SECURITY Technology & Design

Dispelling the Top 10 Myths of IP Surveillance

SECURITY Technology & Design

Securityinfowatch.com

AXIS COMMUNICATIONS
Make your network smarter

Future-proof video surveillance – the seamless switch.

THE SMART TRANSITION

Harsh reality is making surveillance systems based on network video the only viable alternative for meeting today's and tomorrow's security demands. Axis, the world leader in network video systems, is making it easy and cost-effective for you to make the switch.

Now you can move seamlessly into market-leading technology. Axis provides endless integration and scalability that lets you upgrade an existing system or install a new one – covering everything from network cameras and video servers to supporting software. At the pace that fits you best. The result is a reliable, future-proof IP-Surveillance system that boosts your existing infrastructure – and that's fit to meet your future needs!

www.axis.com/security

AXIS® COMMUNICATIONS
Make your network smarter

FREE! Your copy of the Axis technical guide to network video at www.axis.com/free_guide/

Top 10 Myths of IP Surveillance

By Fredrik Nilsson

The following are a series of articles looking at the "myths" that surround the world of IP surveillance. Fredrik Nilsson, general manager at IP surveillance manufacturer Axis Communications, has authored 10 articles dispelling these myths that have been published on securityinfowatch.com and in Security Technology & Design. Mr. Nilsson can be reached at fredrik.nilsson@axis.com.

Originally published on SecurityInfoWatch.com • 2005

Myth #1: IP Surveillance Is Still Five Years Away

Five years from now is an eternity in today's progressive IT industry. With the ever-changing security landscape and continued expansion of network infrastructures, IP surveillance is already upon us.

The initial migration to IP-based installations began in 1996, when Axis Communications introduced the world's first network camera. At that time, the network camera was perceived as merely a gadget for the IT-savvy. Two years later, network cameras and video servers were introduced to the security industry at the ISC West show. Even then, most industry pundits and insiders were unfamiliar with the concept of network video and more than a few were skeptical as to its viability and potential.

Now, it's difficult to find an exhibitor that does not offer an IP surveillance solution. As ASIS (American Society for Industrial Security) has noted, "It's the direction security is moving - and moving quickly - with or without us." In fact, IP surveillance has moved so quickly that it's now at our fingertips and those who wait five years will be left in the 20th century's security market.

The Past

Analog CCTV surveillance systems, i.e. analog cameras, VCRs and also DVRs, are still dominating the security market. While they previously provided unmatched benefits in the surveillance arena, traditional CCTV solutions today are an aging legacy in the security industry. Many CCTV benefits are now considered disadvantages when compared to IP surveillance solutions. For instance, the ability to centralize all surveillance monitoring was once considered a major benefit of CCTV security systems. However, today's security experts are putting increased importance on IP surveillance solutions, which can be viewed from any location in the world. In addition, expensive installation cabling, proprietary hardware for recording and extra staffing expenses have all ignited frustration with CCTV surveillance systems.

The Present

It is estimated that approximately half a million network cameras have already been installed worldwide, clearly making it a viable option in today's market, rather than a technology scheduled to be integrated in five years. IP surveillance is evolving everyday and there are countless numbers of applications for IP-based systems, which can impact an organization's security.

For example, in case of an emergency, law enforcement authorities and emergency crews arriving on the scene of a facility utilizing an IP-based security system can use the wireless modems on their laptops to log in to the system and view conditions inside the building. IP surveillance also allows for a more flexible, scalable and cost-efficient system by using off-the-shelf IT hardware such as switches and PC servers. Almost any existing security installation, from key card access to alarms, can integrate with network video technology to provide one integrated system instead of different islands for access control, video, fire and HVAC. The systems also include more intelligence down to the camera level, as well as resolutions much higher than analog CCTV systems can provide - two additional factors driving the market shift.

IP surveillance solutions such as these are currently being used in hundreds of applications across the country. But these examples are just the tip of the iceberg. Schools are taking advantage of network cameras to increase security and protect students. Government agencies are using IP surveillance for security in police departments, federal prisons and state court systems. In the wake of September 11th, many of the country's transportation agencies have turned to IP surveillance to increase their security umbrella, including Departments of Transportation (DOT), railways and airports.

According to J.P. Freeman, the network camera market is continuing to gain strength and is expected to overtake the analog CCTV camera market by 2008. As physical security continues its merge with the fast moving IT industry, savvy CSOs will realize that IP surveillance is the new security standard.

The Future Is Now

Considering the technological advancements, related market drivers and the changing security landscape, the migration to IP-based solutions will inevitably continue to expand and evolve. Companies that lead the way by using IP surveillance solutions will do more than just enjoy the ability to leverage existing infrastructure and see improvements in performance and functionality; they will gain an edge over their competitors and will be among the first to achieve a greater level of security.

Whether it's cost, performance, reliability, or any other measure, IP surveillance has proven itself to be a security solution for today and one that will grow and improve well into the future.

Originally published on SecurityInfoWatch.com • 2005

Myth #2: Network Cameras Cost More than Analog Cameras, Making IP Surveillance Too Expensive

It is true that network cameras are more expensive than comparable analog cameras. However, to get the true picture, you need to compare not only the price of the camera, but of the whole system, including cabling, recording and monitoring. Consider the fact that network cameras include functionality normally found in the DVR, such as digitization, compression and intelligence. It then becomes clear why the cost of a network camera is higher than that of an analog camera. But cameras aren't the only cost in a video system. In fact, the total IP video system cost is normally comparable and often lower than an analog camera solution with DVR recording.

In an even broader perspective, when you include installation and maintenance costs, the surveillance landscape can favor the network camera-based solution even more.

Cost Efficiencies of IP Surveillance

First, the cost of the system components must be analyzed and understood. The initial price for a network camera can indeed be higher if one compares only the camera. But compare the cost-per-channel, and the network camera with its superior flexibility and performance quickly becomes comparable with an analog system anchored by a DVR.

In many system configurations, the upfront cost for a surveillance system based on network cameras is even lower when compared to analog options. This lower total cost for the network camera system is mainly a result of back-end applications and storage that can be run on industry-standard open systems-based servers, and not on proprietary hardware like a DVR. This radically reduces management and equipment costs, particularly for larger systems where storage and servers are a significant cost portion of the total solution. Added cost savings come from the infrastructure used. IP-based networks such as the Internet, LANs and various connection methods such as wireless can be leveraged for other applications across the organization and are much less expensive alternatives than traditional coax and fiber.

Secondly, the installation cost of an IP surveillance system with network cameras compared to a DVR system with analog cameras differs a great deal. Analog video is typically transmitted by expensive coax, which rarely exists in facilities. Distance also influences image quality. Adding power inputs/outputs and audio further complicates this situation. Standard IP-based networks surmount these obstacles at much lower cost and with many more options. Like viewing website images from anywhere in the world, the network camera produces digital images, so there's no quality reduction due to distance. IP-based networking is an established, standardized technology meaning the resulting costs are comparatively low. Unlike analog systems, IP-based video streams can be routed around the world, using a variety of interoperable infrastructures. Many different streams can be transmitted over the same line because it works through packet-based communications. New construction now has low-cost Category 5 data wiring, and a single wire can carry video streams from hundreds of simultaneous network cameras when running at 1 Gigabit Ethernet speeds.

Lastly, the maintenance aspect is important to understand. The video from network cameras is recorded on standard PC servers using standard hard disks for storage. These can easily be serviced and upgraded just like any other IT equipment within an organization. Also, when higher performance or larger recording capabilities are needed, the server can be upgraded with the latest and greatest offerings from the fast-moving PC industry.

