10 Steps to a Successful IP Surveillance Installation
ALL THIS IS JUST ONE MAN'S RESPONSIBILITY. Guess who he calls about video surveillance?

Big security responsibility? Axis delivers scalable, well-proven network video solutions that offer outstanding video surveillance and monitoring capability, combined with exceptional flexibility that keeps costs down. Axis was first to bring the benefits of network video technology to video surveillance applications. Today we have the world’s largest installed base of network video products, driving the shift from analog to IP-based solutions. And we work with an extensive network of CCTV and IT industry partners to create the perfect video surveillance solution for your present and future needs. We help you manage the responsibility, no matter how big it is.

It’s what you can expect from Axis – the global leader in network video.

www.axis.com
The following are a series of articles looking at the steps to a successful IP surveillance installation. Fredrik Nilsson, general manager at IP surveillance manufacturer Axis Communications, has authored 10 articles on how to successfully install an IP surveillance system that have been published on securityinfowatch.com and in Security Technology & Design. Mr. Nilsson can be reached at fredrik.nilsson@axis.com.

Intro: Starting a Major Video Project? Steer Clear of the Pitfalls and Find the Smooth Route by Using the following 10 Steps to a Successful IP Surveillance Installation........pg. 4

Step #1: From Image Quality to Progressive Scans and APIs, What You Should Consider when Choosing a Camera........pg. 5

Step #2: MPEG-4, Motion JPEG, MPEG-2, License Feeds, Bit Rates and More: What It All Means.....................pg. 6

Step #3: What to Look For in a Video Management System, Plus How Open and Closed Systems Differ...............pg. 8

Step #4: Understanding IP-based Video Storage and Server Systems, Plus How to Calculate Storage Needs........pg. 10

Step #5: Incorporating Analog Cameras with Video Servers........pg. 13

Step #6: Wireless Networking Options for Surveillance Video Transmissions............................pg. 14

Step #7: Designing the Network........................................pg. 16

Step #8: Security.............................................................pg. 18

Step #9: Hot Technologies Defining IP Surveillance: Intelligent Video, Megapixel Cameras and Immersive Imaging.....pg. 20

Step #10: Best Practices for IP Surveillance Projects................pg. 22
Introduction: Starting a Major Video Project? Steer Clear of the Pitfalls and Find the Smooth Route by Using the Following 10 Steps to a Successful IP Surveillance Installation

As IP surveillance is quickly becoming the most flexible and future-proof option for security and surveillance installations, it is important for users to understand common pitfalls, customization options and the advantages of a fully digital system.

Starting with the first step in February and continuing through November - and published jointly via SecurityInfoWatch.com and in Security Technology & Design magazine -- we will examine 10 steps that security professionals can take in order to implement a successful IP Surveillance system. These include:

**Step 1: Choosing a network camera**

It is important to select cameras that meet the needs of your organization and installation. This includes cameras that can be pan/tilt/zoom, vandal-proof, weather-resistant, or fixed-dome products. Each type of camera can be blended into an IP Surveillance system to create a total package that solves your security needs. Also, we have to consider that not all network cameras are created equal. Some low-cost network cameras may look appealing at first, but security professionals need to understand how the components of a network camera affect the camera’s performance and durability.

**Step 2: Compression**

All digital video surveillance systems use some type of compression for the digital video. Without effective compression, our networks would grind to a halt due to the size of the video files. Selecting the right compression is vital, and includes choices between proprietary or industry standard modes such as Motion JPEG or MPEG-4. Compression can also determine whether video is admissible in court cases, an important consideration for security and surveillance installations.

**Step 3: Video Management**

These days, video systems can evaluate situations and take the appropriate action, rather than just passively recording video. Video management tools are dependent on the application and many factors have to be considered. We’ll look at considerations of available bandwidth, storage capabilities, scalability, frame-rate control and integration capabilities.

**Step 4: Storage**

The ability to use open storage solutions is one of the main benefits with IP surveillance. Considerations when determining storage requirements include frame rate, the amount of time the video needs to be stored, the required redundancy, and which type of storage that fits best, e.g. a storage area network, or network attached storage.

**Step 5: Incorporating Analog Cameras**

So you have analog cameras? These also can be integrated into a network video system using video servers. The analog camera is simply connected to a video server, which digitizes, compresses and transmits video over the network. Many times, this is useful in reducing installation costs because older equipment can continue to be used. However, there are instances in which it is not sufficient to simply convert an analog camera video stream into digital due to limitations in video quality.

**Step 6: Wireless Networking**

Sometimes wireless solutions are the best and most cost-effective option for security and surveillance installations. For example it could be useful in historic buildings, where the installation of cables would damage the interior, or within facilities where there is a need to move cameras to new locations on a regular basis. The technology can also be used to bridge sites without expensive ground cabling.

**Step 7: Designing the Network**

Each network design will be specific to the needs of the user and the specified installation. Beyond the actual cameras, it is important to consider IP addressing and transport protocols along with transmission methods, bandwidth, scalability and network security. In this article, we’ll touch on all of those issues - before you encounter them.

**Step 8: Security**

Securing video is one of the most important steps in creating a successful IP surveillance installation. Nearly all security and surveillance applications contain sensitive information that should not be available to anyone with an Internet connection. Understanding and choosing the right security options - such as firewalls, virtual private networks (VPNs) and password protection - will eliminate concerns that an IP surveillance system is open to the public.

**Step 9: Hot Technologies**

Today far more video is being recorded than anyone could ever monitor or search. Therefore, the next big trend in IP surveillance is intelligent video. Advanced network cameras can have built-in motion detection and event handling. In addition, more intelligent algorithms - such as number (license) plate recognition, people counting -- are being integrated into security and surveillance systems. Network cameras and intelligent video have important synergies that make the systems more reliable and effective than those with a digital video recorder or other centralized system.

**Step 10: Best Practices**

Over the last few years, thousands of IP surveillance systems have been installed, and many lessons have been learned. These range from simple tips about camera placement and lighting conditions to working with IT departments and technicians to determine issues such as the peak times for network usage. As we close the series, we’ll touch on these concerns.

By the end of this article series, these 10 steps will enable any security professional to avoid pitfalls and implement best practices, making IP surveillance installations easier to install and manage.
When building a surveillance system, it is important to select cameras that meet the needs of your organization and installation. This includes selecting specific types of cameras to meet the locations where cameras are needed and the intricacies of the venue, including fixed, pan/tilt/zoom (PTZ), vandal-proof, or fixed-dome cameras.

There are all types of network cameras available today, and no matter what your needs are, a network camera is available to meet them. Although analog cameras are available in a similar variety, network cameras are now offering added benefits, including better image quality and more installation flexibility. And for some special applications, such as very high-resolution needs, or wireless, network cameras are the only option.

Selecting the right network camera is a critical for the success of your surveillance system. For example, retail environments will have different needs than schools or highway systems, and every installation has some features that are more important than others. Some may value off-site recording and storage over other features such as Power over Ethernet (PoE) or alarm management.

Off-site recording was particularly important to Todd Jacobson, the owner of a Citgo Super Stop in North Dakota. Within three weeks of installing a network video system, his convenience store was robbed. However, because the video was stored off-site, the thief was unable to steal the video tape during the robbery, as is common with traditional analog CCTV systems. Because of the high image quality and the offsite recording, police were able to identify and apprehend the perpetrator within four hours and Jacobson recovered all of the losses from the robbery.

This example also indicates that not all network cameras are created equal. If Jacobson had been using a low-end network camera, it is possible that image quality wouldn't have been good enough to help the police identify the thief. There are many components that go into creating a quality network camera, and security professionals need to understand how these components affect the camera's performance and durability.

**Image quality** — Image quality is the most important feature of any camera. This is particularly so in surveillance and monitoring applications, where lives and property may be at stake. Superior image quality enables users to more closely follow details and changes in images, making decisions faster and faster decisions. It also ensures greater accuracy for automated analysis and alarm tools, such as object recognition.

When assessing image quality be sure to research the following factors: light sensitivity, the crispness of moving objects, and the clarity level. A camera's datasheet will include part of the story, but it is a good idea to field test a few cameras before making a decision. In addition, there are some simple steps you can take to ensure high quality images - use enough light, avoid backlight and reduce contrast whenever possible.

It is also critical to take into account the location of the cameras, especially if the cameras will be used outdoors. An auto iris lens, which automatically adjusts the amount of light that reaches the image sensor, should always be used for outdoor applications. Direct sunlight should always be avoided. Mount the camera high above the ground to avoid a contrast effect from the sky. If the camera is mounted behind glass, the lens must be placed close to the glass to avoid reflections. If the camera will be used at night, an infrared (IR) camera should be used generate high quality images in very low light conditions.

