THE ESSENTIAL GUIDE TO VIDEO SURVEILLANCE

A SUPPLEMENT TO

GSN. Government Security News

September, 2008

For the best in video surveillance,
follow the leading expert.

CRIME SCENE-DO

A message from Jacob Goodwin, *GSN's* Editor-in-Chief

Periodically, *GSN: Government Security News* publishes special editorial supplements that focus on a single aspect home homeland security that we believe warrants close attention. This supplement, titled the *Essential Guide to Video Surveillance*, presents insights and analysis from some of the leading thinkers in the field of CCTV and video surveillance.

There is no question that video surveillance has become synonymous with homeland security in recent years.

In this Essential Guide, we're pleased to offer thoughtful articles which:

- Explain how concepts of motion imagery and persistent surveillance relate to the use of Unmanned Aerial Vehicles (UAVs) to provide long-distance surveillance along U.S. borders;
- Describe how a marriage of traditional video surveillance with Ultra Wideband Radar (UWB) can enhance perimeter security;
- Discuss steps being taken to model the computer processes used by video analytics after some of the cognitive processes regularly taken by the human brain;
- Introduce the notion of video monitoring being delivered online as a network service;
- Make the case for government-wide video surveillance standards which would help both the manufacturers and the end-users of such technologies;
- Outline the case for wireless mesh networks to be used instead of wired systems when providing video surveillance across long distances;
- Explain the recent advances that have taken place in the digital video recorder (DVR) niche of the security field;
- Describe how thermal cameras can bring special capabilities to a thorny surveillance problem;
- Identify the advantages that a 360-degree panoramic camera can bring to the surveillance field. ■

GSN: Government Security News

Main Number: (212) 344-0759
Fax: (646) 336-3960
www.gsnmagazine.com

EDITOR-IN-CHIEF:
Jacob Goodwin
(212) 344-0759 x255
jgoodwin@gsnmagazine.com

ART DIRECTOR:
Mark Kaplan
(212) 344-0759 x2005
mkaplan@gsnmagazine.com

SENIOR EDITOR:
Louis Chunovic
(212) 344-0759 x2007
lchunovic@gsnmagazine.com

PRODUCTION & MARKETING MANAGER:
Monty A. Mason
(212) 344-0759 x2009
mmason@gsnmagazine.com

RESEARCH ASSOCIATE:
Laura de la Torre

PUBLISHER:
Edward Tyler
(212) 344-0759 x2001
etyler@gsnmagazine.com

ADVERTISING SALES

Director of Advertising / MidAtlantic /
Southern Regional Manager:
Michael J. Madsen
(212) 344-0759 x 2004
mmadsen@gsnmagazine.com

Midwest Regional Manager:
Michael Stack
(847) 367-7120
mstack@gsnmagazine.com

Western Regional Manager:
Adrian Courtenay
(212) 344-0759 x 2002
acourtenay@gsnmagazine.com

Pacific Rim / *GSN* International:
Ken Sugisaki
011-81-44-712-2111
ksugisaki@gsnmagazine.com

SALES SUPPORT MANAGER:
Anne Tyler
(631) 275-0264
atyler@gsnmagazine.com

CIRCULATION DIRECTOR:
Hilde Stein Sprung
(516) 695-9859
hstein@gsnmagazine.com

REPRINTS MANAGER:
Mackenzie Tyler
(631) 433-6690
mtyler@gsnmagazine.com

LIST MANAGER:
Edith Roman
Postal: **Kevin Collopy**
845-731-2684
kevin.collopy@edithroman.com
E-mail: **Maggy Pizzuto**
845-731-3844
maggy.pizzuto@epostdirect.com

WORLD BUSINESS MEDIA, LLC
Edward Tyler, President

Adrian Courtenay, Chairman
(212) 344-0759 x2002
acourtenay@gsnmagazine.com

GSN: Government Security News (ISSN 1548-940X and UPS 022-945) is published monthly except semi-monthly in February (13 times per year) by World Business Media, LLC, 233 Spring Street, 3rd floor, New York, NY 10013. Telephone: (212) 344-0759. Periodicals postage paid at New York, NY and additional mailing offices. POSTMASTER: Send address changes to *GSN: Government Security News,* Subscription Department, P. O. Box 316 Congers, NY 10920-0316. For government decision makers and business executives involved with security products, systems and services. The *GSN* Web site is: http://www.gsnmagazine.com. Copyright 2008 by *GSN: Government Security News.* All rights reserved. Reproduction of this publication in whole or part is prohibited except with the written permission of the publisher. Printed in the U.S.A. *GSN: Government Security News* assumes no responsibility for validity of claims in items reported.

