www.mayflex.com

White Paper

Six steps to successfully designing and planning an IP CCTV system

Infrastructure.
Networking.
Electronic Security.

All together.

MAYFLEX

+Introduction

IP based CCTV surveillance systems can deliver significant advantages over traditional analogue systems such as better remote access, greater integration with other systems, improved image quality as well as scalability. But for end users to take full advantage of the benefits, the design and implementation of the solution needs to be carefully planned and executed. This will ensure the system is flexible and future-proofed and is appropriate for a customer's specific needs.

For designers and installers familiar with analogue surveillance systems, but without experience or specialist training with IP based video systems, this whitepaper explains the basic design concepts and essential considerations vital to implementing a successful network system.

These six steps cover advice about selecting the right equipment, an evaluation of the available technology and help with the choices that need to be made. The additional design considerations for IP CCTV cover bandwidth, network transmission, storage, applications plus how it will integrate with video management software.

+ Choosing the right network camera

For many applications, network cameras offer a range of benefits over their analogue equivalents, including better image quality, flexibility, Power over Ethernet, analytics and other special applications.

However, when selecting a network camera some of the initial considerations about specification are the same as for an analogue camera. There's location, field of view, internal or external deployment, fixed or zoom lens functionality, ambient lighting plus the types of housings and mountings.

When selecting a camera, detailed knowledge about the installation site and the application of the camera are vital to ensure suitable images are delivered to the video management system. Just like analogue models, there are many types of network camera to choose from and most manufacturers produce a variety of models for a range of needs.

There are six main types of network cameras to choose from:

Fixed network cameras have a static viewing direction and come with a fixed, varifocal or zoom lens. Typically, they are “Boxed” or “Bullet” style

Fixed dome cameras are compact and built into a dome casing. They are smaller and more discreet than a standard fixed camera and it’s easy to see which direction the camera is pointing. They also come with a fixed, varifocal or zoom lens

PTZ dome network cameras provide pan, tilt and zoom functions so that coverage spans a wider area and there is a superior zoom image resolution.

Thermal network cameras create images based on the heat radiating from an object, vehicle or person. A thermal camera is less sensitive to problems with light conditions, such as shadows, backlight, and darkness, and deliver images 24 hours a day.

360 Degree cameras are sometimes referred to as panoramic or fisheye cameras and they provide a 360º field of view. They are ideal for retail applications that require a wide area to be covered in a single view. The cameras can also be linked to point of sale terminals and used track the flow of people.

HD & Megapixel cameras incorporate 4K Ultra HD, HD or megapixel technology to give superior video image resolution. An HDTV or megapixel network camera can deliver a resolution at least three times better than an analogue CCTV camera and 4K Ultra HD offers four times the resolution of HDTV 1080p.

Once the camera types have been selected, the choices then turn to the functionality required for each camera. These include:

- Field of view required
- Lens
- Resolution
- Housing/IP rating
- Indoor/outdoor/vandal resistant/Ruggedised (EN50155)
- Built-in IR/Day and Night functionality
- Wireless
- Power over Ethernet
- Audio support
- Integration with the VMS software specified
- Any advanced features required (WDR, Video analytics, on board storage)

+ Extended network transmission

Image transmission is a key consideration when designing a networked based IP security system. Depending on the application there is a wide range of transmission solutions that can be deployed to achieve the desired results such as ethernet switches, baluns, encoders/decoders, fibre and wireless.

As technology improves we are seeing the introduction of very effective wireless IP based systems offering a number of benefits such as:

- Easy installation and very high reliability
- Up to 750 Mbps over 10 miles. A single wireless system can stream up to 4 HD cameras at 25 frames per second dependant on manufacturer and model
- Link buildings and provide data or security networks to and from remote locations
- Low maintenance and on costs

When it comes to wireless networks, the three main types are point-to-point, point-to-multipoint and mesh.

For many installations the benefits of using a wireless solution outweigh the drawbacks even though there are limitations and security concerns. Issues can include video latency and bandwidth, which are affected by the distance from the device to the access point, plus there can be a susceptibility to interference by other wireless technologies and systems. Deployment of video over wireless technology should always be subject to a detailed site survey prior to quotation to confirm suitability of the operating environment.

+ Network design, bandwidth and security consideration

In analogue based solutions the transmission medium, which could be fibre, UTP or COAX, is designed as part of the CCTV system. For IP systems, the video data travels across a network based infrastructure.

Whilst it is unusual for the security integrator to design a corporate network, it is increasingly common for the end user to ask them to work with their IT department so that the security system transitions smoothly on the network. In many cases this will be a dedicated LAN.

Typically, each network design will be bespoke to the needs of the user and the specified installation. The security design considerations include IP addressing and transport protocols along with bandwidth, scalability and network security.

It is important to consider how bandwidth will deploy on a system as this can severely impact the performance of the end user's network traffic throughout the business. It is fair to say that bandwidth usage has in the past, been a key factor slowing down the adoption of IP based systems.

In smaller systems up to 10 cameras, a simple 100Mbit network switch can be used without too much of a knock on effect on bandwidth limitations. This is because a typical camera delivering high-quality images at high frame rates will only use around 2 -3 Mbit/s of the available network bandwidth.