**Power over Ethernet (PoE)** — In most buildings today, TCP/IP infrastructure is available by means of Cat 5 and 6 cabling. The cabling can be used for fast transport of data, and the distribution of power to devices connected to the network, using PoE technology. PoE reduces installation costs by eliminating the need for power outlets at the camera locations and enables easier application of uninterruptible power supplies (UPS) to ensure continual operation, even during a power outage.

PoE technology is regulated by the IEEE 802.3af standard and is designed to not degrade the network data communication performance. When evaluating PoE-enabled network cameras, it is important to look for those that are based on the IEEE standard, to ensure that any brand network switch can be chosen, providing a truly open system.

**Progressive scan** — Progressive scan capability is found only in network cameras, but not all network cameras have this functionality. Progressive scan involves exposing and capturing the entire image simultaneously, as opposed to analog interlaced scanning which is the exposing and capturing of only half of the lines in the image and then the other half 17msec later. With interlaced scanning, if an object is moving the image will become blurry. In a progressive scan image all lines are scanned in perfect order so there is virtually no “flickering” effect.

While interlaced scanning may be sufficient under certain conditions, progressive scan technology allows for far better image quality on moving objects. In a surveillance application, this can be critical in enabling the user to view detail within a moving image such as a person running away or the license plate on a moving vehicle. When cameras capture moving objects, the sharpness of the frozen images depend on the technology used, and progressive scanning consistently produces the best results in clarity and recognizing important details.

**JPEG/MPEG4 standards** — It is important for any network camera to follow JPEG and MPEG-4 standards in their entirety. Many vendors claim compliance with a standard, but do not adhere to that standard 100 percent. Full adherence ensures the flexibility to use video for many different applications. It also guarantees that you can view the video many years from now. If a camera uses one company’s proprietary compression technology and that company goes out of business, the video will be unreadable in the future. Also, if a company is following the MPEG-4 standards, ask if the licensing fees are paid, and how many licenses are included with each product. Proprietary compression technologies are also not always admissible in court, an im-
Important consideration for security and surveillance applications.

Extensive support of Video Management Applications — The security industry migration to network video includes the use of open systems and platforms. Make sure to select a network camera that has open interfaces (an API or Application Programming Interface), which enables a large variety of software vendors to write programs for the cameras. This will increase your choices in software applications and will ensure that you are not tied to a single vendor. Your choice of network camera should never limit vendor options and functionalities.

Vendor history and focus — It is important to make network camera decisions based on estimations of future growth and the need for added features and functionality. This means your network camera manufacturer is going to be a long-term partner. It’s important to choose a solid partner, so be sure to look for a company that has a large installed base of cameras, is profitable, focuses on network camera technology, and offers you local representation and support. You want to choose a camera from a vendor where the innovation, support, upgrades, and product path will be there for the long term.

Just like with analog cameras, not all network cameras are created equal. Far from it, and the differences among network cameras are greater and more significant than buyers have experienced with analog technology. The end user has to be smart. Vendors will tell a lot of great sounding stories, but the user has to have a solid list of evaluation criteria, test the different choices, and understand the differences between the available products.

### Network Camera Check List Suggestions

- **Lens**: f2.0 and auto iris for outdoor applications
- **Image sensor**: Progressive scan CCD image sensor or high quality CMOS
- **Resolution**: 640x480
- **Frame rate**: 30 frames per second
- **Video formats**: MJPEG & MPEG4 at Advanced Simple Profile level 5
- **Power over Ethernet**: 802.3af compliant
- **Audio**: G.711 or AAC-LC format
- **Software compatibility**: Open API supported by many Network Video Recorder software developers
- **Security**: Multi-level user name/password protection minimum and IP filtering and HTTPS for high security requirements
- **Management**: Built in web interface and multi-camera management application

---

**Step #2: MPEG-4, Motion JPEG, MPEG-2, License Fees, Bit Rates and More: What It All Means**

Every digital video surveillance system uses compression in order to manage file size when transporting video over the network for storage and viewing. Bandwidth and storage requirements render uncompressed video impractical and expensive, so compression technologies have emerged as an efficient way to reduce the amount of data sent over the network. In short, compression saves money.

Today there are many kinds of compression available. Compression technology can be proprietary - invented and supported by one only vendor - or based on a standard and supported by many vendors. Selecting the right compression is vital to ensuring the success of a video surveillance installation. It provides the appropriate quality at the budgeted cost and ensures the system is future proof. Selecting the right compression can even determine whether video is admissible in court cases, an important consideration for security and surveillance installations.

**Compression Terminology**

The effectiveness of an image compression technique is determined by the compression ratio, calculated as the original (uncompressed) image file size divided by the resulting (compressed) image file size. At a higher compression ratio, less bandwidth is consumed at a given frame rate. If bandwidth is kept consistent, the frame rate is increased. A higher compression ratio also results in lower image quality for each individual image.

[See Images A, B, C and D to compare how different compression formats can affect your final image quality.]

There are essentially two approaches to compression: lossless or lossy. In lossless compression, each pixel is unchanged, resulting in an identical image after the image is decompressed for viewing. Files remain relatively large in a lossless system, which makes them impractical for use in network video solutions. A well-known lossless compression format is the Graphics Interchange Format, better known as a .GIF image.

To overcome these problems, several lossy compression standards have been developed, such as JPEG and MPEG. The fundamental idea in lossy compression is to reduce portions of the image that appear invisible to the human eye, thereby...
A Note on Still Images

Video is essentially a stream of individual images. The most widely accepted standard for still image compression is the Joint Photographic Expert Groups (JPEG) standard. It was developed in the 1980s and has been integrated into standard Web browsers. JPEG decreases file sizes by making use of similarities between neighboring pixels in the image and the limitations of the human eye. Other lossy image compression techniques include JPEG2000 and Wavelet. JPEG is by far the most common and most widely supported compression standard for still images.

Motion JPEG is the most commonly used standard in network video systems, however it is technically a still-image compression technique. When employing Motion JPEG compression, network cameras capture individual images and compress them into JPEG format - similar to a still picture - and there is no compression between the individual frames. If a network camera captures and compresses 30 individual still images per second, it makes them available as a continuous flow of images resulting in full-motion video. As each individual image is a complete JPEG compressed image, they all have the same guaranteed quality, determined by the compression ratio for the network camera or video server.

Video Compression

Video compression uses a similar method as that of still image compression. However, it adds compression between the frames to further reduce the average file size. MPEG is one of the best-known audio and video compression standards and was created by the Motion Picture Experts Group in the late 1980s. MPEG compression utilizes one frame as a reference. Each additional frame saves and transports only the image information that is different from the original. If there is little change between the images, there will be few differences resulting in a high compression ratio. With significant movement in the images the compression ratio will be much lower. The video is then reconstructed at the viewing station based on the reference image and the “difference data.” MPEG video compression leads to lower data volumes being transmitted across the network than with JPEG.

Images E and F give an example of the difference between how a Motion JPEG storage format works and that of an MPEG format.

The MPEG standard has evolved since its inception. MPEG-1 was released in 1993 and was intended for storing digital video onto CDs. For MPEG-1, the focus was on keeping the bit-rate (the amount of data transmitted via the network per second) relatively constant. However, this created inconsistent image quality, typically comparable to that of videotapes.

MPEG-2 was approved in 1994 and was designed for video on DVDs, digital high-definition TV, interactive storage media, digital broadcast video, and cable TV. The MPEG-2 project focused on extending the MPEG-1 compression technique to cover larger, higher quality pictures with a lower compression ratio and higher-bit rate.

For network video systems, MPEG-4 is a major improvement from MPEG-2. It was approved as a standard in 2000, and there are many more tools in MPEG-4 to lower the bit-rate needed and achieve higher image qualities. MPEG-4 comes in many different versions. Simple Profile is the lowest quality, while Advanced Simple Profile (Part 2) provides much higher quality video. A newer version of MPEG-4 called Part 10 (or AVC - Advanced Video Coding, or H.264) is also available.

With a limited bandwidth available, users can opt for a constant bit-rate (CBR), which generates a constant, pre-set bit-rate. However, the image quality will vary depending on the amount of motion in the scene. As an alternative, users can use a variable bit-rate (VBR) where parameters can be set to maintain high image quality regardless of the motion in the scene. This option is generally preferred in surveillance applications. Because the actual bit-rate will vary with VBR, the network infrastructure must have enough capacity to transport the video.
reducing the amount of data transferred and stored in a network video system. There are advantages and disadvantages to each, so it is best to consider the goals of the overall surveillance system when deciding which of the two standards is most appropriate.

Due to its simplicity, Motion JPEG is often a good choice. There is limited delay between image capturing, encoding, transfer, decoding, and finally display. In other words, Motion JPEG has very little latency, making it most suitable for real-time viewing, image processing, motion detection or object tracking.

Motion JPEG also guarantees image quality regardless of movement or image complexity. It offers the flexibility to select either high image quality (low compression) or lower image quality (high compression), with the benefit of smaller file sizes and decreased bandwidth usage. The frame rate can easily be adjusted to limit bandwidth usage, without loss of image quality.

