network centric Security

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

November 2007

Traveler Biometrics is Here!

The TSA integrates smart cards, fingerprints and iris scanners and multiple government servers and databases 14

THE LONDON EYES

The CCTV system that leads the world 20

HOT SPOTS, COOL CAMERAS

Inside Dallas PD's Wireless Video 24

PLUS

The TCO of IP cameras 8

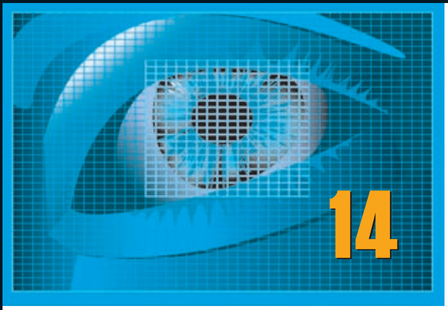
November 2007 Supplement to *Security Products*

network centric Security
WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

Content

NOVEMBER 2007 VOLUME 1 NO. 3

features



departments

Network-Centric Security welcomes vendor information and briefings. To arrange a briefing, please contact our editor-in-chief, **Steven Titch,** via email at **titch@experteditorial.net**. Our agreement to accept or review product material or backgrounders is not a guarantee of publication.

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

The information in this magazine has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been review for accuracy, there is not guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors and/or new developments in the industry.

Politics, Policy and CCTV

by Steven Titch, Editor-in-Chief

During our peer review of "The London Eyes" (page 14), one of the readers asked me to cut certain facts—in particular, the estimated number of surveillance cameras in London—out of fear they would support the case of activists who are fighting the widespread use of video surveillance in the U.K.

It was disconcerting in part because, in my career as an editor with business-to-business magazines, I cannot remember being asked to tone down a report that details the value and potential of an industry in a positive light.

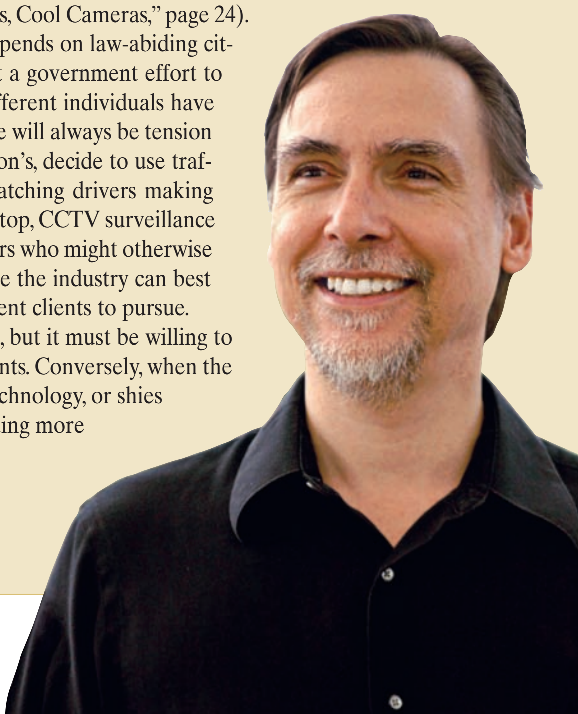
The government use of widespread video surveillance is controversial, both in the U.S. and U.K. But this is the business we're in.

It is not *Network-Centric Security's* role to take on policy issues. Our decision to report on London's CCTV system arose from the number of times I have heard it referred to as a great example of the potential surveillance technology offers. The article by our U.K.-based contributor, John Williamson, addresses how the CCTV system applies IP, analytics, command, control and communications, standards and networking of public and private systems—issues our readers confront when they design and deploy video networks of their own.

The forensic capabilities of London's video technology led to the rapid arrest of the would-be Piccadilly bombers. To be sure, stories like that are exceptional, but what makes the case for video security tough is that day-to-day results are hard to measure. We don't know how many crimes—ranging from car bomb attempts to sidewalk smash-and-grabs—are prevented by a well-placed video camera. The only hints lie in crime statistics, as in Dallas: after the police department installed 15 video cameras in the Deep Ellum area of the city's Central Business District, violent crime dropped 90 percent (See "Hot Spots, Cool Cameras," page 24).

The public's opinion of CCTV surveillance depends on law-abiding citizens feeling comfortable that cameras represent a government effort to protect them from harm, not harass them. As different individuals have different thresholds for security and privacy, there will always be tension in this matter. When city councils, such as Houston's, decide to use traffic cameras to "boost municipal revenues" by catching drivers making right turns on red lights without coming to a full stop, CCTV surveillance indeed stokes backlash from citizens and taxpayers who might otherwise support it. The "common defense" message is one the industry can best promote—and urge their city and state government clients to pursue.

The industry may not win every policy debate, but it must be willing to engage the public with facts and rational arguments. Conversely, when the industry apologizes for the effectiveness of its technology, or shies away from publicizing success stories, it's conceding more than it may intend to CCTV opponents.



Advantage: IP

by Steven Titch

IP-networked CCTV cameras have become more cost-effective than analog in installations requiring as few as 40 cameras, according to a report released in September.

The study, which created a mock request for proposal (RFP) covering a 40-camera installation in a school environment (see box), found that the IP system's total cost of ownership (TCO) came in 3.4 percent lower than an analog-based solution.

The study, funded by Axis Communications, a manufacturer of IP cameras, but conducted independently, attempts to show the overall cost savings and benefits that derive from digital network-centric deployments, despite the fact IP cameras themselves are more expensive per-unit than analog counterparts. The study also underlines the dramatic decline in the cost of IP cameras to the point where many of the benefits that accompany digital video, ranging from plug-and-play components to basic analytics, are within reach of operations that require less than 50 cameras.

> 'TCO for installations above 32 cameras is 5 percent less than analog.'
>
> —Fredrik Nilsson, Axis Communications

"TCO for installations above 32 cameras is 5 percent less than analog," says Fredrik Nilsson, general manager for Axis. "Between 16 and 32 is a wash." For one to six cameras, Nilsson adds, IP is still about 10 percent more.

One exception, however, is that if IP infrastructure—such as pre-installed Category 5 cabling—already exists at the customer location, the cost of an IP system will always be cheaper, the report found.

OFFSETTING CAMERA COSTS

The cost of IP cameras is only part of the equation. While network cameras are 50 percent more expensive than analog cameras, cabling is almost three times as expensive in an analog system (see graph), chiefly because analog cameras require separate cables for power and PTZ control. Furthermore, the total cost of installation, configuration and training is almost 50 percent higher in the analog system.

In addition to measurable cost benefits, Nilsson cites "soft" benefits that increase the value and ultimate return on investment network-based systems offer. These include superior scalability, flexibility in placing and moving cameras (all they need is an Ethernet plug or failing that, a wireless local area network connection) and image quality. IP cameras also can be remotely serviced, and management systems are based on PC servers from firms such as IBM, Sun Microsystems and Hewlett-Packard that usually have superior warranty and service plans compared to DVRs.

Bill Stuntz, vice president and general manager of Cisco System's Physical Security Business Unit, agrees with the TCO equation. "You've got to look at the price of [IP] cameras in terms of the overall system," he says. "While it's true that the price of the camera has been the hold-up, quality and compatibility is where you see them as the better option." Plus, he adds, one off-the-shelf server can support many more digital cameras than can a single DVR, lowering the cost of ownership. "You also stay current through upgrades, versus replacement."

> The trend toward network cameras has given rise to the buzzword 'generic analytics'

ENTRY LEVEL ANALYTICS

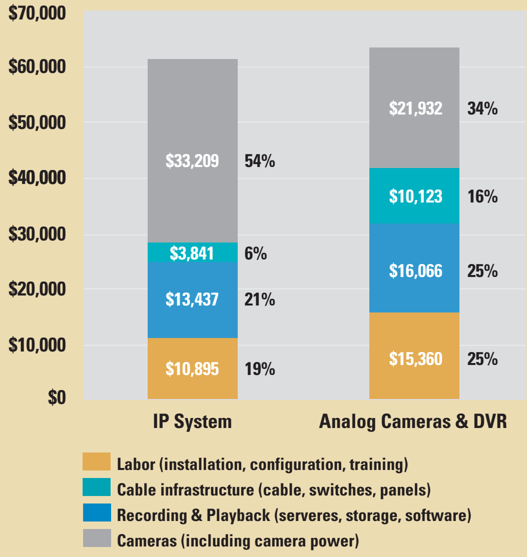
Another key "soft" benefit of network cameras is that they can store and process information like any other IP client, such as a PC or handheld PDA. Combined with the declining cost of ownership in general, the potential of the IP cameras to work as edge network devices has touched off a flurry of "entry level" video analytics that vendors are pricing within reach of smaller users.

The trend gave rise to the buzzword, "generic analytics" on the floor of the 2007 ASIS International Seminar and Exhibits in September, which, in addition to Axis and Cisco, drew comments from companies such as ioimage and IQinvision.