With large systems, a switch connected to a gigabit backbone or a separate LAN could ease bandwidth issues. Other solutions include VLANs on a switched network, Quality of Service capabilities via the switch and event-based recordings.

Making sure network video can only be viewed by authorised personnel is an important step in creating a successful IP surveillance installation. By their very nature most applications contain sensitive information and selecting the right security options - such as firewalls, virtual private networks (VPNs) and password protection - will eliminate concerns about how an IP CCTV system might be compromised.

+ Storage calculations and Servers

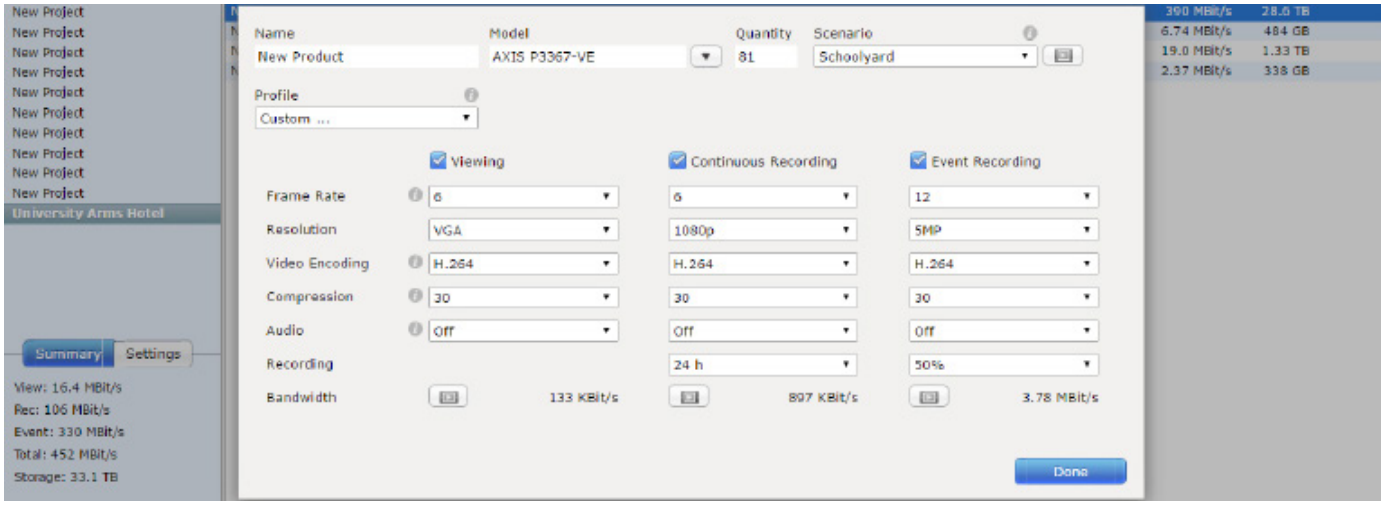
Storage requirements, the accessibility and retrieval of images and related information including scalability, redundancy and performance, are all important to a network solution.

The ability to use open storage solutions is one of the main benefits with IP surveillance and there are two main ways to achieve this. The most common is to have the storage attached to the server running the application, as in a Network Video Recorder (NVR). 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).

SAN systems enable the designer to build redundancy into the storage devices so video data can be saved simultaneously in more than one location. This configuration can include a Redundant Array of Independent Disks (RAID) set up which also enables failover where two servers work with the same storage device (clustering) to reduce system downtime.

Fortunately, most manufacturers provide design tools that enable the system designer to select the correct amount of storage for the specific application. These tools normally make use of the following information:

- Number of cameras
- Type of recording (continuous or event-based)
- If event based how many hours per day of events / motion (can be expressed as a %)
- Frames per second
- Image resolution
- Video compression type
- Image complexity (as in type of scene, for example are we looking at a little used fire exit door or a rail station platform with lots of movement)
- How long data must be stored and archived for



+ Understanding Compression Engines

Video compression methods are used in network surveillance systems to improve the efficiency of transmission and reduce the need for more expensive storage. Most manufacturers use standard compression techniques to ensure compatibility and interoperability.

There are three standards of video compression: Motion JPEG, MPEG-4 and H.264. The latter is the latest standard and is considered to be the most efficient and most widely adopted. Each option has different qualities so it is important to understand the technology to select the best method for a specific application.

Motion JPEG (MJPEG) compresses each of the video frames in a sequence separately using the JPEG format. In doing so it guarantees the same quality for each image so that the compression ratio of MJPEG is relatively low compared to interframe compression standards (such as MPEG4 and H.264). Since there is no dependency between the frames, a Motion JPEG video is robust and can afford to lose frames during transmission without affecting the rest of the video.

MPEG-4 is a licensed standard, so users pay a fee for each monitoring station. MPEG-4 supports low-bandwidth applications and high quality images as it is an interframe video that compresses only the differences between frames in a video sequence, resulting in a better compression ratio than MJPEG.