However, Motion JPEG files are still typically larger than those compressed with the MPEG-4 standard. MPEG-4 requires less bandwidth and storage to transfer data resulting in cost savings. At lower frame rates (below 5 fps) the bandwidth savings created by using MPEG-4 are limited. Employing Motion JPEG network cameras with video motion detection built in, is an interesting alternative, if a higher frame rate is only required a portion of the time when motion is in the image. If the bandwidth is limited, or if video is to be recorded continuously at a high frame rate, MPEG-4 may be the preferred option. Because of the more complex compression in a MPEG-4 system, there is more latency before video is available at the viewing station. The viewing station needs to be more powerful (and hence expensive) to decode MPEG4, as opposed to the decoding of Motion JPEG streams.

One of the best ways to maximize the benefits of both standards is to look for network video products that can deliver simultaneous MPEG-4 and Motion JPEG streams. This gives users the flexibility to both maximize image quality for recording and reduce bandwidth needs for live viewing.

One other item to keep in mind is that both MPEG-2 and MPEG-4 are subject to licensing fees, which can add additional costs to the maintenance of a network video system. It is important to ask your vendor if the license fees are paid. If not, you will incur additional costs later on.

Other Considerations

Another important consideration is the use of proprietary compression. Some vendors don’t allow for a standard 100 percent or use their own techniques. If proprietary compression is used, users will no longer be able to access or view their files should that particular vendor stop supporting that technology.

Proprietary compression also comes into consideration if the surveillance video will potentially be used in court. If so, using industry standard compression ensures that video evidence will be admissible. Some courts believe that evidentiary video should be based on individual frames, not related to each other or manipulated. This would eliminate MPEG because of the way the information is processed. The British court system, which has been leading digital video admissibility, requires an audit trail that describes how the images were obtained, where they were stored, etc., to make sure the information is not tampered with in any way. As digital video becomes more widely adopted, the issue of admissibility in court will be one to watch.

Compression is one of the most important factors to building a successful network video system. It influences image and video quality, latency, cost of the network, storage, and can even determine whether video is court admissible. Because of these considerations, it is important to choose your compression standard carefully ... otherwise, the video may be rendered obsolete for your purposes.

Does one compression standard fit all?

When considering this question and when designing a network video application, the following issues should be addressed:

• What frame rate is required?
• Is the same frame rate needed at all times?
• Is recording/monitoring needed at all times, or only upon motion/event?
• For how long must the video be stored?
• What resolution is required?
• What image quality is required?
• What level of latency (total time for encoding and decoding) is acceptable?
• How robust/secure must the system be?
• What is the available network bandwidth?
• What is the budget for the system?

Video management platforms in IP surveillance systems can be likened to what VCRs did for pure analog systems and what digital video recorders (DVRs) do for hybrid analog and digital systems. However, unlike a simple hardware upgrade, today’s video management platforms also add new possibilities in functionality, scalability and integration.

A video management system is a very important component of IP surveillance systems because it effectively manages video for live monitoring and recording. Video management requirements differ depending on the number of cameras, performance requirements, platform preferences, scalability, and ability to integrate with other systems. Solutions typically range from single PC systems to advanced client/server-based software that provides support for multiple simultaneous users and thousands of cameras.

No matter the type or size, there are common features in almost every video management system including:

• Motion-Based Recording — Video motion detection (VMD) defines activity by analyzing data and differences in a series of images. VMD can be performed at the camera level, which is preferred, or reside

Originally published on SecurityInfoWatch.com • 2006

Step #3: What to Look For in a Video Management System, Plus How Open and Closed Systems Differ
in the video management software. Video management software can provide motion detection functionality to network cameras not equipped with this feature.

- **Alarm Generation** — Video management systems permit users to generate alarms based on motion. For example, parameters can be established so that alarms are not sent during hours of normal activity, such as from 8 a.m. to 9 p.m., Monday through Friday. Therefore, if motion is detected at 3 a.m. on a Saturday, the system knows that this activity is not normal, and can send e-mails or text message alerts to the proper authorities.

- **Frame Rate Control** — Video management allows for frame rate control - meaning that video is monitored and recorded at pre-determined frame rates. It can also be configured to increase frame rates if activity is detected, or to reduce frame rates if there is no motion.

- **Simultaneous Camera Monitoring** — Video management makes it possible for multiple users to view several different cameras at the same time, and increase the resolution for cameras with activity or alarms. This enables the system to be utilized for different purposes and even different departments (such as a system in a retail space used for both security and store traffic studies).

- **Camera Management** — Video management systems allow users to administrate and manage cameras from a single interface. This is useful for tasks such as detecting cameras on the network, managing IP addresses, and setting resolution, compression and security levels. Cameras are often located in distant or hard-to-reach locations, making it impractical for the administrator to visit every location and individually upgrade every camera. Video management systems provide access to every camera on the network and will automatically administer firmware upgrades.

**Open and Closed**

One of the first considerations when designing a video management system is the type of hardware platform that is used. Just like with DVRs, there are closed systems in which the software and hardware come bundled. These are typically referred to as Network Video Recorders, or NVRs.

Although they are networked, NVRs are dedicated to the specific task of recording, analyzing and playing back video. They do not allow other applications to reside on them, so the hardware is essentially “locked.” This means that it can rarely be altered to accommodate anything outside of the original specifications, such as virus protection or intelligent video. NVRs are easier to install, however the number of cameras is often limited to four or 16, and upgrading functionality or security is not normally possible.

Network video systems also allow for open systems with video management software that can be installed on a PC server platform. Most video management systems are available for the Windows operating system, but there are also options for UNIX, Linux and Mac OS.

Open platform solutions run on “off-the-shelf” hardware, with components selected for maximum performance. This allows end users to work with their preferred equipment suppliers and makes it easier to upgrade or replace damaged parts. The systems are also fully scalable because cameras can be added one at a time, and there is no limit to the number that can be added or managed. Open systems are suitable for scenarios where large numbers of cameras are deployed. They also make it easier to add functionality to the system, such as increased or external storage, firewalls, virus protection and intelligent video algorithms.

Some video management systems use a Web interface to access the video from any type of computer platform. Web interfaces allow video to be managed online from anywhere in the world, using the proper safeguards such as password protection and IP address filtering.

It is also important to consider whether a video management system is proprietary and only works with network cameras from select vendors. Video management software should support network cameras from multiple vendors to ensure flexibility. However, even if a system claims to work with many or all network cameras, the system may still not provide the same functionality for all types of cameras, and integration may not be as seamless.

**Integration**

Video management systems based on open platforms have another advantage in that they can be more easily integrated with access control devices, building management systems (BMS), industrial control systems and audio. This allows users to manage video and other building controls through a single program and interface. Integrating a video surveillance system with access control systems allows video to be captured at all entrance and exit points and for pictures in a badge system to be matched against images of the person actually using the access card.

<table>
<thead>
<tr>
<th>Device type</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door contact</td>
<td>Simple magnetic switch detecting opening of doors or windows.</td>
<td>When the door is opened the camera takes action sending full motion video and notifications.</td>
</tr>
<tr>
<td>PIR</td>
<td>A sensor that detects motion based on heat emission.</td>
<td>When motion is detected, the camera takes action sending full motion video and notifications.</td>
</tr>
<tr>
<td>Glass break detector</td>
<td>An active sensor that measures air pressure in a room and detects sudden pressure drops.</td>
<td>When an air pressure drop is detected, the camera takes action sending full motion video and notifications.</td>
</tr>
</tbody>
</table>

Chart A. The range of devices that can be connected to a network camera’s input port is almost infinite.

<table>
<thead>
<tr>
<th>Device type</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door relay</td>
<td>A relay that controls the opening and closing of door locks.</td>
<td>The locking/unlocking of a door controlled by a remote operator (over the network).</td>
</tr>
<tr>
<td>Siren</td>
<td>Alarm siren configured to sound when alarm is detected.</td>
<td>The camera activates the siren either when motion is detected using the built-in VMD or using “information” from the digital input.</td>
</tr>
<tr>
<td>Alarm/intrusion system</td>
<td>Alarm security system continuously monitoring a normally closed, or normally open, alarm circuit.</td>
<td>The camera acts as an integrated part of the alarm system serving as a sensor and enhancing the system with event triggered video transfers.</td>
</tr>
</tbody>
</table>

Chart B. The output port’s function is to allow the camera to automatically trigger external devices by remote control from human operators, or software applications.
Recording and saving video in an IP surveillance environment requires the ability to store large amounts of data for sometimes unspecified lengths of time. There are a number of different factors to consider when selecting the appropriate storage system for an installation including scalability, redundancy and performance.