Generic analytics, says Nilsson, is basic low-end functionality. It takes in people counting, "virtual fence" applications and tamper resistance. Axis itself introduced a tamper-resistant feature on its camera line at ASIS designed to alert monitoring systems if a camera's field of view is changed, or if its lens is covered, obstructed, spray-painted or vandalized.

The Model RFP

In Axis Communications' Total Cost of Ownership (TCO) study, a structured research approach was developed that included step-by-step validation of each project phase by non-vendor industry participants including security integrators, value added resellers and industry analysts. Definition of cost components, deployment scenarios and assumptions were developed with, and scrutinized by, these study participants with the objective of making the research approach and study results as fair and unbiased as possible. In addition to interviews, an industry-standardized approach was used to collect cost data, which included development of a mock request for proposal and then soliciting responses or 'project bids' to collect structured cost data. The major components of that RFP, which determined 32 cameras to be the break-even TCO for networked CCTV systems against analog, are listed below. The full report can be found at www.secprodonline.com.



FACILITY

- Single building school
- Existing building

NUMBER OF CAMERAS

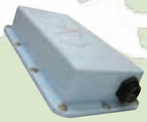
- 30 indoor fixed dome cameras
- 5 outdoor fixed dome cameras
- 5 outdoor PTZ cameras
- All cameras needed to be vandal proof

RECORDING

- 12 hours of recording a day
- 4 fps continuous recording
- 15 fps recording on alarm/video motion detection
- CIF resolution
- Retention of video for 12 days

WIRING

- No existing data, coax or power wiring
- Network switches (wiring closets) and/or multi-camera power supplies
- Plenum airspace above all areas (for cabling, plenum wiring required)
- Category 5e adequate for data wiring
- Power over Ethernet switches can be located in storage area allowing for less than 250 feet PoE cable runs for network cameras
- Coax will have to be a home run from cameras to DVR



AirEther AB54
2.4GHz AP Base Station

AirEther CB54E
2.4Ghz Client Bridge

AirEther BR108
5GHz Backhaul Bridge

AirGoggle NVC210
IP Box Camera

AirGoggle NVC3026
IP Outdoor Speed
Dome Camera

> ‘Price points have to be in line with the problem you're solving.’
>
> —Paul Bodell, IQinvision

"Analytics is still considered complex. People are a bit afraid of it," says Dvir Doron, vice president of marketing at ioimage, which has just introduced the iobox trk1, a single-channel MPEG4 encoder that supports analog and digital cameras, to the U.S. market. "We pre-wrap everything in the encoder and camera and make it easy to install and obtain information."

The trk1 is designed for plug-and-play set-up and operation and is addressable with a standard Web browser. The device provides a wide-area solution that is uniquely accessible to small sites, as well as for supplementing larger installations. Analytics capabilities are largely trip wire and virtual fence functions, says Doron, such as intrusion detection, entry detection and sterile area protection.

"There is a need for a more affordable product to cover the one-channel world, versus four and eight channels," says Doron.

However, Paul Bodell, chief marketing officer for IQinvision, another manufacturer of IP cameras, advises users not to get hung up on price points. Deriding the notion of claims of "30 frames per second, 30 days of storage at $30 a camera," Bodell says the issue is how technology can solve a customer's problem in a cost-effective way. "Price points have to be in line with the problem you're solving," he says. "Expectations need to be in line with real-life parameters."

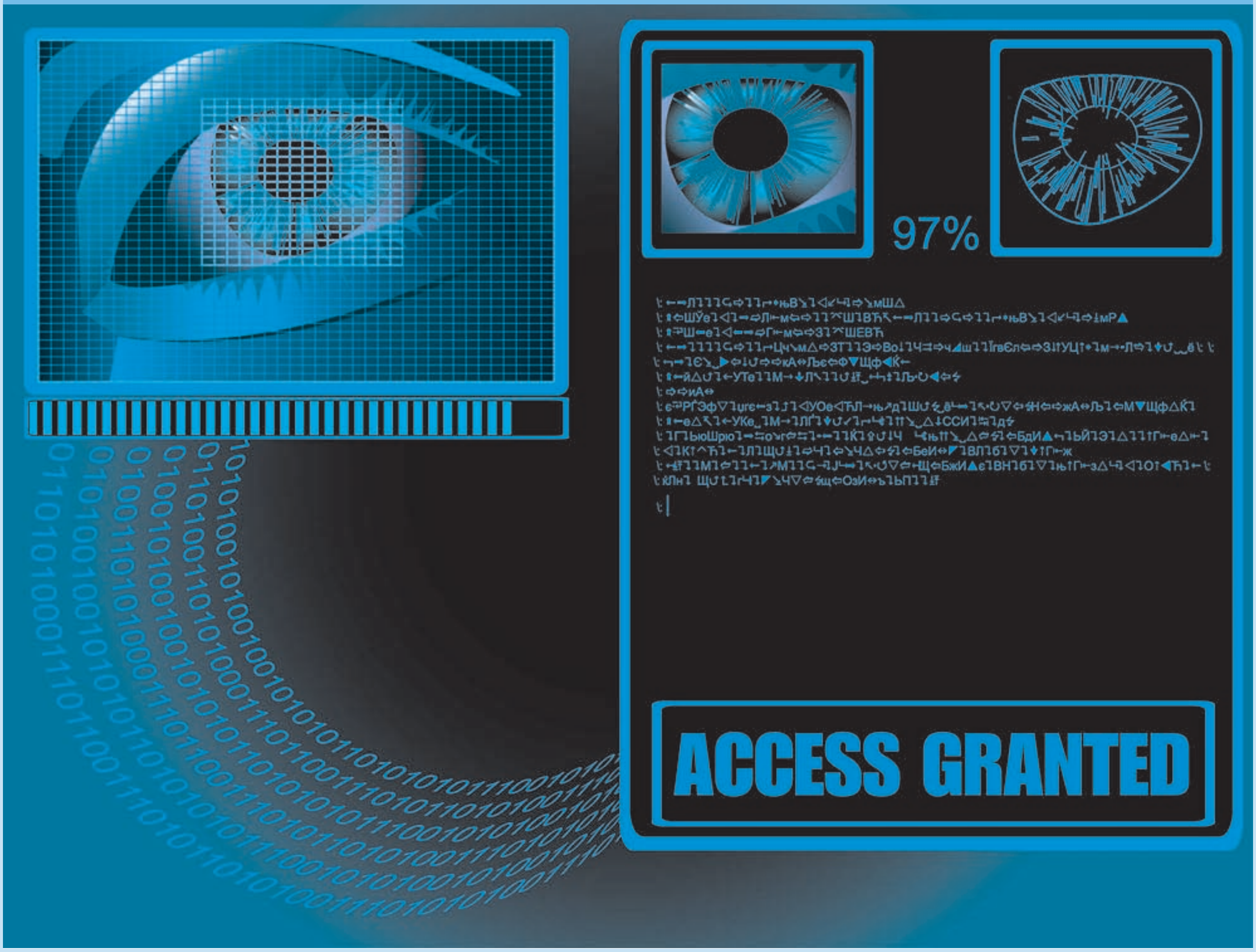
When it comes to analytics, he says, users already expect too much. For purposes of video and analytic processing, Bodell measures resolution in terms of pixels per foot. For general surveillance, including people and vehicle counting, users can get by with 10 to 20 pixels per foot. For forensic detail, such as face and license plate recognition, cameras need to be optimized to 40 megapixels per foot. Casino applications where chip and bill denominations need to be discerned require even finer resolution. Resolution and processing this fine remains expensive.

Axis' Nilsson is quick to agree on managing expectations, but suggests that the perfect not be made the enemy of the good. The quality of video analytics, he says, is largely a function of processing power, which, according to Moore's Law, doubles every 18 months. "Ninety percent is better than nothing," he says when it comes to analytic performance. "For some that's quite good. For others, their requirements might take a few more years."

Traveler Biometrics is ~~Coming~~ Here!

By Frank Barbetta

THE TSA'S REGISTERED TRAVELER PROGRAM, WHICH INTEGRATES FINGERPRINT AND IRIS SCANNING, SMART CARDS AND CARD READERS, AND MULTIPLE GOVERNMENT SERVERS AND DATABASES ON A NATIONWIDE INTEROPERABLE NETWORK, IS READY FOR TAKEOFF.



Since 9/11, transportation officials have been attempting to balance the requirement for heightened airport security with the need to move large volumes of travelers through checkpoints with minimal delays.

Security specialists began discussing a biometric solution, backed by telecommunications networking and information technology, in the months after the attacks. Finally, after several years of trials, combined with declining equipment costs and greater commercialization of the necessary technology, systems that merge sophisticated biometrics with high-speed data networking are positioned to hit the mainstream.

