

network centric Security August 2007

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

CHANGING CHANNELS

Convergence writes new rule for distributors **18**

OPEN BUT SECURE

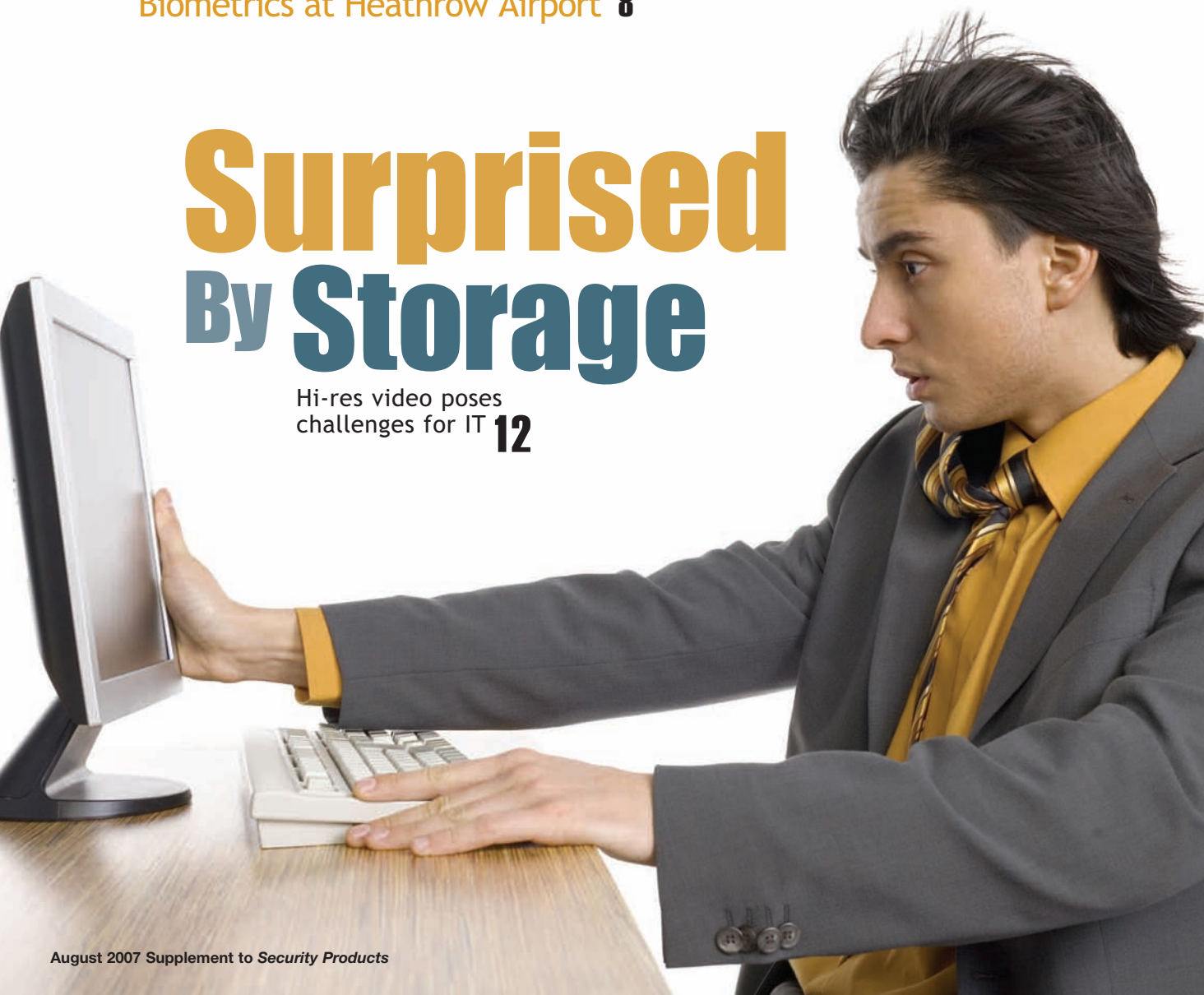
One high-school's lessons with IP Video **24**

PLUS

Biometrics at Heathrow Airport **8**

Surprised By Storage

Hi-res video poses challenges for IT **12**



EDITORIAL

Editor-in-Chief

Steven Titch
281-571-4322
titch@experteditorial.net

Art Director

Dale Chinn

Associate Art Director

Wendy Byle

Publisher

Russell Lindsay
rlindsay@1105media.com

SALES

District Sales Manager

AK, AZ, HI, ID, MT, NV, NM, OR, UT, WA, WY
Barbara Blake
972-887-6718
bblake@1105media.com

District Sales Manager

MA, CT, NJ
Frank D'Isidoro
908-252-6346
disidoro@comcast.net

District Sales Manager

Midwest, Southeast, North TX
Brian Rendine
972-687-6761
brendine@1105media.com

District Sales Manager

Northeast, AR, CO, LA, MO, OK, Canada
Randy Easton
678-401-5543
reaston@1105media.com

District Sales Manager

California
Ben Skidmore
972-587-9064
bskidmore@1105media.com

District Sales Manager

UK
Sam Baird
+44 1883 715 697
sam@whitehillmedia.com

District Sales Manager

China
Jane Dai, New Buddy Limited
86-755-82925229

1105 Media

5151 Beltline Road, 10th Floor
Dallas, TX 75254

Editorial services provided by

Expert Editorial Inc.
www.experteditorial.net

12



SURPRISED BY STORAGE

By Sharon J. Watson

Capturing a definitive identity on video and then storing that video may seem like two distinct issues. Yet video storage is a critical issue shaping how enterprises make the transition to IP-based surveillance networks.

18 CHANGING CHANNELS

By Frank Barbetta

Manufacturers are demanding from their channel partners new qualifications that entail technology efficacy, personnel training, education programs and official certifications. The benefits that accrue to participants who pass muster include customer referrals, potential sales leads, joint sales calls, major project participation, spot price breaks, volume discounts and capital financing aid.

24 OPEN BUT SECURE

By Sharon J. Watson

With features ranging from a high-tech tufted vinyl carpet to special air filtration systems to updated kitchen equipment, Jackson High School in Massillon, Ohio, was designed as a state-of-the-art education facility. So it's little wonder the new building's technology and security systems would also be cutting edge.

departments

2 Enter

The next few years will see a dramatic change in the way manufacturers structure their channel partnerships and the time to prepare is now, writes Steven Titch, *Network-Centric Security's* Editor-in-Chief.

8 Innovate

BAA leads a team of vendors in an airport security trial that links passports and biometric data to speed travelers through check-in and boarding at departure and immigration upon arrival.

28 Launch

New applications, strategies and solutions.

32 Exit

True convergence doesn't simply use the IP network as a wire. It becomes part of an extensible platform: a platform to build new capabilities and, in this case, enhance the physical security group's value to the organization, write Cisco Systems' Bob Beliles.



New Rules

by Steven Titch, Editor-in-Chief

“Many are called, but few are chosen.” That Biblical wisdom also resonates for channel partners in today’s security industry.

As journalist Frank Barbetta reports in “Changing Channels” (page 18), manufacturers are beginning to demand a host of certification requirements, personnel training and education as network-centric convergence calls for greater dexterity with IT concepts among installers and integrators.

“This technology shift is going to require security integrators to respond now—to devote all their available capital, human and technical resources to learning a new core competency of IP design, integration, deployment and installation,” says Tim Holloway, vice president-technology and security solutions at Anixter International Inc., Glenview, Ill.

Distributors, system integrators and installers should heed this statement. Convergence isn’t something you can hide from. It’s not a buzzword that will lose favor in a few years. You can’t hope to sidestep its consequences by invoking platitudes such as “we’ve always been a niche player.”

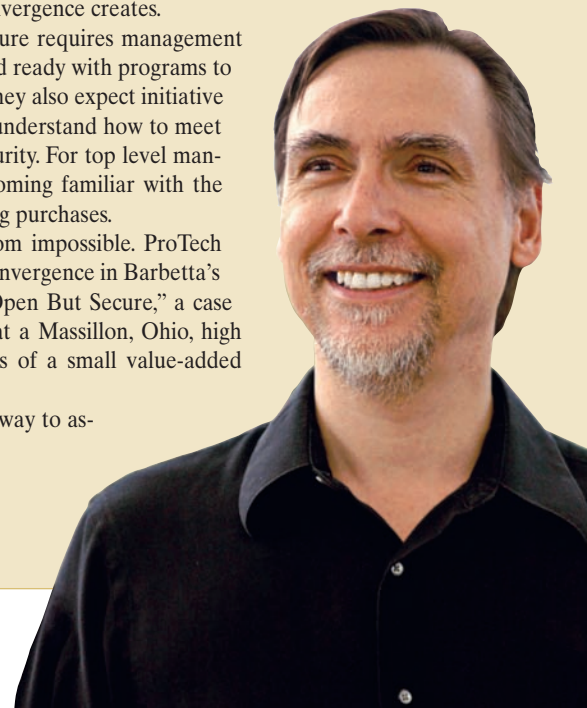
The next few years will see a dramatic change in the way manufacturers structure their channel partnerships. Established end-to-end camera and video security system manufacturers, who have long been a source of steady income for their affiliated distributors, are under attack from a spate of big-caliber IT companies including IBM, Cisco, Accenture, EMC and Microsoft. These companies, who have long worked in environments of open systems, best-of-breed partners, and ISO 9001 certification, are forcing changes in the security supply chain. No matter what the history of your manufacturing partners, the introduction of IT into physical security has pushed their customers’ expectations up several notches. Tools, technologies and packages for surveillance, identity management and access control that fit client needs two or three years ago won’t cut it in today’s market.