The Next Era

Respected industry analysts J.P. Freeman and Co. have forecasted that network cameras are the fastest growing segment in surveillance and will pass the sales of analog cameras in 2008. As security management over the IP network expands in understanding and implementation, it represents the next era in advanced security management. The analog camera represents a lack of flexibility and performance that does not meet the demands of this new era. As network cameras move the frame-grabbing and intelligence capabilities out and away from the DVRs, systems can scale much more easily. Customers will be able to use cost-effective industry standard servers for recording and storage, and they will be able to choose from a wide variety of video management and analytics software. This move towards open systems and away from proprietary DVRs, combined with the benefits of networking, digital imaging, and camera intelligence will constitute a strong impetus to the market's rapid adoption of the network camera and its many advantages.

Originally published in *Security Technology & Design* magazine • March 2005

Myth #3: IP Surveillance is Unproven

Whether it comes in the form of network cameras or video servers, IP surveillance is rapidly replacing and upgrading traditional analog systems. Industry analyst J.P. Freeman Co. predicts that by 2008, more than 50 percent of installed cameras will be network cameras.

When a new technology enters the marketplace, there is usually some confusion about its viability and its uses, which persists until people become educated on the technology. During this learning phase, it is common for misperceptions and myths about the technology to arise. Today there are a number of common myths surrounding IP surveillance. We've addressed two of them over the past few months on SecurityInfoWatch.com: the myth that IP surveillance is still five years away, and the myth that IP surveillance is too expensive. Now we'll examine myth #3: IP surveillance is unproven.

IP Surveillance Is Happening Everywhere

To dispel the myth that IP surveillance is unproven, you simply need to look at all the adopters of the technology. Various facilities such as schools, airports, courthouses and Departments of Transportation are switching to IP surveillance. In fact, it is estimated that approximately a quarter of a million network cameras have been installed in the U.S. alone. Here are just a few examples.

Casinos: Turning Stone Casino, located outside of Utica in upstate New York, is owned by the Oneida Nation and is one of the fastest-growing communities in the country. With more than 40 network cameras in The Tower

Health First
Holmes Regional Medical Center
Emergency
Holmes Regional Medical Center

Health First, a not-for-profit health care organization in Melbourne, FL, uses an IP surveillance system to monitor more than 100 wiring closets in its hospitals and health care facilities.

Hotel at Turning Stone, all of the hallways, elevators and stairwells are under constant surveillance. New IP surveillance technology provides motion detection capabilities that notify hotel security officers of unusual movements. In addition, many of the network cameras are equipped with PTZ capabilities, which can be controlled remotely from any computer.

Education: Canton High School, located in Jackson, MS, installed an IP surveillance system to monitor school grounds. All areas of the school, including hallways, entrances and classrooms, can be monitored at one time from on campus or from a remote monitoring location. The system prevents crime on campus because students know their behavior is being monitored. If a problem does occur, the system allows security officials to e-mail pictures directly to the police.

Health Care: Health First, a not-for-profit health care organization in Melbourne, FL, uses an IP surveillance system to monitor more than 100 wiring closets in its hospitals and health care facilities. The system helps ensure that all personnel and contractors follow documented policies and procedures for maintenance and repairs in the data distribution facilities and allows offsite technicians to assist in troubleshooting.

Transportation: The Minnesota Department of Transportation uses an IP surveillance system to give traffic updates to drivers in the Twin Cities metropolitan area. Real-time images of freeways and traffic conditions from 238 cameras are fed to the MnDOT's Web site, allowing commuters to avoid delays and dangerous conditions.

Retail: Springfield Food Court Inc. uses an IP surveillance system to simultaneously monitor all its food courts, which are located throughout several states. The system enables SFC's management to view deliveries, inventories, cash transactions, customer interactions and employee misconduct.

Clearly, IP surveillance has been proven effective in a range of environments. But it's true that IP cameras do not currently dominate the surveillance market. This leads to a related question: If IP is better, why aren't security providers selling more? The security market's structure and buying practices have a lot to do with the misperception behind this question.

Entrenched Technologies

It's clear that the shift to IP technology is inevitable. As J.P. Freeman Co. states in its latest report, "It is the direction in which security is moving, and moving quickly, with or without us." However, because IP surveillance is a relatively new technology, it requires a new mindset and knowledge base among integrators, consultants, and industry influencers in order to overcome established procedures.

Many of us remember when typewriters provided all the technology we needed and word processors seemed unnecessary. Similarly, over the last couple of years, security systems integrators have become comfortable selling and installing DVRs. Transferring from the totally analog systems with quads and VCRs, which were the bread and butter of the industry until the year 2000, was a big step. The move to fully digital systems with IP surveillance will be an even bigger step, so there is no wonder that some systems integrators are reluctant to adopt yet another new technology shift. Entrenched technologies and interests simply require time to overcome. However, there are structural market changes that are working to speed up this trend.

The Minnesota Department of Transportation uses IP surveillance to give traffic updates to drivers in the Twin Cities.

New Technology, New Players

The video surveillance market landscape is changing, and changing rapidly. New players are entering the scene on all levels.

New vendors: Axis Communications, an IT company, is market leader in network cameras; Cisco Systems is promoting IP surveillance in order to sell more switches; and EMC is selling more storage.

New distributors: Ingram Micro and Anixter, coming from the IT and structure cabling markets respectively, are also focusing on IP surveillance.

New systems integrators: IT systems integrators such as IBM Global Services see IP surveillance as having great new business potential. They see the new technology as a no-brainer, and they already have a relationship with the end user, having provided mission-critical systems.

New end users: The IT manager, CIO and CSO are now involved in the decision for procuring new video surveillance systems.

These new players will drastically influence the security industry and change the way business is conducted. Many of them believe IP surveillance is a better solution.

Why Is IP Better?

It is hard to discuss security in today's industry without mentioning the benefits of Internet protocol. In contrast to analog CCTV cameras that transmit signals only over coaxial cabling, network-enabled security cameras transmit video images over twisted-pair Ethernet cables, the same standard used in the world of IT networking. One of the main advantages of using IP as a transmission medium is that the cabling typically already exists. Alternatively, in a new system, it is normally much cheaper to install Ethernet cabling than analog cabling. Several cameras can share the same Ethernet cable, whereas in an analog scenario each camera needs a dedicated cable. Using computer networks also makes it possible for users to use standard PC servers for video management and storage. Standard equipment available off the shelf is relatively inexpensive to purchase, and it is easy to service and maintain.

Adapt to Survive

Security systems integrators must adapt and adjust to the new technology in order to survive. IP surveillance technology is proven, with products and solutions available that are far superior to analog systems anchored by DVRs, and often provide both lower costs and higher ROI. It is obvious that this shift will happen, but the technology will take some security systems integrators out of their comfort zone. However, they will need to adapt to stay competitive. Otherwise, there is an IT integrator ready to promote and install an IP surveillance system in their place.

Originally published on SecurityInfoWatch.com • 2005

Myth #4: Transferring Video Over My Network Will Overload It

IP surveillance is rapidly replacing and upgrading traditional analog systems. Industry analyst, J.P. Freeman and Co., estimates that network camera sales will exceed those of analog cameras by 2008 and that network camera sales will more than double those of analog camera sales in the network video market by 2009.

When evaluating network video technology, one of the most common arguments against it is that transferring video over a network will overload the network, causing problems with other mission critical applications on the network. There is, in fact, some truth behind this myth. Video can consume large amounts of bandwidth, affecting the overall performance of network. However, with any size network video installation, users can take a few simple steps when designing their systems to ensure that their IP surveillance systems will not overload their networks.