TABLE OF CONTENTS

Border security with UAVs: Persistent surveillance vs. motion imagery

By Jon Damush

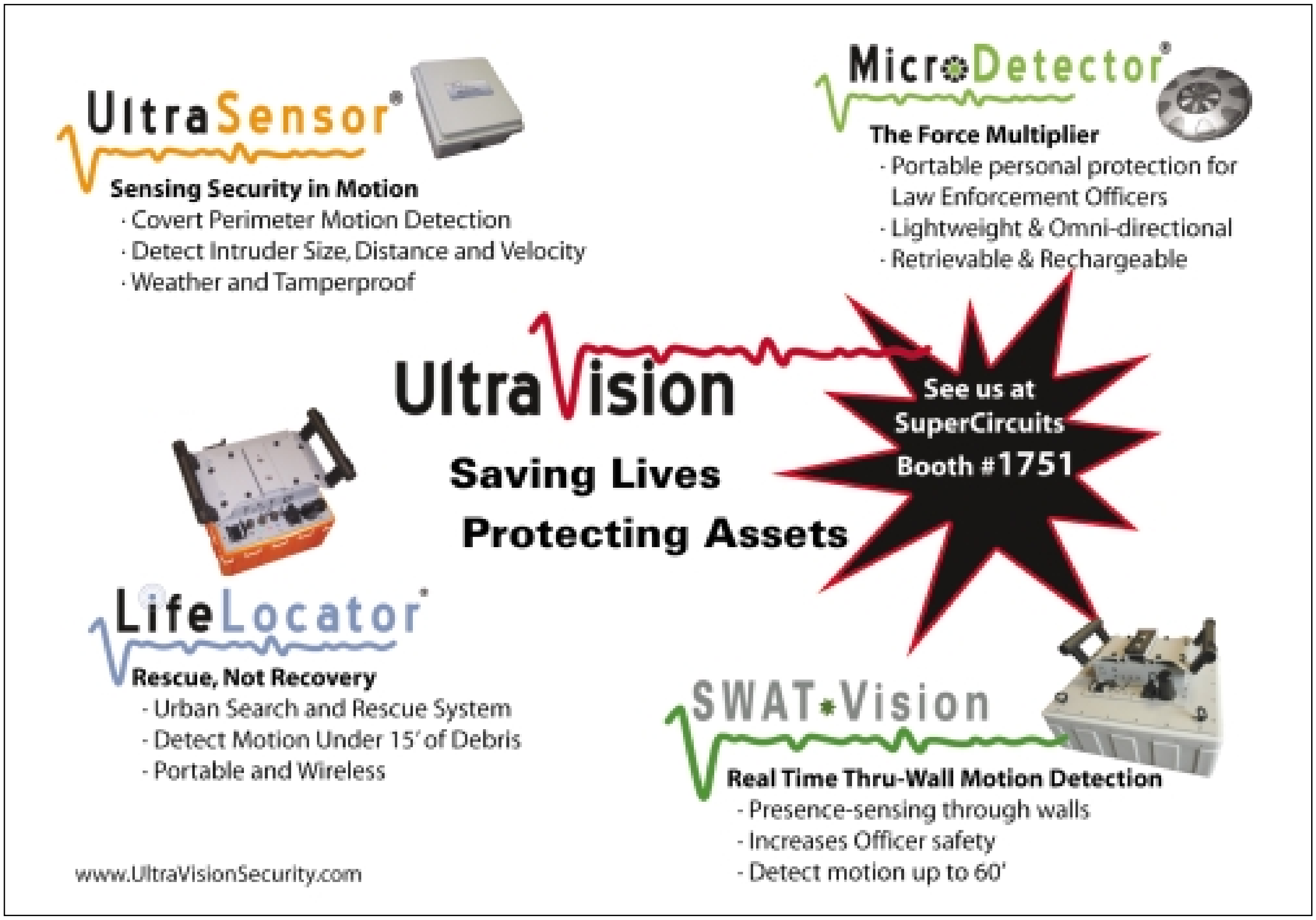
There has been a lot of talk lately about the use of UAVs to patrol the U.S. border, and certainly no more so than in Southern California. Most of us reading this column probably are familiar with land-based security systems and the quality of video they produce, which is *much* better than the quality of imagery produced by typical UAVs.

Land-based systems have the luxury of being connected to their viewers with solid wiring, capable of carrying a great deal more bandwidth than our featherless, flying friends, which are forced to send their data to their viewers over radio links. Those radio links generally offer only enough bandwidth to carry a standard TV (NTSC) signal, plus some accompanying data such as the position of the aircraft, the pointing vector of the camera and the field of view of the camera. This is a key challenge for UAVs which are used by our armed forces in combat areas and by domestic civilian personnel charged with maintaining control over America's borders.

How can we overcome -- or at least deal with -- this challenge, which forces us to use our bandwidth efficiently to perform the required tasks? To answer that question, it might help to differentiate between two common terms used in the UAV community, so readers will understand the subtle differences between the two main missions of UAVs, and begin to appreciate the video technologies required to deliver successful results.

First, *persistent surveillance*, which means pretty much what you would expect it to mean: an ever-present, all-seeing "eye-in-the-sky" that keeps vigil over a large area for long periods of time. Persistent surveillance systems are expected to tell operators where something has changed or where something is happening that might be of interest.

Imagine yourself looking for a golf ball that you just hit into the woods. You are not looking in detail at any one area. Instead, you are basically surveying a larger area to try to pick up any subtle difference in the background that might be your golf ball. You are performing persistent surveillance. You require some distance from the area, and a wide field of view. The prob-



lem is that you might actually find more than just your golf ball, or you might not find your golf ball at all. You might simply need greater detail before you can find it.

That is where *motion imagery* comes in. Motion imagery is akin to taking the same sensor or imager, and sticking a really long lens on it, so you can see the detail of the subject in question from a long distance away. With such a narrow field of view, you obviously cannot see anything else but the object on which you are focusing. Using the golf ball example again, this is what you do once you find a ball you think may be yours -- you walk up close to it so you can see the markings on its surface.

Now that you understand the difference between these two tasks, you can better appreciate the original problem -- the limited bandwidth of a UAV's radio link makes simultaneous performance of persistent surveillance and motion imagery impossible with a single imager and transmitter. Consequently, we either put more than one airplane in the sky (one for persistent surveillance, and one for motion imagery) or we get clever with technology and "exploit" the imagery with computers on the ground.