Distributors and installers who do not embrace IT will find themselves falling behind competitors that do. New companies, drawing almost exclusively on IT talent, will make a run at your business. Vendors will start making strategic decisions about partners. Long-time relationships will give way to the demands that convergence creates.

No one likes change. And success in the future requires management commitment today. Happily, most vendors stand ready with programs to help channel partners become IT experts, but they also expect initiative from you. That means retraining personnel to understand how to meet the new IT challenges involved in physical security. For top level management, it means setting an example by becoming familiar with the companies and technologies that are influencing purchases.

The task might be difficult, but it is far from impossible. ProTech Security Inc., which discusses its approach to convergence in Barbetta’s story and is featured in Sharon J. Watson’s “Open But Secure,” a case study of a network-centric video installation at a Massillon, Ohio, high school (Page 24), is one of the best examples of a small value-added distributor that is making the transition.

IT’s role in security is here to stay. The best way to assure your future is to answer its call.





Heathrow Biometric Security Trial Scores Big

by Steven Titch

Open and interoperable systems, combined with new standards for biometric encryption, have reached a point in their development where network-centric solutions promise to make passenger identity authentication less of a hassle for travelers, yet more fool-proof for security.

BAA Ltd., the company that owns and manages London's Heathrow Airport, working alongside the U.K. Border & Immigration Agency (BIA), Cathay Pacific Airways and Emirates Airlines, recently completed a sixteen-week trial of an encrypted, networked biometric system, called miSense, that automates passenger identity and authentication from initial check-in at departure to baggage claim at the destination.

Accenture, IER SA, Raytheon Co., Sagem Morpho Inc. and SITA provided high-level technology and systems integration for the project.

The primary objective of the trial was to see how well biometrics could streamline authentication while improving customer service, and to gauge if the public would be receptive to using biometric

technology, particularly in Europe, where past consumer studies have shown a greater sensitivity to privacy. Three miSense services were studied: miSense, miSense Plus and miSense All Clear.

"We wanted to remove stovepipes and improve the experience of the traveler while increasing the security of the whole process," says Cyrelle Bataller, biometric specialist

in Accenture's Technology Labs. "The idea is to identify yourself to the government, the airlines, the airport only once. That allows decisions to be taken at a single point. MiSense is part of that."

"The technology is pretty sophisticated, but it is coming together," says Stephen Challis, head of product development for BAA. "The goal was to first see if we could capture people's biometric characteristics, and test the fast recovery of those characteristics. We wanted to see how quickly a fingerprint input could be matched against the data in the system."

HOW IT WORKS

miSense is designed as a voluntary system travelers can use to speed identity checks. For the trial, self-service check-in kiosks were installed where passengers could scan their fingerprint and the photographic page of their passport. The fingerprint was linked to the passport information and stored in the miSense database for later reference. If the passenger was checking baggage, their bag tag

The objective of the trial was to see how well biometrics could streamline authentication while improving customer service

Inscape Data

The Expert in Wireless and IP Video Systems

Long Range Wireless Remote Monitoring Outdoor Installation
Easy Integration User Friendly Software



About Inscape Data Corporation

Inscape Data is the expert in long range wireless and IP video systems, and offers a full suite of turnkey solutions for long range outdoor 2.4GHz, 5GHz and IP based video surveillance applications including IP67/68 (Ingress Protection) certified all-weather IEEE 802.11a/b/g wireless systems and the IP video security based on MPEG-4 video compression standards.

Inscape Data's AirEther long range wireless and AirGoggle IP based video security products based on the latest wireless and video compression technologies offer the most cost effective remote monitoring solution in the market. The AirEther wireless enables long range point to point and long range point to multipoint connections for wide varieties of extended indoor and outdoor remote monitoring applications, i.e., public safety, transportation, law enforcement, industrial and commercial, and homeland security, etc.

Visit us at our next tradeshows

ASIS 2007
September 24 - 27, 2007
Las Vegas Convention Center
Las Vegas, Nevada
Booth 156

ISPCON Fall 2007
October 16-18, 2007
San Jose Convention Center
San Jose, California
Booth 514

Live Demo

AirEther™ Outdoor Long Range Wireless
Wireless and Remote Video Monitoring Applications
Integrated Wireless and IP Based Video Systems
All Dealers, Distributors, and Manufacturer Rep are Welcome

North America Headquarters
Inscape Data Corporation
1611 South Main Street
Milpitas, CA 95035
Phone: 888-267-4507
Fax: 408-935-8900

Asia Headquarters
Inscape International Co., Ltd
34F-1, No. 170, Jingping Road
Zhonghe City, Taipei County, 235,
Taiwan, R.O.C.
Phone: +886-2-8369-1681
Fax: +886-2-8369-5661

Visit our website at www.inscapedata.com

© Copyright 2007, Inscape Data Corporation, All Rights Reserved, AirEther, AirGoggle and Inscape Data are trademarks of Inscape Data Corporation

Circle 95 on card.

numbers could be integrated with the ID information.

At the entrance to security screening, miSense passengers used a self-service gate equipped with a fingerprint scanner and boarding pass scanner. Travelers first scanned their fingerprint and if receiving a positive response from the miSense database, were then prompted to insert their boarding card into the scanner. The data contained on the magnetic strip was then compared against an existing airport database to check against a number of parameters.

If both scans were positive and matched (that is, the traveler had enrolled at check-in and the boarding pass was valid) the gate opened and the traveler proceeded to security screening. The gate featured anti-tailgate sensors; a customer service representative was also on hand to assist if required.

Finally, immediately before aircraft boarding, airline staffers scanned the fingerprint of miSense travelers with a wireless handheld device. Once the data was reconciled against the miSense database, the terminal signaled an OK to board. If the traveler had tried to use the fingerprint scanner to board without enrolling at check-in, or did not use the self-service gate at security screening, the miSense system would send a "no board" message to the scanning device.

All passport information and fingerprint biometric data collected was deleted at the end of the operational day.

miSENSE PLUS

In miSense Plus, travelers agreed to submit passport biographic data and thirteen biometrics—irises, ten fingerprints and one facial image. The traveler also agreed to undergo a comprehensive background check. The checks themselves were conducted in real time against several law enforcement databases. Following examination by an immigration officer and on completion of the background check, biometric and identity data was encrypted on an RFID chip on a miSense Plus card issued to the trial participant.

The average time to fully enroll a traveler was seven minutes and in some cases as little as three minutes, according to BAA's report on the study. The study's goal of 1,000 travelers was achieved with 1,007 people signing up.

The trial was the first to use international encryption standards adopted by the International Civil Aviation Organization (ICAO). These same biometric encryption standards will be incorporated into second-generation ePassports. The miSense Plus trial was a first look at the potential benefits the standard may bring both in terms of data storage and traveler experience.

The miSense Plus card also let travelers bypass long lines upon return to the U.K. For the trial, BAA installed a self-service gate equipped with a fingerprint scanner and a miSense Plus card scanner at immigration and passport control in Terminal 3 at Heathrow. In Hong Kong, airport authorities installed a similar gate.

“The card let you bypass immigration,” said a spokeswoman for nCipher Corp., Cambridge, U.K., which, as a subcontractor, provided encryption technology to the trial. nCipher’s Hardware Security Modules were deployed in the miSense system to generate and protect the unique cryptographic keys that were used to identify and validate each traveller based on their biometric information. “The card would speed you through security with a special lane. An automatic gate scans your fingerprint and passport and matches them.”

If both records matched, the gate opened and the traveler proceeded to baggage claim.

The biometric dimension provides a further security parameter, Challis says. For instance, passport inspectors must often deal with travelers who may have grown beards, wear glasses or changed hairstyles. They must make a fast decision as to whether the picture in the passport matches the person presenting it. “MiSense Plus assures the name, the passport and fingerprint always belong to the same person,” says Challis.

Once a member of miSense Plus, travelers were then able to use the gate at the entrance to security screening during subsequent departures and to use self-service border clearance gates as many times as their journey arrangements permitted.

miSENSE ALL CLEAR

In the third element of the trial, biographic data from a traveler’s passport and travel itinerary were captured in real time during check-in and transmitted to and processed by the BIA for background checks prior to departure.

