IP Video Surveillance Guide

BMG INFORMATICS PVT. LTD.

Overview:

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

This document summarizes high-level design recommendations and best practices for implementing IP Video Surveillance on the enterprise network infrastructure. In some instances, existing network equipment and topologies have the necessary configuration and performance characteristics to support high-quality IP Video Surveillance. In other instances, network hardware might require upgrading or reconfiguration to support increased bandwidth needed to support video. Quality-of-service (QoS) techniques are important for any design because video has similar—in some instances, more stringent—requirements than VoIP for loss, latency, and jitter. IP Video Surveillance is a part of the Media Ready Network—a network initiative to incorporate all forms of video on the enterprise network

IP Video Surveillance Components

There are five components of IP-based video surveillance solution. These are as follows:

1. Cameras—This is addressed by the IP Camera, analog cameras.
2. Video management software—This is addressed by the Video Surveillance software. This software runs on one or more standalone server.
3. Servers- Server for network video recording and playback.
4. Storage—This is aligned with Video Surveillance Storage System, or with off-the-shelf iSCSI servers for archiving and storage of video feeds.
5. Network—This component is the enterprise network—the Media Ready Network.

Steps to a Successful IP Surveillance Installation:

Step 1: Choosing a network camera

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

Step 2: Compression

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

Step 3: Video Management

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

Step 4: Storage

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

Step 5: Incorporating Analog Cameras

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

Step 6: Wireless Networking

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

Step 7: Designing the Network

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

Step 8: Security

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

Step 9: Hot Technologies

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

Step 10: Best Practices

Over the last few years, thousands of IP surveillance systems have been installed, and many lessons have been learned. These range from simple tips about camera placement and lighting conditions to working with IT departments and technicians to determine issues such as the peak times for network usage. As we close the series, we'll touch on these concerns. By the end of this article series, these 10 steps will enable any security professional to avoid pitfalls and implement best practices, making IP surveillance installations easier to install and manage.

Step 1: Choosing a network camera

When building a surveillance system, it is important to select cameras that meet the needs of your organization and installation. This includes selecting specific types of cameras to meet the locations where cameras are needed and the intricacies of the venue, including fixed, pan/tilt/zoom (PTZ), vandal-proof, or fixed-dome cameras.

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

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

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

Power over Ethernet (PoE) — In most buildings today, TCP/IP infrastructure is available by means of Cat 5 and 6 cabling. The cabling can be used for fast transport of data, and the distribution of power to devices connected to the network, using PoE technology. PoE reduces installation costs by eliminating the need for power outlets at the camera locations and enables easier application of uninterruptible power sup- plies (UPS) to ensure continual operation, even during a power outage. PoE technology is regulated by the IEEE 802.3af standard and is designed to not degrade the network data communication performance. When evaluating PoE enabled network cameras, it is important to look for those that are based on the IEEE standard, to ensure that any brand network switch can be chosen, providing a truly open system.

Progressive scan — Progressive scan capability is found only in network cameras, but not all network cameras have this functionality. Progressive scan involves exposing and capturing the entire image simultaneously. With interlaced scanning, if an object is moving the image will become blurry. In a progressive scan image, all lines are scanned in perfect order so there is virtually no “flickering” effect. While interlaced scanning may be sufficient under certain conditions, progressive scan technology allows for far better image quality on moving objects. In a surveillance application, this can be critical in enabling the user to view detail within a moving image such as a person running away or the license plate on a moving vehicle. When cameras capture moving objects, the sharp- ness of the frozen images depend on the technology used, and progressive scanning consistently produces the best results in clarity and recognizing important details.

JPEG/MPEG4 standards — It is important for any network camera to follow JPEG and MPEG-4 standards in their entirety. This ensures the flexibility to use video for many different applications. It also guarantees that you can view the video many years from now. If a camera uses one company's proprietary compression technology and that company goes out of business, the video will be unreadable in the future.

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

Step 2: Compression

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

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

Compression Terminology

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

There are essentially two approaches to compression: lossless or lossy. In lossless compression, each pixel is unchanged, resulting in an identical image after the image is decompressed for viewing. Files remain relatively large in a lossless system, which makes them impractical for use in network video solutions.

