

Wednesday, March 9, 2005



Reality television

Digital video technology joins the physical security arsenal

BY Brian Robinson

Published on March 7, 2005

[More Related Links](#)

Digital video surveillance finally seems set to become a centerpiece of physical security systems, a prospect that was unlikely even a year ago. Questions over issues such as image quality and the bandwidth needed to carry the video over data networks dogged the technology.

Some people argue that those issues still haven't been fully addressed. Despite that, digital video is riding a swell of interest as its cost continues to come down, bandwidth and storage space get more affordable, and demand continues for technologies that can bolster emergency response and facility defenses.

Digital video's appeal is obvious. Older analog video systems require constant monitoring by on-site staff and frequent switching out of finicky tapes to record the video. Digital video can be sent over standard networks so that many surveillance sites can be managed from one location, and the video files can be stored on computer hard disks for near-instantaneous retrieval.

Market research firm Datamonitor sees digital video surveillance as a worldwide market worth \$7.4 billion by 2007, a 55 percent yearly growth from \$1.3 billion in 2003. The firm's analysts expect the public sector to account for as much as 22 percent of that future market.

"I think we are right at the beginning of the take-up of this," said Bruce Dewitte, product manager for

ADVERTISEMENT

Xiotech
 free white paper **Protect YOUR DATA**
 GET IT NOW ►
 Market-leading storage solutions
 As **Simple** as possible

replay ►
 The intelligent networks from Cisco are helping government agencies streamline processes to become as customer-centric as any successful business on the street.
 See how Cisco is helping change governments and business ►
 CISCO SYSTEMS
 innovation. powered by

Eyes on you

Law enforcement is one area where the use of video surveillance systems is attracting attention, both good and bad.

Northrop Grumman's Infrastructure Protection Division. "It will start this year and really blossom in 2006."

Eye on the future

Leading the charge are companies like iMove, which manufactures what it calls wide-area surveillance solutions. Typical surveillance cameras can only pan, tilt and zoom over a relatively narrow field, and many such cameras are needed to cover a broad area.

By comparison, far fewer of iMove's FlexG spherical sensors, each of which uses an array of imaging systems, are needed to continuously cover the same area.

For example, to keep an eye on an area three-quarters of a mile long by half a mile wide, company officials say an iMove solution using just nine of the company's FlexG sensors will do the job. It would take 242 closed-circuit TV cameras to do the same.

The company recently completed a major pilot project for a Navy facility that wants to replace its current video surveillance system, which can't cover enough of the facility's perimeter for staff to see who or what triggers most of the alarms.

With the lessons learned from the Navy project, iMove officials hope they can release a production version of the new solution within the next year or so.

"The target [markets] are such things as nuclear national assets, port security, airports and similar facilities — anything involved with external coverage," said Rick Mandrell, iMove's chief operating officer.

Video surveillance cameras produced by IPIX, which similarly provide complete, continuous coverage of an area, were used at President Bush's inauguration in Washington, D.C., in January. They were also used to guard the G8 Summit held last June in Sea Island, Ga.

Eventually, digital video surveillance cameras will attach directly to a standard IP network, making deployment much simpler. These so-called IP

In New Orleans, Mayor C. Ray Nagin included video surveillance as part of a seven-point plan to fight crime he proposed in 2003. The city's pilot video project, begun last April, distributed several dozen high-resolution IP cameras throughout a 25-square-block area. The cameras were connected to a police command post via a wired backbone network and a mesh wireless network supplied by Tropos Networks.

In the area where the video system was installed, the murder rate fell 57 percent and auto thefts dropped by 25 percent during a six-month period in 2004, compared with the same period the previous year when the cameras were not present, said Chris Drake, a project manager in the Mayor's Office of Technology.

"The digital video system can't take credit for all of that because the police are always doing things to counter crime," Drake said. "But even the district commander said the video system was far and away the biggest contributor to the fall in the numbers."

Elsewhere, the city of Brentwood, Calif., deployed a citywide digital video surveillance system as a way to deter robberies and burglaries. The system operates via a secure, wireless 802.11g wide-area network backbone based on Cisco Systems' wireless bridges and access points. Police patrol cars were outfitted with Cisco client network adapter cards so officers on the beat could receive the video on their in-car computer systems.

The system was designed to be as standard and open as possible so that it wouldn't go out of date quickly and could be updated easily as new technologies came along, said Lt. Kevin King, who heads the project for the Brentwood Police Department.

The standards-based approach was also important for convincing retail businesses to sign on to the project. A major part of its success depends on businesses being able to

cameras, which most of the major camera manufacturers have started to make, include all of the intelligence needed to act as a self-contained node on the network as well as the software needed to compress and encode the digital video. Some even include Web server software and operating systems, which eliminates the need for separate servers to process the images.

Until these newer technologies make a bigger impact, current users of video security technologies will have to find a way to get the most out of their existing investments.

"Many of the surveillance cameras that are in place are still analog. They cost a lot, and customers are looking to use that existing investment," said Lisa Ciappetta, product marketing manager specializing in video surveillance for ADT Security Services. "And the fact is that analog cameras still produce images with the better detail. Digital cameras are getting there, but they are not there yet."

