs by using proven, standards-based technologies to provide the necessary structure to manage geographically and logically distributed systems.

manage geographically and logically distributed systems.

By treating a VMS as an information system and grouping information from different VMSs together by employing an aggregated architecture similar to what is used by news aggregators and web-hosting companies, critical information can be centrally managed even while an expanding user base has access to it.

By keeping the aggregation server stateless, it becomes very easy to scale when the system load increases because of an expanding user base.

An Aggregation Solution

An aggregated architecture approach decentralizes the actual information by keeping it local, while centralizing its flow, or the access to it. This has several advantages over currently available models that focus on system federation, where information within a federation must be synchronized across the relevant systems. Among the advantages are reductions in overall system complexity, reductions in cross-traffic due to synchronizations, fewer concerns about link failures creating database synchronization problems, more efficient latency management and improved load balancing opportunities. The introduction of the aggregation layer also provides an effective way to provide access to new feature enhancements for a legacy install base.

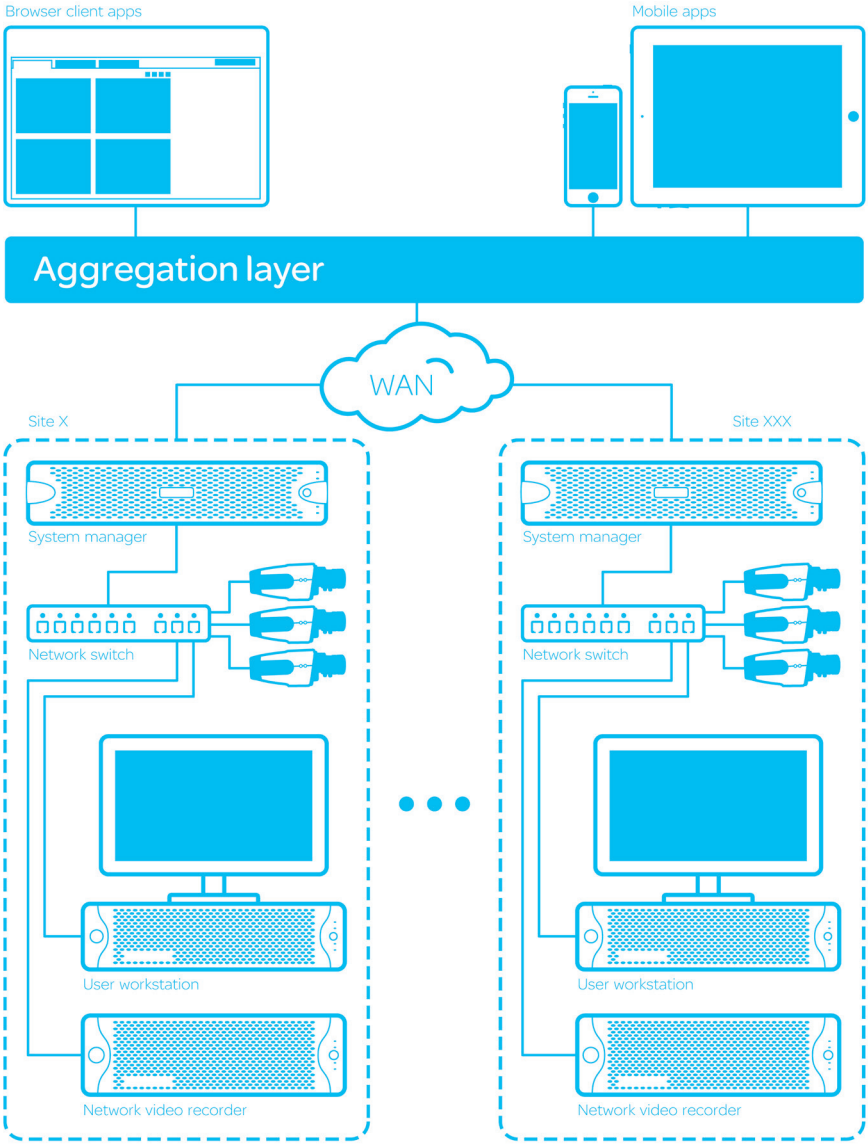
These benefits stem from a reduction in data duplication and

database synchronization operations across the system. Traditional VMSs have had the ability to connect to multiple independent systems for several years. Typically through a common user interface, an operator with appropriate permissions can connect to any number of systems and display the cameras and recorders from those systems.

If a given user's permissions change so that the user now needs to see a new camera or be prevented from seeing an existing camera, it is important to have a method for updating clients and servers with new credential information. Active directory and LDAP interfaces help, but they still require a considerable amount of synchronization information to be exchanged between different servers. This same problem is also present in traditional federated solutions, which attempt to coordinate access across systems by sharing, synchronizing and replicating database information.

An aggregation approach, on the other hand, treats each system as an independent entity, pulling from the relevant systems at run-time through the client interface. While permissions exist on each independent system, an administrator can, through the aggregation interface, manage permissions and push changes out from a central location. Pertinent information can be captured into one database and shared with other enterprise applications instead of repeating the same function on each independent system, one at a time.

While the aggregation architecture enables centralized access to and management of the broader organization, it accomplishes this by providing and facilitating access to the relevant local systems rather than storing a representation of the full organization of systems and attempting to keep that synchronized. This allows the structure



Using system aggregation, each site can be effectively managed locally as an independent entity.

to be separated from user access/ permissions management, pushing those decisions downstream, thus allowing it to scale more appropriately.

As depicted in the diagram, each site can be effectively managed locally as an independent entity. When an organization determines that it is necessary to see across all its installations, the aggregation server software can be installed, creating the aggregation layer.

Once installed, the aggregation layer can be accessed via the same user interface being distributed with systems today. There is no waiting period while the local databases synchronize with some central authority or with each other. The only difference users see is that they now log in to the aggregation server.

In one implementation of aggregation, users may have to create, or request to be created, an account on each of the local machines from which they desire to see information. In alternate implementations, the aggregation server software can manage this account creation automatically for properly permissioned users.

This browser-based user interface helps address concerns related to managing a growing user base. There is no need for a lengthy and costly rollout of client software updates. Every time a user logs in, he or she is getting the most current updates direct from the aggregation server software.

By keeping the aggregation server stateless – meaning it does not have to store information from the local system databases – it becomes very easy to scale when the system load increases because of an expanding user base. Aggregation server software can be placed behind any third-party load-balancer, similar to what is employed in the standard web-hosting model. This allows an administrator to monitor usage and add hardware as needed. Furthermore, the use of a standard load-balancer implementation creates an implicit failover redundancy model.

Conclusion

System aggregation cleanly allows a system administrator to group information across distributed systems by leveraging proven information-sharing architectures and disciplines. Pairing the topology with web-based user interfaces further simplifies the sharing of information with users, regardless of where they are or what device they are using. **Back to TOC**

Jonathan Lewit is senior product manager for video management systems at Pelco by Schneider Electric (www.pelco.com). He can be reached at jonathan.lewit@schneider-electric.com.