For instance, how much bandwidth a network camera will use depends on several factors, including image size, compression, frame rate (images per second) and resolution. Network video products will utilize bandwidth based on how they are configured. Looking at resolution, a high-resolution picture (4CIF) contains four times as much data as a normal picture (CIF). A reduction of the frame rate to half (for example, 30 frames per second down to 15) will reduce the amount of data by half as well. Additionally, because of built-in intelligence, many network cameras will only send video over the network if the video is worth recording, which might only be 10 percent of the time. Ninety percent of the time nothing is being transferred over the network.

Small Wonders

Most small-scale installations - with only a few network cameras or video servers - can operate over an existing network. Because video runs on the same network as all other data transmissions, users should configure their cameras so that high-resolution images are not running at 30 frames a second over the network at all times. This would unnecessarily use up bandwidth and slow down other applications.

A professional network camera can send up to eight Mbps (megabits per second) of data over the network, depending on compression, resolution and frame rate. In order to reduce this, users can utilize the built-in intelligence in the network camera to reduce the size and speed of images transmitted over the network. A network camera can be configured to make "decisions" about video resolution and frame rate, depending on factors such as motion detection and time of day. For example, motion detected at 1 a.m. on Saturday morning - when no one should be in the office - can trigger the camera to transmit the highest resolution video at the highest frame rate. On the other hand, motion detected at 1 p.m. on Tuesday afternoon, would be considered "normal" and would not trigger an increase in resolution or frame rate.

Enterprise Deployments

Today, there are many examples of successful network video installations with hundreds, or even thousands, of cameras. For example, departments of transportation in Minnesota and New York use video servers to digitize the feeds from hundreds of analog cameras, enabling authorities to monitor roadways and commuters to view traffic conditions. School districts are also known for large-scale network video deployments. Districts often have several campuses that are spread out over large areas, which makes network video an ideal security and surveillance solution. Often times, schools piggyback network video onto underutilized data networks or even voice over IP (VoIP) systems.

Unlike small installations, enterprise-level deployments cannot always plug directly into an existing network. These extensive installations require that users take additional steps to ensure that IP surveillance technology will not tax the network.

If the decision is made to use the existing network, then it is best to define the minimum and maximum bandwidth available for the network video system. Enterprise networks consist of multiple segments of different speeds; a connection to a switch may be anywhere from 10 to 100 Mbps, while the backbone communicating between the two switches may range from 1 to 10 Gbps (gigabits per second). A 1 Gbps network can transmit video from hundreds of network cameras, even at full frame rate, over a single network connection.

If the network video system is large enough, a separate network to handle the video transmissions will be required. This is similar to rail transportation: once the existing track becomes too congested, you simply must build another set of tracks. However, because network video operates with standard networking equipment such as switches and routers, separating networks is typically an easy and inexpensive process.

In addition to mapping out potential bottlenecks or building a separate network, enterprise users can rely on some of the following methods to better manage bandwidth consumption:

Switched networks: If many devices are connected to the same network, the network should be divided into segments with switches or routers placed in between. Switches sometimes have built-in router functions. Network switching - a common networking technique - separates one network into two autonomous networks. Even though these networks remain physically connected, the network switch divides them into two virtual and independent networks: one for data and one for video. By designing the system wisely and splitting the number of cameras between different sections or links, the user gains the benefits of higher reliability and improved performance.

Efficient compression: At high continuous frame rates, above 15 fps, considerable bandwidth savings can be achieved by using MPEG-4 compression, rather than Motion JPEG. The two formats usually target different applications, and MPEG-4 is not expected to replace Motion JPEG. However, MPEG-4 is recommended for live viewing and for applications where bandwidth and storage limitations are important factors.

Faster networks: As the price of networking equipment continues to fall, Gigabyte networks become increasingly affordable. Having a faster network alleviates bandwidth concerns, and a faster network increases the value of running security and surveillance applications over networks.

Event-driven frame rate: Full frame rate, 30 frames per seconds (fps), on all cameras at all times is more than enough for most security and surveillance applications. With the configuration capabilities and built-in intelligence of network cameras and video servers, frame rates under normal conditions can be set lower, at approximately 1-3 fps, to dramatically decrease bandwidth consumption. In the event of an alarm, the recorded frame rate speed can be automatically increased to a higher frame level.

Ultimately, a network's ability to handle the demands of a network video system depends on its configuration. It is important to take the time to consider how your network will operate when video is added and ensure that you are properly equipped to handle the extra bandwidth requirements. Although it seems intimidating at first, bandwidth issues can be easily be overcome with a little bit of advanced planning and proper configuration.

Originally published on SecurityInfoWatch.com • 2005

Myth #5: IP Transmission is Insecure for Video

One of the most pervasive misconceptions about using Internet protocol to transmit video for security and surveillance applications is that the transmission is insecure for video. Much of this fear arises from the notion that the Internet is a portal to any and all information. Additionally, there have been several major news stories about intruders accessing network cameras after finding them through Google searches.

The IP-based networks used for video are the same as the networks used by corporations, banks, governments and hospitals for transferring data, e-mail and voice over IP. These networks are safe conduits for sensitive information if the correct security measures, such as firewalls, virtual private networks and password protection, are implemented. The same security precautions need to be taken when transferring video.

There are many examples of network video installations that monitor highly sensitive activities. Network video has been used for security during the Olympic Games, in downtown Washington, DC, and at major airports and government facilities. In all of these cases, those who installed and operated the systems took precautions to ensure that video would be kept secure.

Securing a Security System

There are three important ways to ensure secure transmissions via the Internet: authentication, authorization and privacy protection.

Authentication and authorization: These first two methods go hand in hand. A device or user must identify itself to the network before gaining access, so it provides identity and access information to the network or system, like a username and password. The device or user is authenticated and authorized when the system compares the submitted information to a database of approved identities. Once the authorization is complete, the device is fully connected and operational in the system, or the user is free to use all authorized network features.

Password protecting network cameras and video servers is just as important as protecting your PC or servers. Passwords should be at least six characters long, combine numbers and letters, and mix lower and upper cases. Most network cameras support anonymous user access by default, which means that in the absence of a password, the video is made available to everyone with access to the network. If a video application needs to be highly secure, IP filtering should be used, meaning that the network camera will only send video if the request comes from a certain IP address, preventing unauthorized computers access even if they have the right username and password.

Privacy protection: Encryption prevents unauthorized users from accessing data. Two of the more commonly used encryption protocols are VPNs and hypertext transfer protocol over secure socket layer (HTTPS). A VPN is a way to use public infrastructure, like the Internet, to provide remote users with secure access to a network. The VPN essentially creates a secure "tunnel" between the end points; only authorized devices or users can operate within the VPN. The data itself is not secured, but the pathway it travels on is protected. If the data itself must be protected, HTTPS can be used. HTTPS is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. When a connection between the two devices is requested, the user or a third-party body such as Verisign verifies certificates that have been issued to the two devices. If the user or third party determines that the devices can be trusted, an encrypted communication is opened. HTTPS is commonly used when creating a connection to secure Web sites such as online banking pages.

Firewalls can serve as gatekeepers, blocking or restricting traffic to and from the Internet. They can prevent outsiders from accessing private data and control what information remote users can access.

A Safe Solution, Well Managed

Today's professional network cameras have built-in password protection, along with IP filtering and encryption, which makes them very secure. In addition, the recorded video can include the unique hardware number of the camera, called the media access control address. This confirms the origination of the video and helps make network camera technology more secure than analog. The New York State Unified Court System (UCS) is a prime example of how these security techniques can be used effectively. The UCS, which has more than 30 court buildings in New York State, uses rigid firewalls and security settings to protect its video system from hackers and other security risks. The technology team developed its own Linux-based video management software and created an advanced permissions system to allow different users access to only certain cameras. This means that images can be viewed from any courthouse PC, but only by the people who have permission to view it. For added security, the USC even opted to transmit the video over its own high-speed fiber network, rather than over the Internet.