Passengers are starting to see airports and airlines ramp up introduction of the so-called Registered Traveler (RT) program, an air transport marketing initiative conducted in cooperation with the federal Transportation Security Administration (TSA). RT relies on customer willingness to provide personal information, submit to fingerprint and iris scans and pay registration and subscription fees in return for U.S. government-assessed security clearance and the privilege to use TSA-issued smart cards. Registration permits travelers to use a special line for faster check-in. Then, instead of waiting on line for the standard TSA check of ID and boarding pass, RT participants use their smart card at a kiosk that approves their access to secure areas. RT travelers still must have their carry-on bags x-rayed for expedited entry into secure airport areas.

Dating to proof-of-concept demonstrations around 2002 and an Orlando International Airport trial in 2004 and 2005, RT appears to have the benefits and blessings of biometric, telecom and IT standards.

AAAE TAKES CHARGE

Air transport business interests, technology vendors and the TSA initiated the RT program as a result of the U.S. Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act of 2002, which encourages incentives for the development and deployment of "qualified anti-terrorism technologies."

The RT activity is in the hands of private industry under the auspices of the American Association of Airport Executives (AAAE), which created the Registered Traveler Interoperability Consortium (RTIC), a group comprised mainly of scores of airlines and airports, to spearhead the effort. AAAE also formed various bodies or subsidiaries for the following ongoing tasks:

- Write specifications for TSA approval.
- Operate a conformance lab to test the systems and solutions.
- Act as the single source gateway to the TSA.
- Run computer-intensive clearinghouse operations that maintain biometric/ID databases and secure network communications.

SERVICE PROVIDERS SELECTED

The TSA's role is largely administrative. The agency accepts sets of written applications from travelers and looks at specific criteria to clear and certify RT participants. This process includes the selection and use of authorized service providers that act as the prime contractors for RT services among airports and airlines, which the program calls "sponsoring entities."

Right now there are five service providers: FLO Corp. (formerly Saflink), Kirkland, Wash.; Unisys Corp., Reston, Va.; Verant Identification Systems Inc., Rochester, N.Y.; Verified Identity Pass, New York; and Vigilant Solutions, Jacksonville Beach, Fla. They all have handfuls of partners from the computer, software, systems integration and biometrics security industries to implement and deploy RT installations nationwide.

Sponsoring entities themselves must also apply for TSA approval to participate in the RT programs. Virtually all of the more than 400 airports in the U.S. are potential RT locations. As of September, RT services were in place in airports serving Albany, Cincinnati, Indianapolis, Little Rock, Ark.; the New York City area (Kennedy International, Newark Liberty International); Orlando, Reno/Tahoe, Nev., San Francisco and San Jose, Calif. Participating airlines include Air France, British Airways and Virgin Atlantic.

Requests for proposals (RFPs) and awards reportedly are pending in Atlanta, Dallas-Fort Worth, Denver and Washington Dulles, with more anticipated. The pace of RT rollout, and how widespread RT services will become, however, remain major industry questions. The answers may be contingent on public perceptions of biometrics technology, privacy concerns, security importance and willingness to pay, as well as industry attempts to convince sponsors of the RT program's business imperatives and customer service merits.

SUCCESSFUL SO FAR

"The program success and adoption is positive," says Bryan Ichikawa, the Unisys solutions architect heavily involved in the RT program. Unisys is the supplier in Reno, operating an RT service under its RT GO brand name. "People understand and accept what is being done, but how much faster RT progresses is hard to say," he adds. "The notion in the past that biometric security is scary and unknown is being lifted. Behavior is moving more readily toward acceptance."

"The RT program can change the way people think about security," says Jason Slibeck, chief technology officer at Verified Identify Pass, which operates the Clear brand service for RT installations and counts General Electric and Lock-

> 'There are a lot of things within RT that can really pave the way for biometrics'
>
> —Jason Slibeck, CTO, Verified Identify Pass

Conor White

heed Martin among its investors and vendor partners. "It is a huge, unique biometric program based on standards, with wide public exposure and availability. There are a lot of things within RT that can really pave the way for biometrics. The only expansion challenge is that airports and airlines have to agree to do it."

Airports with pending RFPs could move relatively rapidly, according to Conor White, chief technology officer of Daon, whose ID assurance software has been used with the Clear service in Orlando since 2005. "We can surely see a sharp uptake later this year or early next year," he says. "And I'm not really aware of any technical issue preventing RT's adoption at any airport in the U.S."

User acceptance, which will drive RT's progress, is growing, according to Tim Myerhoff, North American program director at LG's Iris Technology Division, which has worked on providing its iris scan know-how with AAAE, Unisys, Verified, Flo Corp., Daon and Motorola. "RT is in a roll-out mode now nationwide and will be available to a lot more airports very soon," he maintains. "But it may take a while for it to reach its full scale and breadth."

Andrew O. Omidvar, senior director of business development for Motorola's Federal Markets Division, is enthusiastic about future RT deployment, but counsels patience because the initial pace of rollout may be a bit slower than expected. Motorola's contribution to the RT program—a backend biometric system at the AAAE's Transportation Security Clearinghouse—comes from its Biometrics Business Unit, part of the manufacturer's Public Safety and Government sector. Motorola worked with sponsors for about two years before the formal March 2007 system cutover.

SEEKING TRAVELER BUY-IN

"There are 433 airports in the United States. Maybe not every one is a candidate for RT, but at least the primary ones are," Omidvar says. "One of the motives behind RT is to shorten the lines and cut the security waiting time for frequent flyers. RT is handled by the airports and airlines, and they have to convince their customers. This is more of a challenge than just putting in the backend systems.

"Once more RT systems are deployed in more major airports and they begin to permeate the environment, people will see the service benefits," he says. "They also can spread information about RT by word-of-mouth, and then we will see a major difference in deployments."

Meanwhile, like others in the industry, Omidvar maintains that as currently envisioned, RT faces no major technical issues or challenges because biometrics, smart card, computer and networking interoperability and compatibility matters were addressed early on in the RT design, specification and agreement process.

Registered Traveler: How It Works

Registered Traveler's customer process flow starts with service providers and sponsors collecting biometric fingerprint, iris data and other personal information at airports and other designated locations, such as hotels and resorts, or at third party biometrics companies. Iris scans are an optional passenger choice, but vendors must support the technology.

The data goes to the Transportation Security Administration (TSA) for a background check as part of enrollment. Potential RT passengers also are given account numbers that are validated and verified by both the TSA and the AAAE's Transportation Security Clearinghouse, which also uploads data to kiosks at participating airports. The whole data package moves from the AAAE's Security Biometric Clearing Network (SBCN) back to TSA for background security decisions.

TSA's security assessment involves dipping into terrorist, law enforcement, immigration and other government databases to confirm the lawful status of travelers who are citizens, resident aliens and other foreign nationals in the U.S. A TSA clearance results in the five current RT service providers, or their partners, producing smart cards that are sent to customers.

Each time an RT customer swipes a card at an airport kiosk, card information is checked against that day's hot list. The hot list is generated daily by the SBCN, and is always downloaded to kiosks. As an added security measure to prevent hacking or database doctoring, kiosks are not built to upload information.

Customers also opt in favor of primary and secondary ID methods from fingerprints or iris scan criteria or both. Computerized facial recognition isn't yet part of the biometric mix, although facial photographs are stored on the smart cards for optional manual viewing by airport security personnel.

Experts say that while facial recognition technology has been improving dramatically in the last two or three years and standards bodies are doing important benchmarking work, there remain challenges in achieving high accuracy rates. Other adverse factors are expensive cameras and the need for controlled lighting conditions.

No further RT program automation along the various airport security checkpoints in the special RT lanes is envisioned by the industry or approved by the TSA. Future additions to automation aren't entirely ruled out, however. Vendors are testing explosives-sniffing technology for body/clothing scans and are said to be capable of performing so-called shoe scanning, which looks for metal differentiation in footwear so as to end the annoying shoe removal hassle at security checkpoints.

The AAAE and the TSA were able to draw on standards bodies, including the International Standards Organization (ISO), the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST). Omidvar was previously manager for homeland security in the NIST's Advanced Technology Program.

"There have been no major problems; the only operational issue is power outage matters," says Ichikawa of Unisys. "And there shouldn't be any incompatibility challenges. RT was fully designed and tested, confirmed and certified first regarding such interfaces."

RT data, for instance, must be shared among all five service providers, no matter which airline or airport are designated sponsors. "Cards must be interoperable at other airports," Myerhoff of LG points out. "So enrollment and the cards are good elsewhere. This interoperability was required."

As part of the total reliability solution, seamless communications and secure networking are definitely necessary. TSA and the AAAE's Security Biometric Clearing Network (SBCN) maintain constantly updated lists of RT passenger information-including revocations-and these are uploaded one or more times daily to on-site SP systems and kiosks where flyers start their on-site access/entry routines.