Switching channels

The need to incorporate existing analog cameras in current digital video installments means the focus is still on the network's video recorder, which takes the analog video feed from the camera and digitizes, compresses and encodes it before sending it out onto the IP network. Also important is finding the analysis software that makes the best use of the digital video.

A test of a digital video system at the Jacksonville, Fla., International Airport — funded as part of a \$28 million Transportation Security Administration program to develop airport security systems — uses this kind of an analog/ digital mix.

The system takes the video feeds from some 100 analog cameras positioned at security checkpoints and all along the length of the airport concourse, digitizes the video and then "stitches" the resulting digital images together to essentially provide a single, real-time view of the area.

"It essentially produces a movie on the fly," said Gianni Arcaini, chief executive officer of Duos Technologies, the project's prime contractor and integrator. "The idea is that, if a security breach is committed, we can wind back to when the breach happened and security agents can then follow the person who committed the breach everywhere they went."

The software used to combine the video produces a 3-D effect that allows agents to virtually "fly" around the concourse like they would in a video game, Arcaini said. Agents can follow the person in a

tie their own in-building surveillance systems into the city's wireless system, said John Isaac, vice president of sales and project manager for Clare Computer Solutions, the integrator for the Brentwood project.

However, these types of law enforcement applications have drawn their share of criticism. The American Civil Liberties Union, for example, believes "the untrammelled use of video surveillance is a problem that needs to be controlled," said Jay Stanley, an ACLU spokesman.

Isolated use of cameras to protect private property is not a big problem, he said, but large networks of cameras operated by the police or other government organizations raise privacy concerns that must be addressed with clear policies.

"You need rules to govern when cameras are turned on, what they can be used for, what the zoom limits will be, whether night vision will be used and so on," Stanley said. "You also need rules for how long the video will be retained, who has access and how the rules will be verified and enforced."

He added that studies done in the United Kingdom, where law enforcement agencies have used video for years, raise questions about how effective surveillance cameras are in combating crime or preventing terrorism.

— Brian Robinson

fast-forward mode to see what he or she has done since the breach occurred.

The system, which Duos officials hope will be completely evaluated by this summer, could have dramatic consequences if airports around the country decide to adopt it, Arcaini said, because shutting down a concourse for a single security alert can cost \$500,000 or more.

"This system could prevent 90 percent of that kind of thing," he said.

It's that kind of software-driven capability that is behind much of the drive to digital video surveillance, said Craig Chambers, vice president of advanced video systems for L-3 Communications Government Services Inc.

Chambers was formerly the president and chief operating officer of Pyramid Vision, which sold its advanced video security product line to L-3 in December. The former Pyramid's Vision Alert and Vision Flashlight software is being used in the Jacksonville project.

"In many respects, the analysis [of video data] was too far ahead" of the market, he said. "The ability for a computer to take the video and distinguish between objects and whether things should or should not be in areas that are being monitored has been there for some time."

What has changed in the past couple of years, he said, is the development of advanced algorithms that can take advantage of current computer processing power to quickly refine images even more by techniques such as eliminating camera jitter, compensating for background motion such as the movement of grass or waves, or allowing for the distorting effects of rainfall.

Squeezing a signal through

One other technical hurdle that still has to be overcome is the compression that must be applied to the digital video to keep image resolution high while making the data compact enough to transmit over the IP network and store on a hard drive without overtaxing the capacities of either one.

"The problem is that the data networks that this video will be sent over are being used for so many other things," said Mike DeWalt, senior electronic security product manager at Diebold. "If there's a particular need for very high resolution capability then a separate network might have to be provided, but in most cases it's going to be the same network for everything."

Therefore, success hinges on factors such as data transmission and storage capabilities. Given most organizations' experiences with both, they should be the least problematic elements, but that's where some critics say the surveillance industry most often fails.

"Since video makes such a huge demand on bandwidth, it needs careful planning and design, and consideration of such things as security and [bandwidth] provisioning," Dewitte said. "Many people are naive in thinking how easy it is to install digital surveillance systems."

Some video vendors are trying to address deployment and management challenges by teaming with infrastructure providers. For example, officials at JOIN Computer & Control recently announced a product called JOINPRO Video Surveillance System that combines the company's digital video equipment with high-availability storage gear from Digi-Data and storage management and cluster file system software from Sanbolic. The integrated package is designed to support up to 330 terabytes per

system.

Steve Morton, chief executive of Boundless Security Systems, said that employees responsible for video systems should have a computer architecture and networking background, because they will need to know how to address the proprietary nature of much of the technology involved and the interoperability issues that it introduces.

And how do people plan for when that infrastructure breaks but they need to keep some surveillance functionality?

"That requires knowing about such things as distributed architectures," Morton said. "There's no question that the industry is absolutely in transition, but there's also no question that the systems engineering firms involved need to have a much greater understanding of the underlying networking technology."

Given the high interest in the technology, that expertise is likely to come.