This means there are no limitations in frame rate and almost unlimited bandwidth. The advantage for MPEG-4 files compared with Motion JPEG files is the reduced bandwidth and storage requirements, which in turn, generates cost savings.

The downside of MPEG-4, as a more complex compression system, is greater latency before video can be viewed. It also needs to be a higher specification (and therefore cost) to decode the MPEG4 video.

H.264 is the latest MPEG standard for video encoding and it is expected to be the main video compression standard in the future. H.264 can maintain image quality, reduce the size of a digital file by as much as 80% (vs Motion JPEG) and as much as 50% when compared with the MPEG-4 standard. This means much less network bandwidth is used and lower storage space is required.

The downside of H.264 is that other hardware in the systems, such as cameras and monitoring stations, need to be higher performance machines, but this now has less of an effect with advances in PC/Server technology.

+ Video management

In IP surveillance systems one of the most important components is the video management system (VMS) as it's the part the end user client will work with directly. A significant difference between analogue and IP based systems, is the management of the video images and related information. With network systems the user has the ability to retrieve and access images instantaneously. As well as passively recording and displaying images, the technology also evaluates situations and triggers alarms to enable security officers to take the appropriate action.

Video management software (VMS) is feature rich and manages video for live monitoring and recording and provides integration into other systems. Solutions typically range from single PCs to advanced client/server-based software that provides management functionality for thousands of cameras.

This is a key feature as easy integration with access control devices and other systems allows users to manage video and other building controls, such as access control and badging systems, through a single programme.

The choice of video management system depends on a number of factors such as the compatibility of the cameras being installed, available bandwidth, storage, scalability, frame-rate control and integration requirements.

+ ONVIF

Any discussion on IP CCTV would not be complete without mentioning ONVIF. ONVIF stands for Open Network Video Interface Forum and was founded in 2008 by Axis Communications, Bosch Security Systems, and Sony Corporation.

ONVIF was created to provide an open standard across manufacturer's and is designed to make it easier to integrate video management software with third-party cameras and third-party software. It is a single protocol for everything, which means there is no need for the development of custom API's. As it is an open standard this also means the end user is not locked in to a particular camera vendor.

When designing and planning an IP CCTV system the integrator must ensure that he chooses products that are ONVIF compliant to ensure interoperability between cameras and network recording devices.

ONVIF has different versions of compatibility that dictate which features can be integrated into a system. In some cases, a camera can supply a video feed whilst lacking the ability to do more advanced features, such as video analytics. Sometimes companies say that a device is ONVIF compliant when it is not. The only sure bet for full functionality with your NVR or VMS is to check with your distributor who can guarantee compatibility between devices they supply.

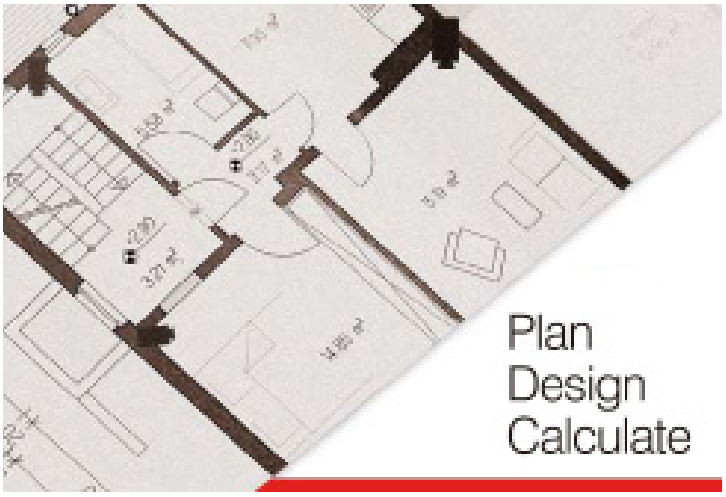
+ Conclusion

When designing an IP based video surveillance system, the variety of equipment available and the rapid pace of technology need to be balanced with the specific needs of the end user to ensure the best solution is delivered to the customer.

The main principles are still the same for designing IP based systems as they are for analogue solutions; specifying the correct camera and evaluating issues, such as the location, lighting, field of view and fixed or zoom lens functionality. Thereafter the IP system takes on a completely different design as the transmission, management and storage of the video is distributed via a network. In addition to this the cameras and recording devices must be ONVIF compliant to ensure compatibility.

This means there is a need for system designers and installers to learn new skills and consider applications from a different perspective if they are to make the most of the technical advantages available from the new technologies in the market today thereby maximising return on investment for their clients.

In breaking the decision-making process down into six distinct, but related steps, all possible scenarios are covered. This information provides the foundations for designing and installing an IP based video surveillance system with first-rate functionality and future-proofed flexibility – concepts a world away from a traditional analogue solution.



Mayflex UK
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
United Kingdom

Tel +44 (0)121 326 7557
Email sales@mayflex.com
Website www.mayflex.com

Mayflex MEA DMCC
PO Box 293695
Office 11A, Gold Tower
Jumeirah Lakes Towers
Dubai
United Arab Emirates

Tel +971 4 421 4352
Email mesales@mayflex.com
Website www.mayflex.com

MF1079_09/15

MAYFLEX