DIVERSE INFRASTRUCTURE

According to Verified's Slibeck, the typical RT infrastructure for transport includes encrypted messages, passcodes, security certificates, XML schema, virtual private networks (VPNs), Internet Protocol (IP) packets, mobile kiosks, broadband cellular and telephone company digital subscriber line (DSL) loops. And there's a lot of network and resource technology for security, including public key infrastructure (PKI) coding for smart cards and all primary local authentication, according to LG's Myerhoff.

"Kiosks won't work if they go for more than 24 hours without updates," adds Ichikawa of Unisys. "If the hot list has negatives—meaning cards that are revoked for whatever reason—the cards and biometric ID won't pass through." Most revocations are attributed to cancelled RT accounts and not security clearance losses, according to TSA and AAAE.

Depending on the configuration, local, regional and wide area networks all can come into play in implementing the RT program. According to Daon's White, good communications among the kiosks, computer systems, databases and all the participating government and business entities was a "core guarantee" among the multiple service providers. Communications then is considered a critical function, piggybacking on well-established protocols and standards, he says.

In fact, White also explains that service providers are bound by service level agreements on networking uptime, kiosk uploads and the integrity of biometrics, enrollment and personal data and other RT information traversing the VPNs.

"Interoperability was agreed to by the prime providers in order to expand the service in contrast with proprietary solutions," Slibeck of Verified points out. "Interoperability guidelines were a huge undertaking and a big step. Different providers at different airports must accommodate all RT passengers like an automatic teller machine. We can't minimize the amount of work and cooperation needed to make it all happen. We all decided to establish such an open program and help the market grow."

By all industry accounts, the RT program is on the verge of a full-scale commercial rollout, although it is still officially designated as a "pilot" under TSA nomenclature. This is because the TSA's $28 fee—paid by passengers for the pre-enrollment background check—requires the agency to conduct a formal notice of proposed rulemaking (NPRM), a regulatory process with rounds of comments and replies. RT-registered passengers also pay separate fees for the service to their respective primary service providers. Clear's fees, for instance, are $99.95, $199.90 and $299.85 for one, two and three year periods, respectively.

ALL STANDARDS ISSUED

Even though no NPRM has begun and no date has been set for its start, the RT project has broad status under its "pilot" designation. Service providers, airports and airlines may go forward with the program, according to Amy Kudwa, media relations officer for the TSA at the U.S. Department of Homeland Security. "TSA has issued all the technical standards at this point. All it needs are the applications from the service providers and sponsoring entities, and those are being turned around quickly," she adds. "The pace is being driven by private industry."

Kudwa indicates that no more Capitol Hill codification is necessary, although late July hearings at the House of Representatives' Homeland Security Committee were held to track RT progress. There were differing opinions among politicians, U.S. bureaucratic officials and industry executives about the pace of the RT program's progress. Yet it was clear from testimony that the TSA regards the RT program more as a business marketing/customer service concept than as a counter-terrorist, security/air safety measure.

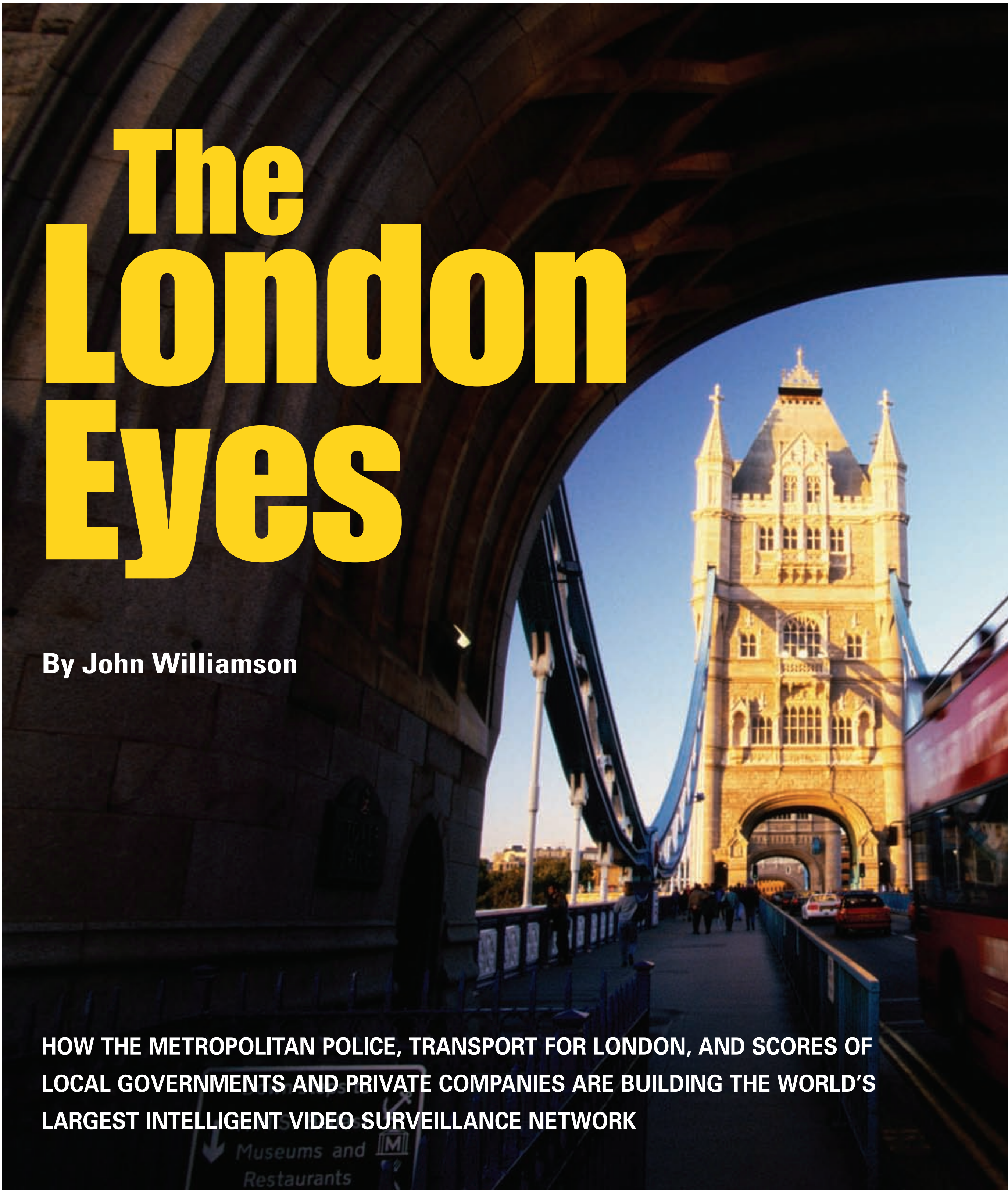
Nevertheless, the industry viewpoint is that RT adds another security layer to the air safety process. RT doesn't eliminate existing security measures, including security personnel and luggage, clothing and body scans. In addition, the industry ostensibly is buoyed by RT's current green light as well as future biometrics security prospects.

LG's Myerhoff sees the U.S. RT program producing renewed interest in biometrics security on both the domestic and international levels. And Motorola's Omidvar, among many others, agrees: "No other country has what the U.S. has with the RT program. It can become a model for the European Union members and other major countries of the world."

The industry thinks RT can help the biometric market in general because it can complement public knowledge and acceptance regarding the likes of iris and fingerprint scanning as long as privacy issues are addressed. "I would say yes, biometrics in general can get more acceptance," Omidvar says.

Daon's White also sums up RT's potential positive impact on the biometrics market : "For RT, we solved the interoperability challenge and the federation challenge [multiple service providers] and there are a lot of adopted systems, so biometrics can be viewed as an enabler elsewhere."

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



The London Eyes

By John Williamson

HOW THE METROPOLITAN POLICE, TRANSPORT FOR LONDON, AND SCORES OF LOCAL GOVERNMENTS AND PRIVATE COMPANIES ARE BUILDING THE WORLD'S LARGEST INTELLIGENT VIDEO SURVEILLANCE NETWORK

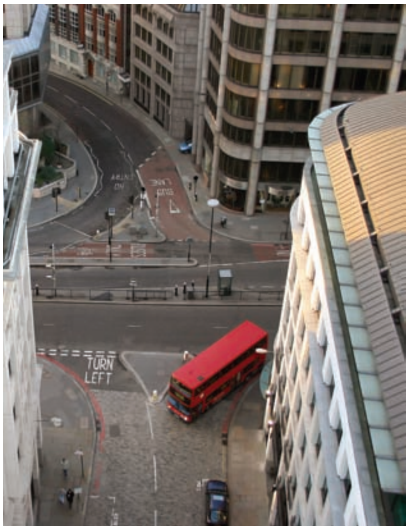
The United Kingdom has become CCTV nation. Conservative estimates place about 10 percent of the world's CCTV cameras in the U.K. The consensus is that the U.K. has more cameras per capita than any other country.