The fundamental idea in lossy compression is to reduce portions of the image that appear invisible to the human eye, thereby decreasing the size of the data transmitted and stored.

Video is essentially a stream of individual images. The most widely accepted standard for still image compression is the Joint Photographic Expert Groups (JPEG) standard. JPEG is by far the most common and most widely supported compression standard for still images.

Video Compression

Video compression uses a similar method as that of still image compression. However, it adds compression between the frames to further reduce the average file size. MPEG is one of the best-known audio and video compression standards. For network video systems, MPEG-4 is a major improvement from MPEG-2. A newer version of MPEG-4 called Part 10 (or AVC - Advanced Video Coding, or H.264) is also available.

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

When designing a network video application, the following issues should be addressed:

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

Step 3: Video Management

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

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

Motion-Based Recording — Video motion detection (VMD) defines activity by analysing data and differences in a series of images. VMD can be performed at the camera level, which is preferred, or reside in the video management software. Video management software can provide motion detection functionality to network cameras not equipped with this feature.

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

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

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

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

Open and Closed

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

Although they are networked, NVRs are dedicated to the specific task of recording, analysing and playing back video. They do not allow other applications to reside on them, so the hardware is essentially “locked.” This means that it can rarely be altered to accommodate anything outside of the original specifications, such as virus protection or intelligent video.

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

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

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

Step 4: Storage

Recording and saving video in an IP surveillance environment requires the ability to store large amounts of data for sometimes unspecified lengths of time. There are a number of different factors to consider when selecting the appropriate storage system for an installation including scalability, redundancy and performance.

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

Calculating the storage needs

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

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

Motion JPEG

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

MPEG

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

Storage Options

As previously mentioned, IP surveillance does not require specialized storage solutions - it simply utilizes standard components commonly found in the IT industry. There are two ways to approach hard disk storage. One is to have the storage attached to the actual server running the application. The other is a storage solution where the storage is separate from the server running the application, called network attached storage (NAS) or storage area networks (SANs).

Direct server attached storage is probably the most common solution for hard disk storage in small to medium-sized IP surveillance installations. NAS provides a single storage device that is directly attached to a Local Area Network (LAN) and offers shared storage to all clients on the network. A NAS device is simple to install and easy to administer, providing a low-cost storage solution. However, it provides limited throughput for incoming data because it has only one network connection, which could become problematic in high-performance systems.

SANs are high-speed, special-purpose networks for storage, typically connected to one or more servers via fibre. Users can access any of the storage devices on the SAN through the servers, and the storage is scalable to hundreds of terabytes. Centralized storage reduces administration and provides a high-performance, flexible storage system for use in multi-server environments. In a SAN system, files can be stored block by block on multiple hard disks.

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

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

Data replication — This is a common feature in many networks operating systems. File servers in the network are configured to replicate data among each other providing a backup if one server fails.

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

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

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

Step 5: Incorporating Analog Cameras

Existing analog surveillance systems can easily be upgraded to IP surveillance systems by incorporating video servers. This allows for digital delivery and control of video without the re- placement of every camera with a network camera.

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

Step 6: Wireless Networking

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

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

Step 7: Designing the Network

Networks allow devices such as network cameras, servers and PCs to communicate with each other, sharing information and, in some cases, a common Internet connection. Network designs can take many forms and vary in terms of performance and security.

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

Wired and Wireless Options

Network devices can be connected over wires or wirelessly. Ethernet cabling provides a fast network at a reasonable cost and is the primary medium for most existing IT infrastructures.

Fast Ethernet is the most common standard used in computer networks today. Gigabit Ethernet (1000 Mbit/s) is the current standard endorsed by network equipment vendors. and is used primarily in backbones between network servers and network switches. IP surveillance systems work with all of these standards, so as networks become faster, they will be able to support higher-quality video.

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

New or Existing Network?

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

Today’s LANs typically offer plentiful bandwidth, with network switches providing 1000 Mbit for each device connected on the network. Since network cameras can consume anywhere from 0.1Mbit to 8 Mbit, some precaution is needed to ensure the network video system will operate as intended. Depending on the number of cameras and required frame rate, three options are available:

Dedicated Network — Professional surveillance applications may benefit from a dedicated network in which the IP surveillance system has its own dedicated switches that are connected to a high-capacity backbone. Dedicated networks handle video traffic more efficiently, without slowing down other general-purpose network applications like voice over IP or file sharing. In addition, keeping the surveillance net- work separate and disconnected from the Internet will make it as secure as—or more secure than—any local CCTV system.

