IP Video Surveillance Guide

ANIXTER

Anixter is a leading global supplier of communications and security products, electrical and electronic wire and cable, fasteners and other small components. We help our customers specify solutions and make informed purchasing decisions around technology, applications and relevant standards. Throughout the world, we provide innovative supply chain management services to reduce our customers' total cost of production and implementation.

Table of Contents

INTRODUCTION

A prominent trend in the security industry today is an evolutionary shift from the traditional video surveillance technology first deployed in the 1950s to newer network-based systems. This migration from older analog-based devices to newer digital equipment provides many functional and financial benefits to companies who need to provide better protection for people and assets. Utilizing advances in microprocessors and other computer technologies, video monitoring, recording and analysis can be made available to responsible parties, wherever and whenever needed. High-quality cameras may now be plugged in wherever there's a suitable port – enjoying the flexibility and manageability of today's telephone and computer systems. Live and recorded video can be accessed from network attached PCs across local area networks (LANs) or the Internet using familiar network technologies such as Ethernet and Internet Protocol (IP).

Networked IP surveillance is proving to be attractive in nearly all vertical markets as it promises to increase safety and reduce the costs of operating traditional CCTV systems. In other applications, it is being used for the first time to solve unique problems and provide additional operator control.

Developments in IP surveillance have allowed security cameras to provide a wealth of additional information to users. (Typically, theft prevention or life safety have been the primary motives for security cameras, but increasingly, the advanced content management provided by today's software gives users a valuable tool to monitor and manage a business.) For example:

- Retail applications utilize security systems to provide information on customer buying patterns or to measure customer footfall at various times during store hours
- Transportation systems now use remote tolling of roads or motorways on top of their normal operational requirements
- License plate recognition at gas stations gives the opportunity to search a plate number across a database to highlight a known offender
- Future developments will include advanced facial recognition at large public gatherings to search for particular people.

As technology advances, additional applications will become available and the software will become a significant part of any system design or installation.

This booklet will review video surveillance security systems and networked IP video migration trends in security. It will also examine system components such as cameras, video servers, physical topology choices and proper cabling infrastructure. Understanding the breadth of these products helps security officers, end-users and IT personnel evaluate the many options available for building flexible and reliable state-of-the-art video surveillance systems while preserving the existing capital investment.

The Business Case for IP Surveillance

The drive within the security market toward IP migration is not only based on the technological advancements offered, but also increasingly due to a solid financial business case.

For many years, organizations have had to accept the proprietary nature and short lifespan of their security installations. This is no longer the case if utilizing the right IT infrastructure has become a key consideration when implementing security solutions.

The gradual merging of facilities and IT departments, similar to what we have already seen with voice and data, has promoted a unified approach to security and data infrastructures. It is this consolidated approach that is the backbone of the financial benefits for today's businesses.

Integrated Management Approach

Taking a consistent attitude toward the planning, installation and management of a common infrastructure for both data and video traffic enables a cost-effective usage of expertise within the IT department. The involvement of the IT department in the early stages of a system design, particularly in terms of the network capability and ongoing bandwidth considerations, confirming that compatibility and functionality meet the required objectives while being in line with allocated budgets.

Open Architecture–Standards Driven

Traditionally, security systems have used proprietary cabling and variants of established protocols for the acquisition of the video signal and camera control. This has forced organizations to become locked into specific products, whether or not they were meeting expectations. Once in an IT environment, the processes and procedures used on data installations will drive a more standards-based approach to system design and, more importantly, provide increased flexibility for future expansion. In addition, more supply and delivery options have become available, assisting companies to manage the supply chain and reduce costs accordingly.

Improved Functionality

One of the most significant benefits of digital and IP surveillance is the ability to effectively store, retrieve and analyze video information easily and quickly, thereby reducing the required operating manpower and associated ongoing costs. Quicker retrieval of sensitive information, particularly in vertical markets such as finance and retail, can lead to an improved problem-to-resolution time, again reducing a cost element of these procedures.

MYTH

IP surveillance cannot meet the demands of enterprise level applications.

REALITY

For many larger installations, scalability of the system is one of the main features that organizations are requesting when implementing a security solution. The increased need for flexibility and provision for future growth, coupled with higher levels of functionality and interoperability with other systems, makes IP surveillance the only real candidate.

MYTH

IP surveillance technology is unproven. If it is better, why are security integrators not offering more of these systems?

REALITY

In reality this is due more to the existing structure, practices and IT knowledge within the traditional security market than any negative factors regarding the performance and reliability of IP surveillance. IP surveillance is a newer technology and as such requires the building up of appropriate knowledge and infrastructure among security integrators, consultants and industry influencers in order to overcome normal resistance to change. It is very much an evolving process, but increasingly the benefits realized in terms of cost saving and functionality are a major driver for organizations.

Once in this open, standardized IT environment other security and networking systems sharing the infrastructure can work more closely together, thus moving further toward more intelligent systems while ensuring compatibility.

The advent of digital solutions can extend the reach beyond just theft or protection. Network connected software packages can provide the user with a host of additional information options that can be used to analyze other facets of the business, such as customer footfall, transactional and behavioral analysis and remote tolling or billing. Increased functionality can reduce costs previously allocated to these other information tasks.

Return on Investment (ROI)

Typically the most expensive portion of the costs associated with a CCTV system, using traditional analog methodology, is the actual installation of the point-to-point cabling, coupled with the amount of cable required. Many analog systems can require three cables per camera to be installed, which is both time consuming and costly. The single most important factor for improving ROI is the maximization of existing IT cabling and/or the strategic design of new IT infrastructures to accommodate security.

Larger scale analog security projects can require the involvement of multiple integration partners, each providing a component of the overall system. Working with each of these integrators requires a great deal of internal administration and cost to raise orders, create and pay invoices, etc. These costs affect the ROI in a very subtle but substantial way. Many integrators can now alleviate a proportion of these costs by offering both the infrastructure and security solutions together. This management of the supply chain coupled with cost savings in the installation is becoming increasingly attractive to many organizations.

Total Cost of Ownership (TCO)

Initial installation savings and improved ROI are not the only considerations for businesses. The longer-term TCO of a system when viewed over a 10- to 15-year lifespan is also a significant factor. The flexibility to migrate and evolve with the changing needs of a business or technological improvements impacts the TCO greatly.

Costs can be reduced not only in the initial installation phase but also when moves, adds and changes (MACs) are required. It has been estimated that MACs using IT cabling and processes can be up to six times more cost-effective than with traditional analog infrastructures.

MYTH

Transmitting video data via the network will overload it, making this an unworkable technology.

REALITY

As with any network, if the bandwidth capacity planning does not allow the system to function within the required parameters, the result could be network downtime. For any sizeable or mission-critical IP surveillance deployment, consider utilizing a separate network for video. With the advancements of network switches and routers, the separation of the network is now even easier. In addition, other specific steps can be taken to confirm that IP surveillance technology can be integrated into an organization's daily operations and will not adversely affect the network performance. The system administrator can decide the appropriate frame rate, per camera, that is sent over the network. This can be based on events, motion detection and time of day. This allows only the most valid information to be sent via the network, further reducing the strain on the capacity and improving system management.

The Evolution of Video Surveillance Systems

Over the last 20 years, designs of CCTV systems haven't changed that much. However, world events have created a need for more sophisticated surveillance systems. Traditional analog CCTV technology can no longer address many of today's needs and future requirements.

Highly advanced video surveillance products are now available that address the latest trends and requirements including:

- New high-performance direct network attached IP cameras
- High-bandwidth networks and wireless infrastructures
- Handheld communication devices (PDA, Cellular, SMS) with video surveillance capabilities
- Lower cost storage solutions
- Higher-quality image processing
- Web-enabled.

MODERN VIDEO SURVEILLANCE SYSTEMS ACCOMMODATE:

- Converged networks where the IT infrastructure serves as part of the CCTV network
- Systems integration of CCTV, access control, biometrics and building automation
- The need for remote monitoring
- Secure but shared event monitoring and recording, which utilize database-type access methods
- Versatile solutions to meet multi-level security requirements
- Co-existence of analog and digital video sources to maximize existing infrastructure
- Flexible frame rates and resolution choices to optimize and conserve backbone bandwidth
- Increased intelligence for first responder personnel.