The intention was to prove the concept of real-time traveler processing, on a traveler-by-traveler basis, by carrying out pre-departure checks. For the trial, so as not to impact airline or airport operations, no responses from the BIA were returned to the airline (although this could have been managed with the configuration in place).


A total of 3,097 traveler records were transferred to the BIA background checking system between February 2007 and March 2007. According to BIA, 85 percent

were processed in fewer than 10 seconds and 96 percent were processed in fewer than 30 seconds.

CONSUMER ACCEPTANCE

As for consumers, BAA also found that 81 percent of respondents in a post-trial survey found the miSense Plus service good or excellent. “We knew if we could produce a

clear benefit, people would be happy to sign up,” Challis says.

Challis says there is no timetable as to when any of the miSense services will be implemented on a widespread basis. BAA, which owns six other major U.K. airports as well as Naples (Italy) International Airport, is involved in several other IT-based security initiatives, he said. 



exacqVision Pro
exacqVision IP

Advanced IP Video Surveillance Solutions

- Software Packages
- Hybrid Systems (analog and IP)
- NVR Systems

Entire line is completely Scalable

exacq
Technologies

317.845.5710
www.exacq.com

See us at ASIS, Booth #313. Circle 96 on card.



feature

Surprised By Storage

By Sharon J. Watson

**MEGAPIXEL CAMERAS BRING HIGHER RESOLUTION IMAGES,
BUT THE HUGE AMOUNT OF DATA THEY GENERATE PRESENTS
NEW CHALLENGES FOR IT AND SECURITY PROS**



“I am not a tech guy,” said Ken Haverlan, director for security, health and safety at Middletown County Schools in New York. That’s why he immediately brought Mike Tuttle, the school district’s IT chief, into discussions about a new IP video surveillance network.

Although Haverlan’s primary goals were capturing identifiable faces and ensuring video was immediately available to first responders, Tuttle recalls his initial question: “How am I going to store all this footage and for how long?”

Capturing a definitive identity on video and storing that video may seem like two distinct issues. Yet, video storage is a critical issue shaping how enterprises make the transition to IP-based surveillance networks.

As security departments replace VCRs and videotapes with digital recording devices, digital cameras and encoders to transform analog camera output to IP, they and their IT counterparts quickly learn that networked video generates a lot of data—potentially terabytes of it every day.

That’s data that must be managed, and IT departments are assuming the responsibility.

“When the data’s on our network, we know how to get it, store it and back it up,” Tuttle said. “Ken relies on us for connectivity, availability and troubleshooting.”

Security departments in some industries, such as casino gaming, can still make a case for running their own networks and storage.

More often, as video networks evolve from closed circuit to IP, they become part of the existing IT infrastructure, although they may be partitioned as a subnetwork or a separate storage area network within the security department’s purview, said Dick O’Leary, senior director for EMC Corp.’s physical security solutions in Hopkinton, Mass.

Such convergence can be driven by regulatory requirements or corporate data storage policies, economies of scale and plans to make video data available to other enterprise applications.

Further, choosing switches and routers and designing network storage topologies requires networking expertise most security

officers don’t have. Similarly, most IT professionals are not qualified to decide placement and angles for cameras or create access and use rules for them.

“You definitely need to work simultaneously as one organization,” Tuttle said of balancing IT requirements with security’s needs.

LESS BANDWIDTH, MORE STORAGE

That’s especially true because decisions about how much video to store, for how long and where to store it can affect where, which and how cameras are deployed.

In general, IT and security professionals underestimate storage requirements, vendors say.

“Video will require less bandwidth and more storage than they expect,” said Fredrik Nilsson, general manager for Axis Communications-North America, headquartered in Lund, Sweden, with U.S. offices in Chelmsford, Mass. He and other vendors estimate that storage costs run as much as 30 percent of a video project.

Though storage devices are steadily becoming cheaper, video is data-intensive, and the higher a camera’s resolution, the more data it generates. For example, Bosch Security calculates that a single camera transmitting at 30 fps using the common interface format resolution of 704 x 576, or 4 CIF, generates 11 gigabytes of data per day. Three hundred of those cameras recording continuously would spew out 3,300 GB each day, or more than 3 Terabytes of data.

Most users on a budget soon drop expectations of running megapixel cameras constantly at 30 fps.

“They would like to have higher resolution if they could afford it,” Nilsson said.

SMARTER VIDEO COLLECTION

Users can reduce short and long-term storage needs while still capturing critical video data in several ways. First, some cameras and controllers are intelligent enough to run at 1 to 4 fps until they sense motion or another event trigger, then ramp up in an eyeblink to a higher frame rate. These cameras can be deployed in less sensitive locations, while higher resolution digital cameras running at higher frame rates are installed at critical points.

Video compression technologies are improving too, reducing the amount of data to store while maintaining image integrity.

“H.264 compression reduces file storage requirements significantly,” said Mike Morper, director of product management for GE Security’s Digital Surveillance Video in Costa Mesa, Calif., noting that the industry compression standard improves storage efficiency by 40 to 60 percent. “It does things that are smart for video streaming.”

Content analysis, done in smart cameras, video management systems or separate analytics programs also can reduce data volumes by determining what video data must be stored at what resolution.

“If nothing’s moving, you can dump 90 to 99 percent of the data,” said Stephen Russo, director for security and privacy technology at IBM Global Technology Services, Armonk, N.Y.

“Move as much intelligence to the edge of the network as possible, and you’ll have fewer bandwidth and storage issues,” said

In general, IT and security professionals underestimate video storage requirements.

Leon Chlimper, vice president of systems for Bosch Security Systems, based in Fairport, N.Y. As cameras and analytics on the network's rim get smarter, he expects users to save bandwidth and storage by transmitting only video that needs to be seen.

WHERE TO PUT IT ALL?

Many camera, software and storage vendors support the idea of moving video storage to the network's edge. Security and IT

chiefs usually agree, say vendors. (See diagram and sidebar.)

"You'll always have a need for storage on the network edge," Morper said. Physical security departments like having data stored locally in case the network should fail.

Local storage also offers users the flexibility to deploy some higher resolution cameras without necessarily tying up bandwidth. For instance, Avigilon, a Vancouver, British Columbia-based maker of megapixel

el cameras, runs its high-resolution video output to a high-capacity redundant array of inexpensive disks (RAID) at the network edge. Clients using the cameras to augment analog cameras may run an analog signal out of RAID storage to DVRs or, through an encoder, to a video management system.

In its edge storage solution, Steelbox Networks Inc. uses a 3-foot-long cable to attach cameras from a variety of manufac-

Storage Alphabet Soup: Of DAS, NAS and SANs

Where and how IP-based video is stored has a big impact on an enterprise's storage requirements. Instead of streaming video throughout a corporate network, most users are opting to capture and store IP video on the network's outer rim. When video is identified as critical, it is then routed to a central point.

This tactic can be implemented in several ways. First, there's direct-attached storage, in which IP output from a camera or encoder goes directly into a storage device like a DVR, an enterprise-class storage server or a purpose-built storage device with a redundant array of independent disks.

A second approach is network-attached storage. With an NAS storage topology, data from cameras and encoders is routed to a collection point on the surveillance network, such as a network video recorder. While a NAS implementation uses bandwidth on the surveillance network, it still segregates video data from the corporate backbone.

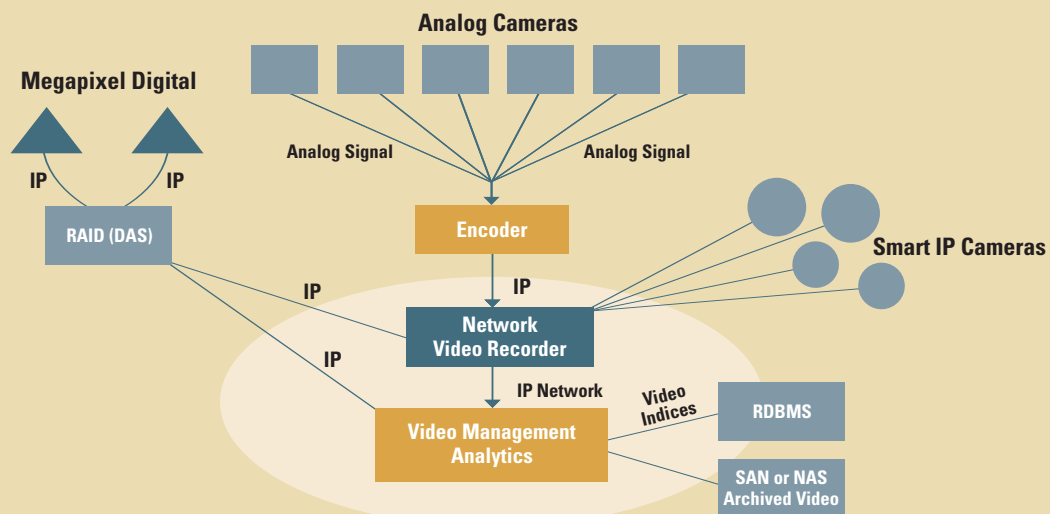
A NAS looks like a file folder to a user or camera, said Jame Ervin at Stonefly Networks. That's a potential disadvantage: many devices can store data in it, but it's slower at retrieving data. So for larger surveillance networks, a storage area network might be the better fit.

