



Your IP Video Surveillance Cheat Sheet

Considering implementing IP video on your campus? Here's a primer on some of the most common technologies currently deployed.

By Robin Hattersley Gray and Margie Gurwin

What Is IP Video? Internet protocol (IP) video uses the computer network infrastructure to transmit security video to recording and viewing stations and dispatch centers. In IP video systems, network cameras output a digitally encoded signal that can be transmitted over the network as data for viewing, storage and integration with other security solutions. Video management systems or software (VMS) allows the user to view the live video, call up recorded video, control the cameras connected to the network and many other functions.

Currently, the majority of video surveillance systems installed in the United States remain analog, with digital video recorders (DVRs) storing video from cameras and providing video playback. This technology has been available for years and is very reliable. That said, many new video surveillance installations are incorporating IP because of its advantages, such as:

- 1. FUNCTIONALITY:** Users can view the video from any location in the world, as long as there is a computer network available.
- 2. BACKWARD COMPATIBILITY:** Because new technologies like megapixel cameras are not backward compatible with analog systems, in order to take advantage of these new systems, campuses must upgrade to IP.
- 3. SCALABILITY:** Depending on the equipment and system installed, there is no limit to the number of devices that can be placed on the network.
- 4. COSTS:** While IP cameras are more expensive to purchase than analog cameras, the operation and in-

stallation costs can be lower, especially for facilities that have more than 32 cameras. This results in a reduced overall cost of ownership. Often a campus will already have a network that can support IP video, so installation costs are less. The expense of running coaxial cable (which is used in analog systems) is also avoided by using the network, which runs Category-5e or Cat-6 cable. Solutions allowing power to run over the same network cable (PoE) also save the expense of additional cabling and equipment.

Many facilities that currently have analog systems are choosing a hybrid approach that uses both analog and IP solutions simultaneously. As the analog cameras reach the end of their life cycles, often they are replaced with IP cameras, thus maximizing the return on investment from both old and new equipment.

For campuses wanting to transition to IP, it is advisable to develop a migration plan. For example, some product lines can use existing analog cameras along with new IP cameras, allowing both to interoperate (communicate with each other and work on the same system). Using a DVR, video server or encoder, analog video can be converted to a digital signal that transmits over the same network as the IP cameras.

For campuses installing video surveillance solutions in new construction or completely replacing a legacy analog system in a pre-existing building, IP might be the wise choice. This is particularly true if the institution has plans to greatly expand its video surveillance program or has a large number of cameras being installed.

The next two pages provide a basic overview of some of the technologies and equipment commonly used in today's IP video systems. ►

Video Management Systems (VMS): Provide a unified user interface so campuses can more easily manage video, access control and intrusion systems. The latest generation of VMS software takes advantage of the open or nonproprietary platforms that facilitate interoperability between different solutions. It offers operational efficiencies beyond traditional security. For example, using VMS, video can help with process control, personnel management, inventory tracking, quality control and

customer service in the healthcare and college campus environments. All VMS applications provide the ability to add and configure basic camera settings, resolution, frame rate and compression format. The more user-friendly ones provide built-in training tools or wizards that assist the operator with common tasks, such as archiving video, automating recording procedures and installation. Most VMS solutions support analytics and multiple types of video compression.

SOLUTION

Video Management Software:

Open platform VMS software may be installed on any commercial, off-the-shelf (COTS) server and storage equipment, provided the hardware meets the requirements established by the software manufacturer.



STRENGTHS

- Server and storage can be selected to obtain the best performance of a specific system
- Allows for integration with other security software solutions
- Supports network cameras and hardware from many manufacturers
- Fully scalable
- Easy to integrate with other systems, such as biometrics, fire, access control and building management

WEAKNESSES

- More difficult to install than preconfigured NVRs or DVRs from the manufacturer
- Feature-rich solutions may be more difficult for users to master
- Software licensing fees can be expensive and complex
- Trouble shooting may require support from multiple manufacturers

APPLICATION COMMENTS

- Appropriate for larger facilities or ones that have plans to expand significantly

Network Video Recorder (NVR):

An NVR is simply a hardware device in which the VMS software is already installed. Some VMS manufacturers offer their solution pre-installed on an NVR. If the VMS software is open platform, the advantages include all those listed above.



- Usually easier to install than a PC server-based system
- Single source for technical support of software and hardware

- If the software is not open-platform, there are limitations as to the use of cameras and other hardware from other manufacturers
- Often doesn't allow other applications to reside physically within the unit

- Appropriate for larger facilities or ones that have plans to expand significantly
- NVR manufacturers often offer other hardware. Purchasing components from a single manufacturer eliminates certain compatibility issues that arise in open-platform systems.
- Some manufacturers offer pre-configuration and software registration of NVRs, further reducing installation and set-up time

Digital Video Recorders (DVRs):

These devices connect directly to analog cameras and convert video to a digital format for viewing and storage. Hybrid DVRs have the added ability to view and control network cameras, much like an NVR.