Viruses and Worms

Network video users are frequently concerned about viruses and worms. Viruses are programming codes commonly transmitted in e-mail attachments or file downloads. While some viruses are harmless, others can erase data and can require that an entire hard disk be reformatted. A worm is a virus that automatically resends itself as an e-mail attachment or as part of a network message. A worm does not alter files but resides in active memory and duplicates itself. Often, worms go unnoticed until they slow down a system and cause errors. Most network cameras do not have an open operating system or hard disks, so worms and viruses cannot infect them. The servers that are used for video management in a network video system, called network video recorders, are standard Microsoft, Unix or Linux servers for which a virus scanner with up-to-date filters can be used. This should be installed on all computers, and operating systems should be regularly updated with service packs and fixes from the manufacturer. In an analog video system with a proprietary DVR, protective software and updates are normally not available. This makes such systems vulnerable if connected to an IP-based network.

Although making IP-based networks safe for video seems complicated, the techniques discussed above are proven methods that the IT industry has used for many years. In contrast, analog systems offer no way to authenticate or encrypt information, making it easier for anyone to tap into the cables and illicitly view "secure" video transmissions. In addition, it is possible to substitute one video stream for another, just as the band of thieves did in the movie Ocean's 11. Had Terry Benedict's security staff used network video technology, the outcome would have certainly been quite different for Danny Ocean and his accomplices.

Originally published in *Security Technology & Design* magazine • July 2005

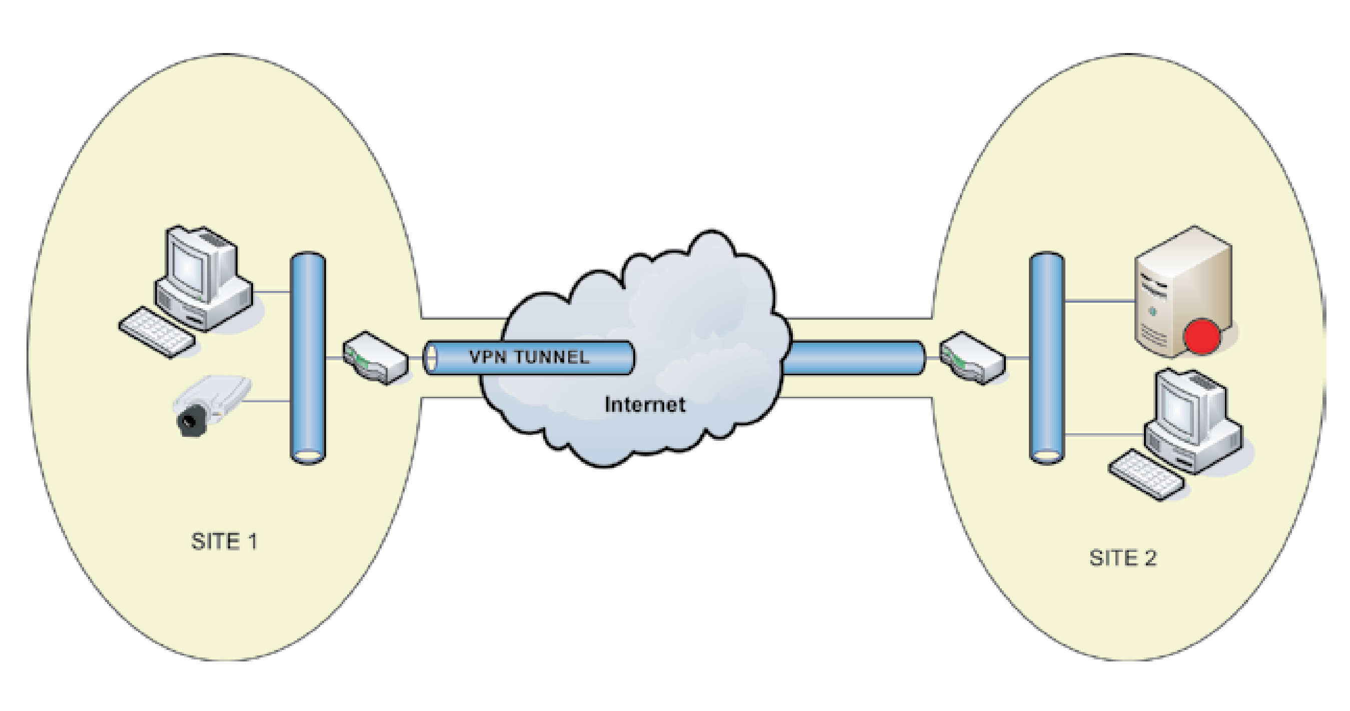
Myth #6: IP Surveillance Cannot Meet The Demands of Enterprise-Level Applications

Many security professionals believe that IP surveillance will not be able to meet the requirements of enterprise installations. The main reason given is usually the management and bandwidth required by the large number of network cameras. At an enterprise install, this could be anywhere from 50 cameras to several thousand cameras. With so many cameras, security professionals often begin to wonder how they will scale and administrate such a large camera system. Concerns such as degrading network quality with too much video traffic or managing firmware upgrades on each camera often take center stage and prevent enterprise-level installations from moving forward.

In reality, the larger the installation and the higher level of performance desired, the more competitive – and impressive – IP surveillance becomes. Because it is based on standard IT components, network video is inherently more scalable and flexible than analog systems, which are still largely based on proprietary technology. These IT standards make IP surveillance ideal for enterprise-level applications because they enable users to easily scale their networks to any size and reduce the amount of time required to maintain and monitor the system.

No Installation Too Big

One of the many advantages of IP surveillance is the scalability of the systems. Enterprise-level network video installations today regularly have 200 or more cameras. There are also several installs with thousands of cameras deployed in educational, governmental and retail environments. Such a large system would not be practical in the analog world.



A VPN creates a secure tunnel between the points within the VPN.

Exactly how does IP surveillance technology accommodate so many cameras? The answer goes back to IP surveillance's basis in IT networking. Just as e-mail systems can accommodate one user or thousands of users, so too can IP surveillance systems scale to handle thousands of cameras. Internet Protocol is the most common computer communication protocol today and is the basis for almost every newly installed network. One of the reasons it is so popular is scalability – it works just as well in small installations as it does in very large ones.

Here are a few more reasons IP surveillance systems scale much more easily than their analog counterparts:

Incremental increases: In network video systems, cameras can be added one at a time. DVR systems typically require cameras to be added in multiples of 16 or more, because of the number of inputs on a DVR. For example, if a site has a need for 17 cameras, then a second DVR box will need to be added, even though 15 of the ports will go unused.

Storage and server technology: As more cameras are added to a system, additional processing power and storage can easily be added with standard IT equipment. Servers, network attached storage (NAS) systems and storage area networks (SANs) are all reasonably priced and readily available off-the-shelf. Because network video systems are standardized with Internet Protocol, they will work with any other IP-based equipment, regardless of the vendor. This means that users will not be locked into a system from a single company, which is unlike most analog-based and DVR-based systems today.

Storage and server technology also makes it easy to back up network video systems. In fact, the servers used in IP surveillance systems are often the same as those entrusted to back up banking transactions.

Camera intelligence: Traditional analog systems are much like mainframes from the 1970s. It creates an environment in which the centralized computing power is a scarce resource that compression, recording, video management and intelligent algorithms are all forced to share. This makes it difficult to operate any video system with more than about 20 cameras and severely limits scalability.

However, today's network video systems build intelligence into the camera itself, revolutionizing video in much the same way that PCs revolutionized computing. With intelligence pushed out to the camera level, individual cameras can decide when to send video, at what frame rate and resolution, and when to send alarms. This means that users can set the camera to alert system administrators of unusual activity, for example, if movement is detected in a hallway at 3 a.m. on a weekend.