Combination Network — In some cases, it might make sense to implement a dedicated IP surveillance network in conjunction with a general-purpose network. Video can be recorded locally and isolated to the dedicated network, except when a viewer on the general-purpose network wants to access it, or when an event triggers video to be sent to a user on the general-purpose network. Because access to video using the general-purpose network (and the extra load it causes) is temporary, it makes sense to have the two networks work in combination.

Existing Network — When there is enough capacity on the network and the application doesn't require heavy security, you may simply add network video equipment onto the existing network. You can further optimize your network using technologies such as virtual local area networks (VLAN) and quality-of-service (QoS) levels. A VLAN uses the existing LAN infrastructure but separates the surveillance network from the general-purpose network. The router/switch is configured to provide a range of IP addresses with assigned features.

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

Step 8: Security

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

Today, IP surveillance systems can be made just as secure as those used by banks for ATM transactions. Network cameras and video servers are currently being used in highly sensitive locations.

Secure Transmission

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

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

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

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

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

Privacy settings prevent others from using or reading data on the network. There are a variety of privacy options available, including encryption, virtual private networks (VPNs) and Secure Socket Layer/ Transport Layer Security (SSL/TLS).

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

Employing the outlined security measures makes an IP surveillance network secure and allows users the flexibility of off-site access without the worry that video will fall into the wrong hands. Understanding and choosing the right security options—such as firewalls, virtual private networks (VPNs) and password protection—will eliminate concerns that an IP surveillance system is open to the public.

Step 9: Hot Technologies

Some of the hottest new technologies available in a network video installation are intelligent video, immersive imaging.

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

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

Immersive Imaging

Another way to utilize megapixel technology is for what's being called "immersive imaging". By using a wide-angle lens attached to a megapixel camera, the cam- era can span a much wider field of view (some camera lenses design even cover a full 360 degrees) than normal cameras. Immersive imaging facilitates digital pan/ tilt/zoom (PTZ). The result is the ability to pan, tilt and zoom in on a field of view, even though the camera stays put. Because there are no moving parts, users don't experience the mechanical wear and tear.

Step 10: Best Practices

Today, there are well over a million network cameras and video servers installed worldwide. These installations range in size from just a single camera to thousands of cameras -- and are found in almost every type of industry application. No matter the size, every installation benefit from a simple set of best practices that will ensure all network video equipment is optimized. These tips range from basic camera placement and lighting conditions to working with IT departments and technicians to figure out issues such as the peak times for network usage.

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

Evaluate Site Conditions - Conditions at the camera locations will largely determine which type of network camera should be purchased. Just as with analog cameras, factors such as placing a network camera in an area with very little light or exposing it to extreme heat or cold, will dictate which equipment will work best. Electrical outlets are another important consideration.

IP Surveillance Cost Structure - Today, network cameras are often installed in areas where power outlets do not exist -- such as on building exteriors, in parking lots, or on bridges. In these cases, cameras with Power over Ethernet (PoE) functionality will be a major time and cost savings because they can receive power directly from their network cable connections. The PoE feature should be in 100 percent accordance with the IEEE 802.3af standard, otherwise it will lock the buyer into proprietary systems that are likely not compatible with equipment from other vendors.

Determine Camera Usage - In addition to site conditions, camera usage also dictates the necessary specifications. Network cameras range from an entry-level model to professional equipment that functions un- der a broader range of conditions and offers improved functionality. For example, a camera that will be used to capture objects moving at high speeds -- such as moving cars -- need a progressive scan sensor that will reduce blur. Pan/tilt/zoom (PTZ) will be necessary for looking at objects at a distance or to set up automatic patrols of an area.

Contact Us:

BMG Informatics Pvt. Ltd.
Disha Enclave, Arunodoy Path, Christianbasti
Guwahati, Assam, Pin – 781005
Phone: 0361 - 2340136
Website: www.bmginformatics.com
Email: marketing@bmginformatics.co.in