Solving a Big Problem for Small Businesses

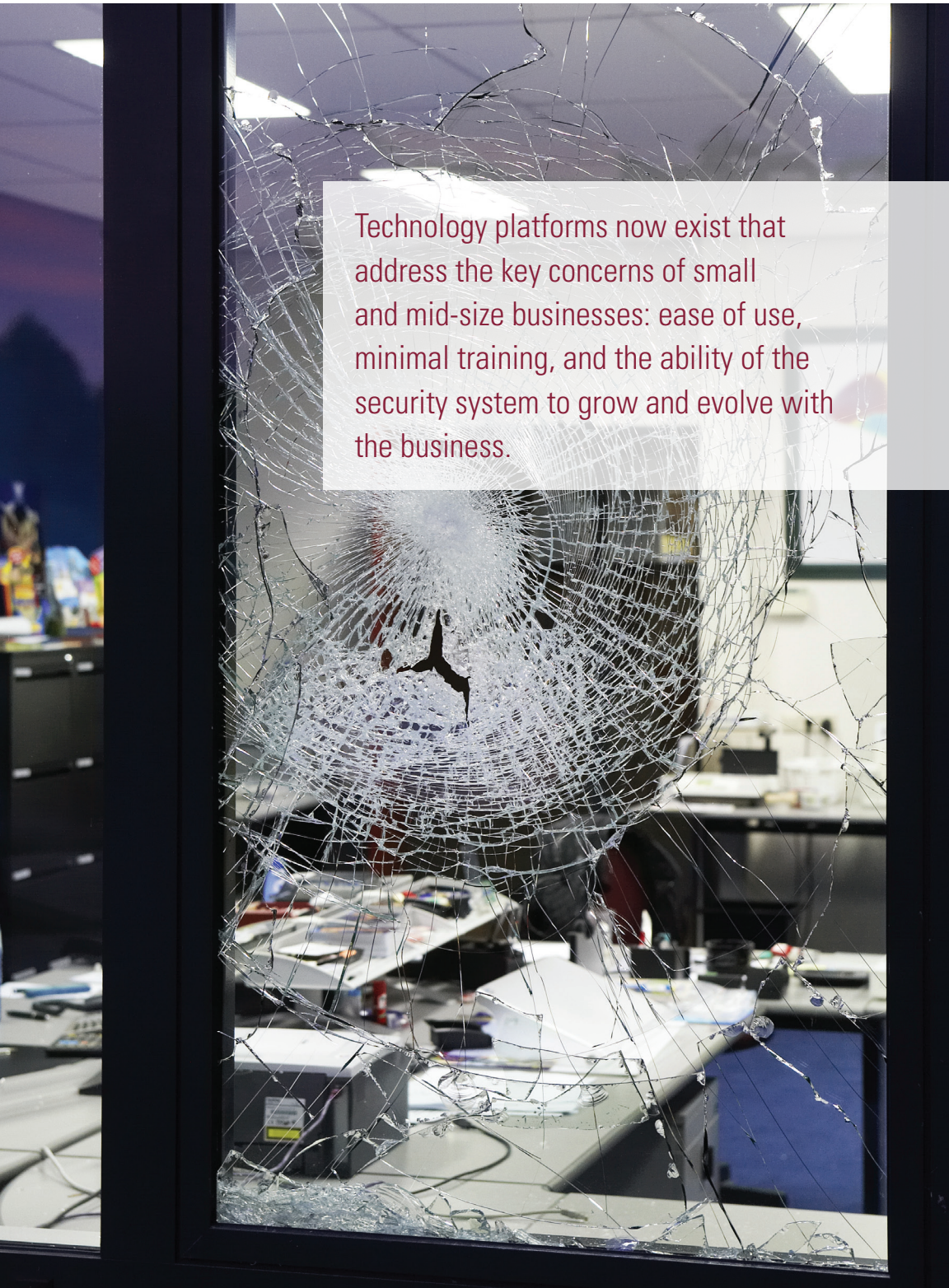
New security technologies offer integrated solutions for small and medium enterprises

By **Scott McNulty**,
Senior Product Manager
Kantech

When it comes to crime, size doesn't matter. Criminals seek opportunity, and that is just as likely to present itself at a small to mid-size retail or commercial enterprise as it is at a larger one.

Small businesses can be especially vulnerable because they typically don't have the resources to guard against crime. The U.S. Small Business Administration (SBA) found that less than half (48 percent) of approximately 400 small businesses surveyed had any security measures in place. And crime is not an inexpensive proposition for a small business. On average, burglaries cost businesses nearly $2,000, while shoplifting weighs in at more than $20 per incident.

Small and medium businesses make up the lion's share of operations worldwide. Statistics from the SBA show that 99 percent of all independent enterprises employ fewer than 500 people, and these businesses account for 52 percent of American workers. In fact, more Americans are



Technology platforms now exist that address the key concerns of small and mid-size businesses: ease of use, minimal training, and the ability of the security system to grow and evolve with the business.

employed by companies that have fewer than 20 workers – about 19.6 million – than firms with 20 to 99 workers and businesses with 100 to 499. So, in reality, small business is big business and runs the likelihood of encountering many of the same security-related issues.

The headlines are filled with tales of smaller businesses that have fallen victim to opportunistic criminals. In a recent theft spree in two states, thieves targeted car dealerships, stealing wheels and rims from dozens of vehicles. Although it's not known what type of security systems, if any, were in place at these establishments, this example shows just how vulnerable smaller businesses can be. And this came at a steep price: the cost of the crime wave was estimated to be in the hundreds of thousands of dollars.

In response, businesses such as these car lots will often look to install a combination of video, intruder alarm and maybe even access control systems that can provide them with the ability to respond in real-time or at least provide evidence that police and prosecutors can use.

In reality, small business is big business and runs the likelihood of encountering many of the same security-related issues.

The drawback, however, has been that small businesses often do not

have a dedicated individual on staff to monitor video, respond to alarms, and stay on top of the latest developments with the system, let alone be responsible for training others. The same person who is responsible for security may also be the one who is selling cars, greeting customers, writing up loan agreements or even managing the business.

And when a business does invest in security – installing a few analog cameras aimed at the lot filled with new cars, alarming the doors or putting in an access control system so employees can swipe a card to enter the building – the systems often are not integrated, so if there is a problem, someone would likely have to sit down and manually view the video, then access the card-based system data or the alarm information separately, comparing the time stamps to see how everything fits together.

> On average, burglaries cost businesses nearly $2,000, while shoplifting weighs in at more than $20 per incident.

Another problem has been that all of this information is often stored on a PC that is vulnerable to viruses and hacking. It could also be the same machine that is used

Continued on page 30

Customizing Video Solutions for Small Businesses

By Joel White
American Dynamics

Small business security applications (those with fewer than 17 cameras) make up nearly 50 percent of the market share in video system installations, yet many small business owners are faced with legacy systems, expensive storage or inefficient cameras that are too complicated to manage and monitor. Many video system manufacturers offer, "good, better or best" packages, which puts small businesses at a disadvantage if they want to implement the same high level of security as larger facilities. Let's face it, whether it's a large health care campus, a medium-size retail store, or a small business location, each facility needs to protect its people, property and intellectual data.

A much better option comes from manufacturers that offer a wide portfolio of purpose-built solutions, providing small businesses with a suite of products that are tailored to meet their needs. Rather than small, medium and large versions of the same solution, with feature sets simply dialed up or down, these tailored approaches take into account how organizations of varying sizes actually use the products. For example, small businesses with no more than 16 cameras typically don't require the feature sets and integration capabilities that a large enterprise might. Instead, they need quick and easy access to images and a simple, intuitive interface that can be used to search and export video.

Additionally, most small businesses have little need for around-the-clock video surveillance monitoring. For example, a daycare facility may need continuously recorded video during its daytime hours while children are present, but only motion-triggered

recording at night in the event of a break-in.

