DESIGN GUIDE

IP-Surveillance design guide

Setting up an IP-Surveillance system using Axis network cameras, video encoders and AXIS Camera Station software

AXIS COMMUNICATIONS

Table of contents

This document is a guide to setting up an IP-Surveillance system in a small- to medium-sized security installation. It provides an overview of network video's functionalities and benefits, and outlines considerations and recommendations for implementing such a system.

1. Introduction to an IP-Surveillance system

This chapter provides an overview of what is involved in an IP-Surveillance system, the benefits of network video, the importance of defining your surveillance application and legal considerations to take into account when setting up an IP-Surveillance system in your area.

1.1. What is IP-Surveillance?

IP-Surveillance is a term for a security system that gives users the ability to monitor and record video and/or audio over an IP (Internet Protocol-based) computer network such as a local area network (LAN) or the Internet. In a simple IP-Surveillance system, this involves the use of a network camera (or an analog camera with a video encoder/video server), a network switch, a PC for viewing, managing and storing video, and video management software. (More detailed discussions of the components are provided in Chapter 2.)

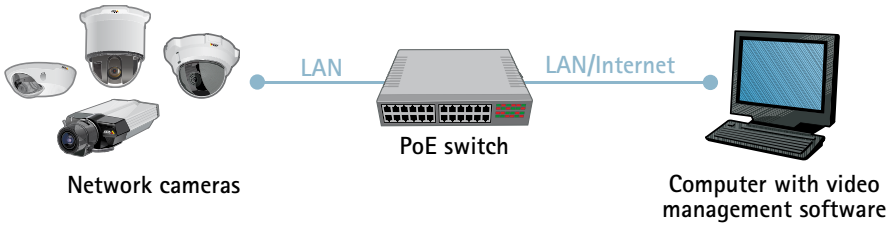


Figure 1.1.a. *An IP-Surveillance or network video system*

Unlike analog video systems that use dedicated point-to-point analog cabling from the camera location to the viewing/recording station, IP-Surveillance (or network video) uses the IP network technology as the backbone for transporting information. In an IP-Surveillance application, digitized video and/or audio streams can be sent to any location—even around the world if desired—via a wired and/or wireless IP network, enabling video monitoring and recording from anywhere with network access.

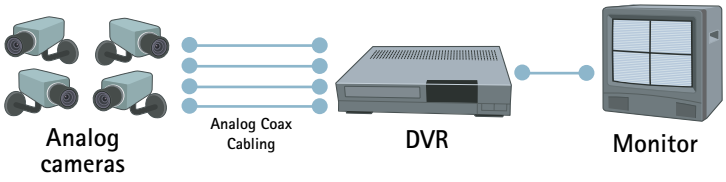


Figure 1.1.b. *An analog video system that incorporates a DVR (digital video recorder)*

While an analog video system is for the most part a one-directional signal carrier that ends at the recording device, a network video system is bi-directional (allowing information to be sent and received) and can be an integrated part of a larger, scalable system. A network camera, for instance, can send video, audio and other data (e.g., SMS) to a user, as well as receive from the user audio and data instructions that could, for example, activate doors or external alarms. In addition, a network video system can communicate with several applications in parallel and perform various tasks such as detecting motion or sending different streams of video. Such a system provides for greater performance possibilities and flexibility.

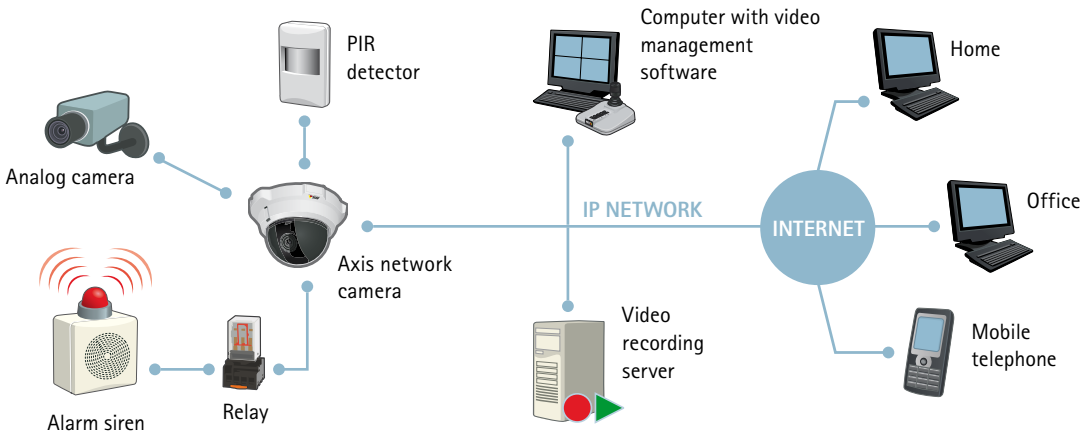


Figure 1.1.c. *A network video system with alarm integration*

Because of the digital nature and method of video distribution, IP-Surveillance provides a host of benefits and advanced functionalities that gives you greater control and management of live and recorded video, as well as alarm events. This makes the system highly suited to security surveillance applications. The advantages include:

1) **Remote accessibility:** You can access live and recorded video at any time and from virtually any networked location in the world. Multiple, authorized users at different locations may be able to access live or recorded video. This is advantageous if your company wants a third-party, such as a security firm, to benefit from and have access to the video. In a traditional analog CCTV system, you need to be in a specific, on-site monitoring location to view and manage video, and off-site video access would not be possible without some additional equipment, such as a video encoder or a network DVR (digital video recorder).

2) **High image quality:** High image quality is essential in a security surveillance application. You want to be able to clearly capture an incident in progress and identify persons or objects involved. In a network video system, the quality of images produced can be more easily retained than in an analog surveillance system. With an analog video system, the captured images are degraded with every conversion that the images make between analog and digital formats and with the cabling distance. The further the analog video signals travel, the weaker they become. In a fully digital IP-Surveillance system, images from a network camera are digitized once and they stay digital with no unnecessary conversions and no image degradation due to distance traveled. In addition, digital images can be more easily stored and retrieved than is the case with the use of analog video tapes.

A network camera that uses progressive scan technology provides clearer images of moving objects because the whole image is presented at one time. With an analog video signal, two consecutive interlaced fields of lines are presented to form an image, and when displayed on a PC monitor, blurriness occurs when objects move between the image capture of the two interlaced fields.

Figure 1.1.d. *Progressive scan*

Figure **1.1.e.** *Analog interlaced scan*

A megapixel network camera (i.e. one that delivers an image comprised of 1 million or more pixels) can also offer resolutions greater than what an analog camera can offer, which means that more detail or larger areas can be covered.

Figure 1.1.f. *Integration with Point of Sales system*

3) **Easy, future-proof integration:** Network video products based on open standards can be easily integrated with computer and Ethernet-based information, audio and security systems, video management and application software, and other digital devices. For instance, a network camera can be linked to specialized software programs that could, for example, integrate video with a Point of Sales system, or analyze the visual and/or audio data to detect wanted persons in a crowd or unauthorized access to specific areas.

4) **Scalable and flexible:** An IP-Surveillance system can grow with your needs. You can add as many network video products to the system as desired without significant or costly changes to the network infrastructure. You can place and network the products from virtually any location, and the system can be as open or as closed as you wish.

5) **Cost-effective:** An IP-Surveillance system has a lower total cost of ownership than a traditional analog CCTV surveillance. Management and equipment costs are lower since back-end applications and storage run on industry standard, open systems-based servers—not on proprietary hardware such as a DVR in the case of an analog CCTV system. Additional cost savings come from the infrastructure used. IP-based video streams can be routed around the world using a variety of interoperable infrastructure. IP-based networks such as LANs and the Internet, and various connection methods such as wireless are much less expensive alternatives than traditional coaxial and fiber needed for an analog CCTV system. In addition, an IP infrastructure can be leveraged for other applications across the organization.

Furthermore, Power over Ethernet (PoE) technology, which cannot be applied in an analog video system, can be used in a network video system to increase savings and reliability.

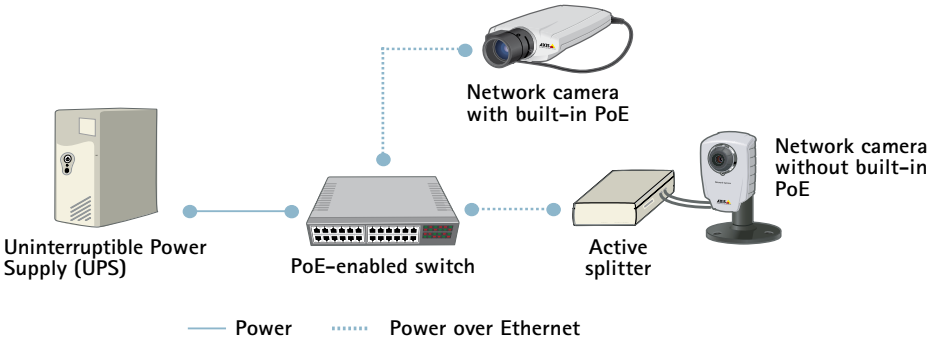


Figure 1.1.g. *A system that uses Power over Ethernet (PoE). A PoE-supported network camera connects directly to a PoE-enabled switch, while a network camera without built-in PoE support can use an active splitter to make use of PoE.*

PoE enables networked devices to receive power from a PoE-enabled switch or midspan through the same standard cable that transmits data (video). Hiring a certified electrician and installing a separate power line are not needed—a big advantage, particularly in difficult-to-reach areas. With PoE, network cameras/video encoders will also be able to receive centralized backup power from a server room with an Uninterruptible Power Supply; so in the event of a power failure, the cameras/video encoders will still be able to operate. (See diagram above.)

6) **Event management and intelligent video:** There is often too much video recorded and lack of time to properly analyze them. Advanced network cameras/video encoders with built-in intelligence or analytics take care of this by reducing the amount of uninteresting video recorded and enabling programmed responses.

Advanced network cameras/video encoders have such features as built-in video motion detection, audio detection alarm, active tampering alarm, I/O connections, and alarm and event management functionalities. These features enable the network cameras/video encoders to be constantly on guard in analyzing inputs and waiting for an impulse to kick-start an action or a series of actions. Having intelligence/analytics conducted at the network camera/video encoder rather than at the recording server reduces network bandwidth usage and storage needs since only actionable data (video) is sent over the network. In addition, less computing power is required from the recording server.

Event management functionalities can be configured using the network video product user interface or a video management software program. Users can define the alarms/events by setting the type of triggers to be used and when, as well as the responses (e.g., recording to one or multiple sites—whether local and/or off-site for security purposes; activation of external devices such as alarms, lights and doors; and notification messages to users).

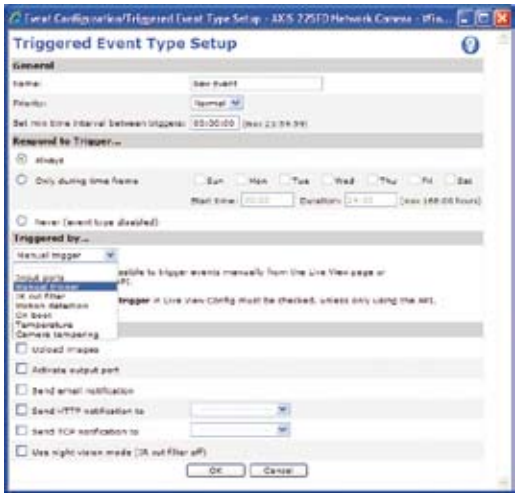


Figure 1.1.h. *Setting up an event trigger using the network camera's user interface.*

A security personnel's ability to protect people, property and assets can be enhanced by the flexibility and power of IP-Surveillance technology. IP-Surveillance systems have been installed in indoor/outdoor and private/public spaces; for example, in stores, homes, day care centers, schools, banks, government offices, factories, warehouses, railway/subway stations and airports.

1.2. Overview of an IP-Surveillance system

An IP-Surveillance system can be as simple or as sophisticated as your needs require. In a simple scenario, you have a PC where you want to view and record video. You have an Ethernet cable between a PC and a network switch (which allows different devices to connect to each other and share, for instance, a common Internet connection) and a cable from the switch to the camera location. You then need equipment that can capture video and send a video stream over the network. This can be a network camera, or an analog camera connected to a video encoder (also sometimes known as a video server).