Camera intelligence also allows users to obtain more "actionable" information from their video. Intelligent video algorithms can be run at the camera level, instead of at the system level, creating an opportunity to run more advanced functions across a larger number of cameras. This makes it possible to manage and analyze video from hundreds of cameras.

Power: In an enterprise installation, network video systems are also easier to power than their analog counterparts. An IT standard called Power over Ethernet (PoE) is rapidly gaining ground in the security industry. PoE combines power and data into a single network cable, which eliminates the need for local power at the camera level and creates a simple, cost-effective solution for installing the network and power supply.

By using PoE, security professionals do not have to worry about installing power outlets at each camera location. In an enterprise application, this can save thousands of dollars in installation costs. It also means that cameras can be easily moved and that the security system can continue to operate even during a power outage, using backup power available in the server rooms.

Being a Better (Video) Manager

With so many cameras required in enterprise installations, security professionals often wonder how they can manage and administrate a system of that size. Fortunately, IP surveillance allows users a unique level of control over the system that analog systems do not.

For example, camera management software is available to simplify the administration of an enterprise network video installation. Camera management software can enable users to perform sequential or simultaneous firmware upgrades for multiple network video products and can be scaled to handle hundreds of network cameras and video servers. This allows users to manage cameras remotely without having to administer individual cameras. It also uses secure protocols to enable users to locate video products on a network, to set IP addresses and to show whether devices are reachable.

Most video management systems provide remote access to video via the Internet or a local area network (LAN). Security managers can also use the systems to control or limit other users' access. This means that some users will just be able to view video, while others will be able to make administrative changes. Most video management systems are just as scalable as the cameras themselves, by providing support to an unlimited number of users, across an unlimited numbers of cameras and facilities.

Working Together

In an enterprise installation, integrating network video with a broader security and surveillance system is often a necessity. Network video devices have an open application program interface (API), which makes it possible to integrate video with systems such as access control and intrusion detection devices from a wide range of manufacturers. Such integration is not easily done with an analog system.

For example, the Michigan State Police worked with Honeywell to design and install a security system for an off-site facility. For the installation, Honeywell integrated network video with its Digital Video Manager surveillance system and a Cisco fiber-optic network infrastructure. Because of the openness of the video system, Honeywell was also able to link the video with access control and intrusion detection data.

This integration allows video to be taken whenever an employee uses a proximity card to access restricted areas. Video of the person accessing the room can be matched against images of the actual cardholder, providing visual proof that the person using the card is authorized to do so. In addition, the Honeywell intrusion detection system notifies police when a door is left open, whether accidentally or otherwise, and the networked video technology allows them to determine whether a security breach has occurred.

When building a network video system with more than 50 cameras, IP surveillance has proven time and again that it is the easiest system to scale, manage and integrate. In fact, there is typically an easy solution for every concern regarding enterprise-level network video applications, which makes a compelling argument for the implementation of the technology.

Originally published on SecurityInfoWatch.com • 2005

Myth #7: IP Surveillance is Less Reliable Than Alternative Technologies

Although the prevalence of IP-based security and surveillance systems has exploded in the past two years, there is still a lingering concern among many security professionals that network video systems are unreliable. Most of this stems from a fear of network failure. Security professionals often worry about what would happen to IP video if the network went down, and these fears cause them to cling to analog technology.

However, IP networking architecture has been developed with reliability as a primary requirement. The stability of an IP-based video system depends in large part on the configuration of the network, and most networks today operate with a high percentage of uptime. If even minimal downtime is unacceptable, there are technologies and configurations available that can add even more reliability.

Eliminating Single Points of Failure

With an IP-based security system, points of failure can occur on several levels. The key is to avoid what IT professionals call a single point of failure. A single point of failure is a component whose failure will interrupt the functioning of an entire system. Possible points of failure include:

•**Cameras.** Network cameras today are just as reliable as their analog counterparts. However, if only one network camera is monitoring a critical area and that camera goes down, the entire surveillance system will stop functioning. This is true for both analog and IP-based environments in which systems rely on a single camera. Therefore, it makes more sense to install multiple cameras so the system will still be usable if one camera happens to go down.

The same concept applies to businesses that rely heavily on desktop PCs for employees. Although a company may require desktops for its day-to-day operations, the failure of any one desktop will not bring down the business as a whole.

Network cameras have other advantages when it comes to reliability. The main advantage is built-in intelligence, which can be used to detect interruptions in the video transmission and determine whether a lens is covered or the camera has been repositioned. Basically, the system can monitor itself and send alerts if any component is faulty.

•**Power.** Another feature available exclusively in network video systems is Power over Ethernet (also referred to as PoE or Power over LAN). PoE integrates power into a standard LAN infrastructure. It enables a network device, such as an IP phone or a network camera, to receive both data and power over the same cable. PoE is based on an IEEE standard (802.3af), which means that compatible components are available from multiple vendors, increasing choice and lowering costs for the end user. Using PoE and an uninterrupted power supply, network video devices can continue to function even in the case of a power shortage. This is not possible in an analog environment.

•**Internet Connectivity.** Internet outages are another major concern. Admittedly, the Internet goes down. Everyone knows that e-mails are occasionally lost, Web pages won't load and modems fail. These same types of outages will cause network video systems to fail if users rely on the Internet to view, share or manage video. However, such connectivity issues can be overcome through what IT professionals call aiming for the "five nines"—meaning that an Internet connection should be 99.999 percent reliable.

Today, there is a buyer's market for network connectivity, which means that the service is relatively inexpensive. If a security application cannot afford any downtime, then Internet connectivity can be purchased from two Internet service providers (ISPs). If one service fails, the network can seamlessly switch over and connect to the other ISP.

With most ISPs, the probability of an outage is only about one percent. Therefore, if you have connectivity from two 99-percent-reliable networks, the odds of a total service outage will be reduced to 0.01 percent. That equals four nines (99.99 percent) of network uptime. If that is still not reliable enough, connectivity can be purchased from a third provider.

•**Storage.** In most security applications, video is recorded and stored for later use. Storing video allows users to review incidents, isolate interesting video and distribute the information in an appropriate manner. Instead of relying on VCRs and videotapes for recordings, networked video images can be recorded on hard disks attached to standard servers. For added reliability, video can also be recorded and stored in multiple off-site locations, which is not possible with a DVR system.

One of the most common ways to back up storage systems is with a redundant array of independent disks (RAID). RAID basically arranges standard, off-the-shelf hard drives so that the operating system sees them as one large, logical hard disk. Data is divided over multiple hard drives, each with enough redundant data on all disks so that the data can be recovered from the remaining disks in case of a failure. Most common RAID systems offer full hot swappable mirrored solutions, where there is no disruption to the system and no lost data in the event of a failure.

•**Servers.** In order to back up servers, it is common to have two servers work with the same storage device, commonly a RAID system. When one server fails, the other identically configured server takes over the application. These servers regularly share the same IP address, making the so-called fail-over completely transparent to the user.

Further Considerations

A network video system uses standard server and network equipment, so replacing faulty hardware takes much less time and costs less than it does with analog or DVR solutions. Replacement parts can generally be procured from any electronics distributor, reseller or retailer, because IP surveillance is based on open standards that allow for the use of products from different manufacturers. Components such as switches, routers and servers can all be purchased off the shelf, which significantly lowers costs and increases choices. Of course, these options are up to the network designer. A small network will not deploy all of these safety measures, but choosing high-quality IT components from the start will make for a more reliable solution than a CCTV/VCR or DVR system.