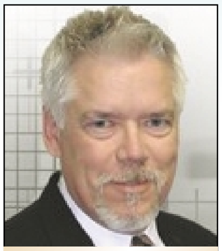
Exploitation can allow a single imager (and one airplane) to perform both tasks through a variety of techniques:

- **Mosaicing** – Using multiple frames of motion imagery to create a single image that encompasses the entire area covered by the motion imagery clip. Think of this as a video paintbrush that allows a user to keep his equipment in motion imagery mode, but leave a trail of imagery behind that provides persistent surveillance information.
- **Super Resolution** – Using multiple frames of video to create a single image that is of higher resolution than any single frame of imagery in the clip. This allows an operator to keep the imager's field of view wider than would normally be needed to see the object in question.
- **Moving Target Indication (MTI)** – Comparisons of the imagery across multiple frames can indicate the people or objects that have moved since the last time you looked at the same area. This enables an operator not to have to try to see things in the video with his own eyes, but instead to rely on the software to inform him where the movement is taking place. You might also refer to this as queuing the motion imagery task.
- **Automatic Change Detection** – Similar to MTI, but used to detect static items that are now in the area which might not have been in the area the last time you imaged it. This is also a queuing capability that alerts an operator to a change in the scene that he might have had difficulty seeing for himself. This can be especially useful when searching for Improvised Explosive Devices (IEDs).

These techniques allow an operator to make intelligent decisions on how to task his aircraft because he can now walk the line between persistent surveillance and motion imagery, without having to choose between the two. ■

Jon Damush is the President of 2d3 Inc., a wholly owned Subsidiary of London AIM listed, OMG plc. Damush can be reached at: jd@2d3.com

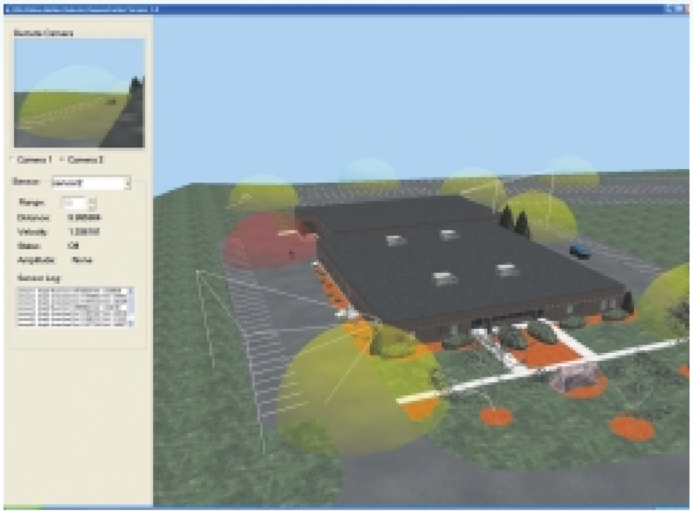
Video surveillance and UWB sensors: The perfect marriage?



By Bill Lozon

It was only a matter of time before some testosterone-fueled biker injured himself during the nightly burnout meets that were being held at the secluded employee parking lot of Geophysical Survey Systems (GSSI) last spring.

The well-lit lot was a natural temptation for area riders to test out their bikes while paying no attention to the "Do Not Trespass" signs clearly posted on the property. GSSI President Chris Hawekotte and the chief financial officer and security director, Don Walcyzk, needed to find a way to alert Salem, NH, police without creating false alarm problems inherent with so many perimeter alarm systems. GSSI called in Davco Security, of Saugus, MA, for consultation. It was quickly decided that video surveillance would be used to spot intruders and verify alarms prior to any police dispatch. But, what could be used to effectively and reliably activate the video equipment?



GSSI is located in a 30,000-square-foot office and manufacturing facility in an industrial park just outside Salem. The configuration and size of the property made fencing an impractical consideration and traditional volumetric motion sensors were sure to cause problems. Though not defined as a rural area by conventional standards, it is not unusual to see fox, deer and other wildlife in

the area, especially during the evening.

After weighing the alternatives, it was decided to use an innovative approach to enhancing video perimeter security known as Ultra Wideband Radar, or UWB, as it's commonly called. UWB has been used for years in the communications field, but it is relatively new to security. UWB sensors operate in the 100-700 megahertz range and their extremely low, long wavelength enables them to penetrate solid materials. As a result, UWB sensors can be installed inside walls, above ceilings or underground. UWB radar also indicates intruder speed and, most importantly, intruder size.

When attempting to discriminate real threats from nuisance alarms, size does matter, and that's where a marriage of UWB and video surveillance really pays off. UWB sensors can be programmed to disregard intruders below a certain size threshold. So, most critters, wind-blown debris and waving vegetation -- factors that often cause problems for outdoor volumetric sensors -- are ignored. And, because UWB sensors can be buried underground, weather conditions and tamper attempts are not relevant considerations.

A sensor's individual detection range is approximately 50 feet in diameter, and installation of the sensors was a simple process of placing the sensors in 3-by-3 foot holes around the perimeter of the facility, linking them to a server via Cat 5 cable. The server, in turn, is integrated to a Bosch video matrix switcher and DVR that aims the PTZ cameras and records the action.

Uniting video surveillance with UWB sensors simply made the GSSI security system more reliable than video alone. Nuisance alarms are not a consideration. UWB can reject troublesome non-human intruders and, because the system is Web-enabled, when a larger target intrusion occurs, Walcyzk can receive on a wireless hand-held device or home PC an image of precisely what the cameras are seeing. He can then decide if police involvement is necessary.