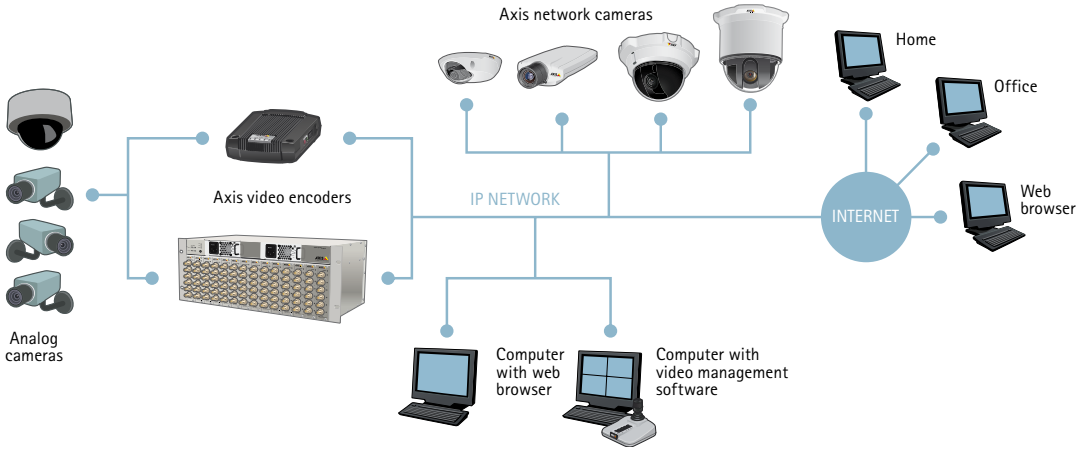


Figure 1.2.a *Overview of an IP-Surveillance system*

A network camera or a video encoder connects directly to the network—not to a PC as is the case with a web camera. Once the network camera (or analog camera and video encoder) is installed and configured, you can view and record live video using a web browser on a local PC or a remote PC via the Internet. If you want to access and record video from many cameras simultaneously, it is advisable to install a video management software program on the recording PC.

As mentioned earlier, an IP-Surveillance system is easy and cost-effective to scale up. It is also flexible, and each component of the system can be customized to your needs. The following is a brief overview of the components that can be tailored to your application:

a) **Network camera/video encoder**: A wide variety of network cameras and video encoders are available. Network cameras range from fixed cameras and fixed domes, to pan/tilt/zoom (PTZ) and PTZ dome cameras, and may be designed for use indoors or outdoors. Other network camera features include built-in support for wireless communication, megapixel resolutions and vandal resistance. Both network cameras and video encoders may offer a variety of capabilities such as: 1) several simultaneous video streams using different video compression formats (e.g. H.264, MPEG-4 Part 2, Motion JPEG) that are optimized for bandwidth and image quality; 2) input/output ports for connection to external devices such as sensors and alarms; 3) built-in intelligence such as video motion detection and tampering detection; 4) sophisticated alarm and event management functions that can communicate with different devices and applications simultaneously, and can send separate video streams in different resolutions, at different frame rates and to different places; 5) audio support; and 6) Power over Ethernet, which enables power to be delivered over the same cable as for data transmission.

b) **Network**: There are many ways to design and secure a network for IP-Surveillance. In addition, a network can be as small or as extensive as your requirements, and it can be wired, wireless or a combination of both. It is also easy to increase the bandwidth capacity of your network simply by adding switches/routers. And different technologies can be used to optimize bandwidth usage. Furthermore, a wired network can deliver not only data, but also power using Power over Ethernet (PoE) technology. This simplifies installation of PoE-enabled network cameras/video encoders and provides cost savings.

c) **Hardware (server and storage)**: The hardware requirements of an IP-Surveillance system are not complex. Simply use standard components found in the IT industry. Today's PC, with a Pentium processor and Windows operating system, is able to run a video management software, and record and store video from up to 50 cameras. If the hard disk on the actual server running the recording application is not enough, there are solutions that enable you to increase storage space and achieve increased flexibility and recoverability. As larger hard drives are produced at lower costs, it is becoming less expensive to store large amounts of video.

d) **Software**: A wide range of software is available to help you in the preparation, installation and management of an IP-Surveillance system. For example, you can use the AXIS Design Tool, which helps you estimate how much bandwidth your network video system will require, and installation software such as the AXIS Camera Management (free download), which makes it easier for you to find, install and configure the video products on the network. A video management software is also recommended. It will allow you to, among other things, centrally manage and configure the network video products to your viewing, recording and security preferences.

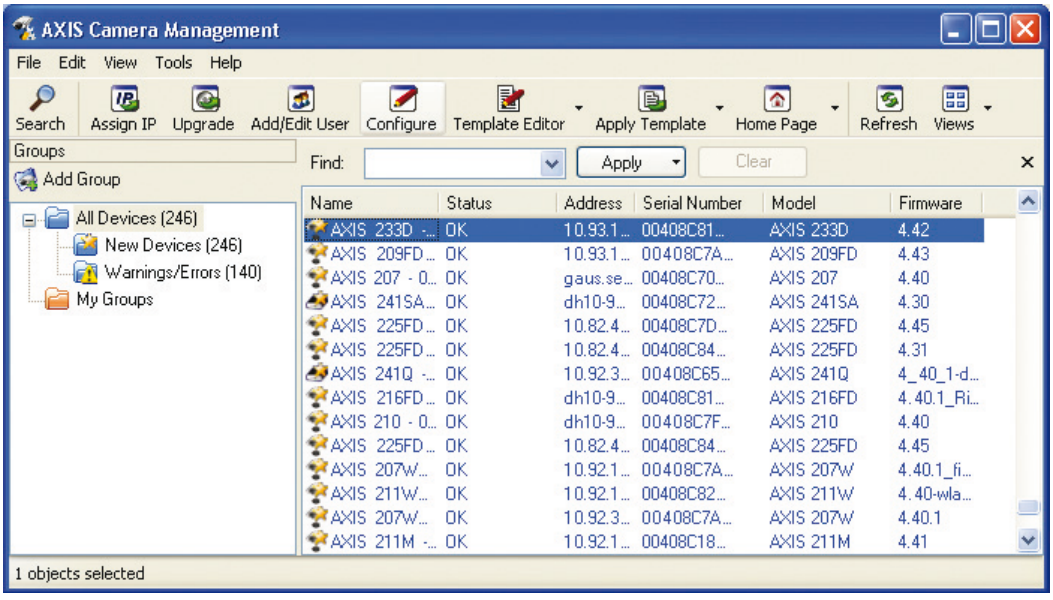
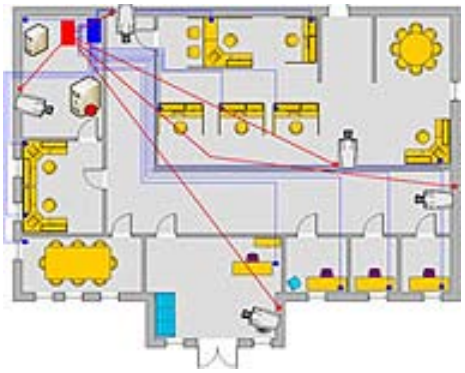


Figure 1.2.c. *AXIS Camera Management software*

A more detailed discussion of the components and the considerations to take into account when selecting equipment is provided in Chapter 2.

1.3. Defining your surveillance application



The first and most important step in implementing a video surveillance installation is determining the goal of your surveillance application. It is a good idea to map out where you want video surveillance to take place and for what purpose (i.e. surveillance overview, identification, people counting). This will determine the type and number of network cameras, as well as other components to install and can influence the overall cost of the installation. More information about how to select a network camera and other components is covered in Chapter 2.

1.4. Legal considerations

Video surveillance can be restricted or prohibited by laws that vary from country to country. It is advisable to check the laws in your local region before installing a video surveillance system. There may be legislation or guidelines covering the following:

a) **License.** You may need to register or get a license from an authority to conduct video surveillance, particularly in public areas.

b) **Purpose of the surveillance equipment.** Is it in accordance with what is permitted by the laws in your area?

c) **Position or location of the equipment.** Is it positioned or located in such a way that it only monitors the spaces which the equipment is intended to cover, and if unintended areas are covered, would you have to consult with the owners of such spaces? There may be rules covering areas where video surveillance is prohibited; for example, toilets and changing rooms in a retail environment.

d) **Notification.** You may have to place signs to warn the public that they are entering a zone covered by surveillance equipment and there may be rules regarding the signage.

e) **Quality of images.** There may be rules regarding the quality of images, which can affect what may be permitted or acceptable for use as evidence in court.

f) **Video format.** Police authorities may require that the video format be ones that they can handle.

g) **Information provided in recorded video.** Video recordings, for instance, may be required to have time and date stamped.

h) **Processing of images.** There may be rules regulating how long images should be retained, who can view such images and where recorded images can be viewed. You may have to keep an audit log.

i) There may be **requirements for drawings** of where cameras are placed.

j) **Personnel training.** There may be regulations that require operators to be trained in security and disclosure policies, as well as privacy issues.

k) **Access to and disclosure of images to third parties.** There may be restrictions on who can access the images and how images can be shown. For example, if video is to be disclosed to the media, images of individuals may have to be disguised or blurred.

l) **Recording of sound.** A permit may be required for recording sound in addition to video.

m) **Regular system checks.** There may be guidelines on how often and thorough a company should perform system checks to make sure all equipment are operating as they should.

2. Component considerations

This chapter describes the major components of an IP-Surveillance system, and provides guidelines for selecting equipment. The components covered in this chapter include network camera, video encoder, network switch, server hardware and video management software (AXIS Camera Station).

2.1. Network camera

A network camera can be described as a camera and computer combined in one unit. It has a compression chip, an operating system, a built-in web server, FTP (File Transfer Protocol) server, FTP client, e-mail client, alarm management and much more. A network camera, unlike a web camera, does not need to be attached to a PC; it operates independently and connects, as with a PC, directly to an IP network. It can be placed wherever there is a wired or wireless network connection. The network camera captures and sends live images, enabling authorized users to locally or remotely view, store and manage video over a standard IP-based network infrastructure.

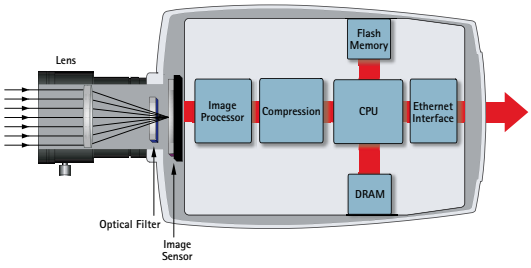


Figure 2.1.a. *Inside an Axis network camera*

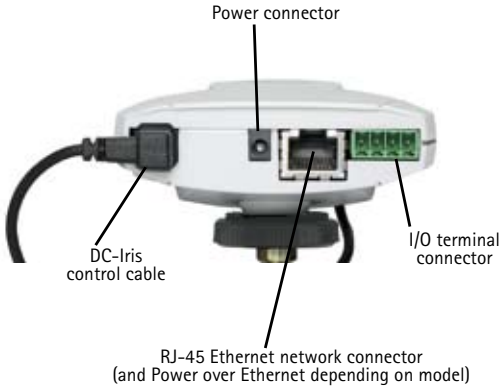


Figure 2.1.b. *Back of an Axis network camera*

Many types of network cameras are available today, and no matter what your needs are, there is a network camera available to meet them. Although analog cameras are available in a similar variety, network cameras can now offer more benefits, including better image quality and greater installation flexibility. For some special applications, such as very high image resolution or wireless needs, network cameras are the only option.

The following sections provide an overview of the types of network cameras available, the network camera features to consider and how to select a network camera.

a) Types of network cameras

Axis offers the widest range of professional network cameras on the market. Network cameras can be categorized into indoor/outdoor versions and types.

> **Indoor or outdoor.** Outdoor network cameras must have an auto iris lens to regulate how much light is received. Many outdoor cameras require a protective housing. Others may already be designed with a protective enclosure. Housings are also available for indoor cameras that require protection from harsh environments such as dust and humidity, and from vandalism or tampering.

> **Types:** Fixed, fixed dome, PTZ (pan/tilt/zoom) or PTZ dome

Fixed network cameras

A fixed camera is one whose viewing angle is fixed once it is mounted. A fixed camera with a body and a lens represents the traditional camera type. In some applications, it is advantageous to make the camera very visible. If this is the case, then a fixed camera represents the best choice since both the camera and the direction in which it is pointing are clearly visible. Another advantage is that most fixed cameras have exchangeable lenses. For further protection, fixed cameras can be installed in housings designed for indoor or outdoor installation.