THE PATH TO NETWORKED VIDEO

Two Key Technologies

In order to fully understand the benefits associated with networked video surveillance, it's important to have a fundamental understanding of Ethernet LAN technology, Internet Protocol (IP) and the part each plays. Today, it's next to impossible to buy a PC for the home or office that doesn't include an Ethernet port and software that utilizes an IP addressing system. We depend on these two technologies to exchange e-mails, access the World Wide Web and share documents with each other. They are prevalent because these standards are universal, scalable, work well and are supported by an increasingly wide range of high-performance, low-cost and industry-proven equipment and technologies. It's only natural that an application like video surveillance, which is experiencing explosive growth, would ultimately move to networked infrastructure with proven stability yet more control and flexibility. Ethernet/IP networks provide an appropriate platform and strategy for growth and enhanced manageability of video surveillance systems.

Ethernet Standards

Existing Ethernet networks are capable of operating at speeds of 10 and 100 megabits per second as well as 1 and 10 gigabits per second (10 Gbps). All utilize unshielded twisted-pair and shielded twisted-pair network cabling. Twisted-pair cabling makes cable management much simpler than earlier coaxial Ethernet systems of the late 1980s. There is a strong parallel between the shift of early data networking systems from coax to star-wired twisted-pair cabling that applies directly to today's video surveillance needs. In fact, there are similar management and financial benefits that should not be overlooked when considering how security technologies are implemented.

Today, most Ethernet networks are 100 Mbps (100BASE-T) and 1 Gbps (1000BASE-T) systems. However, with the extended capacity of 10 Gigabit (10GBASE-T) electronics and cabling, high-quality video easily coexists with data and voice streams on the same network, opening the door to many more security options. Video and Voice over IP (VoIP) are widely seen as applications that potentially justify the installation of high-capacity 10GBASE-T cabling systems as they require near real-time performance and do not tolerate network errors or network latency.

Gigabit Ethernet networks are excellent platforms for modern security systems. There are many sensible methods for building networked surveillance capability and migrating existing systems to digital while still preserving capital investment.

ETHERNET STANDARDS

Fast Ethernet (100 Mbps)

- 100BASE-TX: Uses twisted-pair copper cabling (Cat 5 or greater).
- 100BASE-FX: 100 Mbps Ethernet over optical fiber.

Note: Most 100 Mb network switches and adapters support both 10 and 100 Mbps to deliver backward compatibility (commonly called 10/100 network switch).

Gigabit Ethernet (1,000 Mbps)

- 1000BASE-T: 1 Gbps over Cat 5e or Cat 6 copper twisted-pair cabling.
- 1000BASE-SX: 1 Gbps over multimode fiber up to 550 meters.
- 1000BASE-LX: 1 Gbps over multimode fiber up to 550 meters. Optimized for longer distances (up to 10 kilometers) over single-mode fiber.
- 1000BASE-LH: 1 Gbps over single-mode fiber up to 100 kilometers. A long-distance solution.

10 Gigabit Ethernet (10,000 Mbps)

- 10GBASE-T: Augmented Cat 6 cabling up to 100 meters.
- 10GBASE-CX4: Multi-pair twinaxial cable for server clustering at less than 15 meters.
- 10GBASE-S: Multimode fiber for data centers/campus backbones up to 300 meters, or 550 meters for laser optimized fiber.
- 10GBASE-LX4: Multimode or single-mode fiber for legacy systems.
- 10GBASE-L: Single-mode fiber for campus backbones up to 10 kilometers.
- 10GBASE-E: Single-mode fiber for metro area networks up to 40 kilometers.
- 10GBASE-LRM: Multimode fiber for legacy systems up to 220 meters.

Internet Protocol

The importance of IP to networks and video surveillance systems lies in its universal acceptance as a common method of addressing and connecting to specific devices, whether they are PCs, vending machines or security cameras. In a video surveillance application, this means specific cameras can be viewed and controlled from anywhere on the network by anyone with network access and proper security authorization. IP is a partner to the Transmission Control Protocol (TCP) and both are implemented via software that runs on each connected device. The TCP/IP combination ensures a device can be identified and reached, and ensures errors are detected and corrupted messages retransmitted when necessary. This is a mature and stable technology that is well understood in the computer industry, but is only beginning to be utilized in the security industry.

Accordingly, when a security camera is described as an IP camera, it generally means it can be connected directly to an Ethernet LAN and uses the IP addressing scheme to communicate with other devices on a digital video surveillance network.

MYTH

You cannot protect existing investment in analog cameras.

REALITY

IP surveillance solutions now utilize IP encoders to convert the analog video signal into a digitized video stream that can be sent via the network. In simple terms, it means turning an analog camera into an IP surveillance device. Many of today's large scale security installations use a combination of both analog and IP cameras via encoders. Even an installation with a fully functional analog system already paid for is no barrier to migrating to complete IP surveillance technology.

TYPICAL MIGRATION PATH

ANALOG, DIGITAL AND NETWORKED SECURITY SYSTEMS

The terms analog, digital, networked and IP are often used incorrectly, sometimes leading to confusion. Organizations have many choices when maintaining or upgrading existing systems or when considering new installations. An understanding of the infrastructure options available as well as analog and digital security devices is crucial to designing and planning a system.

Most video security systems today are based on analog equipment and connectivity products designed for analog electrical signals. IP video surveillance is a digital technology that takes full advantage of technical innovations within the computer networking industry. These systems actually employ special computerized devices that communicate over Ethernet LANs using Internet Protocol.

Some systems today are actually hybrids, employing both analog and digital technologies. These hybrid systems are typically in a state of transition—opting to protect the existing investment in video equipment, but enjoying some of the advantages of digital while migrating to newer digital equipment or a fully networked solution.

Most CCTV cameras today output an analog signal; however, the picture imaging is performed by a microprocessor and a digital chip called a CCD or charge-coupled device. This digital image is converted to an analog signal by a digital-to-analog converter (DAC), so it can be recorded on an analog videocassette recorder (VCR) or viewed on an analog monitor. This is often described as an end-to-end analog system. Over time, this approach has become unmanageable. When requirements for many more cameras per site, better

quality images, faster frame-rates, greater storage capacity and search capabilities become factors, analog videotape recording is no longer effective. The cost of replacing worn tapes alone can justify moving to digital technologies. When comparing the time and space needed to collect, store and archive footage on tape with the benefits and ease of storing and searching footage electronically, digital systems are the "hands down winners." This is a major reason why the adoption of digital over analog systems is happening so quickly.

Digital recording features and benefits have become well understood in the retail market. TV-attached TiVo® and replay personal video recorders (PVRs) allow instant playback with simultaneous recording. This capability is extremely valuable when applied to video surveillance monitoring and recording. One such device is called a DVR or digital video recorder and can be used with analog CCTV systems. The DVR converts the analog signal to a digital image for storage. As a reasonable migration approach, this allows investment protection of an existing system, yet provides some of the management benefits of a digital surveillance system.

MYTH

IP surveillance image quality does not match that of analog cameras.

REALITY

In many cases, IP surveillance cameras are now utilizing the same high-quality image devices and circuitry as traditional analog cameras. However, these high-quality network cameras should not be confused with Webcams typically used on the Internet for Web attractions. In certain circumstances, specific analog cameras may be a more suitable option (ultra low-light sensitivity for example), but the advent of IP video servers allows these analog cameras to connect to the network as part of a complete IP surveillance solution.

THE ADVANTAGES OF DIGITAL IP VIDEO SURVEILLANCE

Once a video image is digital, it can be transported over an Ethernet/IP network, where it can be stored, copied, added to a database and used as any other data file might be. Digital video files are easily transported through a network in standard Ethernet packets through switches, routers, wireless and portable network devices.

As the industry moves away from analog to digital, the transmission medium of choice is shifting away from coaxial cabling.

The cabling media of choice for digital networks is four twisted-pair copper wires with fiber and wireless alternatives (for longer distances or to overcome challenges with communication right-of-ways).