"Once the police started showing up as soon as the first couple of bikes arrived on our lot, the problem disappeared," said Walcyzk. ■

Bill Lozon is vice president of sales & marketing at UltraVision Security Systems. He can be reached at: lozonb@ultravisionsecurity.com

Cognitive video analytics

By John Frazzini

cog·ni·tion [kog-nish-uhn] noun

1. the mental process of knowing, including aspects such as awareness, perception, reasoning, and judgment.
2. the product of such a process; something thus known, perceived, etc.
3. knowledge.

WHY VIDEO SURVEILLANCE NEEDS A COGNITIVE APPROACH

The use of vision analytics algorithms for the purpose of assisting video surveillance systems to "see" better has been around for well over a decade. Technologies have been built so a camera can be programmed to look for a specific object or motion with varying degrees of success. These rules-based systems typically require extensive programming from humans, and from a scalability perspective, make it difficult for them to achieve broad market adoption.

These systems also are typically riddled with false positives and become too manpower-intensive to set up and maintain. Developing a video analytics system which follows a path consistent with the cognitive process produces more accurate results, and does so in a way that improves the effectiveness of any video surveillance system over time.

COGNITIVE VIDEO ANALYTICS LEARNS JUST LIKE YOU AND ME

The concepts around the cognitive sciences (the study of how the human brain functions) in the development of technology have been utilized in many different applications and industries. However, creating an connection between vision analytics and a system that emulates the cognitive process -- utilizing various machine intelligence and machine-learning technologies -- represents a breakthrough for the video surveillance industry. A cognitive-based video analytics system is not only equipped with the ability to "see" better, but also to learn, remember and make observations much like a human brain. A cognitive-based video analytics system constructs its own understanding of the world it is observing by evaluating the patterns of activity for any given environment over time. A "mental model" is then created for each scene in order to make sense of the observed activities.

Learning is achieved by continuing to adjust the mental models to interpret and trigger alerts on new activities as they occur, within the context of previous activities. Thus, a cognitive-based system creates an understanding of what is seen through a camera's field of view and establishes what it determines to be "normal" for any given environment. It is therefore able to alert on activity it determines to be "abnormal."

COGNITIVE-BASED VS. RULES-BASED

Every environment and every scene is unique. No one is able to write enough rules to cover the infinite number of possibilities for any given environment. That is why it is important to have a cognitive-based system that is able to learn what is normal for every unique environment and then alert when there are activities that occur outside that normal pattern. The same learning capability is also important in order to adapt to changes that may occur within any given environment over time. These two capabilities -- the ability to adapt to almost any scene and the ability to improve upon its learning over time -- are the most important distinguishing factors of cognitive-based systems versus rules-based video analytics systems.

The benefits to businesses that adopt cognitive-based video analytics systems over rules-based systems can include everything from reduced costs due to less required coding and customization, increased effectiveness from fewer false alerts, and increased return on investment (ROI) on the entire security infrastructure.

A NATURAL EVOLUTION

Just as the IT security business has evolved to include adaptive pattern-detection security solutions, so will video analytics and video management solutions evolve. Building systems along these lines will produce in the future the ability to expand the use of video analytics systems across multiple cameras connected to the same system. For example, this could make it possible to track behavioral patterns from one camera to another. Future capability will also allow operators to teach the system through "supervised" learning activities such as training the system that one specific alert included specific characteristics that will be of interest consistently to other security operators.

Cognitive video analytics is being deployed in security watch centers today to enhance security teams' perception and awareness. It will continue to increase the scalability and effectiveness of security operations over time. ■

John Frazzini is the president of Behavioral Recognition Systems, Inc. He can be reached at: john@brslabs.com

how

Video monitoring as a network service

By Fredrik Nilsson

If you have experience installing, using or maintaining video security systems, either traditional analog or modern networked digital solutions, you will be familiar with tasks such as software installation, software upgrades, network configuration, scheduled service rounds, monitoring of device functionality, replacement of broken hard-drives or analog tapes, etc. Some of these issues may even be so familiar to you that you consider them to be a part of life, something that we simply have to accept and do in order to keep our video monitoring systems up-and-running.

One recent concept, "Software as a Service," or SaaS, which is typically pronounced "Sass," may present a solution to most of the above issues for many video monitoring and security applications. SaaS has in recent years become an increasingly common solution within the IT industry and, as modern video security systems are essentially IT applications, the SaaS concept applies in the security realm as well.

In a SaaS system, the main software application is installed on central server farms. A network, such as the Internet, is used for access by cameras and video recording devices, as well as by users.

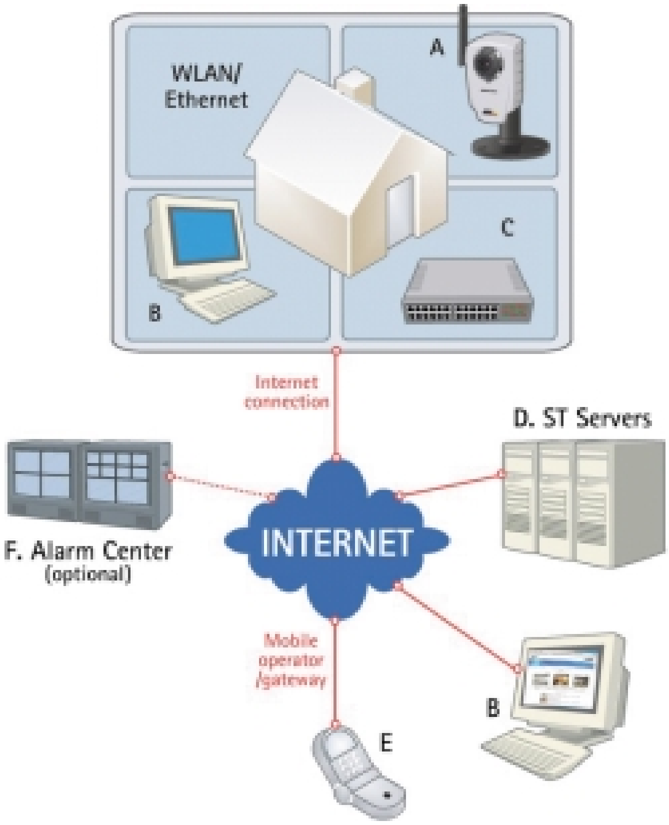
Some advantages of the SaaS approach include the following:

• Economy of scale – The central system supports many users, all of whom benefit from the central servers and storage capacity. Even more importantly, they also benefit from the economic advantages of the shared expert knowledge at the central system site, the expert knowledge of the monitoring system itself, the data and Internet security expertise, and the storage management expertise.

• Monthly recurring fees, instead of high initial investment.

• Central device and system management - All devices in the system are managed by centrally placed experts, who handle everything from daily monitoring of device status to firmware upgrade of devices. On the remote site, only network cameras and a network are needed, there are no local PCs or recording devices.

• Viewing applications are always up to date, and there are no problems concerning updated video file formats or other such compatibility issues.



• Remote and mobile access - As this is a network-centric solution, access can be provided regardless of the viewer's location.

• Remote storage of video eliminates the risk of stolen tape or a damaged local DVR.

Video monitoring provided as an Internet service has been available for some years now. From originally targeting the residential monitoring market, systems are increasingly being used for professional security applications. For example, TeliaSonera, the largest telecommunications company in Scandinavia, provides a basic monitoring service for residential and small business users. Once the cameras are installed on-site, end-users can at any time view live and recorded video triggered by video motion detection, both from a PC and from a mobile phone. The main application enables users to check on their homes or businesses from any remote location.

Another excellent end-user example is from a chain of stores selling high-value goods. Megapixel resolution video is stored locally at each site, and when an event occurs, the security manager at the company's headquarters can remotely and immediately provide the police with a downloaded high-quality video of the event.

We are likely to see a rapid uptake of the SaaS concept in the security market for the following reasons:

• Ease of installation. Using a SaaS system, the installation time for the local devices, such as cameras, are normally reduced dramatically. With the rapid increase in number of cameras, and tighter budgets, this will be a market driver.

• Bandwidth is becoming more readily available at reasonable *prices*, making it feasible and cost effective to transfer video from several cameras at a location to a central server. In many countries, the regular bandwidth to a home or small business is 10MB to 40MB. In the U.S. there are an increasing number of affordable high-bandwidth options (cable, fiber, etc.).

• Better compression. With H.264 compression, the amount of bandwidth required for full-frame rate video is dramatically reduced. H.264 is also supported on many other platforms, such as smart phones, making viewing of video on mobile devices much more effective.

As a result, as in the IT world, SaaS will clearly play an important role in video surveillance going forward. ■

Fredrik Nilsson is general manager of Axis Communications. He can be reached at: fredrik.nilsson@axis.com

Standards required for government market

By Mark Provinsal

For manufacturers working in the government market, the space is vast and broad. Filled with numerous agencies with various needs, requirements and infrastructure, providing quality video surveillance solutions is not a once-size-fits-all process. Because the government market is fragmented -- and each agency is working with different networks and levels of security -- the need for standards that are appropriate for groupings of similarly focused agencies has become paramount.

The video surveillance industry began embarking on a process of convergence between analog and IP video about three years ago, and is following an adoption similar to the transition that the telecommunications industry experienced. Manufacturers of solely IP-based technology are pushing government agencies to use products that require a retrofit of their existing technology instead of leveraging their existing investment.

The creation of national video surveillance standards creates a context for video surveillance products that simplifies the purchasing process for consumers, while at the same time promotes the use of the technology, which is beneficial to both private and public interests. Due to analog and IP convergence within the U.S. video surveillance market, consumers -- in this case government agencies -- are sorely lacking guidelines on how to analyze and assess video surveillance solutions that simplify their processes while also protecting their assets.

The United Kingdom recently published a standard for Digital Video Evidence, BS8495, which establishes a standard for exported image data to be used as evidence in court. Other key standards and codes of practice include the BS8418 Code of Practice, which addresses each of the individual components of a security system -- the installation, monitoring and user procedures. The standard offers vendor-neutral guidance on what to consider when purchasing a system, how to select the right remote video response center and important advice regarding operating procedures.

Vendor-neutral guidance would be beneficial to the U.S. Government market as well. Within the U.S. Government market, there is great debate over whether to convert to IP-based systems. There are two basic hardware components of the IP-based solution: cameras and recorders. The economics of rewiring an existing installation in order to switch out analog cameras for IP cameras do not make sense. For this reason, analog cameras will continue to be viable for the next five to 10 years. The recording platforms for IP-based surveillance systems are categorized as DVRs or NVRs. However, DVRs should be categorized as encoders with built-in storage. Many DVRs are now also recording IP camera video sources, and are ideal for applications that are integrating IP technology without eliminating all of the owner's analog investment. The use of DVRs and NVRs are predominant in our market today. The two types of recording products will continue to co-exist until analog cameras are no longer installed.