A SAN is a network of hard disks devoted to storage, analogous to a file cabinet with many files in several drawers, so storage can be shared across devices and users. This flexibility enables users to partition a SAN so that data from a particular camera or surveillance area is written to a specific area on the SAN, Ervin said.

Most SANs today are the province of corporate IT networks because they were created using Fibre Channel, a high-end data communications protocol. SANs based on the Internet small computer systems interface (iSCSI) protocol could become popular for video networks as more IP-based cameras are deployed.

That's because iSCSI protocol works wherever IP does, so existing equipment and servers can be used. "It lets you write to a storage device as if it were connected to a server," said Fredrik Nilsson at Axis Communications.

Eliminating the server reduces costs—another reason why vendors expect iSCSI to grow.



One possible network set-up to minimize network traffic and storage requirements

turers directly to its Digital Matrix Storage Switch controller and storage appliances of up to 16 Terabytes.

"We store it all and firewall it, so you only get video on the network that you want to see," said Chip Howes, president and CEO for Atlanta-based Steelbox.

Bosch Security, Cisco, GE Security and IBM, among others, also offer storage devices that can be deployed on the network's rim. Other vendors, like On-Net Surveillance Systems Inc. (OnSSI) and IndigoVision, run their software programs on off-the-shelf workstations to manage primary video.

"There's no point buying an expensive disk array for streaming video," said Gadi Piran, president and CTO of OnSSI, based in Suffern, N.Y. OnSSI uses a workstation's storage capabilities to hold about an hour's worth of incoming video for analysis; the

As for long-term storage, analytics keep video volumes manageable.

filtered video is offloaded to archival storage. This buffering balances the network load, provided the user has sufficient server capacity for the real-time video.

As for long-term storage, analytics keep video volumes manageable.

"We're being asked increasingly to prune and archive data," said Steve Collen, director of product management for Cisco's physical security business unit, based in San Jose, Calif. He and other vendors say users want integrated analytics so they can make informed decisions about what video to keep.

For example, IBM analyzes video as it compresses it to create metadata. Only this

high-level, descriptive information, along with a bit of the beginning and ending of the indexed video, is stored in a central relational database, Russo said. The complete video described by the metadata is indexed and offloaded to a separate storage device that can essentially reside on any network.

VIDEO: BEYOND SECURITY

All vendors emphasize their open hardware platforms and application programming interfaces to ensure storage devices work with whatever analytics and other security or business programs an enterprise is running.

Open systems are important because many enterprises plan to integrate video data not only with security applications like access control, but also with traditionally business-oriented applications such as point-of-sale analysis and training.

"The industry is just starting to see video as data," said GE's Morper. He and other vendors say it is possible business users might want to use the surveillance network to study how customers behave in front of specific sales displays, to name just one application.

"As more digital video is deployed, people will come up with interesting ways to use it," said Jame Ervin, product manager for Stonefly Networks in San Diego, Calif.

Security chiefs might initially resist commingling security and business video, but could find that's one way to grow a bigger budget and more support for their efforts.

CSOs can show operating and marketing officers how the video infrastructure can net valuable marketing and training data, said Jeanne Jang, IBM global leader in digital video surveillance. "It's beyond traditional security, so other important players on the management team can support it."

Thinking about the potential business impact of video systems and storage does add another layer of critical planning complexity.

"In this day and age, sitting down with only IT and security at the table is a mistake," Chlimper said. "The systems can do so much more." ☰

Sharon J. Watson is a journalist based in Sugar Land, Texas. She can be reached at sjwatson@experteditorial.net.

Storage Effects

At Middletown County School District in New York, storage issues had a definite impact on Ken Haverlan's wish list. Haverlan, the director for security, health and safety, really wanted to capture video at 30 fps. Then he hoped to store data for three to six months to have the flexibility to address situations in which time went by before an alleged incident came to light.

"Even if you only record when something moves in the camera's field of vision, that takes a lot of storage space given our number of cameras," Haverlan said. The system encompasses 265 Axis Communications surveillance cameras monitoring eight buildings spread across the town.

So he and the district's IT director, Mike Tuttle, agreed initially to store 30 days of video data. To capture identifiable images, cameras in key locations run at 26 fps. Elsewhere, the routine rate is 6 to 10 fps.

In each building, an off-the-shelf Dell Windows XP-based workstation with 1.5 Terabytes of storage collects video from the local cameras. Each storage server reports to a single central server, through which Tuttle can access their data. Because the network is Ethernet-based, he and Haverlan can access video from their own workstations, the Internet or handheld devices.

Tuttle's ultimate goal is to have a storage area network to offload more video data from the individual servers so it can be stored for longer periods. The SAN also would support multimedia data storage for classrooms and an access management application.

The network backbone supporting the surveillance installation includes Cisco switches for power over Ethernet; the school district's VoIP telephony system also is integrated with the backbone. Being certain his infrastructure was secure and stable was vital.

"That's been a real benefit when integrating other applications," Tuttle said.

Haverlan is satisfied too, noting that his staff has easy access to video data while the new system is more reliable than what it replaced. "We're having a good degree of success," he said.



CHANGING Channels



CONVERGENCE
IS WRITING
NEW RULES
FOR VENDORS,
DISTRIBUTORS,
INTEGRATORS
AND DEALERS

By Frank Barbetta

Anixter's Tim Holloway, vice president of Technology-Security Solutions (left), and Don Hoffman, vice president of Marketing-Distribution Products, review a video surveillance system.

Converging IT and IP disciplines have made their way into the once analog-only video security market, firmly establishing new criteria for business relationships among the industry's traditional and emerging vendors, distributors, systems integrators, resellers and dealers.

And by all accounts, the integration of computers, communications and video imaging will accelerate within many of the indirect sales channels as enhancements progress in digital cameras, broadband networking, video management software and open standards.

That has led manufacturers, distributors and systems integrators to impose on each other new sets of qualifications that entail technology efficacy, personnel training, education programs and official certifications. The benefits that accrue for participants who pass muster include customer referrals, potential sales leads, joint sales calls, major project participation, spot price breaks, volume discounts and capital financing aid. But the clear aim of these programs is to push third-party resellers and dealers to adapt to security and IT convergence.

Conventional supply chain strategies need to be restructured to accommodate customers, resellers and new technologies and products driving the video surveillance and security market, said Frank DeFina, president of Panasonic System Solutions Co. of Secaucus, N.J. Its sister unit, Panasonic Security Systems, developed a multi-tiered supply chain structure that encompasses manufacturers' representatives, authorized dealers/systems integrators and authorized national distributors, along with

the dealers who purchase through them.

DeFina posits that the distributor channel has always been "a powerful go-to-market solution" for manufacturers looking to gain access to a wide cross-section of industries and to make products more readily available to resellers serving the core security industry.

"As video surveillance and security system design continues to shift to a network-based platform, the sales channels supporting these systems also are changing," DeFina

said. "Traditional security dealers/integrators are facing new competition from several different and formerly non-competitive resellers from a range of industries, including IT, telephony, cabling and electrical contractors. Additionally, systems designers and installers must familiarize themselves with new technologies, such as IP, networking and software management, to take advantage of new systems capabilities and interoperability."

A NEW CORE COMPETENCY

"In addition to a complete understanding of the products and technologies, security integrators' ability to react quickly to the emerging IP technology applications in the market and meet the demand of their end users is essential to staying competitive," said Tim Holloway, vice president of technology and security solutions at Anixter International Inc., Glenview, Ill. "This technology shift is going to require security integrators to respond



NEW RULES: Panasonic Security Systems Frank DeFina

Panasonic System Solutions Co., Secaucus, N.J., takes measures to ensure that reseller partners have the expertise and practical knowledge to design and/or install its latest IP-based video surveillance products such as i-Pro, said Frank DeFina, president of the unit.

Besides tech training, DeFina maintains the i-Pro certified reseller program's objectives include instilling competitive confidence for resellers and end users in dealing with a company that is directly aligned with Panasonic.

"It's a win-win proposition," he said. "The program encourages resellers to complete certification so they can gain the resources and information they need to best support and service their customers."

The certification process provides resellers with several advantages such as easy access to Panasonic i-Pro network products and free education and training through Panasonic Security Training University.

now—to devote all their available capital, human and technical resources to learning a new core competency of IP design, integration, deployment and installation.”

The once-separate distribution channels associated with physical security and IT have started converging to the point that each side is now aggressively seeking the other’s knowledge base and expertise on a regular basis. Eric Fullerton, president of the U.S. office for Brøndby, Denmark-based Milestone Systems, said, “They do this by partnering with each other, employ-

Physical security and IT distribution channels are converging, with each aggressively seeking the other’s knowledge base.

ing each other or educating each other.”