A variety of plug-and-play camera and storage options make it possible to craft a customized solution at an affordable price. Choosing the appropriate cameras and feature sets is particularly important for a small business in order to maximize its investment, while addressing its specific security needs. For example, the number of hours that a business needs continuously recorded video has a direct impact on the amount of video storage capacity required for that system. And while storage can be expensive, utilizing the latest video compression technology and lower frame rates can provide high-resolution video in a small file size, helping to keep storage costs down. This allows a small business owner to focus on maintaining a high-level of security, without taking on unnecessarily large overhead costs.

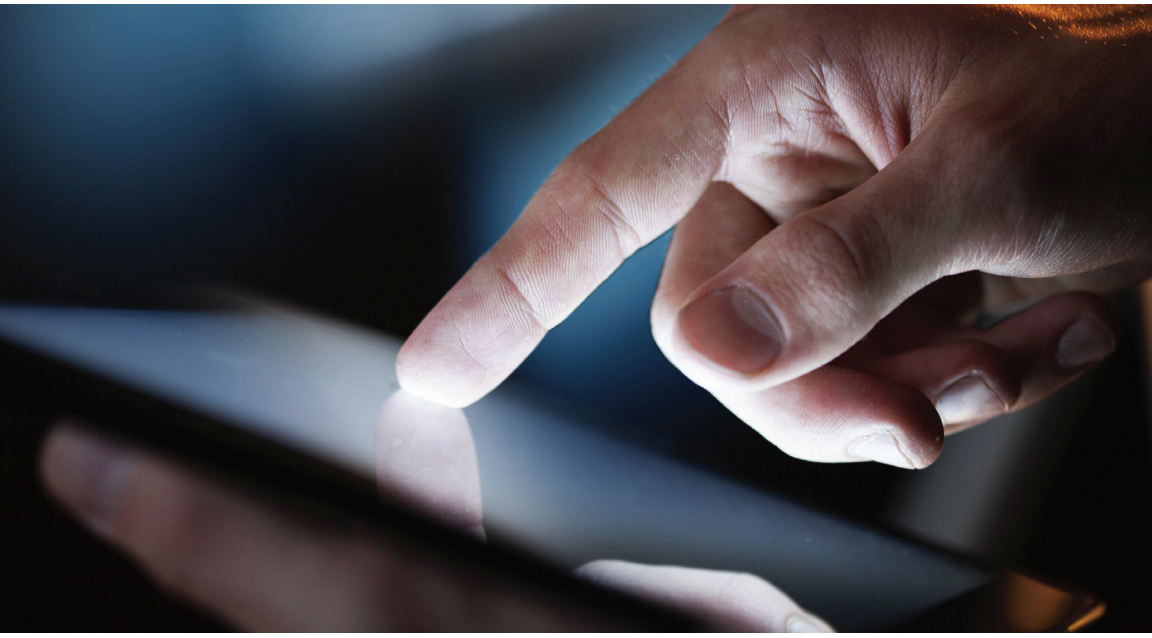
Perhaps one of the most significant changes for small businesses is the accessibility of IP video solutions. For those that now have analog cameras, turnkey hybrid systems make it possible to take advantage of the superior performance of IP technology without discarding their current cameras.

IP video systems offer higher-resolution, crystal-clear video quality with vibrant colors and better performance in low-light conditions. For those of us who are used to the high quality and portability of images captured on smart phones, IP video solutions are comparable. Not only does the switch to IP offer clearer images and easier to manage video, but particular applications demand it, such as monitoring cash registers and watching ATM vestibules.

For those that now have analog cameras, turnkey hybrid systems make it possible to take advantage of the superior performance of IP technology without discarding their current cameras.

The bottom line for all customers is reliability and ease of use. When an event happens, customers expect not only that their system has recorded and preserved the video, but that the video can be easily found and put to use. And with the technology that is now available, high-quality, high-level video systems for the small business world are more obtainable than ever before, allowing small business owners to focus on the other important aspects of running their companies.

Joel White is senior product manager for IP cameras at American Dynamics, part of Tyco Security Products (www.americandynamics.net). He can be reached at joelwhite@tycoint.com.



Continued from page 27

every day by employees who may not be trained on or understand the nuances of the security software that is housed there.

So what alternatives do small to medium business operators have?

One option is to invest in the same type of enterprise-level security solutions that larger businesses have adopted. But this is usually overkill for an individual car dealership, a three-store pharmacy chain or even a small town with two or three school buildings in need of protection. These organizations aren't managing hundreds of cameras or arming thousands of doors or granting access privileges to an army of workers. So the investment could be out of line with current or even future needs. And this also doesn't address the need for a solution that can be handled easily by one or more individuals who are tasked with other responsibilities as well.

Technology platforms now exist, though, that address the key concerns of small and mid-size businesses: ease of use, minimal training, and the ability of the security system to grow and evolve with the business.

Looking again at the car dealership model, the main requirements are a way to monitor the premises, respond to alarms and provide access to employees, ideally all from a single platform.

With one platform for the control of video, intrusion and access control, there is just a single system to learn and one main apparatus to deal with

that isn't a PC but, rather, a dedicated appliance for security. By bringing together three diverse systems, the individual or individuals responsible for security can customize a dashboard so they can move among the different software applications easily, viewing camera feeds or recorded video, locking and unlocking doors, or requesting reports as needed. And because the software is accessible via a phone or tablet-based app, these individuals do not need to be on-site to perform these tasks.

If an alarm goes off in the middle of the night, the car dealership owner doesn't need to hurry to his office to see what is happening. Instead, he can sign on to his mobile device and manage the situation in real-time. It's after hours, but a worker needs to get back into the building? The owner can unlock the door. A new employee needs an access card created? That can also be handled remotely. An event such as a door being forced open triggers an alarm? The owner is able to watch the associated video and take the appropriate action.

While initial training is needed to get a true understanding of how such an integrated system works, the focus in developing these products for small to mid-size businesses has been on keeping training minimal and operations simple. So even if someone hasn't created an access card or developed a new report in weeks, the process is intuitive enough that he or she can easily walk through the process without seeking assistance from an integrator or calling for technical support.

And a business, such as a car dealership, need not invest in all levels of security to reap the benefits of this type of system. Initially, the user may want to focus on building a video surveillance solution for the business, but with this integrated product, access control or intrusion alarms can be added when the time is right. And if an addition is built to house more vehicles, cameras can be added by the integrator with minimal effort.

The need for security at all businesses is growing, and now there are solutions that can allow small and mid-size enterprises to build an integrated system that is just right for them. **Back to TOC**

Scott McNulty is senior product manager at Kantech, part of Tyco Security Products (www.kantech.com). He can be reached at smcnulty@tycoint.com.

Hardware and Security, Today and Tomorrow

Advances in door technology are enhancing both safety and convenience

By **Wil VandeWiel**,
President
DORMA Americas

There's a tempo that characterizes the pace of change in manufacturing in the security industry, and, in recent years, the acceleration of that tempo has been unmistakable. Few in this industry can fail to be engaged by what has been happening through decades of advancement and innovation. And few can look ahead without the sense that still more remarkable developments are on the horizon.

While no one has a working crystal ball, an attentive view of developments in the security hardware manufacturing industry suggests that certain trends already visible are likely to continue and strengthen.

