IP Camera Features & Capabilities

By choosing carefully between available options, you can maximize your IP video savings.

By Randall R. Nason

It is highly likely that many of us purchased or specified our last analog camera in 2006. Ongoing and upcoming projects will probably focus on Internet protocol (IP)-based cameras. Relying solely on the now ubiquitous IP network infrastructure, this class of devices has revolutionized how we use technology to meet our surveillance requirements.

If you're looking at new IP cameras for a security implementation, you and your specifier have a lot of options. Different IP cameras offer different features and capabilities that may or may not be ideal for your project.

Lights Up

In some ways, selecting an IP camera isn't that different from selecting an analog camera. One of the still-present constraints on any surveillance system is lighting. Both IP and analog video systems require appropriate lighting for effective operation.

Specification sheets for many of today's IP cameras show a continual decrease in the amount of faceplate illumination required for useable video. You'll commonly see minimum illumination levels of less than 0.5 lux for color and 0.1 lux for black and white in camera specifications. These numbers are usually qualified with a very low f-stop number, allowing the maximum light in through the lens iris. They are normally further qualified by indicating that the automatic gain control (AGC) is on. In other words, the video at these light levels could be defined as usable, but only barely so.

Don't view published minimum illumination levels as operational recommendations. Your installation location should provide lighting at levels at least a factor of ten above the published minimums. Additionally, it is always appropriate to have the vendor or integrator bring the specified camera to the site in order to actually observe the produced video signal under existing lighting conditions. This allows changes in either the camera selection or lighting conditions before full-scale implementation.

Power Over Ethernet

Of course, another practical requirement IP cameras share with analog is power. But IP cameras have more power options than analog cameras have had. With the approval in June 2003 of IEEE standard 802.3af, power can be delivered to IP-based devices over the Ethernet network cable.

Power over Ethernet (PoE) has greatly streamlined IP camera system design and new installations by providing data transmission and power supply in one cable from a common source. This can offer an installation great benefits, since both the data and power now come from and are

maintained by the IT department. As a secondary benefit, backup (uninterruptible) power now also comes from a common source. Many companies offer rack-mounted devices that provide power, power monitoring with alarm notification, and UPS power, all in one box.

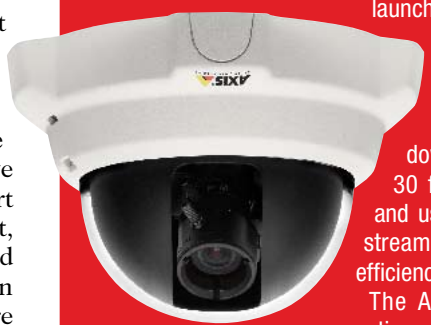
Use of POE features requires that the network connection to the IP camera come from a POE-enabled switch or router. For legacy network hardware, POE-enabled devices are approximately 20% more expensive than non-POE devices. For a 24 port switch recently reviewed for a project, this differential represented around $1,000. However, new-generation POE-enabled switches and routers are often approximately 20% less expensive than non-POE devices.

When your design firm is analyzing the cost benefit of POE for IP cameras, they'll need to keep in mind the type of network devices to be used. Since POE-enabled network devices normally come with ports in multiples of 24, any upcharge for the POE function is minimal on a per-port basis. For example, an upcharge of $1,000 represents approximately $42 per port. This is much less than a typical charge to run a new power drop to a CCTV camera. Conversely, even if power is available at the camera location, use of POE would add a minimal amount to the installation costs while at the same time eliminating legacy, low-voltage power supply hardware.

Product Showcase

Full-Featured Network Camera

Axis Communications' AXIS 216FD-V Network Camera is the compact, discreet and vandal-resistant complement to the best-selling AXIS 216FD Network Camera, which launched in April 2006. The AXIS 216FD-V has a metal base and a durable, transparent cover to prevent damage. It uses progressive scan technology and advanced image processing to deliver crisp digital images of moving objects, even in light conditions down to 1 lux. The network camera delivers up to 30 frames a second (full motion) in VGA resolution and uses simultaneous Motion JPEG and MPEG-4 video streams to optimize both image quality and bandwidth efficiency.

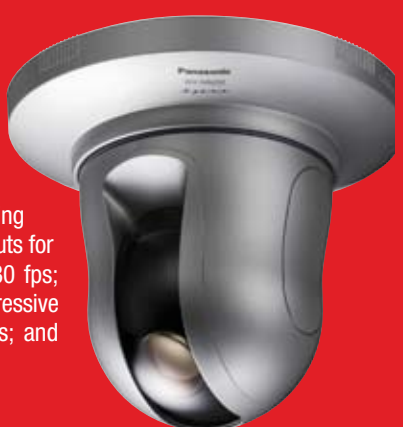


The AXIS 216FD-V has a built-in microphone and connections for an external microphone and speakers, enabling two-way audio communication with visitors or intruders. The camera also provides event management capabilities such as video motion and audio detection, and pre- and post-alarm image buffering. Power over Ethernet allows the AXIS 216FD-V to be powered via the network, reducing cabling requirements and installation costs.

Circle Inquiry #111

Color Network PTZ Dome

Panasonic's i-Pro WV-NS202 Color Network PTZ Dome Camera brings Super Dynamic III (SDIII) technology to a networked platform. The camera's SDIII performance provides 128x dynamic range for superior image reproduction in virtually any lighting condition; MJPEG and MPEG-4 dual streaming outputs for simultaneous monitoring and recording at up to 30 fps; 22x optical zoom; power over Ethernet (PoE); progressive output for smooth reproduction of moving objects; and minimum illumination of only 0.7 lux.