- Have been on the market for more than 10 years and are prevalent
- Are reliable and have a life span of 7-8 years
- Easy to use

- Depending on the model, scalability may be limited
- Hardware is often proprietary and specifically designed for video management

- When purchasing a replacement unit, be certain it will support IP cameras
- Appropriate for smaller applications
- Many DVRs are reaching the end of their life cycle



IP Cameras: Internet protocol (IP) cameras output a digitally encoded video signal that can be transmitted across an IP network. These cameras may provide images in either standard definition or high definition (megapixel models).

SOLUTION

Megapixel Cameras:

These are IP cameras that produce high definition (HD) video. Common HD cameras offer resolutions of 720P (1.3 MP) and 1080P (2 MP), but models are available that go much higher than this.

STRENGTHS

- Provide much clearer images than regular IP cameras or analog cameras
- Now allow for better identification of subjects
- Require fewer cameras to cover a given area

WEAKNESSES

- Are more expensive to purchase, although prices have been dropping substantially in the past few years
- Can have challenges capturing images in low-light or backlight situations (this is true for most IP cameras)
- The size of the files transmitted can be large, which can cause network bandwidth and storage issues

APPLICATION COMMENTS

- Deploy HD cameras to cover a wide area. This allows a campus to avoid installing multiple IP or analog cameras, resulting in cost savings.
- For locations with lighting challenges, analog cameras or thermal imaging might be appropriate
- Flexible frame rate and industry standard compression technologies can help address storage challenges



Data & Video Storage: Because many campuses continue to increase the number of cameras deployed, they will most certainly need more storage as their systems expand. This is particularly true for facilities installing IP video because IP cameras (especially megapixel cameras) create such large files. Fortunately, over the years, the capacity of hard drives has expanded greatly while their prices have fallen dramatically. One key development has been the introduction of solutions specifically designed for video surveillance. It should be noted that some cameras have built-in storage, so when the network goes down, these “edge” devices can record locally.

SOLUTION

Redundant Array of Independent Disks (RAID)

provides increased storage functions and reliability through redundancy. This is achieved by combining multiple hard disk drive (HDD) components into a logical unit where data is distributed across the drives in one of several ways.

STRENGTHS

- Less expensive than SSD
- Better capacity than SSD
- Longer life span than SSD

WEAKNESSES

- More susceptible to physical shock compared to SSD

APPLICATION COMMENTS

- Remember to backup your storage devices

Solid State Drives (SSD)

use microchips that retain data in nonvolatile memory chips and contain no moving parts.

- Less susceptible to physical shock compared to RAID
- Quieter, faster and have less latency than RAID

- More expensive per gigabyte than RAID
- Have a limited capacity
- Short life span

- Remember to backup your storage devices

Compression: IP cameras (especially megapixel cameras) create file sizes that are very large and cause bandwidth challenges. Compression technology, however, makes large video and data files smaller so they won't slow down a network. Some type of compression is a required component of most IP video systems. Note that the advantages and disadvantages listed below are generalizations and do not hold true in all conditions. Seek the advice of a professional system engineer to determine the best compression choice for your specific installation.

SOLUTION

Motion JPEG (MJPEG) Compression

STRENGTHS

- This method can produce any of its frames as a single image for identification purposes
- Minimum latency
- Consistent file size
- Lower CPU requirements
- Lower cost for software and hardware
- No standards

WEAKNESSES

- The storage requirement for cameras incorporating MJPEG is nearly five times more than cameras using H.264

APPLICATION COMMENTS

- A survey of 12 leading networked camera manufacturers showed that about 85% of them incorporate MJPEG as one of their video streams

H.264 Compression

- More flexible than MPEG-4, which makes it suitable for applications ranging from low bit rate, low delay mobile transmission through HD security megapixel cameras
- Better compression efficiency than MJPEG
- Appropriate for megapixel cameras

- H.264 is not more expensive. You may pay more for a more powerful CPU to display it, but you'll conversely save on storage in many cases. It's a wash.
- More powerful CPU required for display

Note: Some material courtesy of Security Sales & Integration magazine and Bob Wimmer

OTHER IP VIDEO TERMS YOU SHOULD KNOW:

Client Software:

This is licensed software that must be installed on user's PCs in order to view and access the VMS system. It is sometimes the same as the one installed on NVRs, hybrid DVRs and workstations (non-recording network viewing stations).

Embedded Software:

This is a dedicated purpose software operating system, such as that running on some stand-alone DVRs.

Browser-Based Interface:

A feature that allows security personnel and administrators to access the video management system using a standard Web browser, such as Internet Explorer, Mozilla Firefox or Chrome. It eliminates the need for special client software to be installed on the computer in order to view video from the security system. As with other viewing options, browser interfaces are secure, requiring a username and password. Almost all video management systems today offer this option, including the most basic, DVR-only systems.

Local Viewing:

This is viewing that is limited to the physical location where the local system is installed. Traditional DVRs provide local viewing and control via front panel controls on the unit or from an on-screen interface. Client software installed on hybrid DVRs, NVRs and workstations can be configured by the network administrator to limit viewing to local cameras.

Remote Viewing:

This type of viewing allows security personnel to monitor video from anywhere in the world via a Web browser or client software. For example, in a campus-wide IP VMS system, security personnel at the central office, as well as the local police station, might have access to live and recorded video from all cameras across all campus properties. On a smaller scale, the owner of a small child-care center with a DVR-only system might use a browser interface to remotely view video of the facility from his or her home computer.