One trend in IT has resellers looking at video and control as a new industry.

“The ability to help that market with channel partners is important,” said John Gaillard, president of security distribution at value-added distributor ScanSource Inc.

of Greenville, S.C.

ScanSource’s value-add proposition to the business includes “ease of doing business” measures such as Web-based tools for accessing product information, assessing prices and conducting procurements, as well as account management, consulting and education programs, the latter involving technology, marketing and sales.

“We want to be more than a transaction-only distributor,” Gaillard said.

Scott Schafer, vice president of sales and marketing at Pelco, a video management system vendor in Clovis, Calif., said their goal is to make sure their products can be sold and used by international reseller partners.

“We have to build the product the right way and provide the training and support beyond the traditional CCTV business. How do we take these technologies and prepare ourselves and our resellers to take advantage of what’s coming up? This is a lot of what we’ve been working on,” he said.

Pelco also operates a special Web portal for reseller education material and runs a video security institute for training. Resellers of the Endura product line for major products and larger customer installations, however, must be certified by the company; this is significant particularly because the technologies embrace both the Linux operating system and Microsoft X clients.

“We cannot just give it to anybody, but that doesn’t mean we can’t train,” Schafer said. “The resellers have to make a commitment to the infrastructure and the people that are different from CCTV. There are a lot of things they need to do.”



NEW RULES: Milestone Systems Eric Fullerton

Since 2004, Milestone Systems has been making a distinction between authorized dealers who merely sign up and are approved to carry low-end products and certified resellers allowed to handle high-end products. It currently has about 150 certified resellers and is looking to double that number within 12 months. The channel is fed by a handful of major distributors, among them Ingram Micro, Anixter, TechData and ScanSource.

Milestone’s manufacturer partner agreements with the likes of Panasonic and JVC are aimed at developing the software features of the products, while the “solutions partners” program involves a range of companies using API know-how to integrate solutions and add value.

“We get at least one solutions partner application every day,” said Eric Fullerton, president of the U.S. office for Brøndby, Denmark-based Milestone Systems.



NEW RULES: ScanSource John Gaillard

Certification prerequisites are moving into the supply chain rapidly, according to John Gaillard, president of security distribution at value-add distributor ScanSource Inc., Greenville, S.C.

“This can be a barrier to market entry, but it is becoming a needed to-do item,” he said.

ScanSource keeps its line of cards to about 50 manufactured brands. Gaillard said the company sits down with such core manufacturers as Panasonic, Sony, Axis and others on an annual or quarterly review basis to dovetail marketing, sales and support initiatives. The distributor also is operating educational Web portals and organizing road shows to help resellers with the newer IT/IP aspects of video security.

COORDINATION LINKED TO GROWTH

Fredrik Nilsson, general manager of Americas for Lund, Sweden-based Axis Communications, indicated that sales channel coordination by this maker of IP network cameras, video servers and video management

software is linked intrinsically to marketplace growth. Its two-tier model involves about eight distributors funneling product to resellers and systems integrators, with some of its big-name relationships being with Ingram Micro, Tech Data, Anixter, Securitas Systems, Lenel Systems International Inc., Honeywell and Milestone Systems.

“With distributors, the focus is on their markets and their expertise to educate resellers and systems integrators,” Nilsson said. “Some distributors are from the traditional security side interested in IT and IP, some are from the network side interested in security, and some are traditional IT looking at video as the new element.”

With a background in manufacturing and factory automation, Robert Lecher, owner and president of value-added distributor RepLogix LLC in Shelby Township, Mich., said his firm is leveraging technology know-how into video surveillance for production plants, the food processing industry and utility market verticals.

Such applications as supervisory control and data acquisition (SCADA) for large-scale, distributed measurement and control, as well as management execution systems (MES), are intrinsic to the RepLogix niche business, and the company is seeing a good deal of action in the water utility and treatment areas.

“A lot of security people don’t understand SCADA and the integration with MES,” Lecher said, suggesting a broad trend of merging security, data collection and plant/process/quality control is making its way into the distribution channel.

Among the RepLogix video security partners are Milestone Systems, Long-Watch and Mobotix. Lecher maintains that despite the disruptive potential of IT and IP, the security business is generally holding true to its traditional model of using systems integrators and distributors to reach end-user buyers.

DEVELOPMENT PARTNERSHIPS

Like several others in the business, Nilsson underscores the key roles that open architectures and application programming interfaces play in total market success. The company also has an application development partner program that involves complete solution work; there are about 400 ADP partners worldwide, including 100 or more in the United States.

“Open systems and IP integration provide the groundwork for true systems integration and the ultimate convergence and interoperability of all physical security and IT systems,” DeFina said. “It is imperative that equipment manufacturers and software developers across all categories of security systems products—video, access control, fire and life safety—share protocols to ensure interoperability between systems and products from dif-



NEW RULES: Pelco Scott Schafer

Scott Schafer, vice president of sales and marketing at video management system vendor Pelco in Clovis, Calif., said his firm’s certification requisites apply to distributors and resellers alike because Pelco wants certification consistency. Distributors funnel product only to certified resellers, which make up only about 10 percent of Pelco’s estimated 5,000 resellers in all. Among the Pelco criteria:

- ▶ Hire network and IT savvy personnel.
- ▶ Have installers, tech support and troubleshooters on staff.
- ▶ Meet a pre-testing stage on designer, sales and support expertise.
- ▶ Pass 2-3 days of training classes.

“We wanted no loopholes in our process,” Schafer said. “We continue to expand with the right distributor and reseller partners, but we’re not out there with a huge recruitment program. We try to coach and convince the more traditional resellers about certification yet are being selective. Have we altered our channels? Yes, but we altered ourselves also with a new IT, IP and network focus. A segment of our resellers have made the same choice, and it is an exclusive group for sure.”



NEW RULES: Axis Communications Fredrik Nilsson

Axis Communications resellers and systems integrators get access to vendor tech and sales support, according to Fredrik Nilsson, general manager of Americas for the Lund, Sweden-based vendor. Nilsson said the U.S.-based numbers have increased from about 100 such third parties in 2004 to more than 3,000 at this time.

The Axis channel partner program is directed at education, training and certification criteria.

“Qualifying resellers and systems integrators may be different, depending on which side or sides of the business they come from, but all must have the training and education,” he said. “We don’t prevent anyone from selling the product, but the ones who qualify and sign up also get the sales leads and price discounts.”

ferent manufacturers. Without this fundamental level of cooperation, true convergence cannot take place.”

The Panasonic Solution Developer Network is a typical initiative; it provides a platform for companies to share resources and encourage enhanced interoperability across formerly disparate product platforms. At least 24 companies have enrolled in PSDN, with Cisco Systems recently emerging as a partner.

Milestone’s Fullerton echoes the corporate message offered by the maker of IP video server/software platforms: the whole video security industry is moving away from the vertically integrated proprietary technology of the CCTV era toward open APIs addressing multiple vertical markets.

“What you will then get is an ecosystem of specializing companies in those market areas,” he said.

The business has progressed from a point several years ago when there were concerns over camera quality and bandwidth, but the intelligent products now are “winners,” and networks are faster, making installations of 80 to 100 cameras or more commonplace, according to Art Morrison, operations manager at value-add distributor ProTech Security in North Canton, Ohio.

ProTech now looks only at IP and open architecture products, seeks out the appropriate vendors, pursues IT training and strives to be more IT savvy, as the industry moves from dabbling with IP video to jumping into IP video with both feet.

“We are not really in the computer business, but guess what, we are,” Morrison said. “The industry is now coming to companies like us with open arms; we are being sought after. They need access control and video in the security mix.”

ProTech’s relationships have included Dell Computer, Anixter, Axis Communications, Milestone Systems, On-Net Surveillance Systems Inc. and Berbee Information Networks, a Cisco Systems contractor.

Robert Hile, vice president of business development at Adesta, an IT, network systems and broadband integrator in Omaha, Neb., said leveraging his company’s expertise into IP-centric video security and sur-



NEW RULES:

Adesta
Robert Hile

Adesta’s contracts with end users involve manufacturers as signatories, and the company is asking producers also to move beyond workmanship warranties into the realm of performance metrics guarantees, according to Robert Hile, vice president of business development at the Omaha, Neb.-based systems integrator.

“We are rapidly approaching the time where if manufacturers won’t sign, we won’t use them,” he said.

In its total video security, IT and network portfolio, Hile described Adesta as product-agnostic, but it has close partnerships with Motorola and Cisco Systems. It is a Cisco physical security authorized technology partner and a Cisco network segment premier partner, plus it is pursuing Cisco wireless ATP status.

“There are training and certification requirements, and we can share sales leads,” Hile said. “But Adesta has to make the financial investment needed for such qualifications and benefits.”



NEW RULES:

Anixter
Tim Holloway

Anixter International’s READY! deployment services allow security integrators to apply best practices in material management to lower their total cost of deployment, improve profitability and scale to the demand their end users will place upon them, said Tim Holloway, vice president of technology and security solutions.