In the Real World

Today, IP-based systems have proven that they are more reliable than their analog counterparts. Network video systems are successfully deployed in some of the most sensitive and demanding locations, including airports, banks, train stations and prisons. In many cases, the cameras can function for years without being touched. Both network and PC reliability have also come a long way. Banks, government agencies and Fortune 100 companies all rely on IT equipment for e-mail, data, and increasingly for voice and video.

For example, a federal penitentiary in California installed a network video system to monitor inmates and provide evidence in the criminal prosecution of inmate crimes. The network cameras and video servers allow high-quality digital images to be recorded throughout the prison on a 24-hour basis, which enables the prison to maintain a greater level of security and surveillance within prison grounds. In the private sector, a New York casino selected an IP surveillance system to monitor its hotel, garden, restaurants, parking garages and exhibition hall. The casino's existing analog surveillance system needed to be upgraded, so the company turned to network video and PoE to provide uninterrupted surveillance.

Ultimately, the reliability of a network video system can be as simple or as sophisticated as you want it to be. IP networks are flexible, and they are the key to wide-ranging possibilities in system design, applications and solutions. Using the benefits of IP networks, network video systems offer many advantages over analog-based CCTV systems. The answer to creating a reliable system is making well-informed decisions during the installation process and properly configuring the network.

Originally published in *Security Technology & Design* magazine • September 2005

Myth #8: DVRs are the Latest and Greatest in CCTV Technology

Eastchester Union Middle School Principal Dr. Walter Moran uses the networked video system to give him direct access to the school's surveillance cameras, all while at his office's PC. The school used extra bandwidth from their Voice of IP (VoIP) network to pipe video from cameras to servers and web-based monitoring stations.

With little fanfare or notice, it's become a digital world. Many of the products we use every day - from cars, microwaves and music players - incorporate digital technology. In the world of security, this shift is also taking place. However, many security professionals believe that digital video recorder (DVR) technology is the most advanced form of digital technology available in the security industry.

However, stopping with DVR technology for security would be the equivalent of the music industry stopping with the CD player. Just as MP3 players offer more functionality than CD players, DVR technology has limitations when compared to truly digital surveillance systems.

Innovation has continued beyond the DVR, and a viable, cost-effective alternative has emerged in IP surveillance. IP surveillance has all the functionality of a DVR and allows users even more performance benefits. In its simplest form, it is video transferred over IP infrastructure - a surveillance concept that is fully digital.

The Digitization of CCTV Technology

Over the past few years, digital technology has become more and more integrated into CCTV systems. DVRs now constitute 80 percent of new CCTV systems. While it is true that DVRs improve upon solely analog systems by adding a digital element, they do not represent an all-digital network technology. End users have started to realize this and some security professionals recognize that DVRs represent just one more step in the digital evolution of surveillance systems.

The DVR is actually a hybrid technology - it is part digital and part analog. DVR systems incorporate digital technology, but maintain the use of coaxial cables. This creates a system where an image is sent over analog cabling, digitized at the DVR, and then presented at a designated viewing station. This processing of the images causes a loss in quality and slows performance. Network cameras and video servers have eliminated this by making the link from the camera to the recorder digitized, using standard computer networks, the Internet, or wireless technologies.

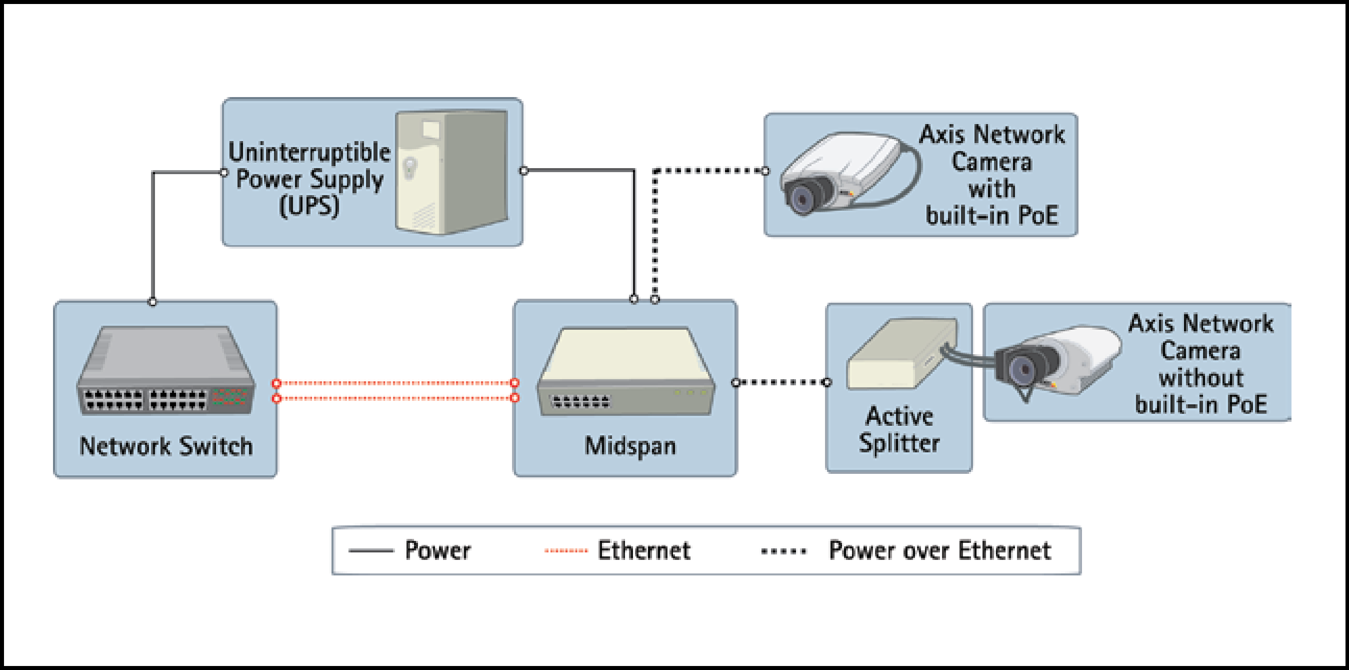
Advantages of IP Surveillance

DVR systems have distinct advantages over a solely analog system, including the elimination of videotapes, consistent recording quality, access to recorded video over IP networks, and more efficient searches for recorded events. However, IP surveillance systems offer all of these same advantages and more:

Scalability: IP surveillance allows users to scale the system from one camera to thousands of cameras in individual increments. In comparison, DVRs usually require users to increase in 16-channel jumps, even if only one additional camera is actually added to the network. This makes IP surveillance a better choice for installations that may need to ramp up in size. For example, the Sooper Stop convenience store in West Fargo, N.D., installed just four network cameras to secure its facility while the New York State Unified Court System installed more than 300 network cameras.

Intelligence at camera level: In DVR systems, most of the "action" takes place within the DVR, including compression, recording and video management. This creates a shortage of computing power and makes it difficult to run intelligent video applications. However, fully digital systems decentralize applications by pushing intelligence out to the camera level, much as PCs did with mainframe computing. Built-in event handling, sensor input, relay output, video motion detection, time and date, and other capabilities allow network cameras to make decisions on when to send alarms and to whom, when to send video, and even at what frame rate or resolution to send the video.

Cost-efficient infrastructure: Most facilities are already wired with networking cables, so no additional wiring is required with IP surveillance. CCTV systems require separate wiring, which can be a major expense. The computer network is also used for applications such as


Uninterruptible Power Supply (UPS)
Axis Network Camera with built-in PoE
Network Switch
Midspan
Active Splitter
Axis Network Camera without built-in PoE
Power
Ethernet
Power over Ethernet

A PoE setup with an uninterruptible power supply.

data and voice, so IP surveillance can be easily integrated and managed along with other systems. As an additional bonus, some network cameras offer a Power over Ethernet (PoE) option, which allows users to power cameras through the network and eliminate the wiring needed for electrical outlets.