Figure 2.1.d. *AXIS 211 Network Camera*

Fixed dome network cameras

Fixed dome cameras, also called mini domes, essentially consist of a fixed camera that is pre-installed in a small dome housing. The camera can be easily directed to point in any direction. Its main benefit lies in its discreet, non-obtrusive design, as well as in the fact that it is hard to see in which direction the camera is pointing. The camera is also tamper resistant. A limitation of a fixed dome camera is that it rarely comes with a changeable lens, and even if it is changeable, the choice of lenses is limited by the space inside the dome housing. However, a varifocal lens is often provided, which enables the camera's field of view to be adjusted. Fixed dome cameras are designed with different types of enclosures such as vandal-resistant and/or IP66-rated enclosures for outdoor installations. No external housing is required. The mounting of such a camera is usually on a wall or ceiling.

Figure 2.1.e. *AXIS 216FD Network Camera*

PTZ network cameras

The camera's view can be remotely controlled, either manually or automatically, for panning from side to side, tilting up and down, and zooming in and out of an area or object. There are now mechanical as well as non-mechanical PTZ cameras.

Mechanical PTZ cameras can pan, tilt and zoom through manual or automatic control. In a manual operation, an operator can use a PTZ camera to follow, for instance, a person in a retail store. PTZ cameras are mainly used indoors and in applications where an operator is employed and where the visibility of the camera's viewing angle is desirable or not an issue. The optical zoom on PTZ cameras typically ranges from 10X to 26X. A PTZ camera can be mounted on a ceiling or wall.

Figure 2.1.f. *AXIS 214 PTZ Network Camera*

A difference between PTZ cameras and PTZ domes is that many PTZ cameras do not have full 360-degree pan due to a mechanical stop that prevents the cameras from making a continuous circular movement. It means that the camera cannot follow a person walking continuously in a full circle around the camera. An exception is the AXIS 215 PTZ Network Camera, which thanks to its auto-flip functionality, can instantly flip the camera head 180 degrees and continue to pan beyond its zero point. The camera can then continue to follow a passing person or object, regardless of the direction. Another difference between PTZ cameras and PTZ domes is that PTZ cameras are not made for continuous automatic operation or so-called 'guard tours'.

Figure 2.1.g. *AXIS 215 PTZ Network Camera in drop-ceiling mount*

A non-mechanical PTZ camera uses a megapixel sensor and a wide-angle lens to enable it to have a viewing angle of 100 degrees to 180 degrees (or even wider in same cases). Such a camera allows an operator to zoom in on any part of a scene without any mechanical movement. The key advantage is that there is no wear and tear since the camera has no moving parts. Zooming in on a new area of a scene is immediate. In a traditional PTZ camera, this can take up to 1 second. Since a non-mechanical PTZ camera's viewing angle is not visible, it is ideal for discreet installations. To obtain good image quality, pan, tilt and zoom should be limited. If such a camera has a 3 megapixel sensor, the recommended maximum viewing angle is 140 degrees with a 3X zoom capability. This type of camera is typically mounted on a wall.

Figure 2.1.h. *AXIS 212 PTZ Network Camera*

PTZ dome network cameras

PTZ dome network cameras can cover a wide area by enabling greater flexibility in pan, tilt and zoom functions. They enable a 360-degree, continuous pan, and a tilt of usually 180 degrees. PTZ dome cameras are ideal for use in discreet installations due to their design, mounting (particularly in drop-ceiling mounts as seen in the picture to the right), and difficulty in seeing the camera's viewing angle (dome coverings can be clear or smoked). A PTZ dome network camera also provides mechanical robustness for continuous operation in guard tour mode, whereby the camera continuously moves between presets. In guard tour mode, one PTZ dome network camera can cover an area where 10 fixed cameras would be needed. The main drawback is that only one location can be monitored at any given time, leaving the other nine positions unmonitored. The optical zoom typically ranges between 10X and 35X. A network dome camera is often used in situations where an operator is employed. This type of camera is usually mounted on a ceiling if used indoors, or on a pole or corner of a building in outdoor installations. With a PTZ dome network camera, all PTZ control commands are sent over an IP network, and no RS-485 wires need to be installed, unlike the case with an analog dome camera.

Figure 2.1.i. *AXIS 233D Network Dome Camera in drop-ceiling mount*

b) Feature considerations

> **Image sensor:** Two types of image sensor technologies are available for use in network cameras: CCD (charge-coupled device) and CMOS (complementary metal-oxide semiconductor). Each has its own unique strengths and weaknesses that make them appropriate for different applications. CCD sensors have been used in cameras for more than 20 years and present many advantageous qualities such as good light sensitivity, which is important in low-light conditions. However, they are more expensive and more complex to incorporate into a camera and may consume much more power than an equivalent CMOS sensor.

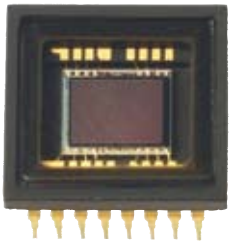


Figure 2.1.j. *CCD*

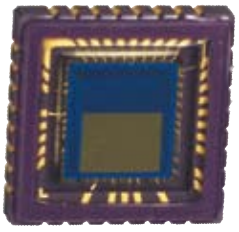


Figure 2.1.k. *CMOS*

Recent advances in CMOS sensors bring them closer to their CCD counterparts in terms of image quality. CMOS sensors lower the total cost for cameras since they contain all the logics needed to build cameras around them. CMOS sensors enable more integration possibilities and more functions. They make it possible for manufacturers to produce smaller-sized cameras.

The most common image sensor sizes used in network cameras are ¼-inch and 1/3-inch and they may use progressive scan or interlaced scan technology (see next point below for more on the technologies). Many megapixel sensors are the same size as sensors used in cameras that deliver VGA 640x480 resolution. It means that the megapixel sensor has many more pixels but the pixel sizes are smaller, and therefore, less light sensitive than a non-megapixel sensor.

> **Progressive scan**: This technology involves exposing, capturing and presenting an entire image at one time—line by line in perfect order, rather than splitting an image into two separate fields and presenting them at separate times as with analog interlaced scanning technology. Since PC monitors use progressive scan technology, moving objects in a video will be presented more clearly on PC screens if the video is captured using progressive scan. If interlaced video is presented on a PC screen, objects that move between the image capture of two interlaced fields will be blurry. All of Axis' current network cameras, with the exception of a couple of PTZ dome cameras, use progressive scan technology.

Progressive scan

Figure 2.1.l.
Freeze frame on moving dot using progressive scan

An interlaced scan image shown on a progressive PC monitor

1st field: Odd lines

2nd field: Even lines [17/20 ms (NTSC/PAL) later]

Freeze frame on moving dot using interlaced scan

Figure 2.1.m.

> **Lens**: Different types of lens are available on network cameras. Lenses may be *fixed* (the focal length or horizontal field of view is fixed), *varifocal* (allows for the manual adjustment of the focal length) or *zoom* (allows the camera to stay in focus when zooming in on objects). Varifocal and zoom lenses offer focal lengths that range from telephoto to wide angle.

Figure 2.1.n. *Fixed lens*

Figure 2.1.o. *Varifocal lens*

A lens' iris, which controls the amount of light coming into the camera, can be manually adjusted (for indoor cameras) or automatically controlled (for outdoor cameras). An auto iris lens can be controlled by the camera's processor (DC-controlled), or by video signal.

> **Lens changeable**: Changeable lens gives users the option of using other lenses (such as telephoto or wide angle) that may be more appropriate for a particular application. You will need to know if the camera's original lens is C-mount or CS-mount so that the new lens you purchase fits the same type of mount. Today, almost all surveillance cameras and lenses sold are CS-mount types.

When choosing the size of a new lens, you will also need to know the size of the image sensor. If a lens is made for a smaller sensor than the one actually fitted inside the camera, you will have black corners in the image. If a lens is made for a larger sensor than the one fitted inside the camera, the angle of view will be smaller than the default angle of the lens since part of the information will be "lost" outside of the sensor.

> **Automatic day/night functionality**: This feature is incorporated into some outdoor cameras and enables the automatic removal of the infrared (IR) cut filter that is incorporated into all color cameras to prevent color distortion from near-infrared light. When there is light, the IR-cut filter is on and the camera delivers color video. In dark conditions, the camera removes the filter to make use of near-infrared light to deliver infrared-sensitive black and white video. Infrared or day/night cameras are particularly useful in outdoor environments or situations that restrict the use of artificial light. These situations include discreet and covert surveillance applications.

> **Minimum illumination/light sensitivity**: A network camera's light sensitivity is often specified in terms of lux, which corresponds to a level of illuminance in which a camera produces an acceptable image. The lower the lux number, the better the camera is at capturing images in low light conditions. If a camera is specified to work down to 1 lux, it means that the camera can produce an image at 1 lux, but it may not necessarily be of high quality. Normally, at least 200 lux is needed to illuminate an object so that a good quality image can be obtained. Different manufacturers also use different references when they specify the lightsensitivity of a camera, so it is important to look at captured images to make a comparison.

Environment: lux
> Strong sunlight: 100,000
> Full daylight: 10,000
> Normal office light: 500
> Poorly lit room: 100

Lux is the amount of light falling onto a surface per square meter. Many natural scenes have fairly complex illumination with both shadows and highlights that give different lux readings in different parts of a scene. It is, therefore, important to keep in mind that one lux reading cannot be an indication of the light condition for a scene as a whole.

> **Type of video compression**: There are three main video compression standards in use today: Motion JPEG, MPEG-4 Part 2 (also referred to simply as MPEG-4 in some references), and H.264 (also known as MPEG-4 Part 10/AVC). Each standard employs different techniques to reduce the amount of data transferred and stored in a network video system.

  H.264 is the latest standard that is expected to become the video standard of choice in the coming years. Without compromising image quality, H.264 can reduce bandwidth and storage requirements by more than 80 percent compared with Motion JPEG and as much as 50 percent more than with the MPEG-4 Part 2 standard. H.264 and MPEG-4 Part 2 are licensed technologies, so if a network video product supports those standards, be sure to find out if the license fee is already included in the product's purchase price. H.264 and MPEG-4 Part 2 provide support for synchronized audio, while Motion JPEG does not. Motion JPEG is an unlicensed technology.

  For the time being, network video products that support multiple compression standards are ideal for maximum flexibility and integration possibilities.

> **Video resolution**: A VGA resolution is 640x480 pixels. (Computer screens have resolutions in VGA or multiples of VGA.) Another common format is 4CIF (704x480 pixels in NTSC / 704x576 pixels in PAL standard). Megapixel cameras provide high resolutions of at least 1280x960 pixels and are used for applications that require the ability to see fine details or cover a large area. A network video product's ability to deliver a specified number of frames per second may vary depending on the resolution.

> **Frames per second:** There may be different frame rates specified for different resolutions. Full-motion video is 30 frames per second in NTSC video standard (in North America/Japan) and 25 frames per second in PAL video standard (Europe). Full frame rate on all cameras at all times is more than what is required for most applications. With the configuration capabilities and built-in intelligence of network cameras, frame rates under normal conditions can be set lower, e.g. one to four frames per second, to dramatically decrease storage requirements. In the event of an alarm—for instance, if video motion detection or an external sensor is triggered—a video management software program can be configured to request that the network video product send a different stream with a higher recording frame rate.

> **Multiple, individually configurable streams**: Network video products with this capability can provide multiple streams and each stream can be configured differently in terms of compression format and level, frame rate and resolution. For example, one stream can be configured with maximum compression and low frame rate for storage purposes; another stream can be sent with higher frame rate and less compression and, therefore, less lag for live viewing; and a third stream with high compression and low resolution can be sent to mobile devices.

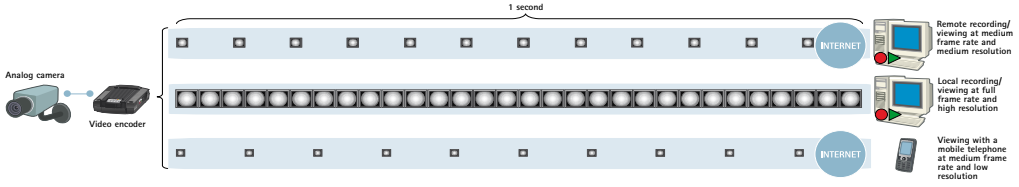


Figure 2.1.p. *Multiple, individually configurable video streams*

> **Audio support**: A network camera with audio support comes either with a built-in microphone or an input for an external microphone. Speakers may be built in or external. An audio feature enables users to remotely listen in on an area and communicate instructions, orders or requests to visitors or intruders. Audio can also be used as an independent detection method. When sound above a certain level is detected, video recordings and alarms can be triggered.