Similar to the way a PC can “save” documents and other files, video can be stored on a server or PC hard disk. Specialized equipment is not needed because a storage solution does not differentiate video data - it is viewed as any other large group of files that is stored, accessed and eventually deleted. However, video storage puts new strains on storage hardware because it may be required to operate on a continual basis, as opposed to during normal business hours with other types of files. In addition, video by nature generates very large amount of data creating high demand on the storage solution.

**Calculating the storage needs**

In order to appropriately calculate the storage requirements of a network surveillance system, there are a number of elements to factor in, such as the number of cameras required in your installation, the number of hours a day each camera will be recording, how long the data will be stored, and whether the system uses motion detection or continuous recording. Additional parameters like frame rate, compression, image quality and complexity should also be considered.

The type of video compression employed also affects storage calculations. Systems employing JPEG or Motion-JPEG compression vary storage requirements by changing the frame rate, resolution and compression. If MPEG compression is used, then bit rate is the key factor determining the corresponding storage requirements.

Storage is usually measured in Megabytes (MB) per hour or in Gigabytes (GB) per day. One MB equals one million bytes, and one GB is one billion bytes. There are eight bits per byte, and these bits are essentially small “pulses” of information.

Fortunately, there are very specific formulas available for calculating the proper amount of storage to buy. These formulas are different for Motion-JPEG and MPEG compression because Motion-JPEG consists of one individual file for each image, while MPEG is a stream of data, measured in bits per second. The formulas are as follows:

**Motion-JPEG**

1. Image size x frames per second x 3600s = KB per hour / 1000 = MB per hour
2. MB per hour x hours of operation per day / 1000 = GB per day
3. GB per day x requested period of storage = Storage need

MPEG
1. Bit rate / 8(bits in a byte) x 3600s = KB per hour / 1000 = MB per hour
2. MB per hour x hours of operation per day / 1000 = GB per day
3. GB per day x requested period of storage = Storage need

Storage Options
As previously mentioned, IP surveillance does not require specialized storage solutions - it simply utilizes standard components commonly found in the IT industry. This provides lower system costs, higher redundancy, and greater performance and scalability than found in DVR counterparts.

Storage solutions depend on a PC’s or server’s ability to store data. As larger hard drives are produced at lower costs, it is becoming less and less expensive to store video. There are two ways to approach hard disk storage. One is to have the storage attached to the actual server running the application. The other is a storage solution where the storage is separate from the server running the application, called network attached storage (NAS) or storage area networks (SANs).

Direct server attached storage is probably the most common solution for hard disk storage in small to medium-sized IP surveillance installations (See image 1, server attached storage). The hard disk is located in the same PC server that runs the video management software. The PC and the number of hard disks it can hold determine the amount of storage space available. Most standard PCs can hold between two and four hard disks. With today’s technology, each disk can store approximately 300 gigabytes of information for a total capacity of approximately 1.2 terabytes (one thousand gigabytes).

When the amount of stored data and management requirements exceed the limitations of direct attached storage, a NAS or SAN and allows for increased storage space, flexibility and recoverability.

NAS provides a single storage device that is directly attached to a Local Area Network (LAN) and offers shared storage to all clients on the network (See image 2, network attached storage). A NAS device is simple to install and easy to administer, providing a low-cost storage solution. However, it provides limited throughput for incoming data because it has only one network connection, which could become problematic in high-performance systems.

SANs are high-speed, special-purpose networks for storage, typically connected to one or more servers via fiber. Users can access any of the storage devices on the SAN through the servers, and the storage is scalable to hundreds of terabytes. Centralized storage reduces administration and provides a high-performance, flexible storage system for use in multi-server environments. In a SAN system, files can be stored block by block on multiple hard disks. Technologies such as Fiber Channel are commonly used, providing data transfers at four gigabits per second (Gbps).

This type of hard disk configuration allows for very large and scalable solutions where large amounts of data can be stored with a high level of redundancy. For example, the Kentucky Department of Juvenile Justice (DJJ) recently updated an analog tape storage system to a SAN system, allowing the department to install a greater number of cameras throughout its locations and centralize the storage of remote video feeds. The DJJ employed EMC Corp.’s Surveillance Analysis and Management Solution (SAMS) to make the video searchable. This system, which handles hundreds of cameras, is easily expanded and managed as each individual facilities’ needs change.

Redundant Storage
SAN systems build redundancy into the storage device. Redundancy in a storage system allows for video, or any other data, to be saved simultaneously in more than one location. This provides a backup for recovering video if a portion of the storage system becomes unreadable. There are a number of options for providing this added storage layer in an IP surveillance system, including a Redundant Array of Independent Disks (RAID), data replication, tape backups, server clustering and multiple video recipients.

RAID — RAID is a method of arranging standard, off-the-shelf hard drives such
Video Surveillance

that the operating system sees them as one large hard disk. A RAID set up spans data over multiple hard disk drives with enough redundancy that data can be recovered if one disk fails. There are different levels of RAID - ranging from practically no redundancy, to a full-mirrored solution in which there is no disruption and no data loss in the event of hard disk failure.

**Data replication** — This is a common feature in many network operating systems. File servers in the network are configured to replicate data among each other providing a back up if one server fails (See image 3, data replication).

**Tape backup** — Tape backup is an alternative or complementing method where a tape backup machine is installed on the server and records copies of all materials saved on a periodic basis, i.e. daily or weekly. There is a variety of software and hardware equipment available, and backup policies normally include taking tapes off-site to prevent possible fire damage or theft.

**Server clustering** — A common server clustering method is to have two servers work with the same storage device, such as a RAID system. When one server fails, the other identically configured server takes over. These servers can even share the same IP address, which makes the so-called “fail-over” completely transparent for users.

**Multiple video recipients** — A common method to ensure disaster recovery and off-site storage in network video is to simultaneously send the video to two different servers in separate locations. These servers can be equipped with RAID, work in clusters, or replicate their data with servers even further away. This is an especially useful approach when surveillance systems are in hazardous or not easily accessible areas, like mass-transit installations or industrial facilities.

The variety of storage options available for IP surveillance systems makes it crucial to consider the different ways the information will be used and stored for the long term. As hard drive technology continues to advance, it is important to utilize open standards to ensure that storage is scalable and future proof. In addition, advances in IP-surveillance such as intelligent video algorithms will make it even more critical to select open storage devices that can handle combinations of data from different sources. Storage systems should be able to accommodate new and upcoming applications so that equipment investments are not lost as technology advances.
Step #5: Incorporating Analog Cameras with Video Servers

As outlined in Myth #9 of our previous article series, The Top 10 Myths of IP Surveillance (available in the archives of SecurityInfoWatch.com), existing analog surveillance systems can easily be upgraded to IP surveillance systems by incorporating video servers. This allows for digital delivery and control of video without the replacement of every camera with a network camera.

By connecting existing analog cameras to video servers, you can digitize, compress and transmit video over the network. This reduces installation costs by incorporating older equipment into the network video system and allowing for better scalability, storage on standard PC servers, and remote recording and monitoring.

Video Servers 101

A video server—sometimes referred to as a video encoder—eliminates the need for dedicated equipment such as monitors and DVRs by using standard IT equipment and infrastructure. Each video server can connect between one and four analog cameras to the network through an Ethernet port. Like network cameras, video servers contain built-in analog-to-digital conversion, compression, Web and FTP servers, as well as processing power for local intelligence. Incoming analog feeds are converted into digital video, transmitted over the computer network, and stored on PCs for easy viewing and accessibility.

Once the video is on the network, it is identical to video streams coming from network cameras. Analog cameras of all types—fixed, dome, indoor, outdoor, pan/tilt/zoom, and specialty cameras—can be integrated into network video systems using video servers.

A video server has a coaxial input that connects it to the analog camera. The server in turn connects to the network via an Ethernet port. All video is digitized and compressed within the video server and sent over the network via a network switch to a PC, which typically runs video management software for storing and monitoring the video.

Rack-Mounted or Stand-Alone?

Video servers save space by fitting into existing server rooms, eliminating the need for dedicated CCTV control rooms. If coax cabling has already been run to a central room, a video server rack can be used. Rack-mountable video servers come as “blades,” which are essentially video servers without their casings. This allows the video servers to be placed in server racks, which are common in IT environments.

Placing blade video servers in racks allows them to be managed centrally with a common power supply. One standard 19-inch rack that is 3U high can fit up to 48 channels—meaning that up to 48 cameras can be digitized on a single rack.

The functionality of a blade server is exactly the same as a standalone video server. Blades are interchangeable and hot-swappable in the rack, and they provide network, serial communication and I/O connectors at the rear of each slot.

In an analog camera system where coaxial cabling has not been run to a central location, it is best to use stand-alone video servers positioned close to each camera. This method reduces installation costs because it uses existing network cabling to transmit video, instead of running coaxial cabling to a central location. It also eliminates the loss in image quality that occurs over longer distances when video is transferred through coaxial cabling. A video server produces digital images, so there is no quality reduction due to distance.