Circle Inquiry #112

Onboard Analytics

Without a doubt, the most promising area of IP camera development is onboard video analytics. Video-based motion detection has been available, and at the same time under development, for at least 30 years. A major breakthrough came after 9/11 when a new level of rules-based video motion detection became widely used around sites where conventional perimeter security could not be cost-effectively deployed, such as ports and airports.

Computationally intensive, these systems generally relied on a high-capacity data link from the camera to either a host or distributed computer that applied the motion filters and algorithms to the video signal. This approach provided a greatly needed and previously unavailable tool; however, scaling to a larger system required increasing the size and/or number of the host processors.

The emerging approach is to place the video analytics in the camera, or as the industry likes to say, on the edge. Fredrik Nilsson, general manager of Axis Communications North America, attributes the creation and continuing growth of onboard analytics to three main factors: increased image quality in IP cameras, which allows more reliable analytic processing; better processing algorithms; and the continuing development of more powerful processors.

While onboard analytics increases the cost of the camera, it solves the scalability problem in that system expansion is no longer limited by the availability of video analytic processing capacity. However, other, more familiar expansion constraints do come into play, such as video storage and network capacity.

The full suite of video analytics is currently not available onboard as it is in server-based applications. Of course, not every application requires this robust analytic capability. Simple video motion detection is commonly available as a standard (no upcharge) feature from most camera manufacturers; for many interior applications, this feature will be more than adequate. Those applications that would require advanced analytics may include exterior environments and complex interior situations. The user should have a very specific need before considering the use of high-end analytics, or cost may be hard to justify.

Security Options

Adding IP-based cameras to a network raises the issue of security. Most manufacturers address this through secure sockets layer (SSL) encryption, which provides secure, encrypted communication between the host and the device. SSL uses a public and private key encryption system that also includes the use of a digital certificate.

Cost effectiveness is one of the practical outcomes of this new class of devices.

Another technique that will be applied in the future is the use of the media access control (MAC) address as a unique identifier for each IP camera. This will allow the host and other network devices to know and verify the identity of the IP cameras on the network. If a MAC address does not match the directory of known devices, the device represents a security anomaly.

Onboard Storage

Most IP cameras also offer optional onboard storage through the use of a secure digital (SD) card. This provides short-term storage in the event the network storage device becomes unavailable. This feature should be considered in mission-critical applications where any loss of storage capability is unacceptable.

Bandwidth to Consider

Finally, a key concern of many facilities regarding IP cameras is bandwidth use. Because of the easy scalability of IP-based camera systems, a large camera system is now measured in terms of thousands of cameras. Therefore, bandwidth use is a key parameter to understand and for which to prepare. This topic has been widely discussed throughout the industry and in previous articles in this magazine. There are several approaches to managing use of this infrastructure asset.

• **Image resolution.** Resolution is measured in terms of the common interchange (or intermediate) format (CIF), which is defined as 352 x 240 pixels. A 4 CIF (704 x 480 pixels) resolution is considered the highest resolution of standard video without taking the step to high-definition. The file size of the video stream is a function of the resolution. Most IP cameras allow you to select the resolution through the setup and management software. Some applications will require the full 4 CIF resolution and the consequent file size burden; skillful use of this option will allow you to tailor the resolution of each camera in the system to the specific field of view and application.

• **Image compression.** Industry-standard algorithms have been developed that reduce the size of the image file. This compression comes at the expense of some of the information contained in the original image. The trick is to balance bandwidth use with image quality. This is a function of existing IT infrastructure and image use. MPEG-4 is probably the most widely used compression algorithm in security applications. Some manufacturers, such as Verint, offer MPEG-4 as well as a proprietary variant, which reportedly offers a slightly smaller file size without further degradation of the original image.

It is common for IP cameras to provide motion JPEG (MJPEG) and JPEG-4 data streams. While the user has some control over compression, MJPEG, a low-resolution format, is often used during non-event periods where high video signal content is not critical. However, in some systems, when an event is detected, the data stream can switch to MPEG-4 with higher resolution. This not only conserves bandwidth during non-critical periods; it also provides the high content signal when needed.

• **Frame rate.** Full-motion video is defined as 30 video frames per second (fps). However, depending on the speed of the anticipated motion in the field of view, a much lower frame rate may appear to be full motion. Simply contrast a man walking in a parking lot and a blackjack dealer in a casino. Something less than 30 fps may be sufficient to obtain the necessary information from the former, while nothing less than 30 fps would be acceptable for the latter.

Fortunately, most-IP based cameras allow the user to select the frame rate to fit their particular application; many models also allow the frame rate to change upon detection of motion or other predefined events. This conserves storage space during non-event periods while allowing the maximum image content to be recovered during those times when predefined events may be occurring. Some cameras allow the user to define the maximum frame rate that may be transmitted as a means of conserving bandwidth.

• **Bit rate.** Some cameras allow the user to define the bit rate that is transmitted over the network cable for storage or viewing. This feature allows users with limited available bandwidth to use a predefined amount that can be accommodated by considering other users on the network.

Efficient bandwidth use is an especially important parameter to consider. Additional intensive bandwidth use, as occurs when a number of cameras are added, may adversely impact overall network performance. However, there are those circumstances in which a complete network or network segment is dedicated to security use; in these cases it is only necessary to ensure that proper consideration is given to future expansion during the design effort.

The capabilities of IP-based cameras provide opportunities for cost-effective security solutions that simply were not available five years ago. Cost effectiveness is one of the practical outcomes of this new class of devices, which require only a standard network drop for both data transmission and power. STD

Randall R. Nason, PE, CPP is a corporate vice president and manager of the Security Consulting Group at C.H. Guernsey & Co. His experience spans a broad spectrum of the security profession including threat assessment, vulnerability analysis and master plan development through complete system design and construction management.