These benefits are particularly important for facilities that need to be cost-conscious. For example, the Eastchester Union Free School District in Westchester, N.Y. was able to set up a network video system using the infrastructure and extra bandwidth from its voice over IP (VoIP) network.

"By piggybacking the video network onto the voice network, we were able to save significant amounts of time and money," explains Anita Better, the school district's director of information technology. "The network cameras are so bandwidth efficient that the video does not slow down or degrade the voice network."

Eastchester Union Middle School Principal Dr. Walter Moran uses the networked video system to give him direct access to the school's surveillance cameras, all while at his office's PC. The school used extra bandwidth from their Voice of IP (VoIP) network to pipe video from cameras to servers and web-based monitoring stations.

Image quality: Image quality is clearly one of the most important features of any camera, if not the most important. Using progressive scan and megapixel resolution, network camera technology has recently surpassed the image quality of analog cameras, allowing users to more closely follow details and changes in images. This is particularly important with rapidly moving objects, where interlacing problems with analog cameras cause objects to blur.

Two-way audio: Besides being able to observe events from any computer via the Internet, there are also products that enable two-way audio communication over networks. This allows users to integrate audio with their IP surveillance systems so that they can hear and speak through the network. With both visual and audio communication, users can observe, hear and question intruders.

Equipment upgrades and replacements: IP surveillance is based on open networking standards, not proprietary equipment like DVRs. This means that standard IT server and storage architecture from any vendor can be used, which reduces wait times and simplifies upgrades and replacements. By comparison, DVRs are difficult to upgrade because it requires replacing proprietary digitizer boards.

Contrary to some popular opinions, the DVR is not an end-point solution, but rather one advance in the continuing development of CCTV technology. As the marketplace assesses DVRs more carefully, it is emerging that the DVR provides only a few benefits of digital technology. While this option will work in the short-term, digital systems allow the user much more flexibility and control in the long-term. IP surveillance technology has quickly proven to be superior to DVR technology. There is an enormous difference between the two technologies and the marketplace is only just beginning to understand this critical point.

Smallest Network Camera

Axis Communications has launched the AXIS 207 Network Camera, a bandwidth-efficient network camera that uses MPEG-4 image compression to provide the best image quality of any camera in its class. At about the size of a deck of cards (approximately 2 x 1 x 3 inches), the AXIS 207 is the world's smallest MPEG-4 network camera. It is designed for indoor surveillance and remote monitoring applications and is ideal for securing small businesses.

Originally published on SecurityInfoWatch.com • 2005

Myth #9: If I Already Have Analog Cameras, DVRs Are My Only Option

Although some digital video recorder (DVR) providers may tell users it is not possible to deploy IP surveillance after analog cameras are installed, video server technology is rapidly smashing this myth. In fact, many IP surveillance installations today combine network cameras and analog cameras that are networked via video servers.

Similar to a DVR, a video server (or video encoder) makes a digital system possible without having to discard existing analog equipment. However, a video server converts the analog video signal into a digital video stream so that it can be transmitted over the computer network, rather than over a separate coaxial network.

Under the Hood: Video Server Technology

A video server typically has one to four inputs for analog cameras, as well as an Ethernet port for connection to the network. The video server can either be located in a rack-mounted version in a server room if all coaxial cabling already exists, or be placed close to the analog camera. Like network cameras, it contains a built-in Web server, a compression chip, network and serial interfaces, and an operating system. These components enable incoming analog video to be converted into digital video, transmitted over the computer network, and then recorded and stored on standard PC servers.

Analog cameras of all types, such as fixed, dome, indoor, outdoor, fixed dome, and even pan/tilt/zoom can all be integrated into a network video system using video servers. Once the video is digitized and on the network, it is identical to a video stream coming from a network camera. Simply put, a video server turns an analog camera into a network camera. Video servers also allow users to control digital inputs and outputs, audio, serial ports, and pan/tilt/zoom (PTZ) mechanisms from any location using a standard PC.

The Future of Digital: DVRs vs. Video Servers

Video servers create truly networked surveillance systems while DVRs are just one step in the ongoing digital evolution of CCTV systems. Analog systems using DVRs are still analog systems; however video can be digitally viewed and recorded. In a DVR, videotapes are replaced with hard drives, which require the video to be digitized and compressed at the DVR level in order to store as much video as possible. Even networked DVRs - which incorporate an Ethernet port for network connectivity - do not provide the same functionality as a system utilizing video servers.

Today, many cutting-edge security integrators and resellers are recognizing these facts and will no longer recommend DVR technology to their clients. For example, David Ly, CEO of IntelaSight Corporation, has worked with DVRs in the past but found the functionality is too limited.

“Even with a network connection, DVRs offer only partial digital conversion and mediocre software support, which limits our ability to offer top-quality services,” said Ly. “Although DVRs are more convenient than VHS tapes, there is no way we can continue to support this technology, particularly with large installations. DVRs simply can’t handle advanced applications like intelligent video or centralized remote monitoring services, and they restrict our customers to proprietary hardware systems.”

By contrast, video servers are much more flexible and offer a range of monitoring and surveillance capabilities that will make them a viable option five or even 10 years down the road. Some of these reasons include:

Ease of management and maintenance: Because video servers use standard PC servers for video recording and management, they are easy to integrate with existing IT systems and managed as part of that infrastructure. Video servers allow the video to be stored on computer hard drives which are easily expandable and can be easily repaired or replaced in case of failure. By contrast, DVR systems require proprietary hardware, which is more costly and difficult to replace or upgrade. Also, DVRs can rarely be used with standard virus protection packages, which is another major consideration in most IT environments today.

Expandability: Although both video servers and DVRs leverage existing investments in analog cameras, only video servers make total use of network infrastructure. This is particularly important when expanding the network video system, as an IP surveillance system is expandable in increments of one camera. A DVR on the other hand, is more difficult to expand. Once the capacity of a DVR is maximized, an entire new DVR box (usually with 16 or more channels) needs to be added to the system, even to accommodate one or two cameras.

Wireless Functionality: Unlike DVRs, video servers allow users to create a wireless system. These systems can be expanded easily without the need to run additional coaxial cabling. This allows cameras to be placed in remote or difficult-to-reach locations that cannot be wired with coaxial cabling. For example, wireless transmission is useful in classified buildings, where the installation of cables would not be possible without damaging the interior. Wireless is also beneficial when camera locations need to changed frequently or when two sites need to be bridged without investing in costly ground infrastructure.

Audio: While audio is now possible in a DVR system, it is much more cumbersome than with IP surveillance. DVRs create a system where audio is routed back to the DVR itself, while video servers allow the audio to be accessed from anywhere on the network. This allows users to communicate with visitors or intruders from any computer connected to the network.

Future-proof: Video servers decentralize the digitization and compression functions found in DVRs. This helps process video faster because more information is handled at remote locations. It also opens the door for up-and-coming applications like intelligent video, which can be used in identifying abandoned luggage at an airport or reading a license plate number in a parking garage. A DVR cannot handle such applications because video is digitized and compressed in one location, creating a system in which centralized computer power is a scarce resource that cannot handle additional functions.

Video Servers in Action

Video servers are often used in professional security systems and enable live video to be viewed remotely by authorized personnel. Easily integrated into larger, complex systems, video servers can also function as stand-alone solutions in entry-level surveillance applications. Video servers can connect to the existing IP-network and enable real-time updates of high-quality video accessible from any computer on the network. Sensitive locations can be remotely monitored in a cost-effective and simple way, over the LAN or Internet.