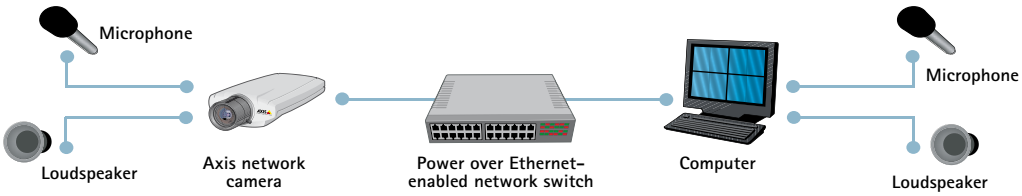


Figure 2.1.q. *Enhancing video surveillance with audio*

Audio modes may be simplex (audio is sent either by the operator or the camera), half duplex (audio is sent in both directions, but only one party at a time can send) or full duplex (audio is sent to and from the operator simultaneously). Audio can be compressed and integrated into the video stream, and sent over a network for monitoring and/or recording. There are four audio compression standards used in network video. They are AAC-LC, which requires a license, and G.711, G.726 and G.722.2 (Adaptive Multi-Rate—Wideband), which are non-licensed technologies. Audio and video are two separate packet streams that are sent over a network. In order for the client or player to perfectly synchronize the audio and video streams, the audio and video packets must be time-stamped. Time stamping using Motion JPEG may not always be supported in a network camera. If synchronized audio and video is a priority, it is better to use H.264 or MPEG-4 Part 2 for the video compression since time stamping is usually supported using those standards.

> **Input and output (I/O) ports**: Input/output connectors enable external devices to be connected to a network camera. Inputs to a camera (e.g. a door contact, infrared motion detector, glass break sensor or shock sensor) enable the camera to react to an external event by, for example, initiating the sending and recording of video. Outputs enable the camera to control external devices such as activating alarms, triggering door locks, generating smoke or turning on lights.

I/Os also allow you to save storage space. For example, if you want to simply capture the identity of a person at an entrance, you do not need the camera to continually send video. You can set up the system in such a way that the camera is triggered to capture and send the necessary image frames only when the door opens. I/O ports are available in all Axis network cameras and video encoders.

> **Video motion detection**: Video motion detection monitors changes in the camera's field of view and if a change occurs (e.g. an intruder enters the scene), an alarm condition is generated. This function can be a built-in feature of a network camera or a feature of a video management software. Using the built-in video motion detection feature in a network camera reduces bandwidth use since no video is delivered on the network unless video motion is detected. Video motion detection is a standard feature in all Axis network cameras.

> **Active tampering alarm**: This is an intelligent video analytics application available in selected Axis network video products. When a camera is manipulated in any way (e.g. accidental redirection, blocking, defocusing spray-painted, covered or damaged), it can automatically trigger recordings and alert notifications.

> **Alarm and event management**: With this capability, event triggers can be programmed based on schedule, I/Os, video motion detection, audio detection, active tampering alarm or temperature, among others. Pre- and post-alarm image buffers within a network camera can save and send images collected before and after an alarm occurs. Once an alarm or event is detected, a network camera can send notifications via e-mail, TCP, HTTP and upload images via e-mail, FTP and HTTP. Note that image uploads consist of sending individual JPEG files and do not mean recordings of video streams. Recording a video stream on an alarm trigger can be done using a video management software program, which has the capability to request a stream based on specific criteria (e.g., an H.264, MPEG-4 or Motion JPEG compression format, higher frame rate and image quality) that may be different from normal recording settings.

> **Power over Ethernet (PoE) (IEEE 802.3af)**: When a network camera supports this feature, it means that the camera can receive power through the same cable as for data. It reduces cabling requirements and installation costs.

> **Wireless**: A network camera with built-in wireless support is a consideration when running a cable between a LAN and a network camera is impractical, difficult or expensive. Wireless network cameras are suitable for use in outdoor situations, in environments such as historic buildings where the installation of cables would damage the interior, or in cases where there is a need to move cameras to new locations on a regular basis, such as in a supermarket. Ensure that the wireless network camera supports security protocols such as IEEE 802.1X and WPA/WPA2 (Wi-Fi Protected Access), which will help secure the wireless communication.

> **Security and management**: At a basic level, a video surveillance network camera should provide different levels of password-protected access to a network camera. For instance, some authorized users may only have access to view images from specific cameras; others have operator-level access, and a few have access to administer all settings in a network camera. Beyond multi-level password protection, a network camera may offer HTTPS encryption for secure communication; IP address filtering, which gives or denies access rights to defined IP addresses; IEEE 802.1X to control network access; and user access log.

> **Network management features**: They include support for Quality of Service (QoS), which can prioritize and reserve network capacity for mission-critical surveillance in a QoS aware network, and support for Internet Protocol version 6 (IPv6) in addition to IPv4 addresses.

c) How to select a network camera:
To determine the type of network cameras required, as well as the number of cameras needed to adequately cover an area, you first need to determine the scene or environment and the goal of the surveillance application.

Consider:

1) **Environment**: This will determine whether you need an outdoor or indoor camera, whether the camera needs to be tamper or vandal proof, and whether special housing is required. Consider also the lighting requirements: Is there adequate light to obtain a good quality image? Do you need to add light sources? How light sensitive should the camera be?

Figure 2.1.r. *Overview*

Figure 2.1.s. *Close-up*

2) **Area of coverage**: A PTZ or dome camera is able to cover a wider area than a fixed network camera. The bigger the area, the more cameras are needed.

3) **Application**:

i. Determine the kind of surveillance you want to conduct (overt/covert—this will help you in selecting cameras that offer a non-discreet or discreet installation).

ii. Determine also the kind of image you want to capture: overview or close-up for identification purposes. The purpose will determine the placement of the camera, the type of camera and camera features required (e.g. megapixel for exceptional details, audio, security features) and lens adjustment/type (normal, telephoto or wide angle).

A security operator using a PTZ or dome camera can cover a large area and capture different images for different purposes. In many cases, different cameras will be needed to capture images for different purposes (i.e. one camera providing a full overview image for capturing an incident in action, and another camera for close-up views of a person/object for identification purposes).

iii. Viewing and recording needs: Consider when and how often you need to view and record: day, night and/or weekends; frame rate capabilities; resolution; type of video compression support (H.264/MPEG-4 Part 2/Motion JPEG) and different alarm management functions and intelligent video features such as video motion detection, active tampering alarm and audio detection, which are also features that provide savings in bandwidth and storage space.

iv. Connection considerations: e.g. Power over Ethernet support, wireless.

Focus on image quality, open API, free upgrades, global product support
Axis' network video products are focused on providing high image quality. The products also have an open API (application programming interface) that enables many software vendors to write programs for. This benefit increases your choices in software applications. Axis also continually supports its network video products with free upgrades for new functionalities that are introduced. Global product support is also available.

In addition to network cameras, Axis offers video encoders and decoders, network video recorders and video management software. A wide range of accessories are also available: protective housings, IR illuminators, Power over Ethernet midspans and active splitter, connectors and cables, lenses and lens accessories, power accessories, as well as third-party accessories.

Before you set out to order or buy many network cameras, it is a good idea to field test a few cameras before making a decision. Try out an Axis network camera with a free AXIS Camera Station One video management software, which is packaged with every network camera purchase and is also downloadable on Axis' web site at www.axis.com. AXIS Camera Station One provides simultaneous viewing and recording of high quality H.264, MPEG-4 Part 2 and Motion JPEG video from a single surveillance camera.

2.2. Video encoder

If you already have existing analog CCTV surveillance cameras and want to move to an IP-based surveillance system, you can still make use of your analog investments by adding a video encoder (also called a video server). Simply connect a video encoder to analog cameras. The encoder converts analog signals into digital video and sends them over an IP network, enabling users to remotely monitor the cameras, as well as record and store video on standard PC servers. A video encoder brings new functionalities and benefits, such as remote monitoring capabilities, event management, scalability and ease of integration with other security systems. It also eliminates the need for dedicated equipment such as coaxial cabling, analog monitors and digital video recorders.

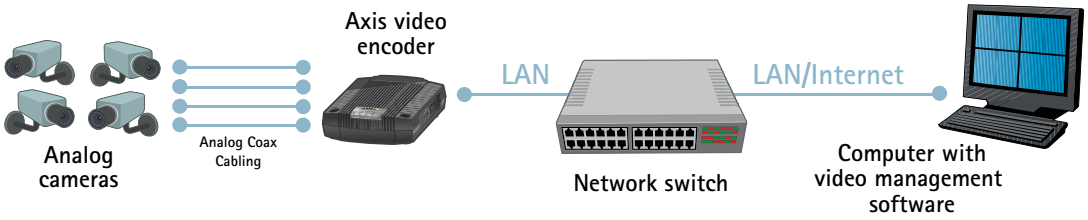


Figure 2.2.a. *A video encoder migrates analog cameras into an IP-based video solution*

Figure 2.2.b. *A one-channel, standalone video encoder with audio, I/O (input/output) ports for controlling external devices such as sensors and alarms, serial ports (RS-422/485) for controlling PTZ analog cameras and Ethernet connection with Power over Ethernet support.*

A video encoder can be connected to a wide variety of specialized cameras, such as a highly sensitive black and white camera, a miniature or a microscope camera, in addition to fixed, dome, indoor, outdoor and pan/tilt/zoom analog cameras.

A standalone video encoder typically provides between one and four connections to analog cameras, as well as an Ethernet port to connect to the network. Like network cameras, it contains a built-in web server, a compression chip, an operating system and processing power for local intelligence.

Besides digitizing analog signals, a video encoder can support a host of other functions: for example, intelligent video functionalities such as video motion detection, active tampering alarm and audio detection; digital inputs and outputs (I/O, which can trigger the encoder to start sending images or to activate alarms and devices such as lights and doors); and serial port(s) for serial data or control of pan/tilt/zoom cameras and devices. With image buffering, a video encoder can also send pre- and post-alarm images.

Some Axis video encoders also support Power over Ethernet (PoE), which enables the video encoders, as well as the analog cameras that are connected to them, to receive power through the same cable as for data transmission. Installation is easier and costs are reduced since there is no need to run separate cables for power. It also makes it easier to move a camera/video encoder to a new location. With PoE, a camera/video encoder can still operate in the event of a power failure if it is connected to a centralized backup power with an Uninterruptible Power Supply.

Figure 2.2.c. *When the AXIS Q7900 Rack is fully outfitted with 6-channel video encoder blades, it can accommodate 84 analog cameras.*

In instances where there are large numbers of analog cameras with coaxial cables running to a dedicated control room, rack-mounted video encoders or blades (video encoders without their casings) are beneficial. A rack can be outfitted with a mix of video encoder blades. Video encoder blades with one, four and six channels are available from Axis. Racks come with network, serial and I/O ports, and may provide a common power supply to all the blades. Axis racks also enable hot swapping of the video encoder blades so there is no need to power down when installing or removing the blades. One 19-inch rack can digitize up to 84 analog cameras and send multiple streams from each channel.

Where no coaxial cabling is in place, it is always best to use standalone video encoders and position them close to the analog cameras. It eliminates the need to lay new, separate coaxial cables since video and PTZ commands can be sent over an IP network infrastructure. This reduces installation costs and also eliminates the loss in image quality that would occur if video were to be transferred over long distances through coaxial cables. With coaxial cables, the video quality decreases the further the signals have to travel. Digital images do not lose quality over distance.

Considerations when selecting a video encoder solution:
(See also guidance provided in the previous section under network cameras.)

> **Image quality:** Axis video encoders provide high-quality, deinterlaced digital video. The deinterlace filter eliminates the artifacts (a series of horizontal lines) caused by analog interlaced scanning technology.

> **Frame rate and resolution:** Axis' high performance video encoders provide full frame rate—30 fps (frames per second) in NTSC, 25 fps in PAL—in all resolutions for all video channels. Common resolutions are: CIF (352x240 NTSC, 352x288 PAL), 4CIF (704x480 NTSC, 704x576 PAL), and D1 (702x480 NTSC, 720x576 PAL), which is the highest available resolution.

> **Video compression:** Many Axis video encoders offer users the option of more than one video compression format. The video compression standards include Motion JPEG, MPEG-4 and H.264. H.264 is the latest compression standard that offers the most efficient format for compressing video and which enables great savings in bandwidth and storage.

> **Multiple, individually configurable streams:** The Axis video encoders that have this capability are able to provide multiple streams from each video channel. Each stream can be configured differently in terms of compression format and level, frame rate and resolution.