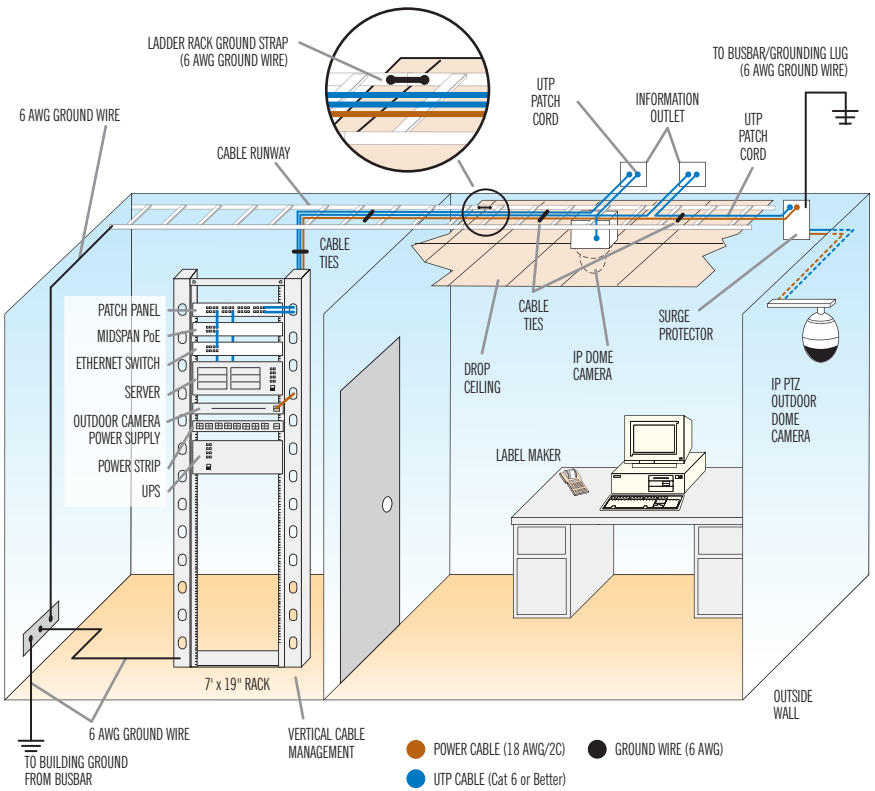
Twisted pair offers the advantages of a single, unified infrastructure capable of handling both legacy analog devices and newer, smarter digital devices. Analog equipment can co-exist along with the newest digital equipment. Twisted-pair infrastructures also support the next transition of transporting digital images over an Ethernet/IP network using digital networked IP cameras as image sources. The twisted-pair infrastructure is the foundation for many advantages gained from the implementation of an IP-based surveillance system.

Digital video provides extensive image analysis that can be used for evidence or data gathering within a business. Even though it is centrally stored, networked IP video is easy to distribute in different formats at different frame rates, quality levels and bandwidths to many users. Using Internet browser technologies, it is possible to do this anywhere in the world at any time. Video can be viewed on any device that is IP enabled and can run video management software to view and manage images.

BENEFITS OF AN IP VIDEO SURVEILLANCE SYSTEM

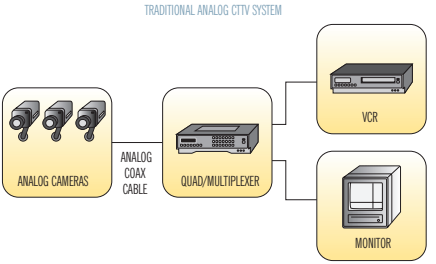
- **Life cycle costs:** Utilizes more cost-efficient infrastructures. Twisted-pair infrastructures are cost effective, well understood and easy to manage.
- **Network convergence:** Only one type of network (IP) supports the enterprise for data, video and voice applications, making management more efficient and cost effective.
- **Systems integration:** IP video surveillance technology provides an open platform for integrating with other security systems such as access control.
- **Scalability:** IP video surveillance scales from one camera to thousands.
- **Remote accessibility:** Any video stream, live or recorded, can be accessed and controlled from any location in the world over wired or wireless network connections.
- **Intelligence at camera level:** Motion detection, event handling, sensor input, relay output, time and date, and other built-in capabilities, such as local file storage, allow the camera to make intelligent decisions (e.g., when to send alarms, when to send video, what frame rate).

A TYPICAL IP VIDEO SURVEILLANCE SYSTEM



Modern Video Surveillance Devices

Today, video surveillance systems may consist of many different products and technologies. Many suppliers build pieces of the system, whether it is part of a hybrid analog/digital implementation or an end-to-end networked IP solution. The following sections explain the evolution of the CCTV system, starting with a fully analog system and adding components until it achieves networked capability.



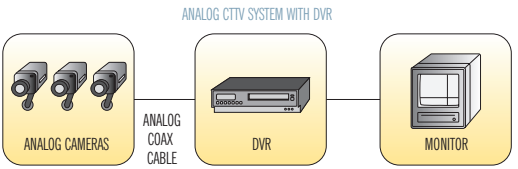
VIDEOCASSETTE RECORDERS (VCRs)

A traditional analog CCTV system, like the one shown at upper right, consists of analog cameras, time-lapse VCRs and monitors. A coaxial cable runs from each camera to a multiplexing device, which allows multiple camera recording on one VCR, with a monitor for viewing. The time-lapse VCR allows the operator to adjust when the VCR records so the standard two-hour VHS tapes can be used for much longer. The trade-off results in lower-quality images in return for less frequent tape changes or image overwriting.

Analog CCTV recording systems have been the basis for surveillance and monitoring for the past 20 years. This technology is extremely old and outdated and is rapidly being replaced by digital recording technology, which now represents over 80 percent of all new installations.

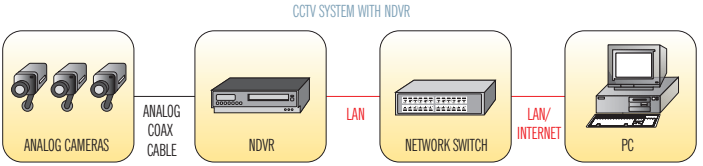
DIGITAL VIDEO RECORDERS (DVRs)

A DVR is a computer with a special video graphics card that connects it to an analog camera via a 75-ohm coaxial cable. This card also converts the analog signal to a digital signal and compresses the resulting image so it can be stored on an internal hard drive to be viewed or transported across a network. DVRs typically utilize a computer operating system such as Windows or Linux along with video management system (VMS) software. DVRs are controlled and accessed via keyboards, a mouse or the front panel in order to set up, monitor and replay stored video. DVRs usually have an internal Ethernet connection for LAN or WAN access so the images can be viewed across a network.



NETWORK-ATTACHED DIGITAL VIDEO RECORDER (NDVRs)

A network-attached digital video recorder is part PC and part "network appliance." A NDVR is very similar to a DVR and is sometimes called a network appliance because it does not require a directly attached keyboard, mouse or video monitor. The device is plugged directly into an Ethernet switch and the only way to access the device is through the network. The device still has an operating system but it resides in firmware burned into a chip on the motherboard. Most of these NDVRs rely on video management software loaded on a network-attached client PC; others have it embedded so that it can be accessed from any PC through an Internet browser. Most of these products have internal hard drives for local video file storage, and some utilize direct attached storage arrays (DAS), network-attached storage (NAS) equipment or storage area networks (SANs) through the LAN or WAN.



NETWORK VIDEO RECORDERS (NVRs)

The "pure" network video recorder (NVR) is not a "turn-key box" or network appliance per se, but created with a combination of network devices. An NVR can be a standard network server with internal or attached storage capability along with recording software, video management or communication software and possibly even intelligent video analysis software. Digitization of the analog video is done by a separate "video encoder" or "video server" (see pages 13 and 14), which is also attached to the Ethernet/IP network. Using an NVR configuration, true IP cameras can act as video servers and input images directly to the NVR and be managed directly by the NVR video software.

VIDEO ENCODERS & DECODERS (CODECS)

Encoders are used to take video signals in analog or digital form and make them suitable for transmission where bandwidth or storage capacity is an issue. Encoding applies to many video surveillance applications where digital recording devices are used or where viewing across a network is desired. Analog signals must first be converted to a digital format, but then each source must be compressed into a smaller size file or video "stream." There are several standards for encoding/decoding and compression (see table below); each one has its advantages and disadvantages. Typically the trade-off is lower quality for reduced file size.

A decoder is a device that does the reverse of an encoder, undoing the encoding so that the original information can be retrieved. The same method used to encode is usually just reversed in order to decode. These are still relatively simple devices, which can be a software program running on a PC, a DVD player or even a cell phone. They may also be hardware devices that take the digital video format and convert it back into an analog signal that can be displayed on an analog monitor. This allows the networked video to become switched across any output device. Usually the decoding and encoding functions reside in the same device and is commonly referred to as a "codec," an acronym for code/decode.