Another widely quoted statistic is that U.K. city residents are captured on camera up to 300 times per day on average. Penny Hayward, spokesperson for the CameraWatch CCTV industry advisory body, says nobody is quite sure of the real tally because nobody has actually counted all the installations. In fact, reckons Pierre Hagendorf, chief technology officer of unified visual communications specialist Radvision, there may be as many as 5 million CCTV cameras in the country, or one for every 12 residents. Other observers put the total even higher than that.

The U.K.'s world leadership in deployment of surveillance systems puts London high in the running for global capital of the video surveillance business. The city's networks are operated by the Metropolitan Police Service (MPS), the Transport for London (TfL) authority, the Department of Transport and local government councils. This is in addition to many thousands of private CCTV set-ups operated by schools, sports stadiums, parking lot owners, shops and banks.

What's certainly not in doubt is the fact that the UK's capital city itself literally bristles with CCTV. Events ranging from the dramatic—such as the U.K.'s largest cash robbery in London's commuter belt in 2006 and the failed nightclub bomb attacks this year in the city's West End—to the more workaday—such as the on-going enforcement of the city's congestion charging scheme and the monitoring of bus traffic lane regulation—are all captured on video cameras operated by, and sometimes shared between, a growing number of different operators.

The MPS surveillance network is a major element of London's CCTV capability. This system is said to manage some 30,000 camera feeds, although the MPS did not respond to interview requests regarding this story. As well as the MPS's own surveillance points, the capital's police force has had access for some years to the CCTV systems set up by local government authorities and the TfL organization, which monitors road traffic, buses and trains, stations and transportation hubs. Until quite recently the local authorities would provide video footage when the MPS requested it to help with information about previous incidents. However, with improved technology, the MPS is now able to work more closely with each local authority to share live images in real time and communicate with officers on or near the scene.



MPS OVERHAULS C3I

The large-scale integration of the city's various video surveillance networks is a key component of a larger MPS initiative to overhaul its command, control, communications and information management (C3i) systems. The entire program involves several different projects and includes the integration of 32 borough control rooms into a Central Communications Command (CCC) housed in three purpose-built special operations centers in the city.

In August 2006, Tyco Fire & Integrated Solutions–Traffic & Transportation won a multi-million dollar order to supply the MPS CCC with what was then thought to be the world's largest video monitoring and control system for public safety and security. Although Tyco declined to address specifics, its system is believed to include a custom video matrix with in excess of a quarter of a million crosspoints acting as a virtual switching matrix, and uses the TV Network Protocol (TVNP) to communicate between switching nodes. TVNP, according to Tyco, will enable further integration of borough and stadium CCTV systems with virtually unlimited expansion in the future.

"The C3i system allows all the cameras that are connected to the system to be viewed and controlled from the Met Police control centers, so in effect they are completely interworked," observes Neal Entwistle, marketing director of Tyco Fire & Integrated Solutions - Traffic & Transportation. "The significance of TVNP is that it is an open protocol standard that allows many disparate systems to work together and is the backbone of how the systems are connected in London for the C3i project."

Two of the three CCC operations centers are up and running, with the third due to go live before the end of the year. Lambeth, one of the two sites already in operation, according to Shushmul Maheshwari, CEO of RNCOS, a market research company, will eventually handle more than 500 public events each year in the capital. RNCOS has published several studies of the CCTV industry, the most recent being "Global CCTV Market Analysis (2007-2010)."

Despite Entwistle's description, others are not so quick to declare TVNP is an open standard in the true sense of the term. "The jury is still out," says Barry Keepence, chief technology officer of IndigoVision, Edinburgh, Scotland, which makes end-to-end IP video and alarm management security solutions for CCTV surveillance applications. "TVNP is not widely deployed." Neither has it been certified by any standards body, Keepence adds, and IndigoVision has installed a number of large surveillance systems that don't use it.

WHAT'S IN STORE?

The government's July decision to exempt TfL and the MPS from certain provisions of the U.K.'s Data Protection Act 1998 sparked the increased collaboration between the MPS and other video network operators. The government decision permitted the bulk transfer of automatic number plate recognition (ANPR) data—used to police London's congestion charging system—from TfL to the MPS. In a statement to Parliament, Tony McNulty, Minister of State, Home Department, said: "The MPS requires bulk ANPR data from TfL's camera network in London specifically for terrorism intelligence purposes and to prevent and investigate such offenses. The infrastructure will allow the real-time flow of data between TfL and the MPS."

The announcement of the MPS ANPR deal caused something of a stir with unconfirmed reports that the MPS was looking to store ANPR traffic data for five years, and that managing and storing what would be the multiple exabytes of data captured in that period could cost as much as $3.5 billion.

Regardless of what happens with the ANPR material, data storage could become more of a concern for everyone in the U.K. CCTV industry as the switchover from analog to Internet Protocol (IP) and megapixel cameras gathers pace, says Chris Williams, marketing director of Wavelet Technology. He calculates that whereas a conventional analog CCTV image might have a file size of 50 kilobytes (KB), a 5 megapixel camera file could go to between 250 and 400 KB.

Given the advantages that the newer technologies can bring to CCTV data analysis, Williams suggests that image compression or recording at a lower image rate might bring only limited relief. "Megapixel cameras are going to enhance the ability to do more forensic work," he contends. "I don't think the file sizes are going to get smaller because you need the detail, and the detail implies a larger file size."

In parallel with pressure on file size and storage, as more U.K. video surveillance systems become networked and distributed, despite the bandwidth efficiencies of IP transmission bandwidth may become more of an issue for users, especially those who rely on leased lines or other carrier arrangements. Asked what he considers to be the challenges attached to managing, switching and monitoring a CCTV system with thousands of feeds, Hagendorf responds: "Bandwidth. Bandwidth. Bandwidth."

The fact that the IP video industry as yet lacks a comprehensive body of standards has implications for bandwidth. For sure there is widespread use of the MPEG4 standard, but as Keepence of IndigoVision notes, "MPEG4 standardized the decoder. How good an encoder is... is left up to the manufacturer. How good the compression is depends on the implementation of the encoder." As a consequence, claims Keepence, the data rate for some CCTV solutions to give good quality video can be in the range of 2 to 10 megabits per second, while those from IndigoVision cut in at around 1 Mb/s.

A further consequence of this lack of robust standardization is that it's not simple to mix and match different CCTV components from different vendors. "Although standards such as MPEG4 exist, there are differing interpretations of these and it is not generally possible to, say, use one manufacturer's IP encoder and then decode the stream with another manufacturer's device," points out Tyco's Entwistle.

But Keepence advises not to blame interoperability problems on poor standards definitions. Using cable TV set-top boxes as an analogy, he points out that MPEG2 signals used in the cable connection will work with any manufacturer's cable box. The set-top remote control, however, will not work with another manufacturer's cable box. That it doesn't has nothing to with the MPEG2 standard, he says.

> With improved technology, the MPS is now able to work more closely with each local authority to share live images in real time

And here it's maybe also worth noting there's some residual reluctance to make a full commitment to IP video systems due to perceptions about their possible vulnerability. "There is, however, still a resistance in the U.K. for major infrastructure projects to switch to pure IP surveillance because of the perceived security risks associated with doing so," acknowledges Steve Gorski, managing director, Axis Communications (U.K.) Limited. "As such the networking of surveillance systems still involves Axis and its channel partners in a great deal of education as to the benefits of network video and the real business continuity and risk management-linked benefits offered through centralised monitoring, management and storage of video output."

ANALYZE THIS

Depending on the chosen architecture, network bandwidth may also be a concern for those operators introducing video analytics, a technology where, in Maheshwari's judgment, the U.K. is at the vanguard. At present most video analytics system deployments in the U.K.—and in many other locations too for that matter—are still in the trial stage. One such pilot is currently running at London's Clapham Junction station, by some measures the busiest rail station in the country. The primary goal of this trial, which uses a system supplied by Agent Video Intelligence Inc. (Agent Vi), Ft. Myers, Fla., is to gauge the effectiveness of video analytics in graffiti detection.

In general video analytics uses image processing algorithms and other technologies to automatically detect and alert operators to out-of-the-ordinary events and occurrences. According to Agent Vi's founder Gadi Talmon, video analytics started out with a firm security focus, but down the road is finding applications in traffic management, retail, and education, as well as graffiti detection. There's even the prospect of boosting revenue in using analytics in retailing, for example, to automatically track and count customers and identify 'hot' and 'cold' spots in a store. "What is the effectiveness of promotion and so on," comments Talmon. "This is very valuable information."

Unlike some other video analytics solutions that do their processing in one location—either in the field or on a server—Agent Vi systems use a distributed architecture called Image Processing over IP (IPoIP). This has a "lightweight" agent algorithm in the field and the major algorithm on the central server. The company claims several advantages for this arrangement: the server is highly scalable, there are bandwidth efficiencies because only the results of the field analysis are transmitted back to the server, and the agent can be readily embedded into a variety of existing video devices. Talmon predicts that scalability will become key in video analytics systems, and that more and more IP cameras will be supplied with analytics pre-installed.