Advantages of Going Digital

The Alaska Department of Transportation recognized the advantages of a network video system and recently incorporated video servers into nine of the largest ferry terminals in the Alaska Marine Highway System.

The organization worked with integrator CamCentral to install the system, which uses video servers to digitize video from analog cameras installed throughout the ferry terminals, enabling staff, security services, and local law enforcement units to monitor the facilities, surrounding waters, and vehicle and passenger traffic via the Internet. When the terminals are closed, local law enforcement officials and other authorized users can access the system remotely and receive alerts if unusual motion is detected in the facilities. The Alaska DOT realized a number of advantages that video servers could bring to its analog surveillance systems.

Recording, management, and storage — Because video servers use standard PCs for video recording and management, they are easy to integrate with existing IT systems and can be managed as part of that infrastructure. Video servers allow video to be stored with standard storage solutions, including network attached storage (NAS),...
storage area networks (SAN) and Redundant Arrays of Independent Disks (RAID). These storage systems are easily expandable, reliable, cost effective, and repairable or replaceable in case of failure. By contrast, DVR systems require proprietary hardware, which is more costly and difficult to replace or upgrade. CamCentral and the Alaska DOT also took advantage of the video servers’ ability to handle firewalls, passwords and other network security technology—something that can rarely be done with DVRs.

**Scalability** — Both video servers and DVRs leverage existing investments in analog cameras, but only video servers make total use of network infrastructure. This is particularly important when expanding the network video system. An IP surveillance system is expandable in one-camera increments. DVR systems, on the other hand, expand in larger increments. Once the capacity of a DVR is maximized, a new DVR box with 16 or more channels must be added to the system, even if only a handful of cameras need to be accommodated.

**Remote recording and monitoring** — Video servers allow users to access and record video at remote locations, provided they have the appropriate authorization and login information. Off-site recording can be beneficial in retail environments where it guarantees that video is protected during a theft on the premises. Off-site viewing allows security personnel to keep an eye on their establishment without being on the premises.

**Decentralization** — Video servers decentralize digitization and compression functions, so information is handled at the source instead of in a centralized place. This 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.

In the case of the Alaska DOT, using video servers allowed CamCentral to create specialized motion-detection software that was optimized for the marine environment. A centralized processing system, like a DVR, cannot handle such applications because computing power is a scarce resource that video and analysis are forced to share. Even networked DVRs—which incorporate an Ethernet port for network connectivity—do not provide the same functionality as a video server system.

Video servers can provide cost savings and more functionality than analog or DVR systems. They create a truly digital surveillance system and allow users to capitalize on almost all the benefits of network video while incorporating network cameras as expansion and upgrades are required.

---

**Step #6: Wireless Networking Options for Surveillance Video Transmissions**

Sometimes wireless solutions are the best and most cost-effective option for IP surveillance installations. For example, wireless networks are a common choice in historic buildings where the installation of cables would damage the interior. Wireless is also a preferred option within facilities where there is a need to move cameras to new locations on a regular basis. The technology can also be used to bridge sites without expensive ground cabling, or to add cameras in difficult to reach locations such as parking lots or city centers.

Using wireless with network cameras and video servers can be done in a few different ways. Some cameras come with built-in wireless functionality, but any network camera or video server can be incorporated into a wireless application using a wireless device point — a device with an Ethernet port and a wireless connection or built-in antenna.

**802.11 and WLANs**

Wireless local area networks (WLANs) are the basis for most wireless networks. They allow mobile users and devices to connect to a Local Area Network (LAN) through a wireless connection which transmits data using high frequency radio waves. The process is similar to establishing a wireless Internet connection to a home computer and laptops; likewise, a company can establish a WLAN allowing devices like computers and network cameras to connect to the network and transmit video.

WLAN standards are well defined, and devices from different vendors can work together, which allows for the vendor neutrality that end-users often request. The most commonly used standard is 802.11g, which provides higher transfer rates over greater distances than 802.11a and 802.11b. While the popular 802.11b has a maximum data rate of 11 Megabits per second (Mbps), the 802.11g provides five times that, with 54 Mbps. These are the maximum data rates, but typical data rates are about half that speed, and the further the device is from the access point the lower the bandwidth will be. 802.11b and 802.11g operate within the 2.4 GHz frequency. Keep in mind that higher frequencies shorten the distance that radio waves can reach.

While 802.11g is sufficient for full frame rate video, it operates at only 25 percent of a typical 100 Mbps wired connection. The next generation WLAN standard will be 802.11n and the “n” standard will greatly increase the speed of wireless data transmissions. This will improve the functionality of wireless IP surveillance systems as it will be possible to transmit video at even higher frame rates.

**Alternatives to 802.11**

Some solutions use standards other than 802.11, and many of these offerings can...
provide increased performance and much longer distances in combination with very high security. This includes the use of microwaves and satellites. A microwave link can provide up to 1,000 Mbps at up to 130 miles. Satellite communication allows for even further distances, but due to the way this system operates -- it transmits up to a satellite and then back down to earth -- the latency can be very long. This makes it less suitable for functions like controlling camera movement and video conferencing where low latency is preferred. If larger bandwidth is required, the use of satellite systems also becomes very costly.

WiMAX, or 802.16, is the standard for broadband wireless access. It enables devices with wireless connections to operate within a 30-mile range. It is being utilized for fixed broadband wireless metropolitan access networks (WMANs), including those in development in San Francisco and Milwaukee. WiMAX supports very high uploading and downloading bit rates to handle services such as Voice over IP (VoIP).

Types of Wireless Networks

There are three major types of wireless networks, each providing different benefits and functionalities. All three utilize wireless radio waves as the primary method for transmitting data, although there are a few other means of transmission.

Point-to-point — When it is necessary to connect two buildings or sites with a high-speed network, a point-to-point data link capable of long distances and high speeds is required. These connections can be wired -- using fiber cabling -- or wireless, using radio waves or an optical link. Point-to-point can be a good option to consider when you’re faced with the challenge of trying to create a central security command center when buildings are spread out among a large campus, or are separated in a town and its suburbs.

Some wireless point-to-point links require direct line-of-sight (LOS) between the two points in order to establish a connection. This means there must be a direct, visible path between the transmitting antenna and the receiving antenna to establish a link. This can prove difficult in mountainous terrain or in urban areas where taller buildings may disrupt LOS. There are cost-efficient solutions for point-to-point in the 900 MHz range that can transmit data a few miles with non-line-of-site (NLOS), and up to 40 miles with LOS.

Point-to-multipoint — Point-to-multipoint distributes data from a single source to multiple targets. The typical range is up to 15 miles at data speeds up to 72 Mbps. Point-to-multipoint links can be done with LOS or NLOS technology, depending on the needs of the surrounding area. Deploying a wireless point-to-multipoint system can require laying cabling across vast distances.

Mesh networks — In a mesh networking setup, all or most devices on the network are connected directly to each other. If one device can no longer operate, all the rest still communicate with each other; it’s the concept of a “self-healing” network. Mesh networks work well when cameras are located at scattered points, but can be very expensive to establish when using wired connections. A wireless network allows these devices to network together without the need for physical cabling.

Security in Wireless Networks

Wireless networks allow for added flexibility in the placement of cameras and other networked devices throughout the system, but they require added security measures. WLANs are not necessarily bound by the walls of the buildings they serve, which open them up to security issues not faced with wired solutions. Due to the nature of wireless communications, everyone with a wireless device within the area covered by the network can potentially access its applications.

To address these concerns, there are a number of different methods for securing wireless networks, including Wireless Equivalent Privacy (WEP), WiFi Protected Access (WPA), and WiFi Protected Access 2 (WPA2), plus a number of proprietary solutions.

WEP — WEP encrypts data transmitted over the WLAN. Once WEP has been established, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks, and authentication can be put in place to further ensure privacy. WEP adds encryption to the communication and prevents people without the correct key from accessing the network. However, the encryption code in WEP is static, which makes it vulnerable to attacks with inexpensive off-the-shelf software. Therefore, it should not be the only method used to secure a wireless network.

WPA — WPA was created as a response to flaws in WEP. WPA works with most wireless network interface cards. With WPA, the access key is changed with every transmitted frame using Temporal Key Integrity Protocol (TKIP). This makes it much more secure, and it is now considered the basic level of security necessary for wireless networks.

WPA2 — For even higher security, WPA2 should be used. WPA2 uses Advanced Encryption Standard (AES) instead of TKIP. AES is the best encryption available for wireless networks today and is currently being used by the U.S. Government to secure sensitive, but not classified information. WPA2 is also referred to as 802.11i.

Some vendors have established proprietary modes of securing information on a wireless network. While these systems may be very secure, keep in mind that these can become cumbersome and difficult to manage when working with a variety of vendors on an installation.

Wireless networks can have a profound affect when used in areas it would be otherwise impossible to deploy a surveillance system. Ace Internet Solutions (AIS) installed a wireless IP Surveillance system when it moved to an industrial park in Chicago. There had been a rash of vandalism and theft in the area, and to help combat the problem, the company wanted to install a surveillance system to monitor an area which encompassed nine square blocks.