ANALOG TO DIGITAL CONVERSION AND COMPRESSION STANDARDS

Standard codec formats are:

- **MJPEG (Motion JPEG)**: A stream of individually compressed still pictures flowed together continuously.
- **Wavelet:** A mathematical function used in compressing images. Images compressed using wavelets are smaller than JPEG images and can be transferred and downloaded at quicker speeds. Wavelet technology can compress color images from 20:1 to 300:1, grayscale images from 10:1 to 50:1.
- **MPEG:** Newer, more robust, potentially higher quality and network friendly format, MPEG focuses on the differences in two compressed frames. The first image is used as the main reference image. Only the differences from that main image are transmitted and combined with the main image to create a new frame for viewing. The Motion Picture Experts Group (MPEG) is a working group of ISO/IEC charged with the development of video and audio encoding standards. Since its first meeting in 1988, MPEG has grown to include approximately 350 members from various industries and universities. MPEG's official designation is ISO/IEC JTC1/SC29 WG11.

MPEG (pronounced EHM-pheg) has standardized the following compression formats and ancillary standards:

- **MPEG-1:** Initial video and audio compression standard. Later used as the standard for Video CDs, and includes the popular MP3 audio compression format.
- **MPEG-2:** Transport, video and audio standards for broadcast-quality television. Used for over-the-air digital television ATSC, DVB and ISDB, digital satellite TV services like DirecTV, digital cable television signals, and (with slight modifications) for DVDs.
- **MPEG-3:** Originally designed for HDTV, but abandoned when it was discovered that MPEG-2 was sufficient for HDTV.
- **MPEG-4:** Expands MPEG-1 to support video/audio "objects," 3D content, low bit rate encoding and support for digital rights management (copyright). Several new (newer than MPEG-2 Video) higher efficiency video standards are included (an alternative to MPEG-2 Video), notably Advanced Simple Profile and H.264/MPEG-4 AVC.

VIDEO ENCODERS

Analog cameras can be integrated into a network video system with the use of a video encoder.

An encoder typically has between one and 16 analog ports for analog cameras to plug into, as well as an Ethernet port for connection to the network. Like network cameras, it contains a built-in Web server, a compression chip and an operating system so that incoming analog feeds can be converted into digital video to be transmitted and recorded over the computer network for accessibility and viewing.

Encoders digitize analog video sources—effectively turning an analog camera into a network camera. This makes them ideal for integration with existing analog CCTV (closed circuit television) systems when distribution of digital images over a computer network is desired. An encoder may include one or more analog video inputs, an image digitizer and compressor, a Web server and a network/phone modem connection.

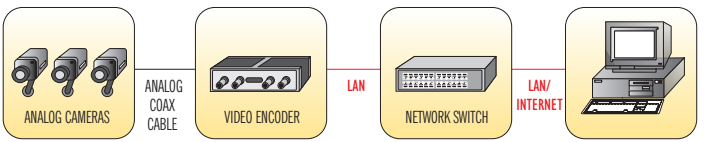
When there's already a substantial investment in an analog surveillance system but a desire to achieve the benefits of digital, adding video encoders can be a worthwhile and cost-effective solution. An encoder can address issues such as poor quality video, worn out tapes, video recorders that constantly need servicing, and a need to access live images remotely. This can be an effective way to maximize equipment investment and begin a migration to networked video.

One of the greatest advantages of a video encoder is that it provides the ability to remotely view live digital images (derived from analog cameras) at any time, from any location using a network computer. This allows the operator to check on events while on the road or at home. (Access to live images can be restricted to only authorized users through several levels of password protection.) In addition, images from an alarm event can be easily distributed to personnel in other locations for further examination via the network. "Going digital" also means crisp, quality images that can be stored on hard drives.

This approach eliminates the need to buy videotapes, change videotapes or service the VCR. Digital storage also reduces the risk of image degradation and provides quick and easy search capabilities.

Video encoders are often considered a good interim step in a planned migration to a full IP surveillance network.

VIDEO SURVEILLANCE SYSTEM WITH ANALOG CAMERAS AND VIDEO ENCODER



NETWORK CAMERAS

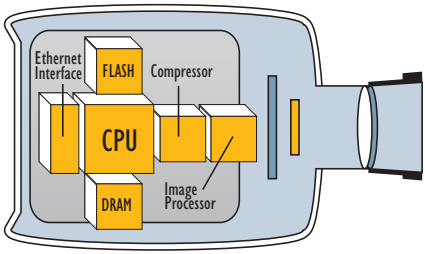
A network camera or IP camera is a video camera with a computer in it. It captures and transmits live images directly over an Ethernet/IP network, enabling authorized users to view, store and manage video locally or remotely over a standard IP-based network infrastructure.

A network camera has its own IP address and connects to the network with a standard RJ45 jack. It often has a built-in Web server, e-mail client, FTP client and FTP server and increasingly supports the latest Power over Ethernet (PoE) standards. Network cameras have alarm management capabilities, programmability and many other special features. Unlike a Web camera that must connect to a PC, a network camera operates independently and can be placed wherever there is an Ethernet connection.

In addition to video, a network camera also includes other functionalities and information being transported over the same network connection, e.g., digital inputs and outputs, audio, serial ports for serial data or control of pan/tilt/zoom (PTZ) mechanisms.

The image processor maintains all the camera functions including:

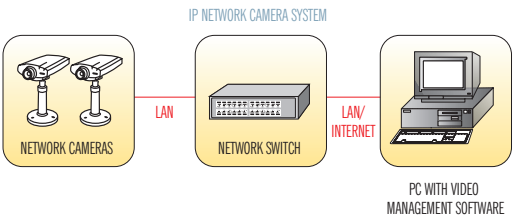
- The drive for the sensor
- Adjustments for lighting
- Image delivery to the computer.



The computer consists of the compressor, the CPU, the flash and the DRAM. The computer functionalities include:

- ASIC to compress and enhance the video
- A response to a request for images
- Image delivery
- A platform for management
- Programmability (e-mail, FTP, notifications).

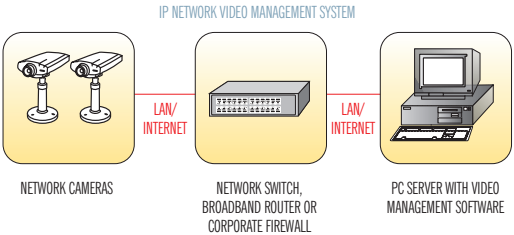
In past years, network cameras did not have the same performance capabilities as analog cameras, but times have changed. Network camera technology has caught up and now meets the same requirements and specifications, and many surpass the performance of analog cameras offering a number of advanced functions. According to JP Freeman, by the end of 2008, the percentage of network cameras being installed will near 20 percent in new installations.



VIDEO MANAGEMENT SOFTWARE (VMS)

Video management software supplies the basis for monitoring network cameras, controlling image analysis and recording. A wide range of software is available, based on user requirements. A standard Web browser provides adequate viewing for many network video applications, utilizing the Web interface built into the network camera.

To view several network cameras at the same time, dedicated video management software is required. In its simplest form, it offers live viewing, storing and retrieving of video sequences.



ADVANCED VIDEO MANAGEMENT SOFTWARE CONTAINS FEATURES SUCH AS:

- Simultaneous viewing and recording of live video from multiple network cameras
- Several recording modes: continuous, scheduled, “on alarm” and “on motion” detection
- Capacity to handle high frame rates and large amounts of data
- Multiple and user-definable search functions for recorded events
- Remote access via a Web browser, client software and even a PDA client
  - Control of pan/tilt/zoom (PTZ) and dome cameras
  - Alarm management functions (sound alarm, pop-up windows or e-mail)
  - Full duplex, real-time audio support
  - Video intelligence.

Migration to a Digital Networked Solution

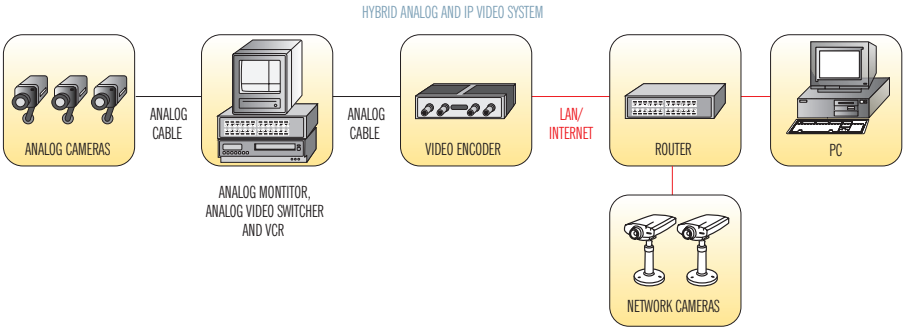
Because there is significant financial investment in analog CCTV, many security managers opt for a phased transition strategy to IP, blending both analog and digital security technologies wherever possible during the migration. Integrating existing analog equipment with products that provide the functionality of a digital system offers several benefits:

- Remote accessibility
- Cost effectiveness
- Flexibility
- Scalability.