There are those who believe that the hoopla surrounding video analytics is somewhat overdone. While accepting that the technology, if properly deployed and configured, can be a very useful tool, IndigoVision's Keepence suggests: "Analytics is one of the most over-hyped and over-promised and under-deployed technologies in the whole CCTV industry."

Nevertheless the U.K. Home Office's Scientific Development Branch is currently engaged in a major effort with industry to standardize what it terms Video Based Detection Systems (VBDSs). Dubbed the Imagery Library for Intelligent Detection Systems, or i-LIDS, this effort is the government's benchmark for VBDSs and consists of a video test library of CCTV footage designed to evaluate systems for government use. Manufacturers meeting the highest level of performance classification will be entitled to use the trademarked i-LIDS logo in their trade literature. The initial 2007-2008 i-LIDS evaluation schedule is focusing on four monitoring and detection scenarios: Sterile Zone (June 2007), Abandoned Baggage (September 2007), Parked Vehicle (November 2007) and Doorway Surveillance (February 2008).

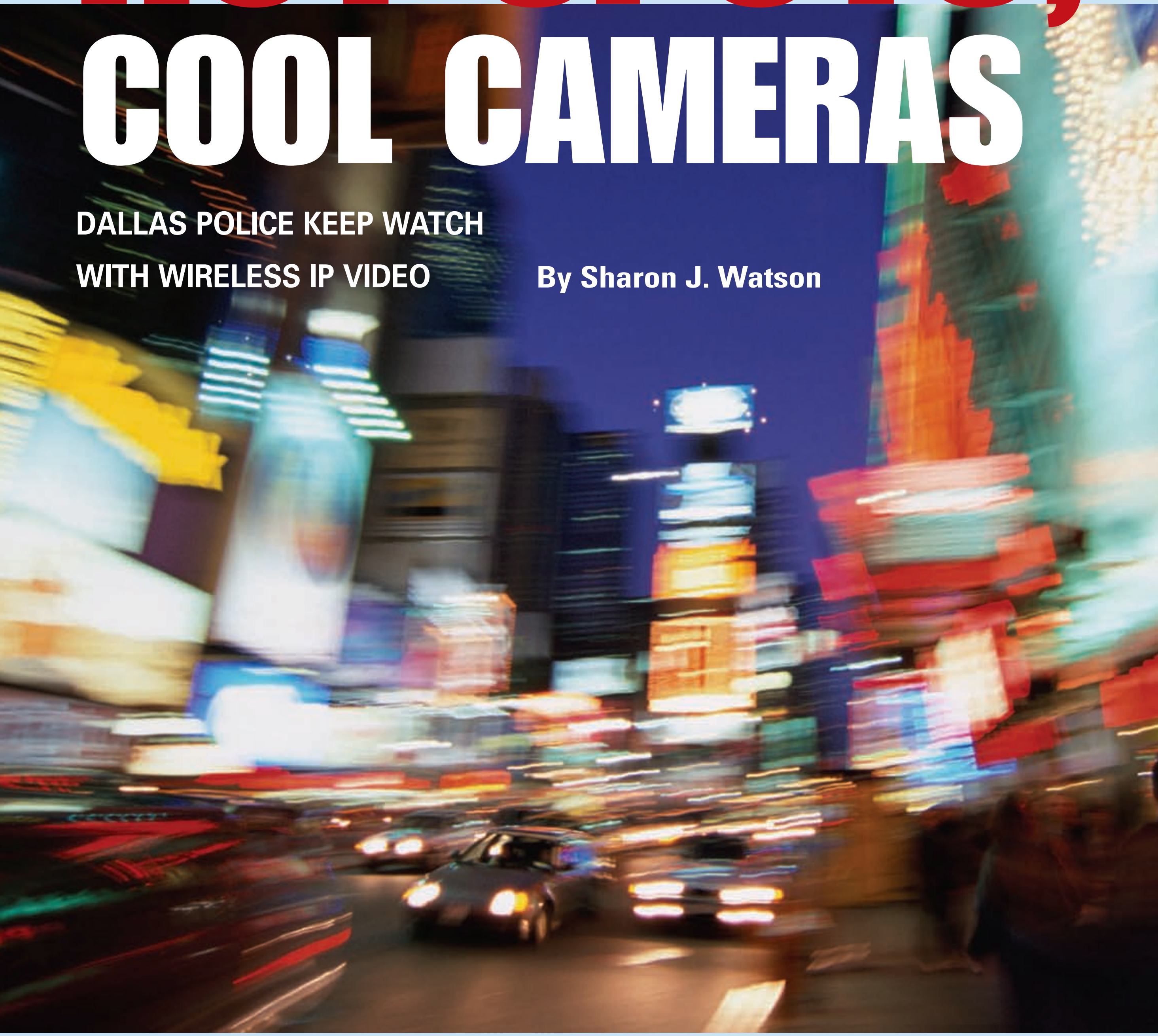
As they say, watch this space.

John Williamson *is a journalist based in Chelmsford, U.K. He can be reached at john.williamson20@btopenworld.com.*

HOT SPOTS, COOL CAMERAS

DALLAS POLICE KEEP WATCH WITH WIRELESS IP VIDEO

By Sharon J. Watson



For the young and hip looking for cool nightspots as well as for families filling a weekend with festivals and fun, downtown Dallas is a popular destination. Once relatively deserted at night, the 1.3 square mile area known as the Central Business District is booming.

Its residential population is growing, along with its amenities, including grocery and drug stores, and nightclubs, restaurants, bars and hotels. The area also hosts more than 200 special events and conventions each year.

The increasing popularity of the Central Business District has raised challenges for the Dallas Police Department. In a presentation it made to the Dallas City Council in February 2006, the department noted that while daytime and evening crime rates had dropped in the business district, the district's late night shift had experienced a 26 percent increase.

With about 3,000 officers patrolling 385 square miles of city, the department wanted an effective solution to the rising crime that drew lightly on human resources. For that, the Dallas police turned to video surveillance. Today, 40 IP-based cameras are trained on the trendy downtown districts of The Core, The Cedars and Deep Ellum, connected by a wireless network that transmits images to officers at Jack Evans Police Headquarters and City Hall.

Similar wireless surveillance networks are being used by other police forces, cities, and schools and universities, with users citing the advantages of relatively easy installation, high quality digital video and the "force multiplier" of permitting fewer security or police personnel to be more effective. Further, being IP-based, the systems are scalable and flexible—conceivably, video can be transmitted to squad cars and handheld devices.

"This application will be a fast-rising, compelling technology," says Kent Huffman, chief marketing officer for BearCom Inc., the Dallas-based integrator who designed and implemented a video surveillance network for the Dallas PD.

A CASE FOR VIDEO

Video network surveillance tests convinced the Dallas police that video would effectively address the Central Business District late-night crime issues. From December 2004 to March 2005, the department deployed 15 cameras in the Deep Ellum area of the District near three nightspots. The results: a 90 percent reduction in violent crimes; a 48 percent reduction in non-violent crimes; a 38 percent reduction in vehicle-related crimes; and a 53 percent reduction in calls for service, according to the department's February 2006 presentation to the Dallas City Council's Public Safety Committee.

Further, the department made 55 responses to suspicious activity based on the camera monitoring and a total of 12 custodial arrests "as a direct result" of the video monitoring.

With about 3,000 officers patrolling 385 square miles of city, the department wanted an effective solution to the rising crime that drew lightly on human resources

While proving video could be an effective crime-fighting tool, the department also developed some specifications for the video network it wanted to use more widely. These included being able to follow suspects with the cameras, being able to read license plates at 300 yards and getting different views from a camera quickly.

In addition, it was unlikely that the city's existing wired infrastructure would be able to handle the traffic loads created by streaming video 24 hours a day, seven days a week.

NETWORK IN THE AIR

After evaluating six bids, the Dallas Police selected BearCom and its wireless solution, which integrates Sony Model 550 cameras; wireless network nodes from Firetide Inc., Los Gatos, Calif; wireless links from BridgeWave, Santa Clara, Calif.; and video management software from OnNet Surveillance Systems Inc. (OnSSI), Suffern, N.Y.

The Dallas Police Department had not specified a wireless network, but the economics of one proved convincing. By Huffman's calculations, a wireless solution cuts about 80 percent of surveillance network implementation costs by eliminating the need to dig up city streets to lay cable. "Our best estimate is that a wired network would be four times the cost of wireless," he says.

Installation began in November 2006 and was completed the following month. The system was trialed in January this year and has been live since.

A wireless camera node in the Dallas Central Business District

Thirty-one IP-based PTZ cameras as well as nine fixed cameras were installed on building exteriors, traffic signals and light poles. The Dallas police based site selections on pedestrian, business and traffic density as well as on "major flash points for activity" it had identified in the Central Business District, according to the department's city council presentation.