> **Power over Ethernet:** Some Axis video encoders have built-in support for PoE. Consider if there is a need for PoE, which reduces costs and makes installation easier.

> **Audio:** A microphone or line-in equipment can be connected to Axis video encoders with integrated audio. Audio enhances the video surveillance capability by enabling users to also listen in on an area or pick up unusual sounds. Audio detection can also be used as an event trigger.

> **Rack solution:** Consider if there is a need for a rack solution, the number of analog channels a rack can support, as well as the types of network connection supported.

> **Event management and intelligent video:** Consider requirements for I/Os and intelligent video functionalities such as video motion detection, audio detection and active tampering alarm. These features can help reduce bandwidth and storage consumption as they enable only actionable data to be sent upon alarm.

> **Advanced security and network management:** Axis video encoders offer many ways to secure access to video. Security features include multi-level password protection; IP address filtering, which gives or denies access rights to defined IP addresses; HTTPS encryption, which provides a secure channel between the video encoder and application; and IEEE 802.1X to control network access. Net work management features include Quality of Service (QoS), which helps secure the necessary band width for streaming video and control commands over a network; and support for Internet Protocol version 6 (IPv6) and standard IPv4 addresses.

> **Video management software:** Axis video encoders are supported by a wide range of application software, including AXIS Camera Station.

2.3. Network

The next consideration to make is assessing your network needs.

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

First, determine what your company is using the network for and how congested your local area network (LAN) or wide area network (WAN) is.

If you are implementing a smaller surveillance system involving 8 to 10 cameras, you should be able to use a basic 100-megabit (Mbit) network switch without having to consider bandwidth limitations. Most companies can implement a surveillance system of this size using their existing network.

If you are implementing 10 cameras or more, you should try to estimate the load on the network using a few rules of thumb:

> A camera will use approx. 2 to 3 megabits of bandwidth when configured to deliver high-quality images at high frame rates.

> With more than 12 to 15 cameras, you should consider using a switch with a gigabit (Gbit) backbone. If a gigabit-supporting switch is used, the server that runs the video management software should have a gigabit network adapter installed.

Determine the pattern of congestion levels over a given period to find out if you have to install additional bandwidth capacity on your network or whether you can make use of the same network as for general business activities. It may be that the network traffic drops off during nighttime and weekends—the times when you may want to activate the video surveillance system. The usage pattern will help you to determine whether you can a) simply use the same network infrastructure for your general purpose needs as for your surveillance needs, or b) use a combination of existing general purpose network as well as a new network for IP-Surveillance. If additional network capacity is needed, new cabling is normally not needed since adding a switch or reconfiguring the patch panel may solve the problem. One tool that helps estimate bandwidth usage is the AXIS Design Tool, which is available at www.axis.com/products/video/design_tool/. See also section 5.d for more about bandwidth control.

Wireless networks

When running a cable between a LAN and a network camera is impractical, difficult or expensive, a wireless solution using a wireless access point—also called a device bridge or wireless router—is a good option. Wireless technology can be useful, for example, in historic buildings where the installation of cables would damage the interior; within facilities where there is a need to move cameras to new locations on a regular basis, such as in a supermarket; or in outdoor installations. Wireless technology can also be used to bridge sites without expensive ground cabling.

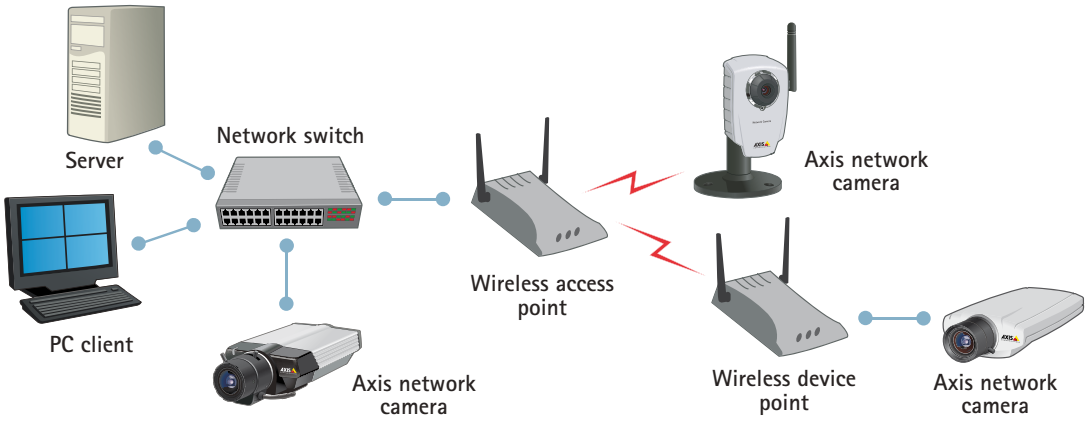


Figure 2.3.b. *A network with wired and wireless connections.*

Security in wireless networks

Securing a wireless network should be addressed. Otherwise, everyone with a wireless device present within the area covered by the network will be able to participate in the network and use shared services. The most commonly used standard today is WEP (Wireless Equivalent Privacy), which adds RSA RC4-based encryption to the communication, and prevents people without the correct key from accessing the network. But as the key itself is not encrypted, it is possible to 'pick the lock,' so this should be seen only as a basic level of security. A new standard, the WPA (WiFi Protected Access), significantly increases security by taking care of some of the shortcomings in the WEP standard with, for instance, the addition of an encrypted key.

When using wireless cameras for surveillance, there are a few rules of thumb:

> Enable the user/password login in the cameras
> Enable the encryption in the wireless router/cameras
> Since wireless routers do not have the same bandwidth capacity as a normal switch, no more than four to five cameras should be connected to a wireless access point.

2.4. Hardware (storage needs)

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 since a storage solution treats video data like any other large group of files that can be stored, accessed and eventually deleted. Video storage, however, 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 amounts of data, creating high demands 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 event triggers such as video motion detection or continuous recording. Additional parameters such as frame rate, compression, image quality and scene complexity (little motion or lots of motion) should also be considered.

The type of video compression employed also effects storage calculations. The H.264 compression format is by far the most efficient video compression technique available today. Without compromising image quality, an H.264 encoder can reduce the size of a digital video file by more than 80 percent compared with the Motion JPEG format and as much as 50 percent more than with the MPEG-4 Part 2 (referred to simply as MPEG-4 in future references) standard. This means much less network bandwidth and storage space are required for an H.264 video file. Or seen another way, much higher video quality can be achieved for a given bit rate.

With Motion JPEG, storage requirements vary depending on the frame rate, resolution and degree of compression. With H.264 and MPEG-4, bit rate is the key factor in determining the corresponding storage requirements.

There is a clear formula for calculating storage requirements when it comes to Motion JPEG (see calculation below) because Motion JPEG consists of one individual file for each image. Calculations are not so clear-cut for H.264 and MPEG-4 because of a number of variables that affect bit rate levels. However, sample calculations for H.264 and MPEG-4 are also provided below:

H.264 calculation:
Bit rate / 8(bits in a byte) x 3600s = Kilobyte (KB) per hour / 1000 = Megabyte (MB) per hour
MB per hour x hours of operation per day / 1000 = Gigabyte (GB) per day
GB per day x requested period of storage = Storage need
(Note: The figures below are based on lots of motion in a scene. With fewer changes in a scene, the figures can be 20 percent lower. The amount of motion in a scene can have a big impact on the amount of storage required.)

Camera	Resolution	Bit rate (Kbit/s)	Frames per second	MB/hour	Hours of operation	GB/day
No. 1	CIF	110	5	49.5	8	0.4
No. 2	CIF	250	15	112.5	8	0.9
No. 3	4CIF	600	15	270	12	3.2

Total for the 3 cameras and 30 days of storage = 135 GB

MPEG-4 calculation:
Bit rate / 8(bits in a byte) x 3600s = KB per hour / 1000 = MB per hour
MB per hour x hours of operation per day / 1000 = GB per day
GB per day x requested period of storage = Storage need
(Note: The formula does not take into account the amount of motion, which is an important factor that can influence the size of storage required.)

Camera	Resolution	Bit rate (Kbit/s)	Frames per second	MB/hour	Hours of operation	GB/day
No. 1	CIF	170	5	76.5	8	0.6
No. 2	CIF	400	15	180	8	1.4
No. 3	4CIF	880	15	396	12	5

Total for the 3 cameras and 30 days of storage = 204 GB

Motion JPEG calculation:
Image size x frames per second x 3600s = KB per hour/1000 = MB per hour
MB per hour x hours of operation per day / 1000 = GB per day
GB per day x requested period of storage = Storage need

Camera	Resolution	Image size (KB)	Frames per second	MB/hour	Hours of operation	GB/day
No. 1	CIF	13	5	234	8	1.9
No. 2	CIF	13	15	702	8	5.6
No. 3	4CIF	40	15	2160	12	26

Total for the 3 cameras and 30 days of storage = 1002 GB

Storage Options

Storage solutions depend on a PC's or server's ability to store data. As larger hard drives are produced at lower costs, it is becoming less expensive to store video. There are two ways to approach hard disk storage. One is to store video on the same server that runs the application. This is called a direct attached storage. The other is to have the storage separate from the server that runs the application. This is called a network-attached storage (NAS) or a storage area network (SAN).

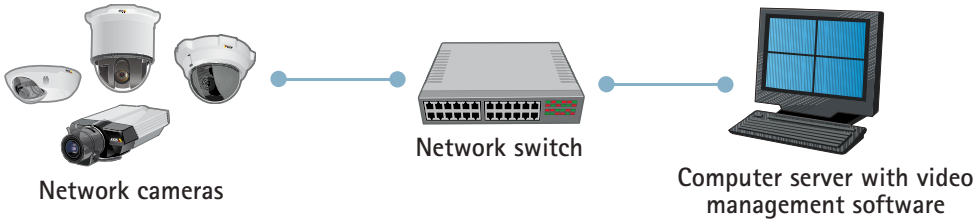


Figure 2.4.a. *Direct attached storage*

Direct attached storage is probably the most common solution for hard disk storage in small to medium-sized IP-Surveillance installations (See image above). The hard disk is located in the same PC server that runs the video management software. The PC and the number of hard disks it can hold determine the amount of storage space available. Most standard PCs can hold between two and four hard disks. With today's technology, each disk can store approximately 300 gigabytes of information for a total capacity of approximately 1.2 terabytes (one thousand gigabytes).

For information about NAS and SAN, please see Chapter 8.

2.5. Video management software

Although video can be managed simply by using the built-in web interface of a network video product, video management software enables more effective management of video from multiple cameras for live monitoring and recording. Video management software is, therefore, an important component of an IP-Surveillance system.

Video management requirements depend on the number of cameras, performance criteria, platform preferences, scalability, and whether there is a need for integration 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.

AXIS Camera Station

AXIS Camera Station is a video management software program that is designed specifically for managing Axis network cameras and video encoders. It enables multi-camera viewing, high-quality recording, playback and event management.

Figure 2.5.a. *AXIS Camera Station video management software*

Key features include:

> **Simultaneous viewing and recording of live video from multiple cameras:** Multiple users can view several different cameras at the same time, and recordings can take place simultaneously. The system can also be used for different purposes; for example, in a retail environment, one user can use the system for security, while another individual may use the same system to study store traffic.

> **Several recording modes:** Continuous, on alarm trigger and/or intelligent video features such as video motion detection, and manually. Continuous and triggered recordings can be scheduled to run at selected times during each day of the week. The software supports recordings in H.264, MPEG-4 and Motion JPEG for optimized quality and bandwidth. For a comprehensive picture of an event, the software's multi-view playback feature allows users to view simultaneous recordings from different cameras. Recording instances can be visualized using a timeline, making searches easy. Recordings can also be searched based on motion and external alarm triggers. Export functionality is also provided.

> **Alarm management functions:** Event triggers can be programmed based on schedule, I/Os and intelligent video functionalities such as video motion detection. AXIS Camera Station can set the amount of pre- and post-alarm image buffers a network camera or video encoder should send before and after an alarm occurs. Once an alarm or event is detected, the software program can send alarm notifications via e-mail and request that a network video product send a video stream with specific settings for recording.

> **Frame rate control:** AXIS Camera Station enables users to set different recording frame rates for selected cameras; for example, one under normal operation and another when alarm is triggered. Different frame rates can also be set for viewing and/or recording purposes and for different recipients.