Integration and Hardware

Mechatronics. As recently as a few years ago, this was a word that would have left even some informed observers of the security scene scratching their heads. Now it's widely

Advances in mechatronics now involve integrated utilization of sophisticated control systems, enabling a host of new security options.

understood as an essential element in the transformation of the mechanical side of security integration.

We have learned over the course of decades that total subsystem integration is a powerfully effective strategy in building security systems. Where the most current developments in access technology are part of such systems, outstanding results in maximized building protection have been proven. And there's every reason to expect that the future will reveal still stronger progress in this direction.

The details around every building's operating situation – location, physical structure, access requirements, traffic patterns and much more – define a unique set of security requirements. We have seen that remarkable new functionalities are continually reshaping the ability of manufacturers, designers and building managers to customize security solutions, structure by structure. And that's where mechatronics comes in.

From the standpoint of integration, the very name is suggestive, bringing together the mechanical with the electronic. But advances in mechatronics now also involve integrated utilization of sophisticated control systems, enabling a host of new security options.

In the past, integrated solutions often relied on software-based control, and integration will no doubt continue to operate in this way. But the advance of smarter hardware means that solutions can be both integrated and distributed. Much of today's very capable access control hardware comes with versatile functionality built in. To cite one example, when a door must close on demand, new, integrative hardware functionality makes that easy to accomplish at the point of access. Such capabilities, with many more on

the way, seem very likely to continue this revolution.

It's also true that integration yields significant advantages in system economy. That's because older approaches that relied on piecing together solutions often increased costs. Integrated planning for solutions usually – though not inevitably – creates installations that are finished sooner and at lower expense. We have already seen this approach make distributors and contractors more competitive as they realize savings and pass them on to their customers.

If we consider some of the specific demands that confront security managers, we can recognize that improved technology will both respond to and shape those demands. Today and tomorrow, commercial and public buildings will require sophisticated and responsive systems for perimeter access control – supple operating systems that can be changed rapidly and reliably.

In the hospitality industry, operators must have simple and effective means of credentialing their guests and distinguishing them from other users who can be admitted to public spaces but not guest rooms or paid amenities. Health care has its own challenges, centering on the need to provide varying yet foolproof access for visitors, staff, patients, vendors and anyone else who enters the structure. Across many categories of buildings in many industries, the uniform need exists to provide access that varies according to time of day and specific entry point. Hierarchies of access based on specified secure areas, individual security clearances, and overall safety/security plans are increasingly important not only for government installations, but anywhere access regulation must be carefully managed.

> Anomalies in the data may reveal security problems that could escape ordinary observation, and these methods of tracking and response enable another exciting dimension in security.

Here's the good news in responding to such a diverse and sometimes daunting array of challenges: contemporary integrated technologies and those that are soon to appear have what it takes to do all of this and more. At our disposal will be a constellation of strikingly effective modalities. Fail-safe and fail-secure action will be governed by versatile electromechanical devices at protected portals. Critical door position management capabilities will come into play. New responsive alarm capabilities will become commonplace. A spectrum of means

The security advantage of revolving doors is one reason they are being installed in larger numbers.

and methods that help to detect and stop intrusion will be widely used. Remote monitoring and control, with all elements linked together in the fully integrated service of carefully devised security plans, will appear more frequently and in more applications.

In addition, a new set of capabilities will likely be useful in many verticals – solutions enabled by constant improvement in the monitoring/control modalities mentioned above. It works like this: data from monitored portals can be collected and analyzed, producing a detailed view of standard operations. If events (or patterns of events) are detected that appear to be out of the ordinary, the monitoring system can spot them and report on them immediately, enabling prompt, decisive action.

Anomalies in the data may reveal security problems that could escape ordinary observation, and these methods of tracking and response enable another exciting dimension in security. As managers come to know and understand usage patterns, this careful information collection and analysis can help them improve their systems, anticipating and forestalling issues that might otherwise not have been recognized at all.

Eldercare and Security

When we consider the needs of those who are served in eldercare centers or Alzheimer's treatment facilities, we're in an area in which correct management and integration are matters of life and death. Hence, this is an excellent category of security service to consider further.

In this category, security planning can require responses to demands that are not necessarily in parallel. For instance, it's critical to the safety of people with psychological or emotional challenges that they not be able to freely leave the place in which they reside; if they do, they may be at serious risk of physical injury or other harm. At the same time, if confronted by life-threatening circumstances, such as a fire inside the facility, they must be able to exit to safety. Simply put, for many residents, egress must be restrained except in emergencies.

Basic hardware for managing such situations has long been available. But the integration discussed above introduces new and diverse security elements. Depending on the specific

needs of the facility and its residents, a host of specialized technologies may be in use. The landscape here may include remote access control, various types of alarms, access recording, video monitoring, card or proximity reading, magnetic locking systems, tamper-proof hardware and much else besides.

For work of this kind, security integration is a great blessing. Augmented by constant improvement in the quality and capability of hardware elements, the systems that serve such facilities can tie together all of the subsystems that keep residents safe. Those elements of the system can be made mutually supporting and can be structured in advance to respond immediately, correctly and in unison to the requirements of normal operation, as well as those prevailing when danger impends. There's every reason to expect that such advantages of integration will only become more pronounced as related technologies continue to advance.

Security Advantages of Revolving Doors

The experience in recent years of revolving door manufacturers reveals an increase in the popularity of this highly engineered access solution. While several advantages associated with revolving doors probably help to account for this trend, it seems likely that the security advantage of such doors is one important reason they are being specified and installed in larger numbers.

Revolving doors, of course, have always been attractive and functional; we're accustomed to seeing them widely used in health care and hospitality applications. In architectural designs that hearken back to bygone styles, revolving doors simply look right. This is just as true in many high-tech, high-touch building projects, where such doors can impart a contemporary appearance – clean, sharp and modern. Wide diameters are excellent at accommodating large traffic volume. And the green characteristics of revolving doors are important to many building owners and managers – such doors interrupt air flow and provide important energy-saving advantages.

But certain security aspects of revolving doors also make them attractive in countless installations, and designers, architects and building managers can be expected in the future to double down on those particular details.

Specifying small diameters on revolving doors can help prevent "piggyback" entries.

Here's a prime example: with swinging or sliding doors, a chronic security problem is entry by unauthorized personnel who "piggyback" behind those who are authorized to pass in. A small-diameter revolving door can prevent this security breach by making it impossible for a second user to enter behind the first (authorized) user.

Revolving doors can be built and installed to permit the passage of traffic in only one direction. In many situations, such as in the secure areas of airports, a properly specified and constructed door ensures that no one can violate the assigned flow structure by entering through the exit. A sensor-activated brake prevents wrong-way passage while enabling the door's motion to reverse and let the would-be entrant move away. The sensor also automatically notifies the facility's security force when such an

> Still to come are bold new technologies that will enhance the ability of security planners and managers to improve their systems.

attempt to reverse correct traffic flow has been identified.

Of course, many of the security elements that can buttress any door's security are available to make a secure revolving door harder to breach. These include bullet-resistant glass, extra physical reinforcement, and various monitoring technologies.

Low-Power Proximity Readers: Combining Security and Convenience

In security planning, the first order of business is always the protection of people and property. But no security system exists in a vacuum. It's also important to find ways to enhance convenience and profitability without compromising security, and technology helps us do that.