For example, video servers have been used in installations as large as Sydney Airport’s international terminal in Sydney, Australia, and in those as small as Canton High School in Canton, Miss. The airport used video servers to network hundreds of analog cameras, while the high school used the same technology to network just 24 cameras. Despite the difference in installation size, both end users were able to use the video server technology to improve their monitoring capabilities and now have the option of easily sharing video with the proper authorities via the LAN and the Internet.

Jim Walker, vice president of CameraWATCH, the company that installed the IP surveillance system for Canton High School, believes that the biggest benefit of video servers is the ability to view images in real time over the Internet.

“It’s better than having a security guard at the school because a security guard can only see what is around him, and we can see all areas of the school at one time,” said Walker. “The video servers also allow us to e-mail pictures to the police so that in case there is a problem, they know exactly what to look for.”

For users searching to migrate from an existing analog CCTV system to the digital world, video servers provide a cost-effective, future-proof solution that goes beyond the functionality of DVRs. As IP surveillance continues to evolve, integrators will increasingly find that DVRs simply cannot meet client demands and fall short of a truly digital system.

Originally published on SecurityInfoWatch.com • 2005

Myth #10: Network Video Image Quality is Not as Good as Analog

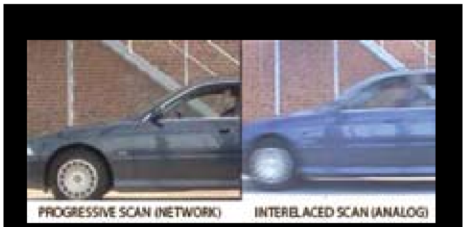


Illustration 1: Both progressive scan and interlaced images can produce a clear image of the static background. However, only progressive scan makes it possible to identify the driver in a motion situation.

Image quality is one of the most important features of any camera. This is especially true in security, surveillance and remote monitoring applications, where lives and property may be at stake. While analog cameras are often thought to have higher image quality than network cameras, this is a myth. Advancements have been made in the past few years that have allowed network cameras' image quality to equal - and in some cases surpass - that of analog technology.

When comparing network and analog cameras, it is best to look at professional, high-quality network cameras. Professional network cameras should not be confused with lower-end network or Web cameras used for Web attraction applications. These cameras cannot deliver the same image quality required for security and surveillance applications. However, even in professional network cameras, image quality can vary considerably and is dependent on several factors such as the choice of optics and image sensors.

Image Sensors

A good image sensor and optics are the most important factors in providing high quality images. Network cameras now have image sensors and optics that are the same as or better than those used in analog security cameras, and network cameras now can make use of progressive scan and megapixel sensors that are not available to analog technology.

The image sensor of the camera is responsible for transforming light into electrical signals. When building a camera, there are two possible technologies for the camera's image sensor: a Charged Coupled Device (CCD) or a Complementary Metal Oxide Semiconductor (CMOS). Analog cameras utilize only CCD sensors, while network cameras can be produced with both types of sensors. This provides further flexibility for optimizing the network camera to fit the installation.

CCD sensors use a technology developed specifically for the camera industry. They are more light sensitive than other sensors, which means they produce better images in low-light conditions. CCD sensors typically are more expensive and more complex to incorporate into a camera because they produce an analog signal that needs to be converted into a digital signal.

CMOS sensors are based on a standard technology that is already used extensively in memory chips, such as those inside of PCs. Recent advances in CMOS sensors bring them closer to their CCD counterparts in terms of image quality. CMOS sensors tend to cost less than CCD sensors and contain all the components needed to generate digital signals. Eliminating the digital conversion process has also made it possible to produce smaller network cameras because fewer components are required.

The Interlacing Issue

At a high 4CIF resolution, the clarity of rapidly moving objects - such as a person running or speeding car - has long been problematic in security and surveillance applications. In an analog environment, a rapidly moving object will appear blurry. This is because an analog video signal, even when connected to a DVR, interlaces to create the images. Interlaced images use techniques developed for analog TV monitor displays, made up of visible horizontal lines across a standard TV screen. Interlacing divides these into odd and even lines and then alternately refreshes them. The slight delay between odd and even line refreshes creates some distortion - only half the lines keep up with the moving image while the other half waits to be refreshed. This causes moving objects to blur (see Illustration 1).

A network camera, on the other hand, uses progressive scan technology to capture moving objects. Progressive scan captures the whole image at one time, and scans the entire picture line by line every 1/16th of a second. This eliminates the delay between odd and even line refreshes and prevents the picture from being split into separate fields. Images from network cameras are also displayed on computer monitors. Unlike TV screens, computer monitors do not interlace. They display images one line at a time in perfect order, so there is virtually no “flickering.”

Resolution

Analog and digital resolution are similar, but there are some important differences in how each is defined. In analog video, the image consists of interlaced lines since, as described above. In a digital system, the picture is made up of picture elements, also called pixels. No matter which system is used, higher resolution provides more visible detail. This is a very important consideration in surveillance applications, where a high-resolution image can enable a license plate to be read or a person to be identified.

When analog video is digitized, the maximum amount of pixels created is dictated by the number of available TV lines. Based on NTSC standards, the maximum resolution of an analog system is 400,000 pixels, or 0.4 megapixel, once the video is digitized by a DVR or video server.

Network camera technology renders NTSC resolution irrelevant and makes higher resolution possible. Network cameras today produce images that are at least one megapixel in resolution, which is 2.5 times higher than the best analog image. Cameras with two and three megapixel resolutions are also available.

Even with megapixel resolution it is still possible to generate lower-resolution images in order to save bandwidth. In this case, low resolution images are sent over the network until a trigger prompts the camera to send images with more detail. That way, the most significant images are presented with the highest possible level of detail.

In addition to providing clearer images, megapixel network cameras also provide different aspect ratios. Standard TVs use a 4:3 aspect ratio, while movies and wide-screen TVs use a 16:9 ratio. The advantage of 16:9 is that the upper and lower parts of most images take up pixels, bandwidth and storage space, but do not contain critical information.

Image Degradation

When an analog installation is spread out over a long distance, the length of the cable will influence image quality. The further a user is from the video source, the lower the image quality becomes. However, IP surveillance does not have these types of problems. Viewing video from a network camera is just like viewing images from a Web site. The network camera produces digital images, so there is no quality reduction due to physical distance.

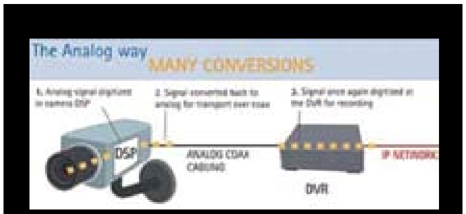

The Analog way
MANY CONVERSIONS
1. Analog signal digitized in camera DSP
2. Signal converted back to analog for transport over coax
3. Signal once again digitized at the DVR for recording
DSP
ANALOG COAX CABLING
DVR
IP NETWORK

Illustration 2: Analog cameras can feature many image conversions. First, the analog signal is digitized in the cameras DSP. Second, the signal is converted back to analog for transport over coax. Third, the signal is once again digitized at the DVR for recording. Every time an image is converted from analog to digital or vice versa, image quality can be lost.

Also, IP surveillance images are digitized once, and then stay digital throughout the transportation and viewing processes. When converting analog video signals to digital through a digital video recorder or other device, the image must go through several conversions from analog to digital, or vice versa. With each conversion, quality can be lost (see Illustration 2).

Network video resolution has steadily increased over the past few years. Now that technology developments have allowed network cameras to feature the same or better image quality as that of analog technology, the security market has a strong incentive to push ahead into the digital future.

Reprinted with permission from *Security Technology & Design* magazine and www.SecurityInfoWatch.com • 2005