“As a distributor, Anixter does not certify customers directly. We do, however, offer an educational curriculum that focuses on best practices, industry standards (on the networking side) and market trends affecting the networking and security markets,” Holloway said. “For example, we offer a program called Anixter University that focuses on IP and networking basics, video surveillance and access control technology, just to name a few. Our National Seminar series includes information on designing an IP-connected enterprise for various subsystems in a building, including voice and data networking, video surveillance, access control and HVAC.”

veillance is an easy evolution, yet there are challenges in product manufacturer selections and sales channel alliances.

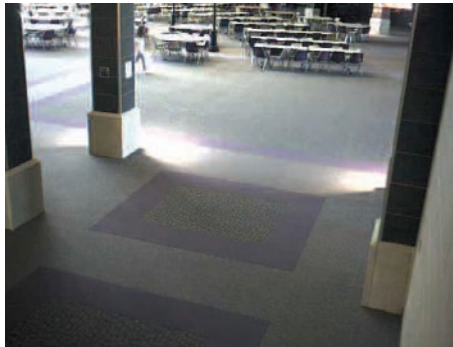
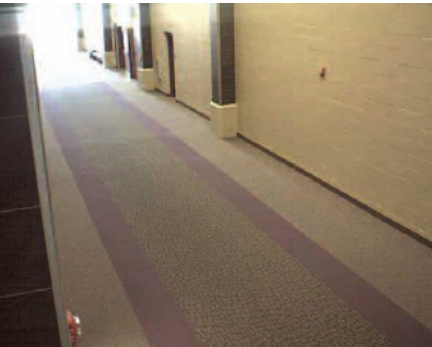
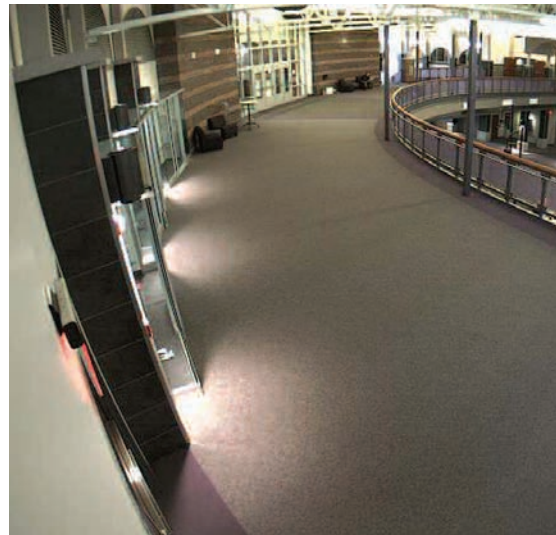
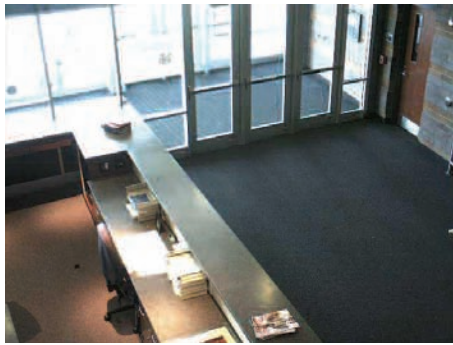
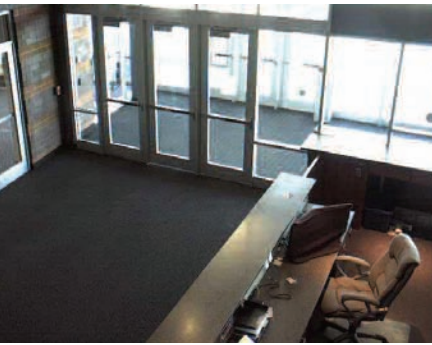
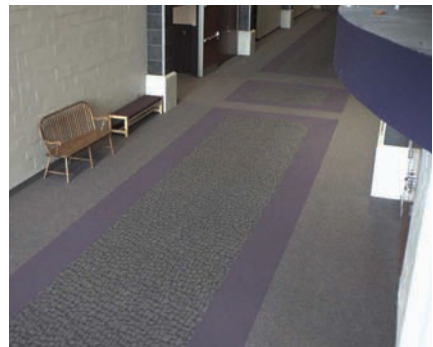
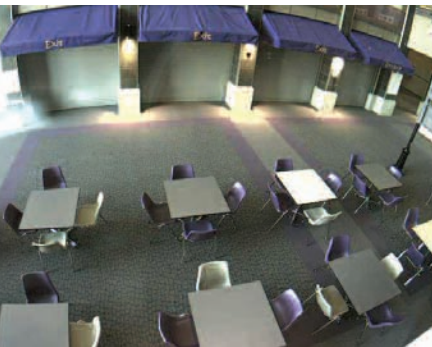
“We are trying to stay with products that are openly integrated with as many protocols as possible,” Hile said. “This whole market is changing, and manufacturers before didn’t always stand behind their products. We are asking vendors to belly up to

the table. If they don’t do that, we will walk away. And many systems integrators are becoming more sophisticated and savvy. They want products that work and integrate well; if the products don’t, they’ll pass on it.”

Frank Barbetta is a journalist based in Little Falls, N.J. He can be reached at frank_barbetta@yahoo.com.



Open BUT

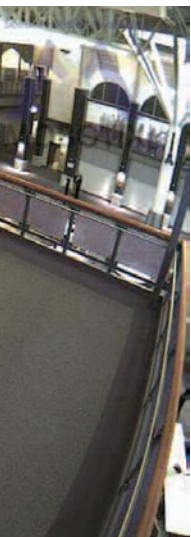
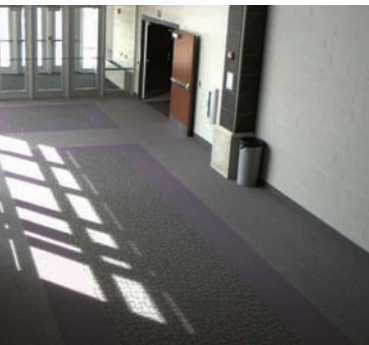


Jackson High School in Massillon, Ohio, as seen through Mobotix wide-angle megapixel cameras. Networked security for the \$45 million state-of-the-art addition was handled by ProTech Security.

SECURE

ONE HIGH SCHOOL'S LESSONS IN IP-BASED VIDEO

By Sharon J. Watson



With features ranging from a high-tech tufted vinyl carpet to special air filtration systems and updated kitchen equipment, the \$45 million addition to Jackson High School in Massillon, Ohio, was designed as a premier, state-of-the-art education facility. So it's little wonder the school's architect determined the new building's technology and security systems also would be cutting edge.

The school's existing analog video surveillance system definitely didn't meet that standard. The school's security officer made that plain to executives from ProTech Security Inc. when they signed in at the school to present recommendations for the new building.

"We told him we were a video company, and he said, 'This video system is the hardest thing I've ever used and the images suck,'" said Art Morrison, operations manager for the North Canton, Ohio-based

company. Morrison was quick to point out ProTech hadn't designed the old system and was, in fact, prescribing a next-generation solution based on IP-based cameras and software.

The company had to convince not just the security officer, but also the school board and other administration officials.

"We offered our vision of the way IP video should be, which is 100-percent open architecture and 100-percent megapixel cameras," Morrison said.

Prices for megapixel cameras could be a barrier, according to McKimm. “But it’s invaluable to get those tools to first responders at a school or campus setting,” he said.

That vision ran counter to the administration’s original thinking.

“They were inclined to stay with analog cameras and DVRs,” said Daniel McKimm, president of ProTech. But he and Morrison demonstrated how using an open architected solution, IP cameras and an NVR would let the school add cameras to the network quickly whenever they were needed.

“They began to understand the network scalability right away,” Morrison said, a point driven home because the old system’s DVRs filled quickly, making storage and retrieval difficult.

The administration also was intrigued that the existing analog cameras could be incorporated into the new surveillance network by using an encoder to digitize signals, McKimm said. That enabled the district to preserve some of its investment in the older system.

IN WITH THE NEW

The surveillance network ProTech designed and installed at Jackson High School uses a virtual local area network off the school’s fiber backbone network. The VLAN supports 62 IP megapixel cameras from Mobotix AG that are deployed at key locations in the new 150,000-square-foot high school building, plus a bus barn.

Images captured by the cameras are routed to an NVR, a Dell Edge server box running under Windows 2003 Server. Video management software from Milestone Systems analyzes the video and determines what data to store. That video is offloaded via an Internet small computer systems interface (iSCSI) connection directly to a Dell MC300 storage area network.

The system enables the school to use the cameras as deterrents, as identity management devices, and as eyes and ears for first responders.

“Mobotix is a security solution with video as its core feature,” McKimm said.

Because Mobotix cameras are IP-based, specific cameras can be addressed by other IP-based devices, such as mobile laptops and digital phones, so that security, police and fire officials can see what’s happening in a particular camera location.