In the simple illustration below, the analog cameras are connected to an analog video switcher, an analog monitor, a VCR and a video encoder. This traditional setup provides sequential monitoring and recording of multiple analog cameras. By connecting an IP video encoder to convert the analog video into digital data, images can be sent over an Ethernet/IP network (through a router/switch), which provides Ethernet connections for several networked IP cameras. With this configuration, authorized security personnel in local or remote locations can view video originating from both analog and digital networked IP cameras.

In the transition from analog to digital surveillance systems, any sized analog system can benefit from some measure of digital technology.

The following section describes system components and illustrates migration rationale and methods that can facilitate transitions from traditional to state-of-the-art video surveillance systems.



CABLING INFRASTRUCTURES

As the video surveillance industry evolves and new digital and IP-based technologies are developed, the cabling infrastructures that support these systems must also change. Today, video surveillance infrastructures range from traditional coaxial and multiconductor cables to twisted-pair and wireless solutions. With so many choices, it can be a challenge selecting a video surveillance infrastructure that is cost effective, provides room for future growth and offers the ability to migrate to new technologies.

Traditional video surveillance infrastructures have not changed for more than 20 years. These cabling systems distribute video signals over coaxial cables like RG59 or RG6, while power and control signals travel over multi-conductor 18 gauge cables.

Traditional Infrastructures

Currently, there are two methods of installing traditional video surveillance cabling systems–the "home run" method and the "star wired" approach–each using coaxial cabling.

Home Run Method

The most commonly used installation method of the traditional video surveillance cabling system is done via the home run method using coaxial cabling. The home run coaxial and multi-conductor cables are run from every camera to a central security headend location where monitors, controls and recording equipment are maintained.

The home run cables for any given camera may use up to three cables and include up to 14 conductors. These wires conduct video signal, power, pan/tilt/zoom (PTZ) capability, blower, heater and preset controls back to the security office. Cabling schemes are often proprietary, thus moving or installing additional cameras is expensive and may require all new cable. Cabling distribution is not structured with a logical hierarchy, as in the case of telecommunications cabling networks, so troubleshooting is often difficult and long system outages can result. Bundles of CCTV cables penetrate walls and floors and travel through ceilings and between floors in a haphazard run to the control room. There are no national standards for cable distance, installation practices or minimum cable performance levels. A lack of standards often results in poorly installed or designed networks. Video signal noise, power phase differences and unintended ground loops can be the result. Electromagnetic Interference (EMI), unsynchronized power and ground loops are common in traditional video surveillance infrastructures and typically result in video signal noise and loss of image quality.

The traditional home run approach is both cumbersome and inflexible. It uses many coaxial and stranded power/control cables that take up a lot of space, contribute significantly more weight to ceiling structures and are difficult to troubleshoot system problems. These systems are difficult to enhance with new technology and lack any migration capabilities toward IP platforms. Additionally, traditional CCTV systems do not have a standardized method to power cameras.

MYTH

Network cameras are more expensive than analog cameras, making IP surveillance too costly an investment.

REALITY

If we were to compare the overall cost of the hardware, an IP surveillance system will usually compare quite favorably to a traditional analog system. But the real value becomes apparent when you consider the additional functionality, open platform architecture and integration with other security devices such as access control. If you then consider the installation element, the advantages with the IP surveillance system become even more attractive. The IP surveillance infrastructure can be added to or run in parallel with an organization's existing IT cabling, achieving both initial and longer term cost savings.

Star Wired Approach

A star wired installation is not commonly used, but does lend itself to be a more maintenance friendly design. Rather than home running coaxial and multi-conductor cables, the star wired design uses wiring closets where the cable runs from each camera to a BNC connector patch panel. From there, bundled coaxial and multiconductor cables are run together to the security headend. These cables are unbundled and terminated appropriately. The video coax is terminated on another BNC panel for breakout to recording and monitoring equipment.

Traditional infrastructures were designed to support only 75-ohm analog video surveillance technologies and do not

provide a migration path to 100-ohm twisted-pair-based systems. These traditional infrastructures are still popular in the security industry today; however, as more and more IP-based technologies appear, traditional cabling installations will continue to decrease. This means security personnel will need to understand, support and manage twisted-pair-based security infrastructures and equipment.

Star wired or standards-based structured cabling systems help create a modular cabling infrastructure that easily expands without disrupting neighboring devices. By simply connecting a new device to the nearest closet, there is no need to install a home run of cable back to the headend. Therefore, devices can easily be added at a reduced cost over home run environments. Additionally, isolating faults within the cabling system is easier because the intermediate patching points allow the troubleshooter to easily identify different segments of the cabling infrastructure, reducing the time it takes to find the cable fault.

Wireless Infrastructures

Wireless video surveillance is perfect for organizations that have multiple remote locations or mobile users scattered throughout a town, city or large campus area. Wireless video provides a cost-effective method of distributing video signals over the air at great distances to mobile security personnel and first responders, or in environments where it is either too expensive or too difficult to install a wired infrastructure.

Wireless infrastructures employ receivers and transmitters mounted on buildings, water towers or any high structure to permit optimal reach. Today, wireless infrastructures are capable of transmitting video surveillance images to recording and monitoring equipment more than 50 miles (80 kilometers) away.

Fiber Optic Infrastructures

Video surveillance over fiber optic cabling infrastructures is an excellent solution for camera installations that exceed the distance limitations of coaxial and twisted-pair cabling. These systems use either multimode or single-mode fibers to transport video images of cameras to recording and monitoring equipment. Fiber infrastructures use various electronic multiplexing devices to convert video and data signals into optical signals at the camera site or in wiring closets. The video and data signals are then reconverted back to either 75-ohm (traditional) or 100-ohm (digital/IP) signals in the security headend for connection to recording and monitoring equipment.

Twisted-Pair Infrastructures

Twisted-pair infrastructures are ideal for supporting both legacy analog systems and digital/IP video surveillance technologies if properly designed to industry data communications standards.

Ethernet/IP devices act as any other node or workstation on a network and can be plugged into any open port or appropriate outlet. Usually, new horizontal runs of twisted-pair cabling are installed high on a wall or in a ceiling so cameras can be placed at appropriate viewing

MYTH

Transmitting video over an IP network is not secure.

REALITY

As with any data network, providing that the correct security measures such as firewalls, VPNs and password protection are implemented, IP surveillance is just as secure as the millions of financial transactions made online every day. If this is compared to typical analog surveillance systems that have no encryption or authentication methods, then it is clear that bringing security into an existing IT security environment has many benefits.

positions. These cameras also need access to power in these spots, sometimes requiring new AC outlets.

Data networks can also be used to support the distribution of analog video through the use of video "baluns" that connect coaxial cables to twisted-pair cables. Baluns (balanced/unbalanced adapters) convert an unbalanced 75-ohm analog video signal to a balanced 100-ohm video signal.

Another type of twisted-pair replacement technology being installed today just replaces traditional coaxial cable with two twisted-pair cables. This reduces the installed cost but doesn't support Ethernet-based IP devices such as cameras or servers, which require high-performance 4-pair twisted-pair cables that meet industry standards such as TIA/EIA-568B.

MYTH

IP surveillance is less reliable than analog solutions; for example, the network could go down.

REALITY

IP surveillance can utilize a whole range of IT devices and practices to allow the administrators a more interactive approach to system management. For example, IP-based environmental monitoring devices can provide alerts based on increased temperature or water ingress, thereby reducing potential downtime. These devices can work in conjunction with network management systems that monitor and manage the overall health and performance of the network. With all the appropriate measures in place, usually as part of the existing data network, IP surveillance is in many cases more reliable.

POWER OVER ETHERNET (PoE)

Power over Ethernet, as defined in the IEEE standard 802.3af, enables DC power to run over Ethernet cables to devices that need to be powered, such as IP telephones, wireless LAN access points, security network cameras and much more. This is economical for many reasons, mainly because of the structured cabling infrastructure already in place. PoE simply utilizes two pairs within the standard twisted-pair cabling system, eliminating the need for running additional wiring for power.