Low-power proximity readers are a good example. Security managers can employ active or passive systems, but, either way, a properly managed system makes it easy to grant the proper credentialing to users and to change credentialing as needed. These arrangements are very convenient for users to employ and are modest in cost for long-term use.

When individual users are at sudden risk for whatever reason, the positive impact of such capabilities can reach far beyond convenience. Because a proximity reader eliminates the need to fish out and manipulate traditional keys or electronic key cards, it can promote user safety in emergencies. By enabling quick, unencumbered access, these systems allow immediate entry if a threat is present.

Those who have worked with these systems also note that the security they provide at the operating level is impressive. In part, this arises from the fact that the cards are hard to forge, and the overall system is difficult to defeat. Little information is stored on the non-rewritable cards, and this simplicity represents a strength in itself. While it is possible to delete data stored on the card, this would in no way help someone who is attempting unauthorized access – a proximity card without its data simply doesn't work.

Still to come are bold new technologies that will enhance the ability of security planners and managers to improve their systems. The less exhilarating corollary of this is that those who strive to defeat such technologies will also improve. The cycle never ends. **Back to TOC**

Wil VandeWiel is president of DORMA Americas (www.dorma.com/us). He can be reached at dorma@dorma-usa.com.

Secure Authentication without the Cost and Complexity

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

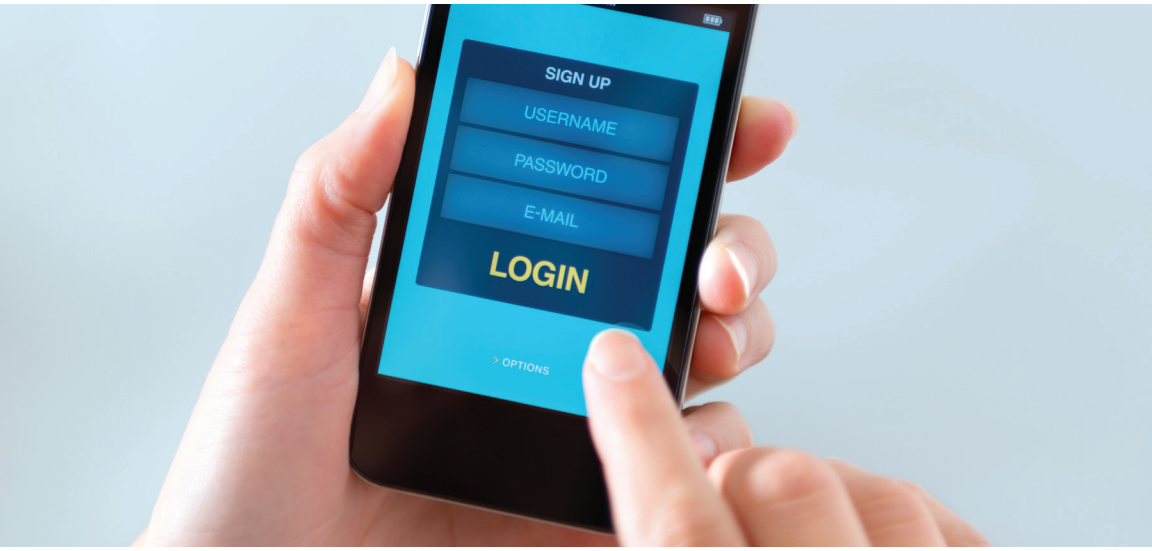
By **Ken Kotowich**,
President & CEO
It's Me! Security

In 2004, Bill Gates declared that "the password is dead." Almost 10 years later, though, passwords and PINs remain the most widely used form of authentication, despite the proliferation of password-hacking technologies such as phishing and key-logging that provide adversaries with user credentials from a relatively easy single log-in observation.

The U.S. Computer Emergency Response Team reported that approximately 80 percent of the security incidents they record are related to passwords, and there are almost daily reports of password compromises and breaches, so why are passwords still so prevalent?

There are a number of reasons including user familiarity, and when you look at passwords, in general, they have numerous advantages over biometrics, hard tokens and out-of-band (OOB) solutions. These include increased versatility in terms of end-point independence, lower acquisition costs, and better user experience as a result of having fewer process steps and faster log-ins than many alternatives. Passwords and PINs are also software-based and do not

Some innovative new authentication systems provide most of the benefits of passwords along with much higher levels of security.



require additional hardware, which makes them usable in applications from e-commerce to enterprise log-ins to ATMs, etc. But the most compelling reason for the continued prevalence of passwords is that it can be expensive and difficult to upgrade authentication security. Passwords are more cost-effective in terms of acquisition costs (free) than having to purchase, install and maintain scanners, smartcards, fobs and similar equipment.

When one looks at the huge cost to individuals, companies and the economy overall of the almost non-existent security that passwords provide, however, one realizes that passwords are, indeed, extremely expensive on a total cost of ownership basis. The average cost to a business for a data breach – not including soft, yet very real, costs (e.g., customer confidence/loyalty, brand reputation) – in 2010 was $7.2 million, or $214 per compromised record.

The common paradigm is that, in order to be secure, strong authentication has to be costly, complex or cumbersome, but that may no longer be the case. Traditionally, more lengthy and complex passwords were indeed more resistant to hacking methods like shoulder surfing and dictionary attacks. Recently, though, we have seen aggressive forms of hacking like phishing and key-logging that provide adversaries with credentials by observing the user's log-in. In this new environment, due to their static nature, strong passwords are not much more secure than weak ones. Complex passwords are no longer secure.

Complex passwords are no longer secure.

To combat these newer forms

of hacking, authentication security providers developed one-time passcode (OTP) solutions, such as hard tokens or smartcards, which do not provide adversaries with authentication credentials from observation of user log-ins. Although most of these solutions are effective, they are much more expensive than passwords, plus they can be cumbersome to use and lack the end-point versatility required to be pervasive in the new mobile environment.

The same is true for most biometric systems. Although biometrics are less cumbersome to use than legacy OTP solutions (it's pretty easy to scan your finger), they too lack the end-point independence of knowledge-based systems like passwords and often require expensive hardware acquisition and maintenance costs. With these types of systems, security does indeed equal expense and, often, poor user experience.

> When one looks at the huge cost of the almost non-existent security that passwords provide, one realizes that passwords are extremely expensive on a total cost of ownership basis.

Some newer solutions include the use of smartphones as a means of strong authentication. The underlying assumption with systems like OOB solutions that send an OTP to a user's smartphone is that everyone has a smartphone and, therefore, it is cost-effective. The validity of this assumption can be argued ad nauseam (smartphones are expensive), but the real issues are, once again, the cumbersome nature of the process (the user must enter his or her username and password, then wait for the OTP to be sent to the phone, then enter it into the log-in site) and the overall security of the smartphone itself. There is really no way to ensure that the person in possession of a smartphone is the authorized user. Many people do not use the authentication alternatives available on most mobile devices, and those who do are relegated to entering easily shoulder-surfed four-character PINs or pattern swipes. Indeed, the authentication security offered by most smartphone providers is woefully lacking.

In an effort to improve this, Apple recently introduced fingerprint authentication on its newest version of the iPhone. Unfortunately, the Chaos Computer Club reported the day after the iPhone release that it had compromised this new authentication security offering and wrote in a blog post that, "This demonstrates – again – that fingerprint biometrics is unsuitable as [an] access control method and should be avoided." It is also important to keep in mind that biometric data is static, making it useless if compromised

on only a single occasion. (You can't change your finger or iris print).