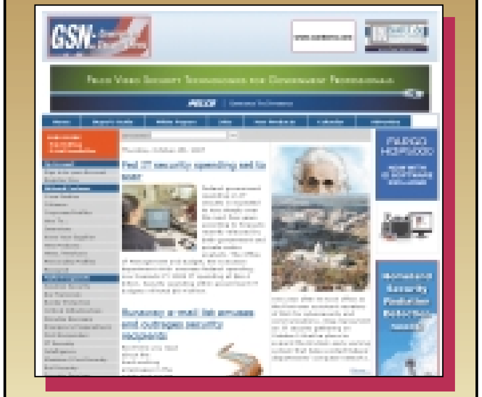
A key challenge for deployments of NVRs and DVRs continues to be remote viewing. Most software applications that are installed on PCs are difficult to configure and operate. Another challenge is from the IT department which approves and maintains the computers and software in the typical business unit. In addition to the security risk and cost of maintaining these computers, there are concerns about network utilization. IT involvement is critical early in the planning process.

Adopting national standards will reduce many of the objections from IT departments. Another solution to the problem is to use dedicated network keyboards that connect directly to monitors. These embedded devices are single-purpose stations that do not require IT department maintenance.

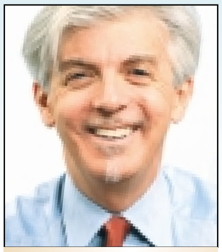
So, what does that mean to government officials who are planning on purchasing or upgrading their video surveillance system? The IT department must be fully integrated with the security team to have the greatest success.

Video surveillance technology manufacturers must work together to assist the government market establish standards that work for their agencies. Today, the Security Industry Association is bringing together leaders in the industry to publish common, open, interoperable protocols and performance standards. It is in the best interest of all parties to establish guidelines that are flexible enough to address the broad range of requirements, but are stringent enough to offer a vendor-neutral approach to specifying and implementing a surveillance solution.

Mark Provinsal is executive vice president of strategic marketing and products at Dedicated Micros Inc. He can be reached at: mprovinsal@dedicatedmicros.com



Switching to wireless mesh



By Stephen Rayment

Networked video surveillance is one of the fastest growing markets in the security industry. Meanwhile, during the next three years, the market for megapixel surveillance cameras (requiring greater network bandwidth) will grow at a compound annual growth rate in excess of 100 percent. This data from IMS Research underscores the increasing impact that video surveillance is having on the IT networking plans of organizations.

Increasingly, because of its benefits over wired networking, wireless mesh technology is being considered as an alternative for delivering video security traffic from both fixed and pan-tilt-zoom (PTZ) cameras to central or remote monitoring stations. These benefits include:

- **Cost-effectiveness and speed of installation:** Wiring requires costly, time-consuming and disruptive trenching, whereas wireless mesh nodes can be quickly and conveniently co-located with the security cameras they support.
- **Resiliency:** Wireline failure will generally result in lost transmission, whereas wireless mesh is an inherently resilient architecture enabling continued transmission in the event of a node failure.
- **Flexibility:** With no wiring limitations, cameras can be set up almost anywhere, and easily moved as required.

Delivering the high-performance and scalability required in a large-scale video surveillance network requires more than just a mesh architecture, as the Port of Richmond, northern California's most diversified cargo handler, discovered when researching wireless mesh alternatives for the 15 square miles that comprise the port's perimeter and facilities.

Port of Richmond was looking for a state-of-the-art IP video surveillance system utilizing advanced analytics, enabling remote monitoring and storage, and supported by a next generation wireless mesh network capable of expanding as needed. Proven reliability, scalability and the ability to support high-quality real-time video transmission were key requirements of the wireless mesh technology. After extensive research, the Port of Richmond now has 31 wireless nodes, based on patented switched mesh technology, supporting the 82 IP cameras that monitor the port's 15 square miles.

MESH CHALLENGES IN LARGE-SCALE NETWORKS

Critical to the delivery of high-quality real-time video security traffic over the port's wireless mesh network is the high-capacity and low latency associated with the patented switched mesh backhaul of the unique quad-radio wireless mesh nodes deployed. While other wireless mesh products are promoted as supporting video security applications, their single or dual-radio node architecture and shared mesh backhaul limits their scalability to support large coverage areas.

The term "shared mesh" refers to the fact that these mesh nodes communicate with neighboring nodes on the same channel of the same frequency. The bandwidth of that single channel, single frequency is shared among all nodes simultaneously limiting the overall capacity of the network and resulting in high, unpredictable latency and jitter as traffic grows. This unpredictable performance is unsuitable for video traffic, which is latency sensitive.

To overcome their inherent weakness, some dual-radio shared mesh products are deployed with both radios combined to operate as a single unit, a workaround that increases capacity but removes the resiliency benefit of the mesh, creating a single point of failure in the network. Deploying these mesh networks over large coverage areas will also require many wired egress points, reducing the cost-effectiveness and speed of installation benefits associated with the mesh architecture.

DELIVERING THE BENEFITS OF MESH

Unlike traditional mesh architectures, in the patented switched mesh architecture deployed at the Port of Richmond, the nodes provide multiple dedicated and isolated point-to-point connections, supporting diverse paths between each node in the mesh. In this switched architecture, all of the available bandwidth of each separate radio channel is dedicated to the link to the neighboring node. So, the total available bandwidth is the sum of the bandwidth of each of the links.