“Because all of the network cameras were set up outdoors, running data cabling to each of them would have been too costly and difficult to maintain,” said Jeff Holewinski, president of AIS. “With a wireless connection, the cameras can transmit images no matter where they are, even from the top of light poles.”

Using the wireless IP surveillance system, AIS deployed a wireless option and later discovered an extensive drag racing operation that was using the industrial park late at night for races. AIS worked with the Chicago Police Department, which was able to bust the ring, impound more than 100 cars, and make more than 300 arrests.

While wireless networks have many benefits, there are still a few drawbacks. Wireless networks can affect the frame rate and latency of video delivery, and bandwidth is affected by the distance from the device to the access point. Wireless networks are also susceptible to interference by other wireless technologies and systems.

However, wireless networks allow for cameras and other devices on the network to be moved quickly and easily without the need for expensive cabling. While there are still limitations and security concerns, they can still prove advantageous when used correctly for installations that would otherwise be too difficult or costly with wired networks. It is important to understand the benefits and challenges and analyze whether a wireless solution will meet your organization’s demands before installing the network.
Networks allow devices such as network cameras, servers and PCs to communicate with each other, sharing information and, in some cases, a common Internet connection. Network designs can take many forms and vary in terms of performance and security.

It is useful to think of building a network as a layering process, beginning with the physical cabling configuration and connections. The number of cameras, the physical environment, the sensitivity of the application, and the protocols and software will impact the operation of the IP surveillance network.

### Types of Networks

Networks can be local area networks (LANs), metropolitan area networks (MANs) or wide area networks (WANs). Each network covers a progressively larger area. For example, LANs exist within a building or company, while MANs could cover a campus or city center. WANs cover the largest areas—anything from multiple distant areas to the entire world. WANs often connect several smaller networks, such as LANs and MANs. The largest WAN is the Internet.

### Basic Network Layout

Networks are made up of cabling such as Ethernet or fiber, and equipment such as servers, routers and hubs. There are many ways to physically lay out networks, but the main four designs are bus, ring, star and mesh. You can determine the right layout for any IP surveillance system by considering requirements such as redundancy, cost and number of cameras.

- **Bus** — A bus network connects each device to a main cable or link called “the bus,” creating a simple and reliable network configuration. If one device fails, the rest can still communicate with each other, unless the bus itself is broken. This setup is most often found in older LANs.
- **Star** — Star is the most popular topology used in LANs today. In star networks, all devices are directly connected to a central point. If one device is disconnected or crashes, none of the others will be affected. However, if the central switch goes offline, the entire network could fail. This makes it important to build redundancy into the system.
- **Ring** — In a ring network, devices are connected in a closed loop, meaning that adjacent devices are directly and indirectly connected to other devices. MANs and WANs often use ring configurations, but this design can be used for LANs as well.
- **Mesh** — Mesh networks come in two varieties: full and partial mesh. In a full mesh network, devices are connected directly to each other. In partial mesh, some devices are connected to all the others, while some are connected only to those with which they exchange the most data. Mesh networks are becoming popular as the use of wireless technologies grows.

### Wired and Wireless Options

Network devices can be connected over wires or wirelessly. Ethernet cabling provides a fast network at a reasonable cost and is the primary medium for most existing IT infrastructures. Ethernet connections—which resemble phone jacks—are usually integrated into network cameras and video servers, making it easy to connect them to the network.

Fast Ethernet is the most common standard used in computer networks today. It supports a transfer rate of 100 megabits per second (Mbit/s). Gigabit Ethernet (1000 Mbit/s) is the current standard endorsed by network equipment vendors and is used primarily in backbones between network servers and network switches. The upcoming standard is 10 Gigabit Ethernet (10,000 Mbit/s), which will soon be incorporated into network backbones. IP surveillance systems work with all of these standards, so as networks become faster, they will be able to support higher-quality video.

Another benefit of Ethernet cabling is Power over Ethernet (PoE), which powers devices through the network cables. This eliminates the need to install power outlets at camera locations and enables a more continuous power supply.

Sometimes a non-wired solution is beneficial, particularly for buildings where cable installation will damage the interior, or where cameras will be regularly moved. Another common use of wireless technology is to bridge two buildings or sites without expensive and complex ground works. Wireless LANs are available in a number of well-defined standards that allow for vendor neutrality. The most common standard is 802.11g, which provides higher transfer rates at greater distances than 802.11a and 802.11b.

### New or Existing Network?

With all of these networking options available, it is sometimes difficult to determine whether to run IP surveillance on an existing network or to build a new network dedicated to security and surveillance needs.

Today’s LANs typically offer plentiful bandwidth, with network switches providing 100 Mbit for each device connected to the network. Since network cameras can consume anywhere from 0.1 Mbit to 8 Mbit, some precaution is needed to ensure the network video system will operate as intended. Depending on the number of cameras and required frame rate, three options are available:

1. **Dedicated Network** — Professional surveillance applications may benefit from a dedicated network in which the IP surveillance system has its own dedicated switches that are connected to a high-capacity backbone (see Figure 1). Dedicated networks handle video traffic more efficiently, without slowing down other general-purpose network applications like voice over IP or file sharing. In addition, keeping the surveillance network separate and disconnected from the Internet will make it as secure as—or more secure than—any local CCTV system. Dedicated networks are preferable in very sensitive applications, like those in casinos or airports, and for systems requiring high frame rates and more than 50 cameras.
2. Combination Network — In some cases, it might make sense to implement a dedicated IP surveillance network in conjunction with a general-purpose network. Video can be recorded locally and isolated to the dedicated network, except when a viewer on the general-purpose network wants to access it, or when an event triggers video to be sent to a user on the general-purpose network (see Figure 2). Because access to video using the general-purpose network (and the extra load it causes) is temporary, it makes sense to have the two networks work in combination.

3. Existing Network — When there is enough capacity on the network and the application doesn’t require heavy security, you may simply add network video equipment onto the existing network. You can further optimize your network using technologies such as virtual local area networks (VLAN) and quality-of-service (QoS) levels.

A VLAN uses the existing LAN infrastructure but separates the surveillance network from the general-purpose network. The router/switch is configured to provide a range of IP addresses with assigned features. In Figure 3, the router/switch manages the IP addresses, bandwidth and security allocated to users on VLAN A (with access to video) and VLAN B (general-purpose traffic). No matter where users might physically be, all those on VLAN A will have access to the video while those on VLAN B will not.

QoS ensures that bandwidth will be available for surveillance equipment on the general-purpose network by setting priority levels for specific ports on a switch. Connections to network cameras and storage servers can be set at high priority, while desktops can be set for low priority to ensure that bandwidth is always available for critical surveillance video.

Transmitting Data

Once your network layout is established and your devices are connected, information will be transmitted over the network. Transmission Control Protocol/Internet Protocol (TCP/IP) is the most common way to transmit all types of data. It is the protocol used for nearly every application that runs over a network, including the Internet, e-mail and network video systems.

TCP/IP has two parts: TCP breaks data into packets that are transmitted over the Internet and reassembled at the destination. IP is the address that enables the packets to arrive at the correct destination. For identification and communication purposes, every device on the network needs a separate IP address.

Network Performance

After the network is set up, it is critical to consider how much information will
pass over the network and the contingency plan if critical components fail.

The amount of bandwidth required is dictated by the amount of information passing through your network. In general, avoid loading a network to more than 50 percent capacity, or you risk of overloading the network. When building a new network or adding capacity to an existing network, build in 30 to 40 percent more capacity than calculated. This will provide flexibility for increasing use in the future. Bandwidth calculators—available freely on the Internet—will analyze your bandwidth and recommend an appropriate capacity.

**Security Considerations**

With the success of the Internet, securing networks has become a mandate. Today there are several technologies available, such as virtual private networks (VPNs), SSL/TSL and firewalls.

A VPN creates a secure tunnel between points on the network, but it does not secure the data itself. Only devices with the correct access “key” will be able to work within the VPN, and network devices between the client and the server will not be able to access or view the data. With a VPN, different sites can be connected together over the Internet in a safe and secure way.

Another way to accomplish security is to apply encryption to the data itself. In this case there is no secure tunnel like the VPN, but the actual data sent is secured. There are several encryption techniques available, like SSL, WEP and WPA. (These latter two are used in wireless networks.) When using SSL, also known as HTTPS, a certificate will be installed in the device or computer that encrypts the data.

A firewall is designed to prevent unauthorized access to or from a private network. Firewalls can be hardware or software, or a combination of both. All data entering or leaving the intranet passes through the firewall, which examines it and blocks data that does not meet the specified security criteria. For example, using a firewall, one can make sure that video terminals are able to access the cameras while communication from other computers will be blocked. Some network cameras have built-in IP address filtering, a basic form of firewall that only allows communication with computers that have pre-approved IP addresses.