Adding electrical outlets in multiple locations can be costly. Surveillance cameras, for example, often need to be installed in highly elevated places for optimum surveillance. Supplying AC to out-of-reach locations is cumbersome, and getting an electrician to pull power cable costs valuable time and money. If an electrical circuit goes down, the surveillance coverage becomes inconsistent. If PoE is available, the cameras can be installed where they are most effective, regardless of where electrical outlets exist.

Power over Ethernet is the ideal power solution for a vast array of data and security equipment for business and industry use. Primary markets include virtually any enterprise with an existing Ethernet network.

PoE System Design

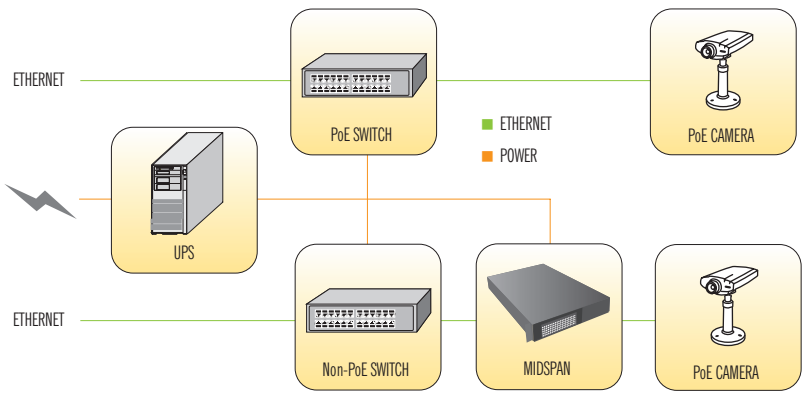
There are two main components of a PoE system. The powered device, which is on the receiving end of the system, is the device that needs power in order to work. It can include IP telephones, wireless LAN access points, security network cameras, or any IP device that needs power. The power source is the element of the system that is responsible for supplying the power onto Ethernet cable, and ultimately to the device that needs power. If the power source is located in the Ethernet switch, it is referred to as an endspan configuration. If it is located between the switch and the device that needs powering, it is known as a midspan configuration. The midspan is a form of patch panel that receives data from the switch and sends power out over the unused pairs to the devices that need to be powered.

Power over Ethernet midspan is the first system on the market to supply reliable, uninterrupted power to IP devices using an existing LAN cabling infrastructure. This technology, when used in conjunction with a centralized UPS, helps maintain continuous operation during power failures, while eliminating the time and cost of installing separate power cabling and providing a dedicated, uninterrupted power supply for individual terminals and devices.

BENEFITS OF PoE

- **Cost Saving:** Installation of separate data and power infrastructures is avoided saving both time and money.
- **Simplicity:** Powering devices in areas where there is no outlet is as easy as installing the device anywhere there is an Ethernet connection.
- **Mobility:** Moving powered devices is no longer strategically planned by the proximity of an electrical outlet.
- **Safety:** No mains voltage usage, only safe direct-current 48 V levels.
- **Control:** SNMP management offers complete management capabilities for easy online supervision, configuration, monitoring and control.

POWER OPTIONS FOR IP CAMERAS



IEEE 802.3af Specification

Supplying Power over Ethernet according to the IEEE 802.3af standard is strongly recommended. This standard specifies the following:

- Operating voltage should always be under the maximum Secondary Low Voltage (SELV) requirement of 60 V DC as defined by the EN60950, the standard for Safety of Information Technology Equipment. Typically it is 48 V DC, but it can vary from 44 to 57 V DC.
- In order to protect the Ethernet cables from over-heating, the maximum current generated by the power source must be between 350 to 400 mA.
- The maximum wattage a power source can output is 15.4 watts; the delivered power to the device can be as low as 12.95 watts.

Currently, there is a study group in IEEE attempting to modify the current 802.3af standard to increase the source power delivered to a PoE device from 15.4 watts to a minimum 30 watts. The new standard will be called 802.3at, or PoE Plus, and is required for most PTZ IP cameras and newer Wi-Fi end stations. This new standard will allow significantly more markets to take advantage of the benefits of this advanced technology.

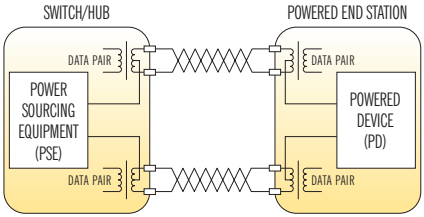
Market	Application	Power Requirement
WLAN	Dual band APs	~20 W
	802.11n APs	~20 W
	Outdoor APs/Bridges	20 W – 30 W
Security	PTZ Network camera	15 W – 20 W
IP Telephony	Video phones	15 W – 25 W
New Markets	RFID readers and access control systems	Up to 25 W
	802.16 Base stations	15 W to 60 W
	Workgroup switches	Up to 50 W
	Residential gateways	~20 W
	Industrial sensors	1 W to 30 W
	Laptops	Up to 70 W
	Point of sales and information kiosks	13 W to 60 W

MEDIUM-DEPENDENT INTERFACE (MDI) SETTINGS

The Medium-Dependent Interface (MDI or RJ45) serves as the data/power interface between Ethernet elements. It has two optional connection methods to carry the power, named alternatives A and B.

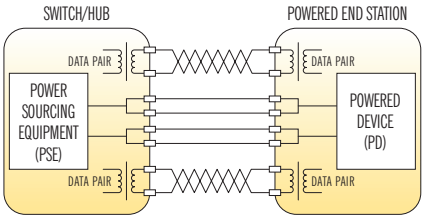
In alternative A, power is carried on two pairs (1/2 and 3/6). This method guarantees that bi-directional flow is maintained, regardless of the module's power status. Alternative B uses the spare pairs (4/5 and 7/8) for power. Endspans typically use the alternative A wiring option, and midspans use the alternative B wiring option.

ALTERNATIVE A (MIDSPAN)



ENDPOINT PSE, ALTERNATIVE A

ALTERNATIVE B (ENDSPAN)



ENDPOINT PSE, ALTERNATIVE B

PoE CHALLENGES

There are many challenges that need to be considered when putting a PoE system in place. The power source must not damage any of the cabling infrastructure or any of the non-powered devices that are attached to the infrastructure. A valid power device must be detected by the power source before any power is applied, thus ensuring safety to non-powered enabled devices. This "line detection" requires the power source to look for a 25 KΩ signature resistor. If the line detects a signature resistor, it means there is a valid power device and power can then be distributed to that device.

Conclusion and Recommendations

PREPARE FOR NETWORKED VIDEO SURVEILLANCE

The state of the CCTV industry and video surveillance equipment is changing rapidly as new technologies force security professionals into the domain of Information Technologies (IT) and vice versa. Cameras will ultimately reside on networks in some form, whether they are directly attached as Ethernet/IP devices, or converted to IP devices through encoders or video servers. Operating systems and video management software will become open-source, have a wider range of capabilities and be customizable for specific vertical markets.

In today's environment, companies must continually explore new and better ways to protect people and assets. Computer networking and microprocessor technologies along with innovative software applications are making video surveillance immensely more effective and manageable. With today's sophisticated equipment and the promise of continued technological advancement, networked IP video surveillance will become better understood. It will quickly move from the realm of future consideration to a "must have." The financial benefits of IP surveillance and anywhere/anytime access are already resonating within businesses large and small. With the exponential growth in Internet use and mainstreaming of Ethernet/IP networks, the benefits of computer networked security solutions are quickly becoming evident to the security industry's risk management professionals and IT organizations alike.

CREATE A MIGRATION PLAN

Video surveillance solutions are moving from traditional designs through planned hybrid phases of combined analog and digital equipment to ultimately rest on an Ethernet/IP network. In order to facilitate this transition with minimal financial and logistical impact, the physical cabling infrastructure must be designed with security requirements in mind. It must provide a stable foundation throughout this migration period.

With a myriad of advancements in voice and data communications, video surveillance and other security applications, companies are poised to reap the benefits of greatly improved protection, increased flexibility, simpler management and significant return on investment. Advanced planning is essential to a smooth and cost-effective transition.