> **Camera management:** AXIS Camera Station enables administration and management of network cameras and video encoders to be done from a single interface. It is useful for tasks such as detecting cameras on the network, managing IP addresses, and setting resolution, compression and security levels. The software can provide access to every camera on the network and will automatically administer firmware upgrades. This is practical particularly in situations where cameras are located in distant or hard-to-reach locations. The administrator does not have to visit each location to upgrade every camera.

Each AXIS Camera Station installation lets you monitor up to 50 cameras at the same time. You can install as many AXIS Camera Station programs as required. Based on a PC Server platform solution, the software enables full scalability as cameras can be added one at a time and there is no limit to the number of cameras that can be added or managed. The limitation is only in the storage hardware capacity rather than the software. Since AXIS Camera Station uses common, "off-the-shelf" hardware, the hardware components can be selected for maximum performance.

Recordings are saved directly onto the hard disk(s) of the local PC server where the AXIS Camera Station is installed. A Windows-based software, AXIS Camera Station has a Windows client program that is used to provide local or remote viewing, playback and administration. All settings are inherited and downloaded from the video management software. This means that the 'server' can be placed anywhere; for example, in the server room or basement.

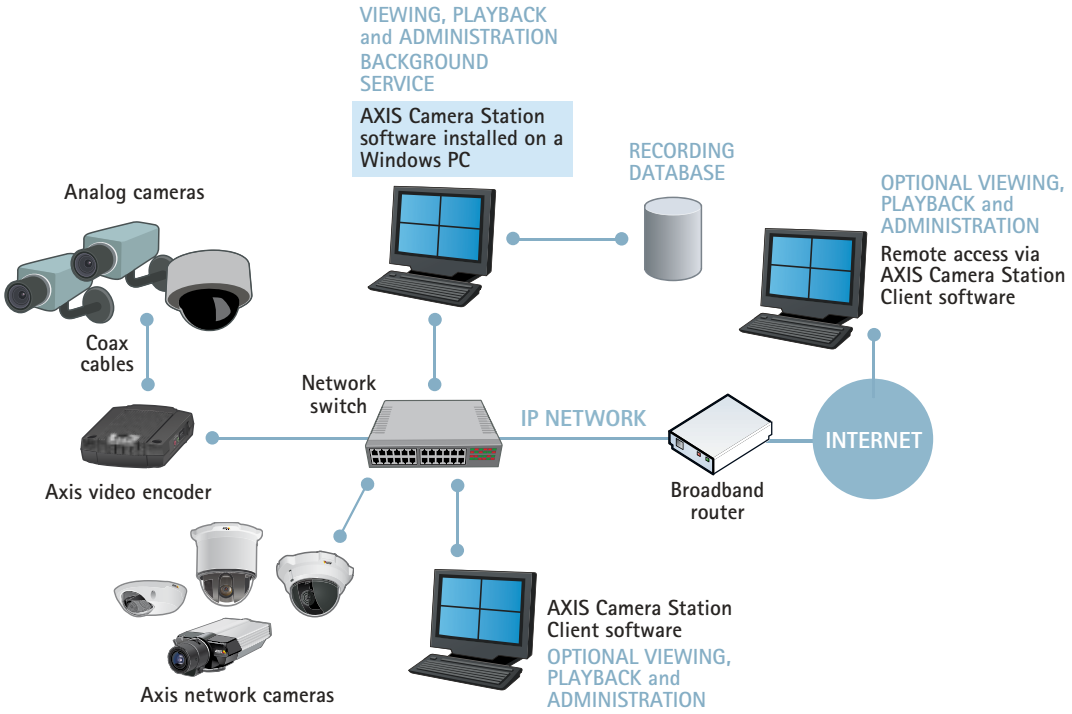


Figure 2.5.b. *AXIS Camera Station is installed on a Windows-based PC. Remote users can access the software via a Windows client.*

The AXIS Camera Station Client enables users to switch between different servers with the video management software installed. This makes it possible to manage video at many remote sites or in a large system. AXIS Camera Station runs as a background service on a Windows PC with XP Professional or Vista Business. This means that even when you are logged off the PC that is running the software, the AXIS Camera Station program is still operating.

AXIS Camera Station can also be integrated with other systems such as point of sale, access control, tracking (e.g. radio-frequency identification), building management and industrial control. When video is integrated, information from other systems can be used to trigger functions such as event-based recordings in the network video system, and vice versa. In addition, users can benefit from having a common interface for managing different systems.

AXIS Camera Station comes with a base license for four Axis network cameras/video encoders. The number of licenses required is based on the number of network cameras/video encoders that are to be used with the program. Additional licenses, as well as software upgrade licenses, are available for purchase at your local Axis reseller.

More details about AXIS Camera Station are covered in the latter half of this document.

3. Mounting surveillance cameras

This chapter provides recommendations on how to best achieve useable, high-quality, surveillance video based on camera positioning and environmental considerations.

The following are some guidelines:

> **Surveillance objective**

When positioning a surveillance camera, it is important to keep in mind the kind of image you would like to capture. If the aim is to get an overview of an area to be able to track the movement of people or objects, make sure you are using a suitable camera and that it is placed in a position that achieves this goal.

If the intention is to be able to identify a person or object, you will need a suitable camera that is positioned or focused in a way that will capture the level of detail needed for identification purposes. It may be favorable to place a camera in a high position to limit tampering. However, a lower placement may improve identification of faces or detailed objects, avoiding a "bird's eye" perspective. Local police authorities may also be able to provide guidelines on how best to position a surveillance camera. A letter chart, with varying letter sizes (attached as an appendix in this document), can be used as an indicator of the level of detail an installed camera can provide. A spinning Rotakin (see device at right) may also be used to test how well a camera displays moving objects.

> **Housing**

If a camera is to be mounted outdoors or in a relatively hostile environment, it needs a protective (weatherproof and/or vandal-proof) housing. Camera housings come in different sizes and qualities and some versions have built-in fans (for cooling) and/or heaters. There are vandal-resistant cameras that are already designed with an IP66-rated casing and have a built-in heater and fan, such as the AXIS 225FD Network Camera. In such a case, no additional housing accessory is required.

Figure 3.b. *Outdoor casing suitable for use with Axis network cameras.*

> **Reflections**

If a camera is mounted behind a glass in a housing, the lens must be placed close to the glass. Otherwise, reflections from the camera and the background will appear in the image. To reduce reflection, special coatings can be applied on any glass used in front of the lens.

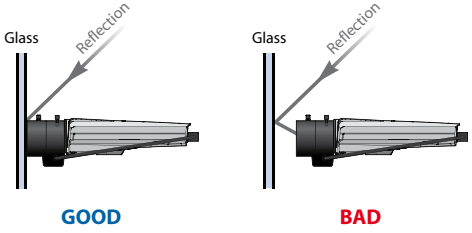


Figure 3.c. *How to position a camera to avoid reflections.*

> **Secure support**
A camera should be placed on stable supports to minimize camera movement. As PTZ cameras move around, the action can cause image interference if the camera mounting is not properly secured. In outdoor situations, sturdy mounting equipment should always be used to avoid vibrations caused by strong winds.

> **Use lots of light/Add light if needed**
The most common reason for poor quality images is lack of light. Generally, the more light, the better the images. With too little light, the images will become blurred and dull in color. You can easily and cost-effectively add strong lamps in both indoor and outdoor situations to give you the light conditions necessary for capturing good images.

Environment: lux

> Strong sunlight: 100,000
> Full daylight: 10,000
> Normal office light: 500
> Poorly lit room: 100

Lux is the standard unit of measurement for light. The table at right shows the available light in different kinds of conditions. At least 200 lux is needed to capture good quality images. A high-quality camera might be specified to work down to 1 lux, which means that you can capture an image at 1 lux, but it may not be of high quality. Different manufacturers use different references when they specify the light sensitivity of a camera, and this makes it difficult to compare cameras without first testing them and comparing the images captured.

When using external, artificial lighting in outdoor environments, reflections and/or shadows should be avoided.

For covert security or in areas where the presence of artificial light is unwanted, you can choose to use an IR-sensitive, black and white camera, or an automatic, day/night camera. In a day/night camera, color video is delivered during light conditions, while at night, the camera makes use of near-infrared light to generate IR-sensitive, black and white video. An IR illuminator, which provides infrared light, can also be used in conjunction with an IR-camera or a day/night camera to further enhance a camera's ability to produce high-quality video in low-light or nighttime conditions.

Figure 3.d. *IR-sensitive network camera with IR illuminator attached below the camera housing*

> **Avoid direct sunlight**
Direct sunlight should always be avoided. Direct sunlight will "blind" the camera and can reduce the performance of the image sensor chip. If possible, position the camera with the sun shining from behind the camera.

> **Bright areas in the images should be avoided** as they might become overexposed (bright white) and objects can then appear too dark. This problem typically occurs when attempting to capture an object in front of a window. To solve this problem, simply reposition the camera or draw the curtains and close blinds if possible.

Figure 3.e. *Avoid very bright areas in an image by changing the camera position.*

Figure 3.f. *Advanced cameras include the feature to compensate for backlight.*

> **Contrast**
In outdoor environments, viewing too much of the sky results in too much contrast. The camera will adjust in order to achieve a proper light level for the sky. Consequently, the object/landscape of interest will appear too dark. One way to solve this problem is to mount the camera high above the ground, using a pole if needed. In advanced network cameras, users may be able to set which part of an image should be more correctly exposed.

> **Lenses**
An auto iris lens should always be used for outdoor applications. An auto iris lens automatically adjusts the amount of light that reaches the image sensor. This optimizes the image quality and protects the image sensor from being damaged by strong sunlight.

> **Adjust camera settings**
It is important to adjust the white balance settings for different environments (indoor/outdoor/fluorescent), as well as for brightness and sharpness.

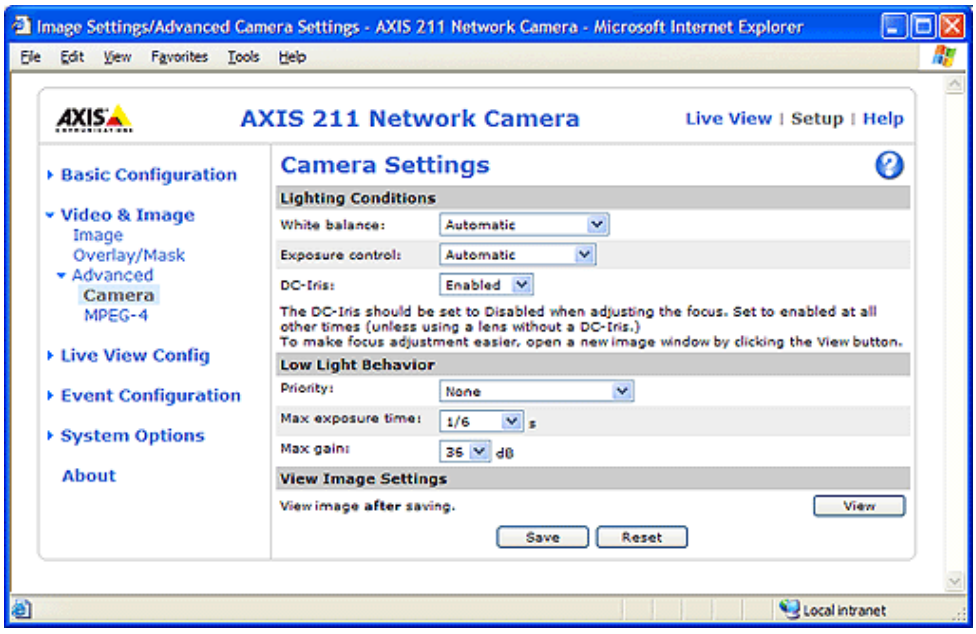


Figure 3.g. *Example of a camera user interface showing options for advanced camera settings.*

When deciding upon the exposure, a fast shutter speed or shorter exposure time is recommended when capturing rapid movement or when a high frame rate is required. A longer exposure time will improve image quality but it may lower the total frame rate and result in increased motion blur. In Axis network cameras, an automatic exposure setting means the frame rate will increase or decrease with the amount of available light. It is only as the light level decreases that you need to have artificial light or prioritize frame rate or image quality.

The following chapters outline how a small- to mid-sized IP-Surveillance system can be implemented using Axis network video products and AXIS Camera Station software.

4. Server selection

This chapter discusses general server recommendations, hard disk selection, network-attached storage and RAID as they relate to the installation of the AXIS Camera Station software and its hard disk clean-up procedure.