Each dedicated mesh link is on a separate channel, ensuring that forwarded traffic does not use any bandwidth from any other link in the mesh and enabling the network to effectively scale as more nodes are added. As a result, even in large-scale deployments, a switched mesh is capable of delivering and maintaining much higher capacities and transmission rates and lower latency and jitter than a shared mesh, making it an ideal solution for the Port of Richmond's video security network.

Stephen Rayment is chief technology officer of BelAir Networks. He can be reached at: srayment@belairnetworks.com

Tapeless video surveillance: Advances in digital video recording for law enforcement

By Mark Playdon

Having effectively transformed the broadcasting industry, the digital revolution is beginning to have a profound impact on many other areas as well, including law enforcement. Learning solid lessons from the broadcasters, police organizations are seeing advanced digital video recording and surveillance technologies as antidotes to the inefficiencies, inferior recording quality, inflexibility and high storage costs of videotape.

This article will discuss the latest advances in digital video recorder (DVR) technology and the compelling benefits they offer to law enforcement agencies at all levels.

BEYOND TAPE: THE DVR ADVANTAGE

Growing numbers of police agencies are taking a hard look -- with good reason -- at DVR technology possibly to replace their older surveillance systems which record onto tape. Unlike tape-based systems, recordings made by DVRs can be stored as electronic files on a central server for fast and easy access, retrieval and viewing from either field laptops or other computers. Rather than spend their time searching through piles of tapes *manually* to find the right piece of footage, officers can access the desired segment in a flexible, non-linear fashion by simply jumping to the exact point in the recording that they need; with no time consuming fast-forwarding or rewinding required.

Because computer files won't degrade over time, digital systems offer a more durable alternative to tape, which has a finite shelf life and a tendency to stretch and wear with each use. This makes DVRs a much better choice for field surveillance in remote, often rugged locations, where conditions such as sand, dust, heat and cold would wreak havoc on tape media. As an added bonus, digital systems eliminate the costs and hassles of storing and maintaining bulky tape stock.

In addition to the physical storage considerations, digital systems offer advantages that are critical to accomplishing the highly detailed and accurate video surveillance often required by officers to gather evidence and build their cases. Some of today's most advanced DVR systems are capable of recording at extremely low compression rates, such as 4:1 to 6:1, which deliver significantly higher video quality than the Hi8 compression used by traditional tape media.

Also, unlike tape recorders that require a few seconds to roll before recording and thereby lose valuable footage that might be crucial to a case, DVRs have near-zero lag between the time "start" is pressed and the first frame is captured. Picture the DVR that is deployed in a remote and rugged field location and sits idle for weeks, but then powers up and instantly begins recording for as long as

Panoramic imaging captures it all

By Yves Messier

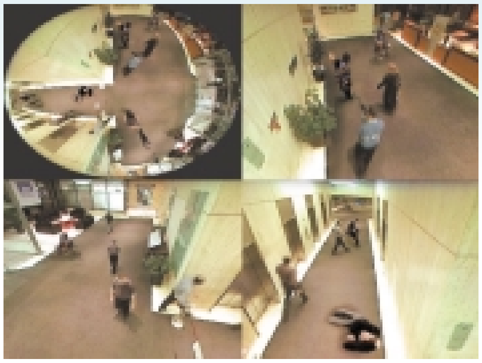
The location is a state prison. What seems to be an average day with inmates roaming the grounds outside the buildings will quickly escalate into an incident that could have been avoided. Inmates start arguing in one corner, a fight breaks out in another. Soon, all the surveillance cameras are pointed at the four or five diversions that have been planned by the inmates themselves, leaving an area out of the field of view of the surveillance cameras. An inmate is stabbed and no one saw it happen.

A person walks towards a government building, places a parcel next to the main entrance and walks away. Two minutes later, the parcel explodes. The camera pointing at the entrance captured the incident, but not where the person came from, where he went or what vehicle he got into.

Could these scenarios have been avoided? Is there enough evidence to capture the culprits?

Images captured and recorded using pan-tilt-zoom (PTZ) and fixed cameras are typically limited by their field of view and by where the camera was pointing at any specific time. This may leave important areas unmonitored and blind, creating the potential for crimes to occur and providing little or no historic video to fall back on for evidence.

Technology exists that can eliminate those blind spots and potentially reduce these types of incidents, or at a minimum record events that can lead to the apprehension of the perpetrators.



For instance, a surveillance system featuring a panoramic panomorph lens for event detection and recognition over a 360-degree by 180-degree area with 100 percent coverage provides an innovative approach with enhanced performance. This ability to capture and navigate a full-view image without distortion makes it particularly valuable to many government agencies, facilities and end-users.

Intelligent video technology, sometimes known as analytics, can also be applied directly to the native elliptical image, enabling the video camera to serve as more than just a video camera; it allows the panoramic image to follow events (such as moving objects or unauthorized behavior) in real-time, which in turn allows the operator to focus his or her activity on a narrow-field pan/tilt camera, without losing any information in the field.

Operators have the ability to navigate within the live or recorded panoramic image using standard PTZ controls provided by most DVR/NVR products. Thus, little to no special training is required to use this technology, and installation can be as simple as replacing the lens on an existing analog or IP surveillance camera and upgrading the DVR/NVR software or hardware.

Applications can be found in the fields of border surveillance, high-security environments, aerospace and defense, mass transit, public security and wherever the need for total situational awareness is a prerequisite. Actual use of this technology has already demonstrated a reduction in violent crimes, theft and other security threats. ■

Yves Messier, vice-president of video surveillance applications at ImmerVision. He can be reached at: yves.messier@immervision.com

required. That performance is simply not possible with a tape-based system.