Using the secure 4.9 GHz band reserved for public safety, the cameras transmit images to 32 Firetide HotPort wireless mesh nodes that comprise six main wireless mesh sectors, says Mike Butler, install project manager at BearCom. Each sector is scaled for a maximum of ten cameras, ensuring there are no bottlenecks, he says.

Transmissions over the 4.9 GHz band ensure the video doesn't interfere with signals from consumer wireless services like WiFi. In addition, Butler notes that the physical layout of the area being surveyed permits re-use of frequencies.

The wireless mesh sectors are self-regulating as well as self-healing: if a node reached capacity or failed, it would automatically direct its traffic to another node without using a switch to do so.

Using line-of-sight connections, high-capacity BridgeWave 60 GHz point-to-point gigabit and 100 megabit per second (Mb/s) wireless links aggregate the video traffic from all sectors and backhaul it to the monitoring stations at police headquarters and City Hall, where the city's 911 center is located.

Bumping up traffic bound for City Hall and police headquarters to 60 GHz saves more of the 4.9GHz frequency for city's emergency services. That was a feature the Dallas Police especially liked, says Butler—once they understood it.

"They hadn't heard of gigahertz backhauling and thought we'd made an error," he says. But once the department understood how much bandwidth the 60 GHz wireless link would save on the emergency frequency, they were sold, say Butler and Huffman.

"We have 1.2 gigabits per second (Gb/s) going through the air," says Butler.

ON THE WATCH

The BridgeWave links route the aggregated video to a fiber switch that connects to two video servers. The OnSSI workstations retrieve and display video from these servers.

Officers control the cameras from the workstations, using a joystick to change angles and views. Video monitors offer thumbnail views from the cameras, which capture images at 15 to 25 fps, with a camera's specific frame rate generally determined by its location.

BearCom selected OnSSI's software because it is scalable, designed for a large number of cameras and for its NetGuard feature, says Butler. NetGuard presents video from multiple servers in multigrid view sets, allows users to remotely access camera controls and centrally manages user profiles.

In addition, OnSSI "does a really good job of record-on-motion," says Butler. The company's software is rules-based. It can immediately display live video from any camera capturing an event that police users can predefine, such as when an individual walks into a camera's field of view. In effect, the software monitors the video along with the officers.

> By Huffman's calculations, a wireless solution cuts about 80 percent of surveillance network implementation costs by eliminating the need to dig up city streets

When an incident or suspicious activity is identified, the monitoring officer can display it on a bank of three 62-inch monitors BearCom installed within the city's 911 dispatch center, ensuring prompt relays of information to patrol officers in squad cars and on bicycles.

Video images are stored in Dell PowerVault 2.1-terabyte (TB) storage devices using redundant arrays of independent disks (RAID), with one PowerVault directly attached to each server. Images can be held for two weeks to a month.

"OnSSI has really excellent search-based-on-motion features," says Butler. "You can find and archive what you need to keep to DVD."

A VIEW OF THE FUTURE

Secure image storage was one of the selling points the Dallas Police Department used in presenting the video project to the Dallas City Council as well as the public. The department also emphasized to the council and to the public that the cameras would be crime deterrents, not the eyes of Big Brother.

Each camera is clearly marked as belonging to the Dallas Police. Further, signs inform the public that they are in an area being surveyed by video. "The Dallas Police were very upfront with the local media, citizens and businesses about the network, making sure they saw it as a good thing and a way to prevent crime," says Huffman.

The Dallas Police Department paid for the Central Business District video network with an $840,000 grant from the Meadows Foundation, a group devoting to improving the quality of life in Texas. If additional funds are secured to expand the video network, the vendors involved say it should be relatively easy to do so. Wireless nodes can be installed quickly because there's no cabling involved. More IP-based nodes and cameras can be brought online in plug-and-play fashion.

However, cameras still require a nearby power source, which can be challenging, says Butler.

The current network also could be linked to county and federal law enforcement agencies with a downtown presence, as well as to existing external city building cameras and even private business camera systems, according to the Dallas Police Department's 2006 City Council presentation.

In mid-September, the neighborhood of Jubilee Park, which is just east of the Central Business District, installed seven wireless PTZ surveillance cameras at key intersections. The Dallas Police also monitor these cameras with the OnSSI software. Private donations paid the $250,000 cost of the Jubilee Park network.

Huffman says the city's long-term plans may include putting video monitors inside patrol cars within the area covered by the video network. Each patrol car would have an "indoor" wireless node in its trunk so it could receive video transmissions, enabling officers to see video of the suspects and incidents they are responding to.

"That would be a great tool for officers on the street," says Huffman.

Since installing the camera network, violent crime is down 31 percent in the Central Business District, according to Dallas Police Deputy Chief Vincent Golbeck, Central Patrol Division. However, he said, via email, that the department's goal is to better use the surveillance technology to arrest suspects in the act.

"We want to insure that the video operators have the necessary training in place to recognize illegal behavior," Golbeck said, noting that such training is under way. Operators must recognize signs of gang activity and open air drug sales, and be skilled at conducting counter-surveillance- and promptly calling on patrol officers to take action, he said.

"We should see an increase in the number of requests made by video operators to patrol," said Golbeck.

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

Applications, Strategies, & Solutions

1 Petards Wireless IP Camera

Petards Vision Ltd. has added a new integrated outdoor unit to its line of Swift wireless mobile cameras. Weighing 12 lbs., the Swift Solo can be deployed as a single camera system or a multi-camera system, with a maximum of 13 Swift units transmitting at the same time in the same area.

Simple plug and play operation enables the Solo to be deployed within minutes, which makes it ideal for gaining camera coverage in rapidly changing environments. The system is compatible with existing control systems and recording equipment used by CCTV monitoring stations. Transmission range can be configured for a range of up to 2.5 miles using an array of unlicensed transmission frequencies. Increased range is possible using licensed police and public safety frequencies.

www.petards.com

2 Bosch Control Panel

Bosch Security Systems Inc. has added support for Inovonic Corp.'s latest commercial wireless platform—Echostream—to its G Series control panels.

The Echostream platform uses 900 MHz spread spectrum technology to provide superior range and reliability for wireless peripherals. Inovonics' range of universal transmitters, intrusion detectors, smoke detectors, emergency pendants and repeaters for the Echostream platform can be seamlessly integrated with G Series control panels—the D7212GV2, D7412GV2 and D9412GV2—using the Bosch D8125INV interface modules. The modules will provide up to 238 wireless points per Bosch G series panel.

www.bosch.com

3 Lantronix Device Server

Lantronix Inc. has introduced a USB-to-Ethernet device server supporting the USB isochronous data transfer standard typically used for audio and video applications.

The UBox® 2100 lets users can put virtually any off-the-shelf USB 2.0 peripheral device—web cams, speakers, microphones, sensors, security access equipment, multi-function printers, hard drives and scanners—on an Ethernet network or Internet virtual private network, removing all distance limitations.

Support for isochronous data transfer lets users access and share fully synchronized audio/video web cams in real-time over an IP network without needing to connect them directly to a computer.

www.lantronix.com

4 ATV Bullet Camera

Advanced Technology Video Inc. (ATV) has unveiled a day/night bullet-style camera incorporating a high resolution color charged-coupled device (CCD) with aspheric auto-iris lens into a 2.5-inch by 5.71-inch weather-resistant housing with sunshield.

ATV's SDN650PS camera, incorporating a Sony HQ1 chipset, uses 18 infrared LEDs projecting IR illumination into the camera's field-of-view for night time visibility. Additional features include a top, bottom, rear-style swivel mount bracket and a 12v DC power supply.

www.atvideo.com

5 IndigoVision Wins Bangkok Deal

IndigoVision is providing its technology as a backbone for an integrated traffic monitoring system for Bangkok's outer ring road network. Existing toll plaza CCTV surveillance systems located across 45 miles of the ring road have been integrated into a new central control room. Staff in the control room can now view high-quality video from inside and outside of the four toll plaza complexes, providing central monitoring for traffic management and staff safety.

Analog video feeds from the 64 existing dome and fixed cameras are connected to IndigoVision's model 8000 transmitter/receiver modules locally at each toll plaza. The 8000 modules convert the analog camera signal to DVD quality, high-resolution digital video for transmission over the newly installed gigabit Ethernet local area network. IndigoVision's MPEG4 compression technology ensures that the control staff receives CCTV images that are indistinguishable from analog while minimizing bandwidth on the LAN. Additional modules are installed in the control room to convert selected camera feeds back to analog for display on one of the 16 wall-mounted monitors. The system was supplied by Industronics and its Thai partners, Smart Traffic Co. Ltd.

www.indigovision.com

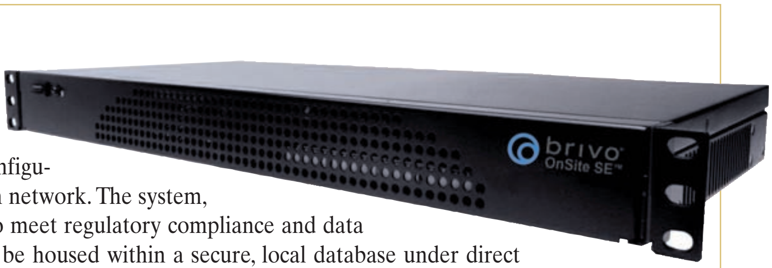
6 Integral Technologies Database Engine

Integral Technologies Inc. has released an event and alarm management database engine that merges video data with intelligence captured by cash registers, ATMs, barcode scanners and truck scales, as well as HVAC, fire and burglar systems.