UTILIZE ANIXTER RESOURCES

Anixter is uniquely qualified to help security and IT professionals plan and implement traditional hybrid or IP-based video surveillance systems. Anixter's resources not only understand technology, equipment and infrastructure, but also understand how to meet risk management challenges with proven security solutions. Anixter can help your organization make solid choices on systems, equipment and manufacturers. Use Anixter's industry expertise to help you build a utility-grade infrastructure to support your video surveillance requirements. Anixter can help you customize your systems with whatever combination of video surveillance and security products meet your specific requirements.

Security Systems Accessories

If you are managing a security project, products such as the camera, the DVR and the cable are obviously required. But there are many ancillary items, everything from grounding lugs to cable trays to racks, that are vital to making your security project a success. Installers waiting around on the job for a part to arrive or driving to a big box retailer to overpay for material can wreak havoc on a project's time schedule and budget.

You can count on Anixter to provide you with all of the products you need for any project big or small. If you are doing a video surveillance, access control or sound project, Anixter has all the products necessary to build your complete bill of materials.

- Access control products
- Batteries
- Cable ties
- Cameras
- Copper cable and connectivity
- DVRs
- Electrical and electronic wire and cable
- Encoders/decoders
- Fiber cable and connectivity
- Firestop
- Grounding equipment
- ID products
- Intrusion products
- Lenses
- Monitors
- Mounts and enclosures
- Networking products
- Outside plant products
- PoE
- Racks, cabinets and cable management
- Software
- Test equipment
- Tools
- UPS and power protection
- Video management software
- Voice and sound products
- Wireless products

Appendix–About Anixter

THE ANIXTER DIFFERENCE

We're proud to serve more than 100,000 customers across 50 countries every day with our world-class inventory, global capabilities, technical expertise and Supply Chain Solutions. Our specialized sales forces focus on Enterprise Cabling Solutions, Security Solutions, Electrical and Electronic Wire & Cable and Fasteners.

- We stock more than 450,000 items from the world's premier manufacturers and move them cost effectively through our global distribution network that encompasses more than 7 million square feet of distribution space.
- We view technical know how as an essential part of our value to our customers. You can always count on Anixter for reliable up-to-date technical advice and assistance.
- With a wide variety of Supply Chain Solutions to choose from, we provide our customers the opportunity to save money by increasing their ability to be efficient and to avoid costly delays.

OUR PRODUCTS

It seems simple enough: you need something, you call a distributor and buy it. Unfortunately, nothing is really that simple. In the real world, there are complicated systems, small parts, and constantly changing technical developments and requirements. Just determining what you need can be an all-consuming process, one that is only aggravated by hard to find or out of stock items. Missing a crucial component can significantly add costs and delays to your projects.

At Anixter, we take the worry out of just-in-time product availability. We maintain more than $1 billion in our global inventory, and the product expertise you need to make sure you get the right product, when and where you need it.

Anixter is the distributor to call if you need products and systems for:

- Network cabling (copper and fiber)
- Security (video surveillance, access control, door-locking hardware)
- Electrical wire and cable (power cable)
- Electronic wire and cable (coax, multi-pair, multiconductor cable, etc.)
- Networking, wireless and voice electronics
- Fasteners and other small components ("C" Class).

OUR TECHNICAL EXPERTISE

Across the world, we have more than 2,600 sales specialists who support our customers. We have three specialized sales forces that focus on enterprise cabling and security systems, electrical and electronic wire and cable, and fasteners. These sales specialists have years of experience in specifying products and solutions for customers. Our salespeople are well trained to truly identify and understand your needs and requirements.

Anixter's expert Systems Engineers (SEs) receive ongoing, extensive training about new products, technologies, applications and market trends. In addition, many of our SEs participate in local standards and industry committees and associations, which keeps them current on the latest standards being introduced into the market. Anixter also employs over 135 RCDDs (Registered Communications Distribution Designer), the highest networking infrastructure design certification.

In every part of our business, we welcome the opportunity to support our customers' purchasing

decisions. You can rely on our technical experts to keep you current on the latest products, applications, industry trends, standards and emerging technologies.

THE ANIXTER INFRASTRUCTURE SOLUTIONS LAB

Anixter's Infrastructure Solutions Lab allows us to actively demonstrate the best practical technological solutions from best-in-class manufacturers in the area of enterprise cabling solutions, video security and access control systems for our customers. Our mission for The Lab is simple—educate, demonstrate and evaluate.

- Educate customers on the latest industry standards and technologies.
- Demonstrate the latest infrastructure product solutions available from our manufacturer partners.
- Evaluate our network infrastructure and security solutions to help our customers select the right products for their specific needs.

We are continually testing products in our Lab:

- Quality products are recommended and delivered to our customers
- Consistency of performance across product lines and within systems
- Interoperability of products and systems to help customers integrate systems and follow the trend toward convergence.

NETWORKING AND SECURITY PRODUCT TESTING AT OUR LAB INCLUDES:

- Random performance testing of Anixter inventory to ensure quality of standards compliance
- Network throughput and interoperability testing
- Copper and fiber cabling compliance verification (TIA/EIA, ISO/IEC, IEEE)
- Customer proof of concept
- Application testing
- 10 Gig Ethernet cabling testing
- Video over IP, video quality and bandwidth utilization
- Power over Ethernet (PoE) capability and verification
- Digital compression image quality vs. analog technology testing
- Evaluation of analog and IP cameras, video management software, DVR, NDVR and NVR products.

OUR SUPPLY CHAIN SOLUTIONS

The foundation to an efficient security deployment is having a fundamental distribution network that you can leverage for product inventory and coordinated deliveries. Fundamental distribution services should include:

- The ability to view and allocate inventory in any warehouses in the nationwide network
- A significant investment in a diverse breadth of inventory
- IT systems that provide customers real-time information
- Predictable (e.g., next day ground service) delivery times to help you plan your projects.

Anixter takes fundamental distribution a step further by applying the best practices of supply chain principles to our industry and the reality we face every day with technology deployments.

Our goal is to help you:

- Reduce costs
- Complete projects on time and on budget
- Improve efficiency
- Create scalable and repeatable services.

READY! BY ANIXTER
DEPLOYMENT SERVICES

READY!℠ Deployment Services by Anixter maps our distribution and Supply Chain Solutions to the construction or deployment process of any technology project. We combine sourcing, inventory management, kitting, labeling, packaging and deployment services to simplify and address the material management challenges at the job site(s). READY! Deployment Services by Anixter will help you improve the speed to deployment, lower your total cost of deployment and deliver your product specifications as planned.

READY! Deployment Services Can:

- Simplify material management at the job site
- Simplify on-site storage requirements
- Confirm product specifications
- Increase speed of deployment
- Reduce damaged, lost or stolen material at the job site
- Reduce packaging waste at the construction site
- Minimize will calls, go backs and set-up time
- Increase productivity
- Decrease total cost of deployment

"Poor supply chain design regularly increases project costs by 10 percent or more; project duration might be similarly affected."

University of Florida

A Case Study: Anixter Helps Secure A Large U.S. City

CUSTOMER CHALLENGE

A large, global security integrator secured an assignment to develop and implement a security system for a major metropolitan city. The challenge: not just deploy surveillance cameras throughout the city's business district – one of the largest in the U.S. – but also seamlessly integrate them into the recent beautification efforts without sacrificing security. The initial phase of the security project called for installing over 260 cameras on existing light poles. As it often does, the integrator turned to an alliance partner, Anixter, for assistance with the complex infrastructure required.

ANIXTER SOLUTION

Customized cameras, camera housings and wireless infrastructure were required for this project. In addition to providing all of the necessary products for the project, Anixter worked with the integrator to better understand the installation build out process. By doing so, Anixter was able to leverage its READY!℠ Deployment Services to develop a customized, value-added services plan that helped with a smooth installation process while meeting the city's deadline. Among the benefits that READY! Deployment Services offers are simplified project/material management; a reduction in lost, damaged or stolen materials from a job site along with reduced packaging waste; and more accurate product specification.

The deployment plan for the security cameras included sourcing and inventorying the product, coordinating with multiple manufacturers and subcontractors, managing lead times as well as providing Kitting and Pre-Assembly services for the READY! Camera kits in our local warehouses. As a result, Anixter was able to decrease the time it took the installers to install the cameras and make them fully operational.

PROGRAM RESULTS

To minimize disruption to local businesses, the project was completed after business hours, and within a few days of installation, the cameras went "online." Prior to the system's implementation, it was not possible to keep a watchful eye on as many potential "hot spots" that now have an added layer of protection.