Network video systems can take a number of different forms depending on the requirements of the individual installation. No matter what form your network takes or what elements you choose to deploy, it is important to work with a well recognized and reliable vendor to ensure all components work well together and you have maximized the system’s functionality.

Nearly all network video installations transmit sensitive information that should be protected from unauthorized users and potential hackers. There are several ways to provide security within a wired or wireless network and between different networks and clients. Everything from the data to the use and accessibility of the network should be controlled and secured.

Today, IP surveillance systems can be made just as secure as those used by banks for ATM transactions. Network cameras and video servers are currently being used in highly sensitive locations such as the Logan Airport in Boston (see Case in Point, page 101) and by the largest ferry terminals in Alaska for homeland security purposes.

**Secure Transmission**

Some of the most common ways to secure communications on a network and the Internet include authentication, authorization, IP address filtering, VPNs and Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Some of these methods secure the data as it travels over the network, while others secure the network path itself.

Authentication identifies the user to the network and is most commonly done by providing verifiable information like a username and password, and/or by using an X509 (SSL) certificate.

The 802.1X standard is a new port-based authentication framework available for even higher levels of security in a both wired and wireless system. All users’ access requests are filtered through a central authorization point before access to the network is granted.

During authorization, the system analyzes the authentication information and verifies that the device is the one it claims to be by comparing the provided identity to a database of correct and approved identities. Once the authorization is complete, the device is fully connected and operational within the network.

IP address filtering is another way to restrict communication between devices on a network or the Internet. Network cameras can be configured to communicate only with computers at pre-determined IP addresses—any computer from an IP address that is not authorized to interface with the device will be blocked from doing so.

Privacy settings prevent others from using or reading data on the network. There are a variety of privacy options available, including encryption, virtual private networks (VPNs) and Secure Socket Layer/Transport Layer Security (SSL/TLS). In some cases, these settings can slow down network performance because data has to be filtered through multiple applications before it is accessed at its final destination. This could have a negative impact on the performance of an IP surveillance installation, which often requires real-time access to video.

A VPN uses a public infrastructure, such as the Internet, to provide secure access to a network from remote locations. A VPN secures the communication through security procedures and tunneling protocols like Layer Two Tunneling Protocol (L2TP), effectively creating a connection that is just as secure as a privately owned or leased line. The VPN creates a secure “tunnel” so that data has to be properly encrypted before entering the tunnel. Data that is not properly encrypted cannot enter the tunnel.

SSL/TLS—also known as Hypertext Transfer Protocol over Secure Socket Layer

**Step #8: Security**

Originally published in *Security Technology & Design* magazine • September 2006

18 SECURITY TECHNOLOGY & DESIGN / SECURITYINFOWATCH.COM
(HTTPS)—encrypts the data itself, rather than the tunnel in which it travels. There are several different types of encryption, including SSL, Wireless Equivalent Privacy (WEP) and WiFi Protected Access (WPA) for wireless networks. When using SSL, a digital certificate can be installed from the server to authenticate the sender. Certificates can be issued locally by the user or by a third party such as Verisign.

Additional network security can be created with the use of firewalls. Firewall software normally resides on a server and protects one network from users on other networks. The firewall examines each packet of information and determines whether it should continue on to its destination or be filtered out. The firewall serves as a gatekeeper, blocking or restricting traffic between two networks, such as a video surveillance network and the Internet.

**Wireless Security**

Wireless network cameras can create additional security requirements. Unless security measures are in place, everyone with a compatible wireless device in the network’s range is able to access the network and share services. To better secure IP surveillance installations with a wireless component, users should consider using Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) encryption.

WEP creates a wireless network that has comparable security and privacy to a wired network. It uses keys to prevent people without the correct key from accessing the network, which is the security commonly found in home networks. Data encryption protects the wireless link so that other typical local area network security mechanisms—including password protection, end-to-end encryption, VPNs and authentication—can be put in place.

However, WEP has several flaws that make it unsuitable for use in a corporate environment. The standard uses a static key, making it easy to hack into the network with inexpensive, off-the-shelf software.

For additional protection, wireless IP surveillance should employ WPA, which changes the encryption for every frame transmitted. WPA is considered the base level of security for corporate wireless networks, but for even higher security, WPA2 should be used. WPA2 uses Advanced Encryption Standard (AES), the best encryption available for wireless networks today.

**Protecting System Access**

In addition to protecting data, it is critical to control access to the system via a Web interface or an application housed on a PC server. Access can be secured with user names and passwords, which should be at least six characters long—the longer, the better. Passwords should also mix lower and upper cases and use a combination of numbers and letters. Additionally, tools like finger scanners and smart cards can be used to increase security.

Viruses and worms are also major security concerns in IP surveillance systems, so a virus scanner with up-to-date filters is recommended. This should be installed on all computers, and operating systems should be regularly updated with service packs and fixes from the manufacturer. Network cameras and video servers with read-only memory will also help protect against viruses and worms—programs that write themselves into a device’s memory. If you use network cameras and video servers with read-only memory, these programs will not be able to corrupt the devices’ internal operating systems.

Employing the outlined security measures makes an IP surveillance network secure and allows users the flexibility of off-site access without the worry that video will fall into the wrong hands. Understanding and choosing the right security options—such as firewalls, virtual private networks (VPNs) and password protection—will eliminate concerns that an IP surveillance system is open to the public.
Network video allows for new capabilities in the surveillance industry that were not feasible in an analog environment, either because they were impossible to implement, or just too cumbersome. Some of the hottest new technologies available in a network video installation are intelligent video, megapixel cameras, and something called immersive imaging.

Today, far more video is being recorded than anyone could ever monitor or search. Studies from the Sandia National Laboratories, which develops science-based technologies to support U.S. national security, suggest that personnel can only watch one monitor for up to 20 minutes before losing focus. Without some form of built-in algorithm compiling relevant information, there is simply no way to monitor all the surveillance cameras in a system - unless you’ve got an almost unlimited budget.

That’s where video analytics enters the picture. Intelligent video (IV), the next big trend in video surveillance, will allow cameras to monitor events within the field of view. Advanced network cameras can have built-in motion detection and event handling. In addition, more intelligent algorithms, such as automatic number plate recognition (a.k.a. license plate recognition) and people counting, are being integrated into security and surveillance systems. Network cameras and IV have important synergies that make the systems more reliable and effective than those using analog cameras with a digital video recorder (DVR) or other centralized system.

**Intelligent Video Defined**

Different vendors have referred to IV by various terms including “actionable intelligence”, “video analytics”, and “intelligent video”. No matter how it is referred to, IV turns video into “actionable information,” which allows users to receive alerts and make decisions regarding appropriate next steps.

The “intelligence” in IV applications is actually a mathematical analysis of video streams. The data can be used in a multitude of ways, many of which are still under development. The overarching idea is that the surveillance system itself analyzes the video and alerts its operator by triggering an alarm when there is a change to the appropriate level of activity in the field of view. IV is not designed to fully replace human analysis. People will still be needed to assess the entire situation and act accordingly, because human vision is extremely advanced, and is impossible to replicate with mathematical algorithms.

IV can be used in numerous capacities, including object tracking, object counting, license plate recognition, face recognition and object identification. For example, the Boston Police Department has network cameras monitoring the entryway door to their own building. The camera follows each individual as they enter until it gets enough data points for facial recognition. The system then automatically compares this image against an existing database of outstanding arrest warrants. In this way, if someone with an outstanding warrant enters the building for any reason - such as to bail out a friend - the officers know within minutes whether they should detain the person longer.

Offering this sort of intelligence in the video system creates major advantages, the most central of which is the ability to reduce the workload on staff. The IV system is never idle. It is constantly on guard, waiting for an impulse to send an alarm or start recording. There are a number of different ways to set up an IV surveillance system and important factors, like image quality that should be taken in to account.

**Surveillance System Architecture with IV**

IV can be incorporated into an existing surveillance system, or built into the architecture of a new system. There are two different types of network security architectures that utilize network video. Those two methods are 1) centralized intelligence, in which all intelligence features and algorithms occur in one location, and 2) distributed intelligence, in which the IV functions occur at dispersed points throughout the installation.

**Centralized intelligence —** This is most common in a system utilizing DVRs to convert and store video from analog cameras. In this type of system, all IV algorithms are housed at the DVR level along with digitization of the video and video management functionality. In this set up, all computing power is centralized in the DVR, which means the number of cameras that can be analyzed is limited, making the system less scalable.