The challenge for CISOs, then, in this budget and capital expense-constrained economy, is how to achieve the cost and versatility benefits that are inherent with passwords while enhancing security and reducing the risk of fraud in a cost-effective, secure and user-friendly fashion.

Until fairly recently, there has been a significant gap in terms of cost and security between passwords and most two-factor authentication systems. This gap is now being narrowed by some innovative new authentication systems that provide most of the benefits of passwords along with much higher levels of security. These new solutions use a variety of knowledge-based methods to enable users to create very secure OTPs. Most are completely software-based, which makes them much more cost-effective, both in terms of acquisition and on-going costs, than hard tokens and smartcards (and arguably OOB) systems. Their non-hardware nature also makes them much more versatile and end-point independent in uses from enterprise systems to remote web access to physical area access to, even, banking machines.

The security, versatility and usability characteristics of these systems differ by vendor and method utilized, but all represent very viable alternatives to existing mainstream solutions. The following is a brief summary of some approaches that are on the market.

One solution employs two knowledge elements, pattern recognition and the use of simple arithmetic and/or logical operators to create very secure OTPs. This system presents users with a (typically) 36-cell reference table populated by a single digit in each cell. The user memorizes a pattern of cells on the table and looks at these cells each time they log in. The reference table is randomized at each log-in so individual cells will have different numbers in them each time. The user simply references the numbers in each of the chosen cells as the OTP.

To add to the security of the system, a user can also elect to perform operations – addition, difference, multiplication, greater or less than (between cell values) and more. This second knowledge factor creates little reference ability between the OTP created and the reference table, making it extremely difficult for adversaries to compromise it. In fact, a four-character OTP created in this fashion has roughly the same entropy as an eight-character strong (upper/lower case, numeric, special

character) password yet cannot be key-logged or easily phished.

Although this may initially seem complex, the process is very fast and easy to use, and university studies and user experience indicate that it is very intuitive and easy to remember. In addition, adversaries would have to observe multiple log-ins in order to determine how the user created the OTP.

Another technology employs a single knowledge element, pattern recognition, in a similar fashion to create OTPs that are far more secure than passwords. The single knowledge element makes this solution much more secure than passwords but requires fewer observations to be defeated.

A third approach converts static passwords to randomly generated OTPs by presenting the user with a graphic of a standard keyboard with numbers in the corner of each keyboard key. Every time the user logs in, the numbers in the corner of each keyboard key are randomly populated. This system utilizes two knowledge elements. The first element is the location on the corner of the keyboard keys containing a number and the second is the static password. If, for example, the user's password is "Password1," they would first look for the number in the top-right corner of the upper case "P" key, then the number in the top-right corner of the lower case "a" key, then the number in the top-right corner of the lower case "s" key, and so on. This process creates a randomly generated nine-character OTP (one number for each corresponding character in the static password). This system lacks a degree of end-point independence because of the need for larger displays to present all of the keyboard pads (upper/lower case, numbers, special characters), and it takes a fairly significant amount of time and effort to log in. Notwithstanding these concerns, it is far superior to conventional passwords and requires more than a single observation to determine the user's static password.

There are a number of other very effective knowledge-based password replacement solutions that bridge the gap between conventional passwords and high-cost, high-complexity authentication solutions. They all have their relative strengths and weaknesses, but all, to varying degrees, meet the top criteria for a good authentication system, as defined by Dr. Ant Allan of Gartner Research: risk-appropriate authentication strength, low total cost of ownership, good user experience, and end-point independence.

Generally speaking, all of these newer methods defy the old paradigm that, in order to be secure, authentication systems need to be complex, expensive and cumbersome. These new knowledge-based alternatives provide solutions that are not only secure, but also cost-effective, user-friendly and versatile.

Back to TOC

Ken Kotowich is president and CEO of It's Me! Security (www.itsmesecurity.com). He can be reached at ken@itsmesecurity.com.

From Access Control to Building Control to Total Control

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

By **Michael Kremer**,
Marketing Manager
Intertek

Though no one knows for sure what the future has in store for access control systems, one thing we definitely do know is that the days of simple key-and-lock enterprise systems are long gone. Years ago, the luminaries and experts who led such discussions in the security industry would have bristled at such a statement and said, "Nonsense." The technologies and systems deployed were tried and true, and varying from those methods indicated a willingness to put a facility and whatever was inside it at risk. Perhaps the only two words more frightening to a well-seasoned industry veteran than "at risk" are "what if."

You see, "what if" begins with the supposition of the unknown. That's a bad thing in the security business. So it took years for product innovation to really take hold. The good news is that more people started asking "what if," and they also asked "why not" and "how about" until they finally landed on "Yes, we can." Innovation became exponential from there, and it continues at an ever-increasing clip today.

Open systems allow devices to be upgraded and customized and tinkered with to provide more than just access control or building control. Now systems can provide total control.

Giving the Customer More

One of the challenges with security hardware in recent years has been that most equipment is locked in to proprietary software. We know hardware is the meat-and-potatoes of any system, but software provides the added value and features. The side dishes and dressings, if you will, that make the entire presentation better than a stand-alone device.

Today, open systems allow devices to be upgraded and customized and tinkered with to provide more than just access control or building control. Now systems can provide *total control*, and that's a concept that people are far more familiar with – and comfortable with – in the security industry.

What exactly does "total control" mean? For one, it means that any antiquated notion of what a security system can do is tossed right out the window. Rather than simply allowing access to a user, it monitors that user's presence in a certain area. It can intelligently manage the lights and HVAC system to be more energy-efficient. It can enable remote system access when needed, lock the system down when appropriate, and accumulate data on potentially any user in any area at any single point in time. That's total control.

Complying with Standards

When manufacturers today begin the R&D process or design stage for a new access control device, they have more to consider and more to contend with. The recently released *UL-294 Sixth Edition*, which is the U.S. product safety standard that governs all access control system units, takes into account many of the recent technological advancements.

UL-294 Sixth Edition includes several new requirements that could have a significant impact on how manufacturers design their products.

In terms of the quantity and range of the revisions, this edition is practically a new standard. For instance, it has significantly expanded the scope of the products that are covered and added additional performance and safety testing requirements.

Rapid technology advancements have resulted in systems that incorporate more electrical components. Access control units, from card readers to biometric scanners, are no longer separate components; they are increasingly integrated into complete opening systems. As a result, one of the more prominent changes in UL-294 is the inclusion of tiered access control performance levels. The sixth edition defines four performance levels for "destructive attack," "line security," "endurance" and "standby power."

Manufacturers will now be required to declare the appropriate performance levels for their access control systems. It is especially crucial for manufacturers to be mindful of this new requirement during the design phase. In some cases, particularly for products that fall under Level I, the effect on manufacturers will be minimal. In other cases, however, manufacturers may find that their products will require additional compliance testing as they become more complex and more sophisticated. If a product uses a secondary battery as a standby power feature, for example, the battery will require a construction review and performance testing, as well as markings that indicate the rated standby power capacity. The sixth edition also includes new performance testing requirements for biometrics devices and for Class 2 and Class 3 circuits, as well as more detailed definitions of electrical spacing requirements and enclosure openings for product construction.

Additional new requirements are outlined in the standards for items such as Power over Ethernet (PoE) functionality, data processing and IT equipment, burglar alarm functionality, products to be used in air-handling spaces, key locks, lithium batteries and more. Given the drastic changes to the standard, it is in a manufacturer's best interest to understand that there is no one-size-fits-all approach to complying with *UL-294 Sixth Edition*. Working with a testing and certification partner that can provide guidance regarding the changes and details about the standard is recommended.