Further, in a feature Mobotix claims is unique, its cameras also support two-way audio direct via session initiation protocol. That means first respondents can use IP devices to address a specific camera and hear what’s going on in a room. If appropriate, they could also speak through the camera to a room’s occupants.

“An IP camera can give first responders the ability to be there, visually and audibly, at the scene of a crisis,” said McKimm, a former law enforcement officer and FBI Academy graduate.

The open system offers convenience for users, as well as increased security. For example, a secondary entrance door at the school is routinely locked after a certain time each morning. The door is monitored by a network camera and a door intercom linked with a Cisco IP-based phone system. If a student arrives at the door to find it locked, he or she can use the intercom to reach the security officer on duty, who can confirm the student’s identity via the intercom, as well as with the camera’s visuals.

Cameras can be deployed quickly as deterrents because they are IP-ready right out of the box, Morrison said.

That was proven when the school’s bus garage was badly damaged by vandals while ProTech was installing cameras in the new school building. The administration decided to add cameras to the garage, and ProTech deployed them within a day.



ProTech’s Daniel McKimm: “An IP camera can give first responders the ability to be there, visually and audibly, at the scene of a crisis.”



ProTech's Art Morrison: "They began to understand the network scalability right away."

BUILDING A BETTER NETWORK

Technical challenges for the new video network at Jackson High included increasing storage capacity and retrieval capabilities and greatly improving image quality without bogging down the VLAN. The functionality of the cameras and video management software helped ProTech address these.

One increasingly popular way to reduce the load on a video network is to put intelligent recording devices at the network's edge. Mobotix cameras do have intelligent capabilities, but Jackson High preferred the greater searching and retrieval capabilities offered by the video management system.

"The intelligence here is all in the server," Morrison said.

In addition, the school uses Microsoft's Active Directory and wanted to integrate its functionality with the video management system.

The NVR is another critical piece of the network.

"The server specifications have to be matched to what you're trying to accomplish," Morrison said.

The first issue is how many cameras are feeding data to the server and at what

frame speeds, which will determine the network load. For storage reasons, ProTech specified using the same 8 fps rate on all the cameras. With the cameras' megapixel capabilities, this rate still offers excellent image clarity, yet a reasonable network load, Morrison said.

A second consideration is how many people will be logging in to view the video data and how. At Jackson High, the school

principal and assistant principals access the video from the NVR via thin desktop clients and Web browsers. A resource officer from the local police department and a school district-employed security officer also monitor video.

Then there's long-term storage. The SAN easily stores 14 days of video, Morrison said. The plan is to deploy a second

SAN to accommodate data from 40 more cameras to be added in the second and third school renovation phases.

OPEN IS MORE SECURE

As former law enforcement officers, McKimm and Morrison are sold on the value of IP megapixel cameras for their clarity and ease of use.

Prices for megapixel cameras could be a barrier, McKimm said. But it's invaluable to get those tools to first responders at a school or campus setting. They also counsel security and administrative executives to make sure technology teams help map the transition to IP.

"Even when we talk with a security official first, we won't go any further until we talk to the information systems people," Morrison said. "We want to work closely with the tech guys too."

ProTech executives urge would-be IP video users to gain more security by keeping their networks and video solutions open. "Buy products that'll talk to each other via IP," Morrison said. True IP compatibility should make it easier to integrate video networks into access management solutions and other applications that could use digital image data.

Finally, be sure to vet the capabilities of

The Mobotix cameras have intelligent capabilities, but Jackson High preferred the greater searching and retrieval capabilities offered by the video management system.

the products, McKimm said.

"We're seeing a lot of companies come out of the woodwork with product offerings, but they don't know networks," he said. 📞

Sharon J. Watson is a journalist based in Sugar Land, Texas. She can be reached at sjwatson@experteditorial.net.



Applications, Strategies, Solutions



1 Pelco Multi-Channel Encoder

Whether planning a new IP video system, integrating analog cameras into a network-based system or expanding a digital video system, Pelco's NET5308T multichannel video encoder for its Endura video security system environments offers flexibility without the need to redesign the network.

The NET5308T is a high-performance, dual-stream eight-input video encoding unit, expandable to 16 video inputs, that optimizes use of network switch ports. Ideal for applications with requirements for clusters of cameras, it converts live analog video signals into dual MPEG-4 streams of high-quality digital video at up to 30 frames per second per stream, all while occupying a single port on a network switch. This multi-channel encoder allows any analog camera to easily integrate into the Endura environment.

In addition, the NET5308T uses motion adaptive deinterlacing technology to enhance image quality when viewing images. The NET5308T incorporates EnduraView video stream optimization technology to select the best image quality and frame rate for the target Endura product (decoder, workstation, console), all without affecting the system recording rate. For example, the unit selects a high rate and quality setting for recording and alarm conditions and would select a lower rate for simple monitoring.

www.pelco.com

2 GarrettCom Edge Switch



GarrettCom Inc. has added an industrial-grade PES42P Power Source Edge Switch to its growing line of Magnum Power over Ethernet (PoE) switches that support clusters of IP video surveillance cameras or Ethernet-enabled industrial access control devices. The PES42P edge switch is designed to support up to four surveillance or access control devices as well as a fiber trunk back to a central control point. This makes the product ideal for applications such as traffic monitoring and control where up to four cameras at an intersection can be hooked to a single PES42P switch. This still leaves fiber ports that can daisy-chain with other intersections for high-bandwidth, secure transmission to the central monitoring point.

Using the same principles, the PES42P can support access control and video monitoring at a warehouse, and security for areas such as shopping mall parking lots and transportation terminals. The new PoE Power Source Edge Switch offers 17 different port configurations with a 48VDC power input for PoE and an outdoor temperature rating to address a wide variety of application needs. Prices start at \$690.

www.garrettcom.com

3 ioimage Intelligent Video Appliances

ioimage has introduced a line of intelligent video encoder/decoders that provides high-resolution video, constant bit rate streaming with latency at less than 50 milliseconds. The new lvm series delivers exceptional video quality, optimizing bandwidth for real-time video compression and streaming. Ideal for mission-critical, long-range surveillance devices, the lvm enables homeland security and defense organizations to effectively carry out audio, video and data-link applications in which timing, quality and bandwidth are critical.

The plug-and-play lvm encoders/decoders support high-quality bit streaming from as low as 64Kbps, thereby enabling visual communication with remote sites at up to 6Mb/s. The lvm series also is available with optional built-in video analytics.

www.ioimage.com



4 StarDot Technologies IP Camera

The StarDot SecureCam is a highly integrated 5 megapixel IP camera that supports both a Power over Ethernet connection and a standard BNC video out connection at the same time. Other features include an automatic mechanical day/night filter (for nighttime IR mode), DC auto iris and alarm triggers. Internal video motion detection can upload images or video via NVR, FTP or email. Image resolution is adjustable and both 720P and 1080P HD modes are supported.

www.stardot-tech.com



5 Mirapoint Email Appliance with Embedded Policy Engine

Mirapoint's RazorGate email security appliance with an embedded policy engine provides enterprises and service provider customers with a more secure, scalable and affordable architecture for enterprise email. The Mirapoint solution's unique architecture reduces total network traffic, reduces load on the corporate directory and closes holes in the firewall.

Traditional email security products have to query the corporate directory for each and every piece of incoming mail to check whether the recipient is valid. As a result, every single message, whether ultimately accepted or rejected, generates additional load on the firewall, internal network and the corporate directory. Mirapoint's RazorGate with Embedded Policy Engine eliminates this problem by validating recipients autonomously at the edge of the network for each message.

www.mirapoint.com



6 Cieffe Chooses Pixim Chipset

Cieffe S.p.A. will use Pixim Inc.'s Orca chipset in its first composite security surveillance camera. Based on Pixim's Digital Pixel System (DPS) technology, Cieffe's composite CamPX complements its Nettuno CamPX network surveillance camera with Power over Ethernet (POE) capability.

Pixim's Orca chipset enables Cieffe's CamPX to deliver excellent images in both normal and wide dynamic range scenes in any lighting conditions, 24/7. Pixim's 720 x 540-pixel, progressive scan image overcomes typical impediments of existing analog technologies caused by variable lighting and limited color accuracy to provide positive subject identification.

www.cieffe.com



7 Integral Technologies Hybrid Digital Video Management System

Integral Technologies' DigitalSENTRY (DS) 1000 is an MPEG-4-based digital video management system (DVMS) supporting IP and analog cameras. The system offers 16- and 32-channel configurations, capturing five to ten fps. The DS 1000 seamlessly integrates with any Integral DVMS through a single user interface. It supports the Integral IT software suite consisting of network health monitoring, archive utility and automatic online updates. The system also supports PTZ cameras and other industry-standard devices, while the MPEG-4 compression provides a smaller file size with improved image quality.

www.integraltech.com

8 Moxa Video Encoder

Moxa Technologies, a manufacturer of industrial Ethernet products, has introduced the VPort 351, a one-channel industrial video encoder that provides up to full D1 resolution at 30 fps. The unit supports a dual MJPEG4/MJPEG algorithm, making it suitable for use with distributed surveillance systems in critical industrial applications. Two-way audio is provided for the convenience of real-time communication between system administrators located at the central site, and engineers in the field. In addition, a continuous pre/post event video record function can help system administrators determine why an alarm was triggered.

www.moxa.com





9 Advanced Technology Video DVR

Advanced Technology Video Inc.'s Falcon FA-DR Series DVR merges the processing power of high-end PCs and the functionality of high-end embedded video recorders to offer a cost-effective, high-performance DVR. Features include a built-in DVD-RW archiving capability. Users also can connect their own external archiving options via a USB port. Other features include video motion detection, video obscuration detection, digital zoom and search. www.atvideo.com



10 Bosch DVR Software

Bosch Security Systems Inc. has released new software for the DiBos 8 digital video recorder. Software Version 8.21 enables the DVR to deliver crisper images and alert users to degraded video quality or lost camera signals.