DigitalSENTRY (DS) DataPoint is designed as a real-time loss prevention solution for industries affected by fraud or theft by giving users a single access point to critical data from both video and transactional devices. Customers can view and retrieve the information necessary to react quickly to protect their property. The application's database retains detailed information from each transaction, resulting in a fast and efficient method of conducting in-depth searches of events in real-time or from archived data. Synchronized video and transaction data displayed on separate or overlaid windows enables event intervention through real-time human monitoring, or through visual or audio alarms.

www.integraltech.com

7 Brivo Systems Access Control System



Brivo Systems LLC has introduced an IT-based access control system for users who wish to retain configuration and event data within their organization's own network. The system, based on Brivo's ACS OnSite product, is designed to meet regulatory compliance and data privacy requirements that call for personnel data to be housed within a secure, local database under direct control of the user.

Brivo's ACS OnSite SE uses a rack-mounted embedded Web platform capable of provisioning and managing multiple networked control panels supporting up to 300 readers and 25,000 users, with a database capacity of up to 1 million events. With appropriate network engineering by the end user or integrator, the system will operate across multiple facilities. The OnSite SE appliance increases system capacity and range by using a dedicated controller that manages multiple control panels attached to a corporate local area network, or, for multi-site configurations, across the Internet.

www.brivo.com

8 GarrettCom Router

A new router from GarrettCom Inc. lets plant engineers and IT departments link industrial sites in remote, harsh environments to central systems and operations centers using digital wide area networks.

The Magnum DX900 Industrial Router works over public or private digital facilities, frame relay services and virtual private networks. The DX900 is suitable for small- to intermediate-sized locations such as power distribution substations, transportation systems and water/waste water and pipeline operations. The unit can operate in temperatures from -40 to 85° C without fans or open venting and has rigorous electrical surge and electromagnetic immunity, meeting specifications for power substations. Conformal coating is available for deployment in high humidity or harsh atmospheres such as refineries and pipeline operations.

www.garrettcom.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.

H.264 Rocks the CCTV World

by Barry Keepence

What do Apple iTunes and YouTube videos share in common with the video surveillance industry? H.264, the latest standard for video compressor/decompressors, or codecs.

Developed by the ITU-T Video Coding Experts Group and ISO/IEC Moving Picture Experts Group, H.264 follows the highly successful MPEG2 and MPEG4 video standards and offers improvements in both video quality and compression.

Video codecs compress digital video in order to reduce the amount of bandwidth required to transmit and store the images. Compression is necessary because the raw data rate of uncompressed, digitally-encoded analog CCTV video at 30 fps is more than 158 megabits per second—300 times the capacity of a 512 kilobit-per-second asynchronous digital subscriber line (ADSL) connection. In terms of storage, a one-hour recording would fill an 80 gigabyte hard disk.

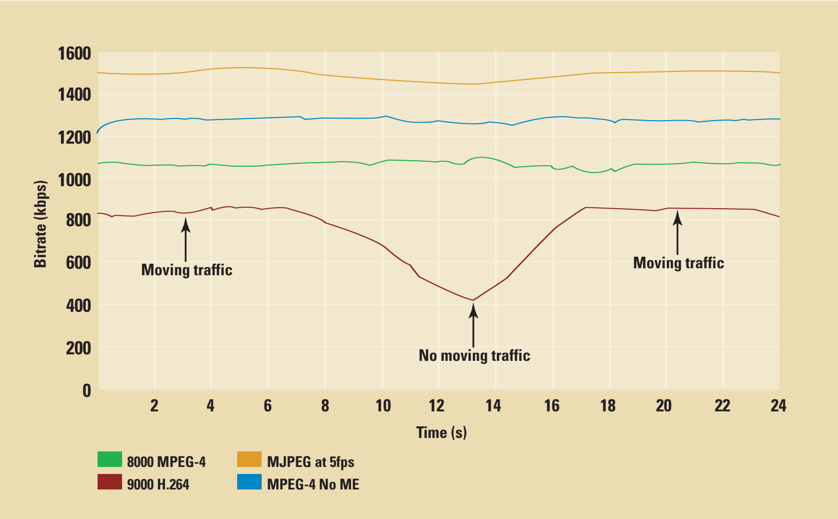
Scaling the video to lower resolution and compressing it with standard utilities such as WinZip or gzip could achieve 10:1 compression. However, at least 300:1 compression is needed to stream live video over an ADSL connection and to achieve 300 hours recording to an 80GB hard disk. This level of compression can be achieved with H.264.

An example of the bandwidth savings that can be achieved from a typical traffic surveillance camera, which must alternately transmit images of moving and non-moving traffic, is demonstrated in the following graph. In this example, the same 24-hour video sequence has been encoded using four different encoders: the IndigoVision 8000 MPEG4, the IndigoVision 9000 H.264, an MPEG-4 encoder with no motion estimation, and an MJPEG encoder. All were encoded at 25fps (with the exception of MJPEG at 5fps) to the same subjective video quality.

> At least 300:1 compression is needed to stream live video over ADSL and achieve 300 hours recording to an 80GB hard disk

The graph shows that compared to MPEG4, H.264 can achieve savings of typically between 20 percent and 25 percent in bandwidth usage and in excess of 50 percent during periods of scene inactivity—i.e., when there is no moving traffic. Not only does this reduce the overall bandwidth requirements of the IP video system but more importantly, it can significantly reduce the amount of storage required for recording the video, often one of the most expensive items in the system.

continued on page 34



IMPLEMENTING THE STANDARD

It is important, when looking at H.264, to understand the difference between comparing a standard versus an implementation of a standard. The two are very different. Thus when people say H.264 provides better video quality than MPEG2, it is a little misleading.

As a compression standard, H.264 defines the syntax of an encoded bitstream—in other words, the underlying language and grammar of the code. Naturally, a H.264-compliant decoder must conform exactly and be able to implement all the necessary tools defined by the standard in order to decode the bitstream.

An H.264 encoder, conversely, can implement a subset of the syntax defined by the standard, something akin to a language dialect, providing it produces a compliant bitstream. So it is more appropriate to say that H.264 provides a richer syntax and toolset than MPEG2. In addition, various implementations and algorithms within the encoder are also not defined by the standard, so manufacturers are free to innovate with design and functionality. As such, H.264 encoders from different vendors will compress streams at the same bit rate, but at differing quality, or generate the same quality video at a much lower bit rate.

H.264 has caught on. Apple uses it for all iTunes video and by the end of this year, YouTube hopes to have all of its video encoded in the standard. Its application in video surveillance will be no less significant.

Barry Keepence is chief technology officer of IndigoVision, Edinburgh, U.K.

LINKS

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

Advanced Technology Video	atvideo.com
Agent Video Intelligence	agentvi.com
Anixter International	anixter.com
Axis Communications	axis.com
BearCom	bearcom.com
Bosch Security Systems	bosch.com
BridgeWave	bridgewave.com
Brivo Systems	brivo.com
Cisco Systems	cisco.com
Daon	daon.com
DIVR	divrsystems.com
DSX Access Systems	dsxinc.com
Exacq Technologies	exacq.com
Firetide	firetide.com
FLO Corp.	fastlaneoption.com
GarrettCom	garrettcom.com
General Electric	ge.com
Hakin9	hakin9.org
HID	hidcorp.com
IndigoVision	indigovision.com
Inscape	inscapedata.com
Integral Technologies	integraltech.com
IQinvision	iqeye.com
ioimage	ioimage.com
Lantronix	lantronix.com
LG Iris Technology Division	lgiris.com
Lockheed Martin	lockheedmartin.com
Milestone Systems	milestonesys.com
Motorola	motorola.com
OnSSI	onssi.com
Panasonic Security Systems	panasonic.com/business/security
Pelco	pelco.com
Petards Vision Ltd.	petards.com
Radvision	radvision.com
RNCOS	rncos.com
Sony	sony.com
Tamron	tamron.com
Tyco Fire & Integrated Solutions	tycofis.com
Verant Identification Systems	verantid.com
Verified Identity Pass	verifiedidpass.com
Vigilant Solutions	vigilant-solutions.com
Wavelet Technology	wavestore.com
Unisys	unisys.com
Zebra Technologies	zebra.com