How can a manufacturer build in features and functionality that they may not have even considered yet?

Knowing the Options

Manufacturers should start thinking about how they will adapt to the new requirements early in the design phase. When designing access control systems, manufacturers will now need to consider which of the four performance levels the product falls under (destructive attack, line security,

endurance or standby power). The level declaration will depend on how the equipment will be used and where clients will install it.

There are definitely options for how a manufacturer approaches compliance with UL-294. Complying with the requirements of the sixth edition right away may be one way to differentiate products from competitors. In some cases, however, manufacturers may find it more effective to comply with the fifth edition requirements while preparing for the seventh edition, which is anticipated around 2017.

It is also important to note that when the Occupational Safety and Health Administration (OSHA) developed the Nationally Recognized Testing Laboratories Program in the United States two decades ago, it opened the testing industry to allow multiple organizations to show competence, gain expertise and compete for business. This model applies to life safety and security products the same way it does to lighting, HVAC, medical devices or any other type of electrical product that requires safety certification.

> There are limitations to relying exclusively on a standards-based approach to compliance to mitigate product safety risks.

Looking Ahead

Manufacturers recognize that the market drivers for innovation aren't about to stop any time soon, and that

certainly adds a level of complexity to their product mix. Users want customization, but they don't want to pay for "proprietary" devices. What they really want is flexibility. How can a manufacturer build in features and functionality that they may not have even considered yet?

One of the areas in which the security industry is changing the most is integration with wireless infrastructure, from 4G wireless carriers to local Wi-Fi and near field communication, and the software applications (or mobile apps) that control the entire system. These bring in additional standards and protocols that need to be considered, along with performance and reliability certifications, but the security industry certainly isn't the only one facing this evolution.

So how does a product evolve from a stand-alone device to one that includes two-way communication? Manufacturers have grappled with this transition for more than a decade and the skill-sets and backgrounds of their design teams have shifted as a result. Mechanical engineers now work side-by-side with electrical engineers and software developers. Sales and marketing teams hold meetings with quality and compliance teams to discuss Federal Communications Commission (FCC) certification as well as ZigBee specifications. All for what used to be known as "a door." It's a brave new world.

Every year, manufacturers develop new technologies to give clients the products and solutions they want, but they certainly aren't foolish enough to believe that they have an answer for everything. There will always be a new use or a new request or an extreme spec that needs to be met. That's what drives innovation. If one customer needs a specialized solution, the manufacturer can leverage the experience gained from that project to create something that's more universal for a larger audience. Over time, who knows how far that path could lead?

Taking a Risk-Based Approach

Designing new products that meet the needs of customers *and* meet the requirements of the technical standards is a delicate balance. Adding a third layer of complexity to the model is the concept of the "risk-based approach."

A product's compliance with regulations and standards may satisfy a company's minimum legal obligation to its customers, but mitigating a product's overall safety risk is a much larger task. It involves a wide range of considerations, from the types of materials that will be used in the product's construction to how the product will actually be used or installed by the customer to environmental issues and the product's final disposal.

Many leading manufacturers have adopted a broader, more risk-based strategy in the development of new products that spans the entire life cycle. Some new standards have incorporated risk management because a risk-based approach has the potential to anticipate and mitigate the impact of a new product on a wider range of stakeholders, including society as a whole. *UL-294 Sixth Edition* does not incorporate risk management, and it is unknown if the seventh edition will, so it is critical that manufacturers tackle this on their own.

There are limitations to relying exclusively on a standards-based approach to compliance to mitigate product safety risks. First, as noted above, the standards development process often lags behind technological advances. The incredible speed with which technology drives new innovations is a primary factor in this. In addition, simply demonstrating compliance with the requirements of a given standard is not sufficient to fully ensure the safety or performance

of a product. User errors, defective products and malfunctions happen. Understanding the potential risk and designing the product to mitigate the effects of those events are sound business practices.

Looking in the Mirror

Speaking of sound business practices, all of the issues discussed in this article – from product innovation to standards compliance to risk-based design – add up to one of the single most important attributes of a product and a company: brand reputation.

All companies are fighting for share of market, but they also are fighting for share of mind. Every little detail that makes up a product and every decision that is made by a company can have a positive or negative effect on the market's perception of it. Having a standards compliance mark on a product shows a willingness to comply with safety requirements. Some manufacturers go one step further and conduct benchmarking or independent performance tests to validate product quality. In some cases, having a strong brand reputation can pay off by allowing the manufacturer to charge slightly higher prices because buyers know that they are getting the quality they are seeking.

Giving customers what they want – and then some – is the best way for a manufacturer to grow its brand reputation and make its product successful.

Giving customers value is good. Giving them innovation is better. Giving them *total control* is the way to earn their loyalty for the long run.

Back to TOC

Michael Kremer is marketing manager for building products and life safety/security products at Intertek (www.intertek.com). He can be reached at michael.kremer@intertek.com.

Integrating Technology with Telephone Service at Central Stations

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

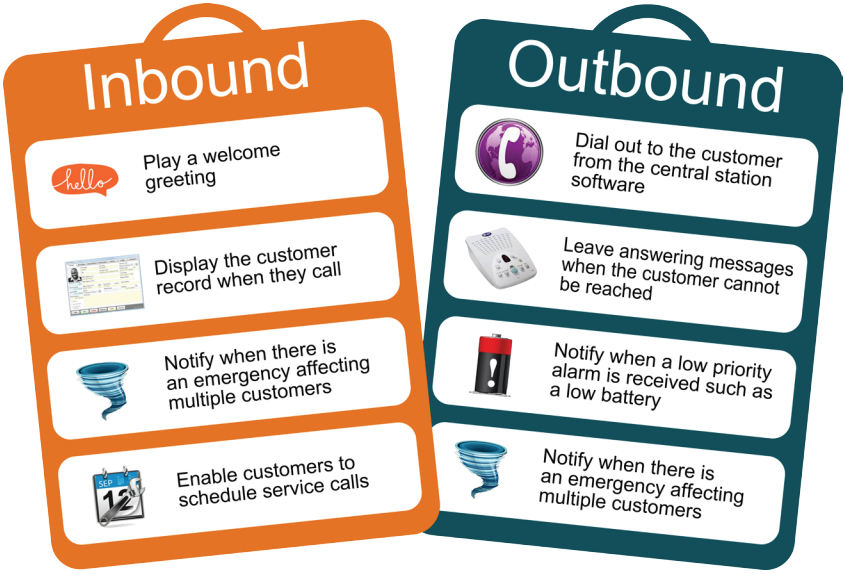
By **Jens Kolind**,
Vice President
Innovative Business Software

The plain old telephone service is a central station's lifeblood. Signals are received and alarms are dispatched using the same technology Alexander Graham Bell invented almost 140 years ago. While this is changing with the move to signals received over cellular and IP devices, operators, for the time being, are likely to continue to interact with customers over the telephone when handling alarms, scheduling service calls, and managing billing questions and other customer queries. Managing calls efficiently can be difficult and is a key differentiator between cost-effective and non-profit-making central stations. High volumes for a typical central station mean that seconds count.