4.1. General server recommendations for AXIS Camera Station

Number of cameras	Server: Recommended hardware				Client: Recommended hardware		
	Hard disks	Bandwidth	CPU (GHz)	RAM (GB)	Graphics	CPU (GHz)	RAM (GB)
10	1	100	Dual Core 2.0	1	256	Dual Core 2.0	1
20	2	1000	Dual Core 3.0	2	512	Dual Core 3.0	3
30	2-3	1000	Core2 quad	2	512	Core2 quad	2
40	3	1000	Core2 quad	3	512	Core2 quad	3
50	4	1000	Core2 Extreme	4	768	Core2 Extreme	4

The table above outlines the recommendations for server requirements in implementing an IP-Surveillance system using AXIS Camera Station as the video management software. The recommendations are not minimum requirements.

Notes:

> The figures are based on viewing and recording video with a 640x480 resolution and a 25 percent compression rate using Motion JPEG. Raising the resolution, frame rate and image quality will raise the requirements for the server.

> The CPU recommendation is based on Intel Dual Core processors. Other options such as Xeon Dual may lower the CPU requirement.

> Using H.264 or MPEG-4 recording will reduce bandwidth and hard disk requirements.

> For best performance and stability, use local hard disks or a high performance network storage solution for storing recordings.

> Software-based RAID systems should not be used since performance bottlenecks could result. A good hardware RAID controller with fast disks could be a good option to secure your recordings.

> The disk drive (normally C:) where Windows and AXIS Camera Station are installed should have enough disk space for the AXIS Camera Station log files. Allow at least 1 GB free disk space for the log files.

> The AXIS Camera Station Client requires a good graphics adaptor with at least 256 MB of memory and support for DirectX 9.0C.

4.2. Hard disks

When selecting hard disks for your surveillance solution, keep in mind that the recording of a continuous stream of video from multiple cameras will add more load on the hard drive than a standard office PC or mail server.

There are three main hard drive solutions on the market:

1. SCSI
2. Serial ATA
3. IDE

4.3. SCSI is the best solution in terms of reliability (and also the most expensive), followed in order by Serial ATA and IDE. Note that Serial ATA and IDE are made for office desktops and not for 24-hour server operations, as a surveillance solution demands. Since it is difficult to predict how long such hard disks will last, Serial ATA and IDE disks should be installed in a way that makes them easy to replace.

Network-attached storage (NAS) and RAID

This section describes how AXIS Camera Station can use NAS to store recordings.

AXIS Camera Station will record video on the hard drive. The video will remain there for the number of days specified in the configuration.

For each drive that is used for recording, you will need to specify how much disk space should be dedicated for recording purposes. If the amount of disk space used is exceeded, AXIS Camera Station will remove the oldest recording to ensure that there is enough space for ongoing recordings.

For each camera, you will need to specify the number of days that recordings should be stored. A special option called "Unlimited" can be selected. The camera will then record for as many days as there is space on the hard drive before AXIS Camera Station removes the oldest recordings.

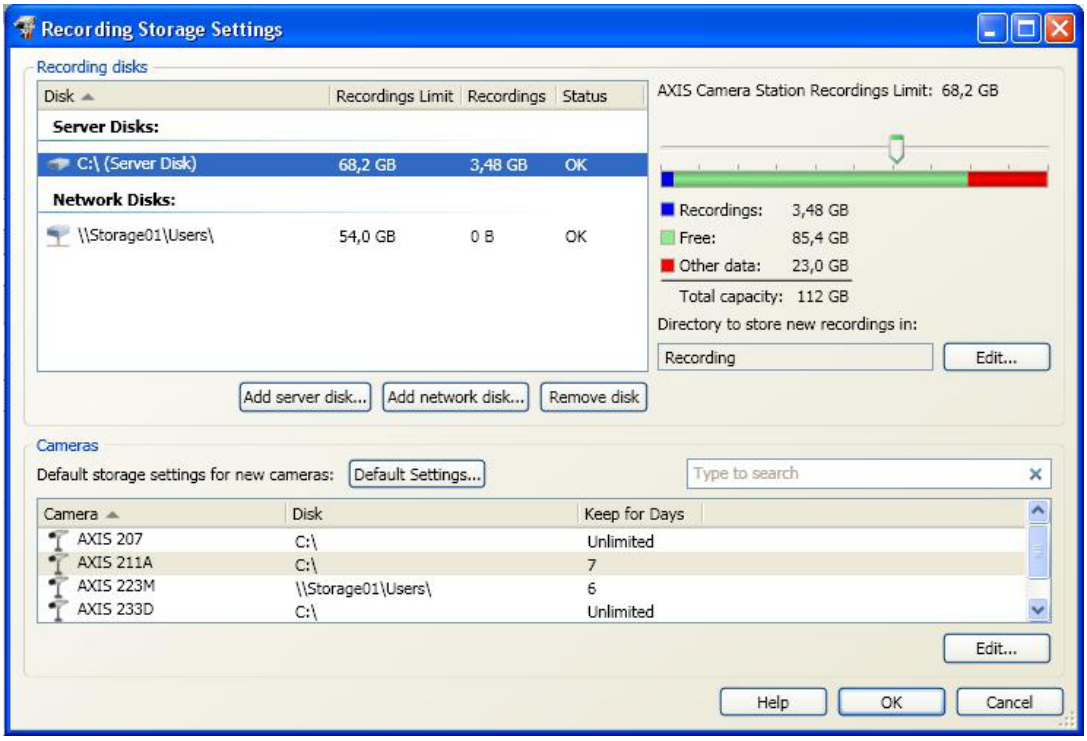


Figure 4.3.a. *AXIS Camera Station: Recording storage settings*

When using remote disks or NAS, you will need to ensure that the necessary bandwidth is available to move recordings from the AXIS Camera Station server to the archive drives. Keep in mind that in a network-attached storage setup, live streams from the cameras are running while data is being moved to the NAS.

Using Redundant Array of Independent Disks (RAID) setup

RAID—which is a method of arranging hard drives in such a way that the operating system sees them as one large, logical hard disk—can be used to secure your recordings and configuration, but it must be implemented with caution.

RAID is mostly configured in three different ways:

RAID Level	Characteristics
RAID-0	Data is being striped (divided) over two or several hard disks for improved read/write speed but no redundancy. There is no advantage of using this setup with the AXIS Camera Station.
RAID-1	This is also known as disk mirroring since all hard disks are mirrored one by one. At least two disks duplicate data. Both disks can be read at the same time. Write performance as for single disk storage.
RAID-5	Minimum of three hard disks. One of the hard disks is used to mirror the others (in theory).

When RAID 1 or 5 is used, data is written twice, over two hard disks (one for the primary data disk and one for the mirror disk). This has an impact on performance since all disk writes are doubled in a RAID setup. When multiple cameras are streaming data to the hard drives, the RAID controller will handle the load using buffers and distribute the data to the disks. Since the hard disk write is doubled and there is a limit of how many write per second the setup can handle, a RAID setup can become a bottleneck in a video surveillance system if it is not implemented correctly.

There are three usual ways to implement RAID:

1) Using a software solution that can configure two or more hard disks into a RAID setup. This is a very slow implementation and should never be used for a video surveillance system.

2) The CPU comes with an on-board RAID solution. This is a hardware implementation that may have limited performance and should be used with caution.

3) Full hardware implementation with a separate RAID controller. This is the only recommended way to implement RAID for a video surveillance solution. Make sure you use a well-known and well-proven RAID technology as your surveillance solution will rely on it.

4.4. AXIS Camera Station hard disk cleanup procedure

While the AXIS Camera Station recording engine is running, some procedures are continuously executed to ensure that your hard disks do not become full. The procedures include:

1) Comparing recorded images with the current date and configured "days to record." If the saved recordings have passed the number of days that they should be stored in the primary hard drive, the images are removed.

2) Freeing up space on the primary hard drive for current recordings. If the space available on the primary drive is less than what is specified in the configuration, an emergency cleanup is invoked. This means that the oldest recordings from all cameras are deleted and space is freed up for current recordings.

5. AXIS Camera Station installation and configuration

This chapter provides an overview of the AXIS Camera Station installation and configuration processes covering registration, camera setup, recording methods, bandwidth control and security.

5.1. Installing AXIS Camera Station

AXIS Camera Station should be installed on a dedicated, standalone PC where you wish to run the main administration of your network cameras and video encoders. When the program is installed, it will ask you to register your license. The license key can only be used on one computer. Once the license key is registered, it cannot be used again. Therefore, the AXIS Camera Station must be installed on the target computer when activating the software.

You can choose to activate one of four AXIS Camera Station alternatives, either automatically or manually:

a) Licensed Version

b) Grace Period (which allows you to use the software for five days)

c) Demo (30-day trial version for four cameras. When the period expires, you will be required to register the software.)

d) AXIS Camera Station One – Free Version

Figure 5.1.a. *AXIS Camera Station installation alternatives*

5.2. Setting up a network camera/video encoder in AXIS Camera Station

After installing the AXIS Camera Station, it must be configured for your network cameras and video encoders. The first time the software is configured, a search function automatically finds and installs the network cameras/video encoders on your network. If there are more cameras/video encoders on your network than you have licenses for, this procedure will be stopped. To add or remove a network camera/video encoder at a later date, you can either manually enter the IP address of the network video product, or click the Search button to get a list of video products on your network. Once a video product is imported into AXIS Camera Station, you will need to choose a master user name and password if the cameras are set up to use a common user name and password, or enter a specific user name and password for a specific camera.

Customize the view in AXIS Camera Station

AXIS Camera Station offers a number of different ways and layouts to view one or many cameras simultaneously. These are called Auto views, My Views, Shared Views and Camera Views. Auto Views are predefined (showing views from cameras that are added to AXIS Camera Station) and cannot be changed. My views and Shared views enable users to customize the viewing layout. Cameras can then be arranged by simply dragging and dropping a camera into the desired viewing location. Camera Views enables the user to select the specific camera to open its Live View.

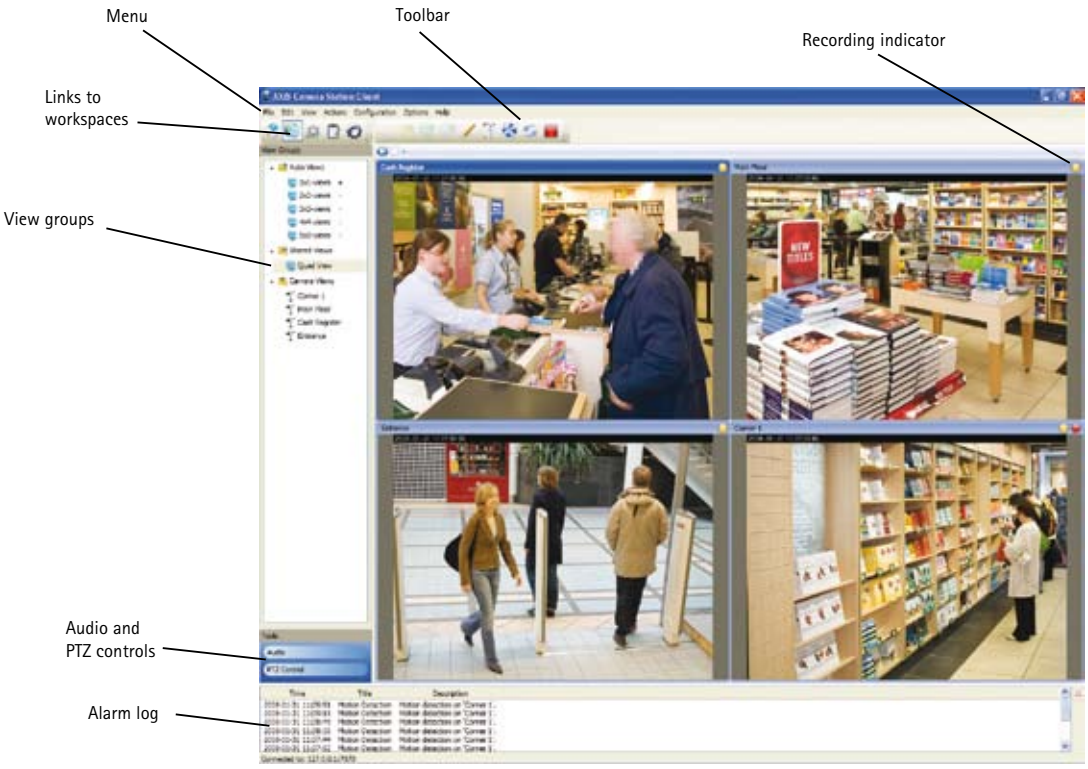


Figure 5.2.a *AXIS Camera Station's live view screen*

For each individual camera, you can specify the image settings (streaming format, quality, frame rate and size) to be used for live viewing. This setting will be used in live views except in views with nine or more cameras where the settings are fixed to optimize the performance of the PC.