**Distributed intelligence -** Distributed intelligence can be used in a network video system using analog or network cameras. If analog cameras are already installed, video servers can be added to the system and used to digitize analog video and run IV algorithms closer to the camera level. The processed information is then funneled through a network switch to storage devices and monitoring stations. In a network video system the edge devices -- the video servers or the network cameras themselves -- have built in computing power to run the IV algorithms, pushing the intelligence all the way to the periphery of the surveillance system. This makes the system scale from one to thousands of cameras without over burdening the centralized recording device, like in the DVR scenario. It also decreases the amount of video sent over the network because the cameras themselves “decide” when recording is necessary. This in turn reduces the overall strain on the IT infrastructure by freeing up bandwidth for other applications.

**IV and Image Quality**

Along with the mathematical algorithms, image quality is of extreme importance for the accuracy of the IV system. Without clear images, the best IV algorithms will not be able operate accurately. Network cameras bring an end to the interlaced scan problems of analog systems utilizing DVR technology. Interlaced images are created from two sets of lines that update alternately. This delay causes a blurring of the overall image. Network cameras utilize a newer technology to create images called progressive scan. Progressive scan captures the entire image at once, so even with a high degree of object motion, the image is clear.
**Megapixel and Immersive Imaging**

Analog video systems are tied to television specifications, meaning the maximum resolution is 0.4 megapixels when digitized. Standard digital still cameras available at retail stores are now 5 megapixels and 1.3 megapixel cameras are built into cell phones. Network video cameras can also utilize megapixel technology, which has some obvious benefits, beyond just getting a clearer image. Details from megapixel cameras are more easily recognized in the image. More details means additional data points for IV algorithms, which in-turn improves accuracy of the analytics.

**Immersive Imaging**

Another way to utilize megapixel technology is for what’s being called “immersive imaging”. By using a wide-angle lens attached to a megapixel camera, the camera can span a much wider field of view (some camera lenses designs even cover a full 360 degrees) than normal cameras. Immersive imaging facilitates digital pan/tilt/zoom (PTZ). The result is the ability to pan, tilt and zoom in on a field of view, even though the camera stays put. Because there are no moving parts, users don’t experience the mechanical wear and tear that exists in analog PTZ cameras which must physically move. There’s also a potential gain in speed, since an analog/mechanical PTZ can be no faster than its drive motor.

**Important Considerations**

IV, megapixel and immersive imaging offer a number of benefits to an existing or new surveillance system. IV can lower the total cost of a surveillance system by generating fewer false alarms, and by reducing the amount of people required to operate the system. The surveillance system will alert personnel as appropriate when an unusual event occurs. Megapixel imaging allows for even higher resolutions, which in turn allow IV algorithms to act even more exactly.

To be most effective it is critical to work with vendors that employ open standards for the use of IV. This allows the user to choose the best IV algorithms and applications for their needs without having to worry about interoperability challenges.

IV, megapixel and immersive imaging remain hot because they will greatly improve system performance and will continue to evolve creating even greater user advantages in the coming years. Network video is a best of breed system, utilizing open computing platforms and storage systems, which will result in new hot technologies on the horizon faster than usual.
Today, there are well over a million network cameras and video servers installed worldwide. These installations range in size from just a single camera to thousands of cameras -- and are found in almost every type of industry application. No matter the size, every installation benefits from a simple set of best practices that will ensure all network video equipment is optimized. These tips range from basic camera placement and lighting conditions to working with IT departments and technicians to figure out issues such as the peak times for network usage.

**Take Inventory**

When first installing IP-based surveillance, it is important to take note of any existing inventory. For example, there may be analog cameras currently installed or the IT department may have a standardized server platform in place, such as a certain type of HP server and Windows operating platform. Also evaluate the speed of your network and work with the IT department to determine how much bandwidth is available or whether network video can be piggybacked onto other infrastructure, such as that for Voice over IP (VoIP) applications. Security professionals are often surprised as to how much equipment their organization already has at its disposal for an IP-based video system.

Although existing analog cameras can often be upgraded using video servers, it is sometimes necessary to make a total migration to network cameras in order to simplify the installation. A large retailer recently changed its analog closed-circuit television (CCTV) system to an IP-based system for about 200 of its stores. Although the company already had some analog cameras in place, it decided not to digitize them with video servers. Instead, the retailer switched everything over to network cameras to simplify what the IT industry refers to as MACs -- Moves, Adds and Changes related to IT equipment. When all hardware is standardized, it limits maintenance, reduces the need for spare parts, and makes adjustments to the system simpler and more cost effective. For many installations however, it is typically not necessary to replace all analog cameras with network cameras, so video servers are more viable.

**Evaluate Site Conditions**

Conditions at the camera locations will largely determine which type of network camera should be purchased. Just as with analog cameras, factors such as placing a network camera in an area with very little light or exposing it to extreme heat or cold, will dictate the installation's success. Electrical outlets are another important consideration. Although it may seem like a minor consideration, it costs an average of $300 to install power to a single location. Today, network cameras are often installed in areas where power outlets do not exist -- such as on building exteriors, in parking lots, or on bridges. In these cases, cameras with Power over Ethernet (PoE) functionality will be a major time and cost savings because they can receive power directly from their network cable connections. The PoE feature should be in 100 percent accordance with the IEEE 802.3af standard, otherwise it will lock the buyer into proprietary systems that are likely not compatible with equipment from other vendors.

**Determine Camera Usage**

In addition to site conditions, camera usage also dictates the necessary specifications. Network cameras range from less than $200 for an entry-level model to professional equipment that functions under a broader range of conditions and offers improved functionality. For example, a camera that will be used to capture objects moving at high speeds -- such as moving cars -- need a progressive scan sensor that will reduce blur. Pan/tilt/zoom (PTZ) will be necessary for looking at objects at a distance or to set up automatic patrols of an area. Megapixel cameras provide higher resolution and help reduce the number of cameras needed.
Make Friends with IT

Beyond just taking inventory of available networking equipment, the IT department can be helpful in making sure that network video runs smoothly and does not interfere with other applications. While communicating with people in IT jargon may seem intimidating at first, it is very important to build these relationships to ensure that the integration of security and networking is smooth. The IT department will have a vast knowledge base that will ensure an IP-surveillance system is installed properly, but that will only happen with good collaboration between the two departments.

For example, the IT department will know whether bandwidth is genuinely a concern. In most cases, video traffic is only detrimental for older networks. In this case, it will be time to upgrade the network according to company protocol. The amount of bandwidth has increased exponentially the last few years, so standard network ports today are one gigabit a second, and backbones are typically 10 gigabits a second or higher. For these networks, IP-surveillance creates no bandwidth issues whatsoever. Because today’s corporate networks are highly regulated, the IT department can also ensure that Internet Protocol version 6 (IPv6) and Quality of Service (QoS) agreements are supported. If bandwidth is still an issue, network cameras have enough built-in intelligence that they can be programmed to only send video based on triggering events such as motion or time of day.

The IT department can also help establish a separate network for the video. This does not require running a separate set of cabling, but simply segmenting the video traffic from the rest of the network using a network switch. The switch routes data to different network ports and boosts overall performance.

The Eastchester Union Free School District, located in Westchester, N.Y., successfully used network switching to utilize extra bandwidth from its existing VoIP network. Select Telecom Inc., the integrator for the project, worked with the district to set up virtual local area networks (VLANs) for the video traffic, separating the voice network from the video network.

“By piggybacking the video network onto the voice network, we were able to save significant amounts of time and money,” said Anita Better, director of information technology for Eastchester. “The cameras are so bandwidth efficient that the video does not slow down or degrade the voice network.”

Security will also be a primary concern for the IT department. Anything that connects to the network opens up the possibility of new attacks and security breaches. Although the Internet regularly transfers all types of sensitive information, it is necessary to use security safeguards, including VPNs (virtual private networks), encryption, port-based network access control (IEEE 802.1X), and password protection.

Manage and Budget the Project

Besides managing equipment and the relationship with the IT department, it is essential to select the right systems integrator and understand the cost structure of an IP-surveillance system. This will help in establishing -- and sticking to -- a budget and managing the project roll out.

One of the most important items to ask a systems integrator is how many other IP-based surveillance systems have they successfully installed. Talk to their customers and understand whether the integrator embraces new technology, or if the end user had to push for the latest equipment. Integrators and consultants who are not familiar with new technology sometimes over-specify systems, and customers end up with equipment and functionality they never need.

In terms of budgeting, it is important to understand that the cost structure of an IP-surveillance system is quite different from that of a CCTV system. Although the price of a network camera is usually higher than that of an analog camera, the total system cost must be considered in order to generate a correct comparison. For example, network cameras include considerably more functionality than analog cameras, such as built-in digitalization, image compression and intelligence. IP infrastructure -- including cabling, storage, and recording -- is also considerably less expensive than analog infrastructure and provides more functionality. (See figures 1 and 2 at right, explaining surveillance cost structure.)

IP-surveillance is rapidly gaining momentum. However, the technology is still frequently misunderstood, which can lead to frustration for security professionals and IT departments that try to support them. Following the basic best practices outlined above can help simplify IP-surveillance rollouts and ensure that the systems operate as smoothly as possible.
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

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