Interactive Voice Response Systems Can Drive Efficiency

Large companies have, for many years, loosely integrated their central station software with telephony systems, letting the operator dial the phone directly from the software. Dramatic improvements in technology now allow computers to support complex integrations with telephony systems, collectively known as

Central stations report that up to 40 percent of all calls made by an operator can now be managed with IVR intervention.



IVR systems can handle many functions at central stations.

interactive voice response (IVR) systems. For example, converting computer text into spoken language now works well enough to make IVR a suitable solution for providing information to the customer without operator intervention.

This technology is no longer only available to large central stations. With cloud-based IVR services, smaller companies are able to participate without significant upfront costs. Cloud companies now provide transparent per-call fees of less than 2 cents per minute, access to newer technologies, integration into existing telephone systems through voice over IP (VoIP), and a lower cost of ownership.

The cloud technology is mature. In 2007, nearly as much money was spent on cloud-based IVR solutions as on those that were premise-based. Since integration standards often remain the same, well-designed central station software that has been integrated with existing premise-based solutions should also be able to integrate with cloud-based versions.

IVR is widely used within the financial services community for personalized account management, helping customers locate the closest branch or ATM and providing alerts, reminders or account balances. With tighter integration into central station software, this more advanced processing is also possible in the security industry.

Upfront Investments Generally Returned in Less than a Year

The potential cost savings and increase in call handling capacity when implementing an IVR solution are significant. On average, once the

technology is implemented, handling a call via IVR costs around 2-4 cents a minute, versus an operator at 20-50 cents a minute.

Central stations report that up to 40 percent of all calls made by an operator can now be managed with IVR intervention. While this can translate into cost savings, freeing up operators can also enable quicker responses to higher priority calls. When implementing newer technology, the investment costs can be recovered as soon as one year after going live.

Customer satisfaction with successful IVR implementation is high. Interacting with a machine can take less time than talking to an operator, and the knowledge that priority situations will be dealt with faster than in central stations without a similar technology can be comforting. As for the operators themselves, they usually report spending more of their time providing services to customers, rather than wasting time waiting for a connection or talking to an answering machine. This, combined with having knowledge of who the customer is and what the likely issue is, increases operator job satisfaction.

Customer satisfaction with successful IVR implementation is high.

Take Care in Choosing What to Automate

With any technology, following good practice is essential to achieving goals. Time and effort spent analyzing existing calls made and received by an operator will pay off.

For a central station, analysis starts with defining the categories of calls and determining the level of automation desired. This will be a balance between factors such as complexity, types of customers served, and signal priority. If a cloud-based solution is used, care has to be taken to review the terms of service carefully, since many do not permit calls directly to emergency services. Best use of an IVR will vary significantly from one central station to another.

Automation can be for either outbound calls, where the system dials the customer, or for inbound calls, where the IVR intervenes when a customer dials the central station. For inbound calls, the customer will generally be prepared for a conversation and already has the mental context to complete the task. For an outbound call, the lack of context will affect the attitude of the person taking the call and his or her willingness to receive the information. People will, therefore, be prone to ignore calls if they are delivered inefficiently. Offering the option to reschedule an outbound call can increase success.

The automation may be partial, where the system deals with certain aspects of the call before passing it to an operator, or full, where the system manages the whole interaction. Even small interventions can make

a big difference. Implementing an automated greeting when customers dial in and displaying the customer record to the operator enables a more professional response. For a monitoring station managing 50,000 residential accounts, saving 10 seconds on each call can free up an operator half a day every week.

Technology also plays a part in call selection. Modern IVR systems are able to detect the presence of an answering machine. When integrated with the central station software, this permits new types of automation not previously possible. For example, when verifying an alarm, the list of contacts can be dialed by the software and only presented to an operator when a successful call to a contact has been made. When the IVR detects an answering machine has been reached, an automated message can be left that is appropriate to the alarm type. In this scenario, the operator is no longer required to wait for a connection, wait for the end-user's voice message greeting, or leave the actual message. In addition to the benefit of an IVR's ability to leave messages with consistent information, operators may also be able to verify alarms more quickly by connecting with an available person on the call list.

In instances in which life or property is not endangered, some central stations are now managing signals without any operator intervention. A common case is informing customers that a panel battery may be low. IVR implementations that have been tightly integrated with central station software may also inform the customer that service is necessary and schedule an appropriate time for a technician to be on-site.

IVR technology can also help manage catastrophic events that may affect a large group of customers or the central station. When power failures occur, callers to the central station can be informed of the appropriate actions to take, increasing the capacity at peak times to deal with higher priority calls.

There will always be instances in which call automation is not appropriate. Calls regarding complex accounts that require quick thinking or

represent unique cases that are difficult to translate into hard and fast business rules are better left to skilled operators. The IVR is better thought of as an assistant that improves communication rather than as a way to replace the operator. That is why a successful IVR implementation will always provide the option for the customer to be put through to speak to a live person.

Learn from Other Industries

IVR has been successfully used in many industries outside of security. Some basic guidelines have been developed that should be followed if the investment in IVR is not to be lost.

Whenever a set of options is provided to a customer on a call, these should be kept short and should be ordered so that customers are not frustrated by a long series of unnecessary menus. Five options is generally the maximum that should be offered. Offering rarely chosen options before popular options are all signs that the menu system is not likely to work well.

Voice prompts should be recorded by professionals to ensure they are easy to understand. In a multilingual environment such as Canada, providing the prompts in the language appropriate to the customer will also be essential. Even in the United States, providing a choice of languages can be a market differentiator for a central station.

Measuring and tuning the IVR after it has been implemented is vital. In the same way that a central station monitors the types of calls and adjusts the processes that an operator will follow, IVR requires the same attention. Key metrics that will help with this include call completion rates, the category and type of calls, the time and purpose, the number of calls required for resolution, and the number of calls requiring operator intervention.

The IVR is better thought of as an assistant that improves communication rather than as a way to replace the operator.

Whatever the scenario, keeping the customer informed is essential. In October 2013, the Federal Communications Commission (FCC) implemented new rules that require prior written consent before the auto-dialing of numbers when this results in an advertisement or telemarketing. Making the customer aware that a machine may be used to schedule service calls or handle lower priority alarms will avoid debate about whether an auto-dialed phone call constituted an advertisement.

Setting Goals and Finding Vendors

Good implementations of IVR are not easy. Selecting the right types of calls and choosing the correct telephony technology all affect the implementation. Within the security industry, the level of

integration with central station software is also a key factor.

The first objective should be to define the purpose of implementing an IVR. This goal can be, but is not always, reducing costs. Providing a better customer experience may also be important. The goal will drive the definition of the return on investment. For example, retaining existing customers through better peak demand management will require different measures compared to maximizing the automation of operator tasks. Where existing telephony solutions have been implemented, the goal may be to make better use of that technology through tighter integration with the central station software.

Once the goals are clear, one of the first people to contact before implementing a new IVR or augmenting existing telephony systems is the central station software vendor. In many cases, the vendor will have experience implementing solutions and will know what expertise is required. They should be able to provide guidance regarding the types of automation that they have successfully developed with other customers. They are likely to know IVR implementation experts who understand the specifics of the alarm industry. They will also have strong partnerships with telephony and cloud IVR technology firms.

The rewards of IVR implementation in terms of customer satisfaction and efficiency are well worth starting the exploration. **Back to TOC**

Jens Kolind is vice president, external partnerships, at Innovative Business Software (www.ibsoft-us.com). He can be reached at jkolind@ibsoft-us.com.

securityindustry.org/techinsights

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