At the end of the day, Anixter was able to deliver a unique, customized solution to the city and the integrator on time and on budget. "Working on such a high-profile project requires the expertise and professionalism that we have come to count on from Anixter," said the integrator customer. "More than just a partner, in many ways they operate as an extension of our technology adoption area by anticipating our needs and providing sensible, cost-effective solutions."

OUR GLOBAL CAPABILITIES

We are very proud of the quality products we distribute (more than 400,000 items from the best manufacturers in the industry) but the reason our customers count on us day in and day out isn't just about world-class, quality products. Our customers know they can count on Anixter to deliver consistent, superior service and support around the world. And when we say we're global, we mean it. We don't just ship products from the U.S. to various countries. We stock inventory in each country and we are specialists at moving inventory across borders efficiently and cost effectively. We're physically located in 49 countries around the globe, and our in-country sales specialists are familiar with the trends and needs of the local market, as well as local currencies, standards and customs. We speak 30 different languages, to serve our customers' diverse needs.

Anixter is located in 249 cities in 49 countries.

See if Anixter is located in a city near you at the end of this guide.

For more detailed information on networking standards or security infrastructure, order one of Anixter's helpful reference guides at anixter.com/literature

Anixter's Global Presence

Anixter is located in over 260 cities around the world in more than 50 countries.

Anixter Association and Committee Memberships

- Telecommunications Industry Association (TIA)
- International Organization for Standardization (ISO)
- Institute of Electrical & Electronics Engineers (IEEE)
- ONVIF
- Building Industry Consulting Services International (BICSI)
- Security Industry Association (SIA)
- Control Systems Integrators Association (CSIA)

Technical Certifications

- More than 100 Registered BICSI RCDDs
- PSPs (Physical Security Professional Certification)
- CCNAs (Cisco Certified Network Associate)

Corporate Snapshot:

Year founded: **1957**
Number of employees: **Over 8,200**
2011 Revenues: **$6.1 billion**
Products: **More Than 450,000**
Inventory: **Over $1 billion**

Customers: **Over 100,000**
Stock symbol: **AXE**
Countries: **More Than 50**
Fortune 500 List

NORTH AMERICA – USA

Worldwide HQ
Glenview, IL
224.521.8000

CANADA HQ

Toronto, Ontario
905.568.8999

LATIN AMERICA HQ

Glenview, IL
224.521.8000

EUROPE/MIDDLE EAST/AFRICA HQ

Enterprise Cable & Security HQ
Uxbridge, England
+44.1895.818181

Wire & Cable HQ
Warrington, England
+44.1925.838658

Fasteners HQ
Gloucester, England
+44.1452.880500

ASIA/PACIFIC

Asia/Pacific HQ
Singapore
+65.6508.1600

South Pacific HQ
Sydney, Australia
612.9.333.0800

INTERNATIONAL SERVICES

Glenview, IL
224.521.8000

AFTER HOURS

USA
800.323.8167

Canada
800.361.0250

USA

Alabama
Dadeville
Alaska
Anchorage
Arizona
Nogales
Phoenix
Arkansas
Fort Smith
California
Anaheim
Burbank
Fresno
Los Angeles
Pleasanton
Sacramento
San Diego
San Jose
Colorado
Denver
Connecticut
Cheshire
Florida
Delray Beach
Fort Lauderdale
Jacksonville
Miami
Orlando
St. Petersburg
Tampa
Georgia
Americus
Atlanta
Dublin
Vidalia
Idaho
Boise
Illinois
Bloomington
Mount Prospect
Princeton
Wood Dale
Indiana
Columbus
Fort Wayne
Indianapolis
Iowa
Des Moines
Kansas
Hesston
Kentucky
Cadiz
Louisville
Louisiana
New Orleans
Maryland
Baltimore
Massachusetts
Boston
Michigan
Detroit
Grand Rapids
Minnesota
Eden Prairie
Minneapolis
Thief River Falls
Windom
Mississippi
Gulfport
Missouri
Kansas City
St. Louis
Nebraska
Grand Island
Omaha
Nevada
Las Vegas
New Hampshire
Nashau
Salem
New Jersey
Cranbury
Florham Park
New Mexico
Albuquerque
New York
Albany
New York
Rochester
North Carolina
Charlotte
Raleigh
Rocky Mount
Ohio
Ashland
Chillicothe
Cincinnati
Cleveland
Columbus
Oklahoma
Tulsa
Oregon
Portland
Pennsylvania
Allentown
Erie
Lewisberry
Philadelphia
Pittsburgh
South Carolina
Greenville
North Charleston
Tennessee
Jackson
Memphis
Nashville
Texas
Austin
Dallas
El Paso
Houston
McAllen
San Antonio
Tyler
Utah
Salt Lake City
Virginia
Dulles
Norfolk
Richmond
Washington
Renton
Seattle
Wisconsin
Appleton
Kenosha
Manitowoc
Milwaukee
Tomah

CANADA

Alberta
Calgary
Edmonton
British Columbia
Vancouver
Manitoba
Winnipeg
Nova Scotia
Halifax
Newfoundland
St. John's
Ontario
Hamilton
Kitchner
London
Ottawa
Toronto
Sudbury
Thunder Bay
Quebec
Abitibi
Montreal
Quebec City
Saskatchewan
Saskatoon

LATIN AMERICA

Argentina
Buenos Aires
Cordoba
Brazil
Curitibal
São Paulo
Caribbean (English)
Miami, FL
Chile
Santiago
Colombia
Bogotá
Medellin
Costa Rica
San Jose
Dominican Republic
Santo Domingo
Ecuador
Quito
Jamaica
Kingston
Mexico
Aquascalientes
Guadalajara
Juarez
Mexicali
Mexico City
Monterrey
Panama
Panama City
Peru
Arequipa
Lima
Puerto Rico
San Juan
Venezuela
Caracas
Uruguay
Barbados

EUROPE/MIDDLE EAST/AFRICA

United Kingdom
Aberdeen
Barrow in Furness
Belfast
Birmingham
Bredbury
Chesterfield
Coventry
Diss
Dorset
Edinburgh
Ellesmere Port
Gateshead
Glasgow
Gloucester
Leeds
Liverpool
Luton
Newtonabbey
Nottingham
Peterborough
Plymouth
Rotherham
Sheffield
Uxbridge
Warrington
Austria
Vienna
Belgium
Willebroek
Czech Republic
Prague
Denmark
Ansvej
Copenhagen
Finland
Helsinki
France
Lyon
Paris
Sarreguemines
Germany
Bielefeld
Dillingen
Frankfort
Mannheim
Stuttgart
Hungary
Budapest
Republic of Ireland
Dublin
Italy
Bari
Brescia
Milan
Reggiolo
Rovereto
Morocco
Casablanca
Netherlands
Capelle aan den IJssel
Norway
Oslo
Poland
Warsaw
Portugal
Lisbon
Russia
Moscow
Saudi Arabia
Riyadh
Slovakia
Bratislava
Spain
Barcelona
Madrid
Sweden
Gothenburg
Stockholm
Switzerland
Montreux
Zurich
Turkey
Istanbul
United Arab Emirates
Dubai
Oman
Qatar

ASIA/PACIFIC

Australia
Brisbane
Melbourne
Perth
Sydney
China
Beijing
Shanghai
Shenzhen
Suzhou
Hong Kong
India
Bangalore
Chennai
Mumbai
New Delhi
Indonesia
Jakarta
Japan
Tokyo
Malaysia
Kuala Lumpur
Penang
New Zealand
Auckland
Philippines
Manila
Singapore
Singapore
Taiwan
Taipei
Thailand
Bangkok
Vietnam
Ho Chi Minh

Electrical and Electronic Wire & Cable • Enterprise Cabling & Security Solutions • Fasteners
Anixter Inc. World Headquarters • 2301 Patriot Boulevard, Glenview, IL 60026-8020
Anixter Inc. • 1.800.ANIXTER • 224.521.8000 • anixter.com

Anixter is a leading global supplier of communications and security products, electrical and electronic wire and cable, fasteners and other small components. We help our customers specify solutions and make informed purchasing decisions around technology, applications and relevant standards. Throughout the world, we provide innovative supply chain management services to reduce our customers' total cost of production and implementation. A NYSE listed company, Anixter, with its subsidiaries, serves companies in 50 countries around the world. Anixter's total revenue approximated $6.1 billion in 2011.

12H0012X00 © 2012 Anixter Inc. • 09/12