THE NEW WORLD OF MOTION-JPEG

For video surveillance applications, motion-JPEG is probably the single most important recent development in DVR technology. Motion-JPEG is a compression technique that uses a pixel block match system, allowing minimal degradation to images with the amount of compression selected by the user. Motion-JPEG takes the original JPEG still file compression technique, originally created for use with still image distribution in the computer and print industries, and applies it to every frame or field of a video or film sequence. This leaves all frames intact and accessible. This approach is in contrast to MPEG, which handles video compression by using the difference between frames to decrease file size. MPEG does not retain every whole frame; thus frame integrity is often compromised.

So what does all this mean for law enforcement video surveillance? Since motion-JPEG focuses on areas within each frame that lack detail (such as a blue sky that doesn't change from frame-to-frame) and compresses those areas first, with the highly-detailed areas compressed last. The result is much higher image quality and image integrity. This, in turn, preserves the final details in each frame that can be so critical for identifying suspects or providing evidence in a criminal case.

CHOOSING A DVR SYSTEM

With a fairly large choice of broadcast quality DVRs on the market today, how does a police agency go about choosing a system that is ideal for video surveillance? In addition to the motion-JPEG codec, look for a system that's compact and easy-to-install in the field, and designed to withstand the rugged and often harsh conditions in which surveillance commonly takes place. For downloading and transferring video, make sure the system employs detachable storage media in a standard format which is easily available, such as off-the-shelf hard drives or compact flash. An easy-to-use interface that will accept generic power and camera inputs is also essential, as are external control capabilities to provide an interface with remote computers for control setup.

Mark Playdon is sales director for Fast Forward Video. He can be reached at: mplaydon@ffv.com

Thermal cameras for border and large-perimeter surveillance

By David Lee

For many years now, thermal cameras have proven themselves to be the best solution available for long range daytime and nighttime imaging. Today, they are a vital component in our country's round-the-clock SBInet installations.

Through dust and smog, even in the darkest nights, thermal cameras let security professionals see intruders and vehicles alike. No matter what they need to see, or where they need to see it from, thermal cameras keep border surveillance officials seeing clearly.

By detecting minute temperature differences between objects and their surroundings, and turning these temperature differences into video that can be displayed on almost any TV monitor, thermal cameras enable security professionals to see unauthorized intruders in plenty of time to react and respond.

By providing better threat detection and assessment capability -- day and night -- than comparable visible-light and infrared illuminated cameras, thermal cameras give watch standers and law enforcement personnel the time they need.

But what makes thermal cameras so much better than other technologies for long-range daytime/nighttime surveillance? The short answer is *range*. And, in this business, range equals time; time to react, time to adjust, time to respond effectively.

Thermal security cameras detect the minute differences in heat that are all around us, all the time. This heat energy is easier to detect over longer ranges than visible light, giving thermal cameras a distinct advantage. Not only can thermal security cameras see from further away, they are not vulnerable to the most common countermeasure available to someone trying to avoid detection with a camera that depends on visible light: camouflage. Why? Simply because you can't hide your heat.

Some cameras are made to see visible light at night, like so-called "infrared illuminated" and "night vision" cameras. An infrared illuminated camera was less than 50 feet from a person dressed in dark clothes on a moonless night and it came up empty. The same thing happened with the night-vision camera -- nothing. But the thermal security camera picks out the intruder easily.

The range advantage enjoyed by thermal cameras can benefit other large government installations as well. Large facilities commonly have to deal with perimeter areas that cannot be fenced or lit for practical, economic or logistical reasons. For instance, they may have miles of perimeter to cover, often along waterfront areas or across wetlands, which is impractical -- if not impossible -- to fence and light.

Thermal cameras can see far enough to make this a non-issue, and they can do it for less money than it would take to install the lighting infrastructure required for lowlight and infrared illuminated cameras.

Thermal cameras, coupled with video analytics and electronic tripwires, let security professionals monitor these areas with a "virtual perimeter" that is more affordable and just as effective as a physical perimeter in the same area.

Thermal cameras give operators clearer images with better contrast than they get from CCTV cameras. Thermal cameras give large facilities better performance, added flexibility, and greater utility by working with radars, fence sensors and analytics to improve automated efficiency and reduce responses to false alarms.

All of this comes from the thermal camera's ability to see heat, not light. Another benefit of thermal security cameras is that they see things from farther away than comparable CCTV and infrared-illuminated cameras.

Thermal cameras are an affordable, available, low-risk option for 24-hour video surveillance anywhere, any time.

David Lee is a writer and editor who has worked with thermal imaging cameras for more than 10 years. He can be reached at: david.lee@flir.com

DMS
WARNING
This Location is Protected by
a Digital Surveillance System
Netvision Mobile Surveillance
800-380-9365
netvisionmobile.com

NETVISION
Remote Video Surveillance

SONY®

Megapixel cameras that aren't afraid of the dark.

Megapixel cameras can be remarkably scared of the dark. Because their resolution comes at the cost of poor low light performance. To compensate, some rely on slow shutter speeds—which produce severe motion blur. Sony did better, carefully balancing megapixel resolution with the super sensitivity of our ExwavePRO sensor and Light Funneling. And Sony's JPEG constant-bitrate algorithm is easy on your network and your storage. So choose the SNC-CM120 with true day/night operation, SNC-DM110 mini dome or SNC-DM160 ruggedized mini-dome with day/night operation. Because crime never sleeps.

click: **sony.com/security to register for a Megapixel Webinar, and to download the latest information on new megapixel products.**

IPELA