The DiBos 8 DVR now offers recording, live viewing and playback of analog and IP video at a higher resolution (4CIF). With improved video quality, security personnel can capture clearer images that show a greater level of detail.

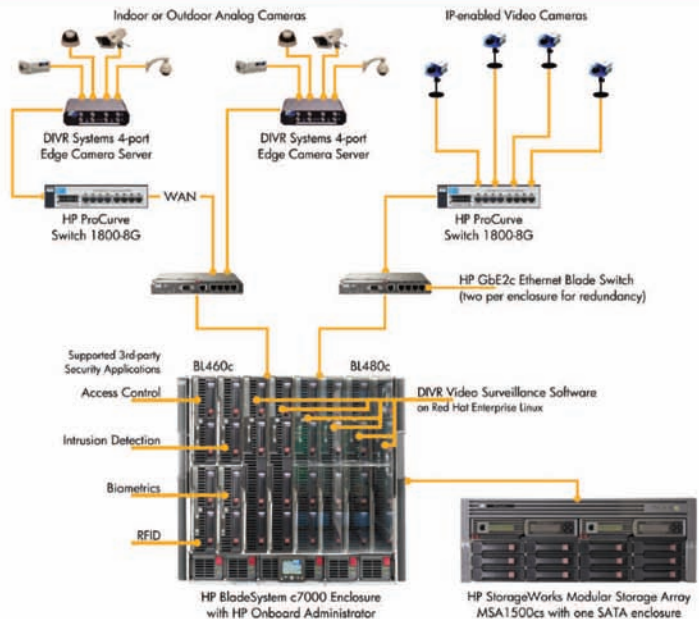
The sophisticated tamper detection system included in Software Version 8.21 will generate an alarm if a camera has been repositioned or if the video signal is lost. DiBos 8 can also forward the alarm by e-mail, SMS, NetSend and the malfunction relay to ensure security personnel are immediately alerted when video surveillance is interrupted. The DVR automatically displays camera alarms in live viewing mode and logs all alarm acknowledgements and deletions. www.bosch.com

Information in this section has been supplied by the respective vendors. *Network-Centric Security* magazine does not accept responsibility for the timing, content or accuracy of the product data or for the quality or accuracy of the photos.

Network-Integrated Video Surveillance on HP BladeSystem



Clearly superior surveillance technologies from HP, Blade Network Technologies®, and DIVR Systems, Inc.



Rising security concerns are accelerating the need for enhanced, proactive network-integrated digital video surveillance solutions that take advantage of the latest computer, network, and storage technologies. But doing so without negating investments in legacy analog surveillance systems has been a serious challenge—until now. To learn more about moving to the next-generation of video surveillance or to tailor a solution for your organization, contact your HP representative, visit www.divrsystems.com or call (661) 393-5546 extension 4.



© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Circle 99 on card.

More Than Just a Wire

by Bob Beliles



IP networking adds value to physical security

Convergence is not new. The IT networking industry has experienced multiple waves of convergence over the past 20 years. And with each wave, convergence has delivered new capabilities and some unexpected high-impact, even game-changing, innovations.

The ability to deploy physical security operations securely and effectively over an IP network has been available for some time. Factors that contribute include high-performance computer chips that can efficiently digitize and process analog video from surveillance cameras; falling costs for the digital storage of information, including video recordings; and a wide range of fault-tolerant features that are an inherent part of IP networking.

Some of the expected capabilities of running a physical security operation on an IP network include access to information from a remote location, such as a manager's home, via a secure, virtual private network connection. This might allow security management to respond more quickly to a given event and coordinate with on-site personnel. New devices also can be used to access information. You might find it helpful to view video on a PC or even a cell phone, for example, rather than on an analog display.

THE EXTENSIBLE PLATFORM

But true convergence doesn't simply use the IP network as a wire. It becomes part of an extensible platform: a platform to build new capabilities, to realize new uses and to sup-

port new users, thereby unlocking the true value of these systems—and in this case, enhancing the physical security group's value to the organization.

Today, almost every business and organization is concerned with the safety and security of its

Convergence also creates processes that encourage employee compliance with security policies.

people and assets, regardless of whether those assets are material or electronic. Physical attacks can target people and buildings; they also can be part of the theft of goods or other assets. Of course, the job of physical security professionals is to stop those attacks.

Cyber, or logical, attacks have similar aims of harming business operations or stealing intellectual property. The job of IT security is to thwart those efforts. Thus, common goals and opportunities exist between physical and IT security, thereby helping to drive convergence.

When physical security is brought onto the IP network, it can strengthen both physical

continued on page 34

and logical security efforts. By tying physical access and network access systems together, IT security personnel can assert specific policies for what, when, where and how certain network resources can be accessed. For example, a converged security system can deny network access to an employee who does not badge in when entering a building. Restricted or classified documents can be better protected if security officials can set a policy that allows only certain PCs in certain locations to access them. The system can be programmed to automatically terminate a network connection from an employee's home if the employee logs on in the office. As a result, physical presence becomes a network-access policy criterion.

CONVERGENCE CAN CHANGE BEHAVIOR

Convergence also creates processes that encourage employee compliance with security policies. For example, employees who must badge in upon entering a facility,

even when the door is held open for them by another person, will be more likely to do so if they can't otherwise log on to the network. Interestingly, this requirement also creates the opportunity for some subtle social re-engineering. While many employees do not feel comfortable challenging someone who may follow

them into a building without presenting credentials, these same employees can courteously hold the door and remind the stranger to badge in to avoid having to make a return trip to the front of the building. Thus, tailgating by all individuals is likely to decrease.

Through convergence, non-security uses for video can significantly increase the value of an organization's investment in a surveillance system. Video can be used to

understand customer behavior or alert management to opportunities to enhance the customer experience, for instance, by shortening check-out lines.

These new applications are only the beginning. Think about how your systems can bring new value to your organization. Ask other departments what problems they

Think about how your systems can bring new value to your organization.

have. You might have a solution.

We can debate about converged physical security systems becoming the norm, but given the opportunities and benefits they offer, the question is when, not if, they will arrive. And, because of those benefits, it may be sooner than most of us think. ☰

Bob Beliles is senior manager of physical security market management at Cisco Systems Inc. He can be reached at bbeliles@cisco.com.

LINKS

A navigational guide to **advertisers** & companies mentioned in *Network-Centric Security*

Accenture accenture.com	HID hidcorp.com	OnSSI onssi.com
Adesta adestagroup.com	Honeywell honeywell.com	Panasonic Security Systems panasonic.com/business/security
Anixter International anixter.com	IBM Global Technology Services ... ibm.com	Pelco pelco.com
Avigilon avigilon.com	IER SA ier.fr	ProTech Security Inc. ... protechsecurity.com
Axis Communications axis.com	Ingram Micro ingrammicro.com	Raytheon Co. raytheon.com
BAA Ltd. baa.com	IndigoVision indigovision.com	RepLogix LLC repllogix.com
Berbee Information Networks .. berbee.com	Inscape inscapedata.com	Sagem Morpho Inc. morpho.com
Bosch Security Systems bosch.com	Integral Technologies integraltech.com	ScanSource Inc. scansource.com
Cieffe cieffe.com	Ioimage ioimage.com	Securitas Systems ... securitassystems.com
Cisco Systems cisco.com	Lenel Systems lenel.com	SITA sita.aero/default.htm
Dell Computer dell.com	LongWatch longwatch.com	StarDot Technologies stardot-tech.com
DIVR divrsystems.com	Microsoft microsoft.com	Steelbox Networks Inc. steelbox.com
DSX Access Systems dsxinc.com	Milestone Systems milestonesys.com	Stonefly Networks stonefly.com
EMC Corp. emc.com	Mirapoint mirapoint.com	Tamron tamron.com
Exacq Technologies exacq.com	Mobotix mobotix.com	Tech Data techdata.com
GarrettCom garrettcom.com	Moxa moxa.com	Zebra Technologies zebra.com
GE Security www.gesecurity.com	nCipher ncipher.com	