5.3. Recording methods

For each camera, you can select one of three recording methods to use:

1) continuous

2) triggered by motion or alarm

3) manual (start/stop recordings from the user interface)

Continuous and triggered recordings can be scheduled to run at selected times during each day of the week.

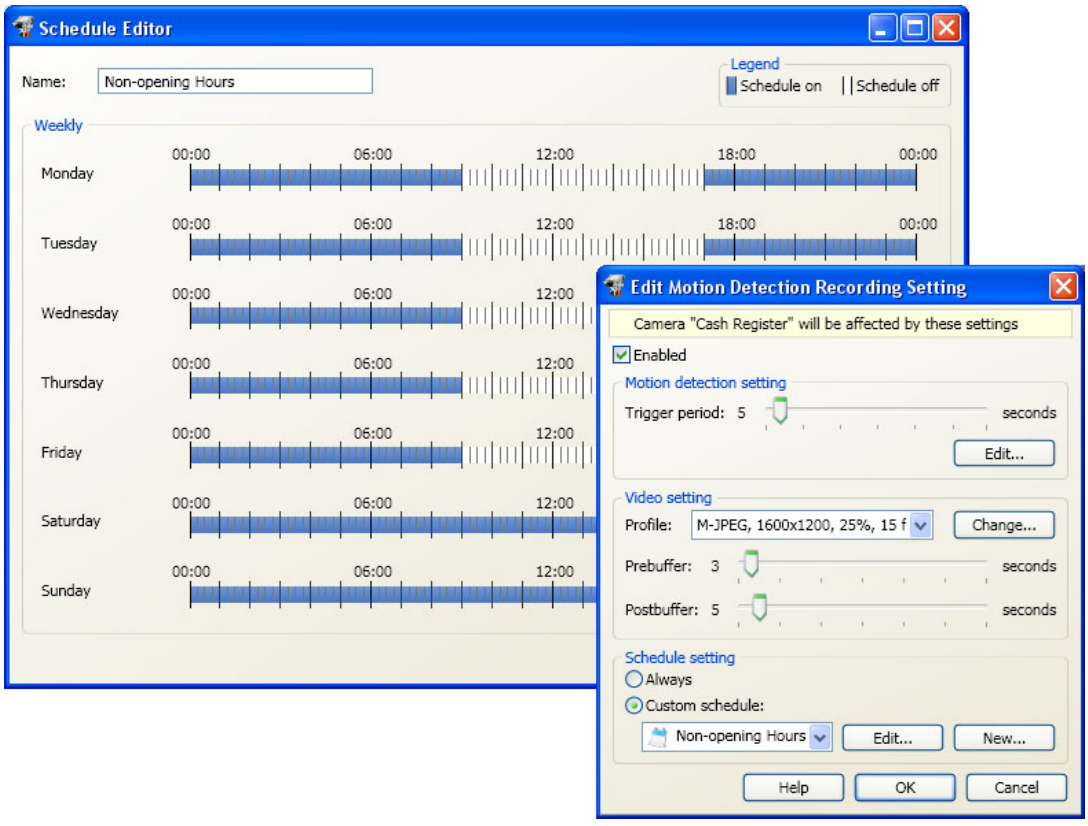


Figure 5.3.a. *Making recording settings using AXIS Camera Station.*

For each camera, you can specify the image settings (streaming format, quality, frame rate and size) to be used for recording. The settings will affect the amount of bandwidth used, as well as the amount of storage space required.

For recordings triggered by video motion detection, AXIS Camera Station uses the Axis network camera/encoder's built-in motion detection functionality. This reduces bandwidth usage and processing load on the server. (More about video motion detection is covered in Chapter 6.) With recordings triggered by external inputs/outputs (I/O triggered recording), simply define the alarm trigger for the selected camera(s) that will record when the alarm is triggered. The length of the pre- and post-alarm image buffers can be set by defining the number of seconds the camera/encoder should record before and after an alarm is triggered. The image buffers help to provide a more comprehensive picture of an event. Recording only when motion or alarm is detected will save hard disk space compared with continuous recording.

The AXIS Camera Station's background service automatically starts running upon system start-up. When the background service is running, recording will continue even after a user has logged out from the PC where AXIS Camera Station is installed.

5.4. Event handling

AXIS Camera Station has an event handler that is built into the recording engine. It allows you to configure the actions to be taken when defined events are triggered. Triggers in AXIS Camera Station are classified under two categories: video motion detection and input/output.

Video motion detection is triggered when an Axis camera/video encoder detects motion within its defined viewing area. The detection is performed by the Axis camera/video encoder so there is no processing load on the AXIS Camera Station server. (More about video motion detection is covered in Chapter 6.)

External devices such as a door contact, a glass break detector or a passive infrared detector (PIR) that are connected to the input or output ports of a camera/video encoder can also be used as triggers by AXIS Camera Station. In addition, other intelligent video functionalities—for example, active camera tampering—that are supported in a network camera/video encoder can be used by AXIS Camera Station if they are first configured (through the network video product's web interface) to trigger the output port of the network video product.

Event/alarm responses include initiating recordings from selected cameras, raising an alarm, showing a live image from a selected camera, setting an external output device such as sounding a siren, and sending e-mail notifications.

5.5. Calculating your hard disk requirements

Network video products utilize network bandwidth based on their configuration. Bandwidth usage depends on five criteria:

1) Image resolution (the higher the resolution, the more bandwidth is required)

2) Compression type (H.264 requires much less bandwidth than MPEG-4 and Motion JPEG)

3) Compression ratio (the higher the compression, the lower the bandwidth usage)

4) Frame rate (the higher the frame rate, the higher the bandwidth usage)

5) Image complexity (the more motion or scene changes, the higher the bandwidth usage)

The above criteria can be set either in the AXIS Camera Station software or in the network camera or video encoder itself. A simulation-based calculation tool called the AXIS Design Tool is available at www.axis.com/products/video/design_tool/ (or on a DVD) and helps provide guidance on a network video product's bandwidth and storage requirements based on the five criteria mentioned earlier.

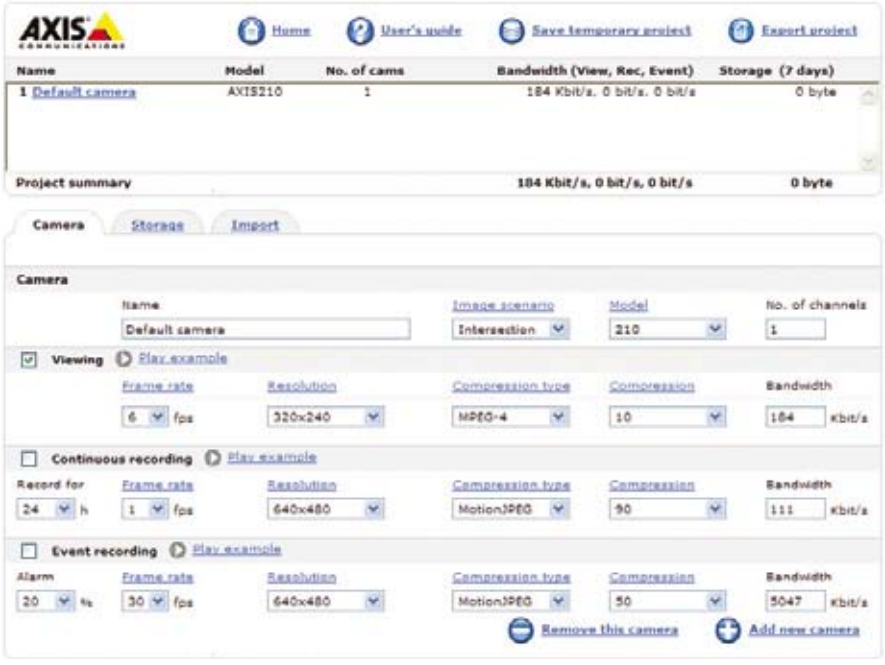


Figure 5.5.a. *AXIS Design Tool user interface*

You can reduce the use of bandwidth and storage space if you record only when motion or alarm is detected compared with continuous recording and if you use the H.264 or MPEG-4 compression format.

5.6. Security aspects

A high level of security can be implemented in the AXIS Camera Station. The software can inherit the Windows user database (local or LDAP/Domain) and you can grant or deny users access to a specific camera. This feature allows you to use your current user database without having to set up and maintain a separate database of users.

Once a user is defined, you select the user-access level. Three levels are available:

1) Administrator – full access to all of AXIS Camera Station's functionalities

2) Operator – Access to all functionalities (including recorded events) except the configuration pages under Options

3) Viewer – Access only to live video

For each user, you can choose which cameras the user will be allowed to access. There are also options to allow/deny access to functions such as audio and PTZ control for each user or camera.

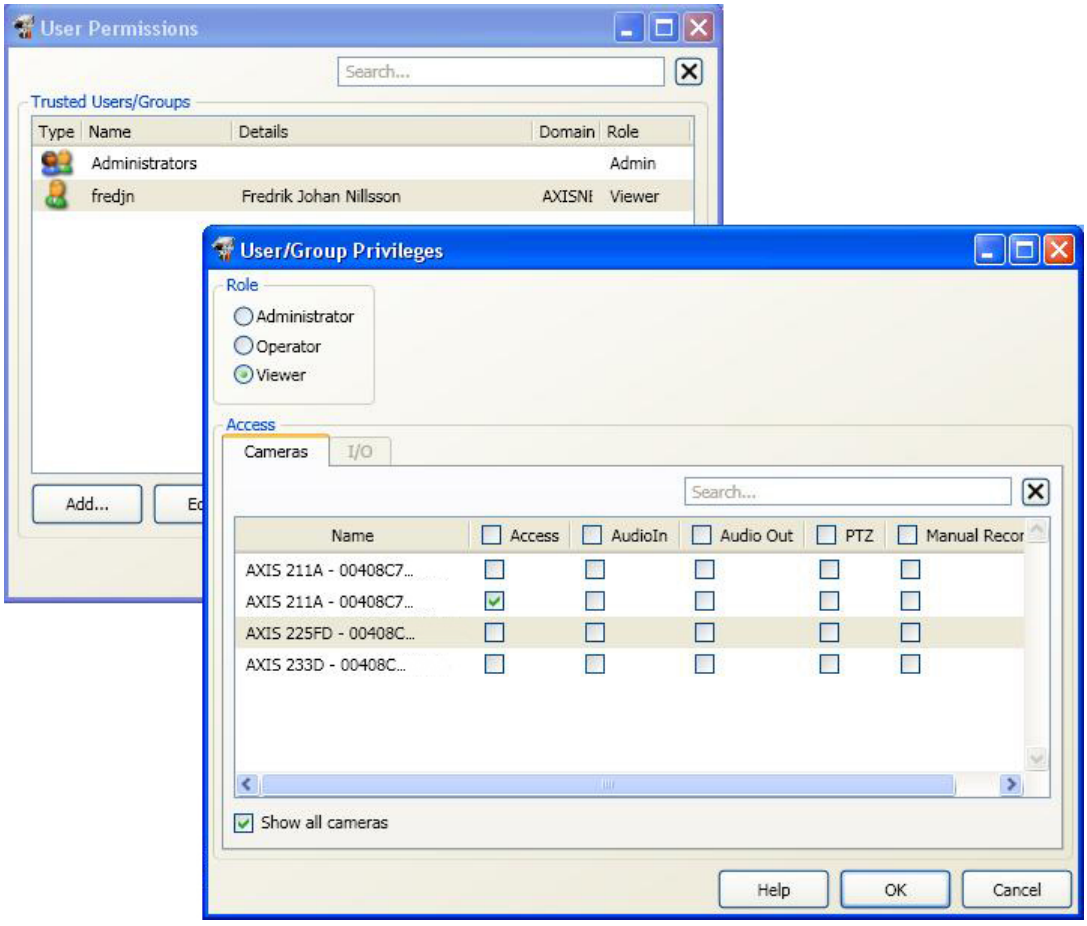


Figure 5.6a. *AXIS Camera Station allows an administrator to select which camera and functionality a user may have access to.*

6. Video motion detection

This section describes how video motion detection works in the network camera or video encoder and how it functions with AXIS Camera Station.

The built-in video motion detection feature in Axis network cameras or video encoders is used to generate an alarm whenever movement occurs in the viewing area. You can configure a number of "included" windows (a specific area in an image where you want motion to be detected), as well as "excluded" windows (areas within an "included" window that should be ignored).

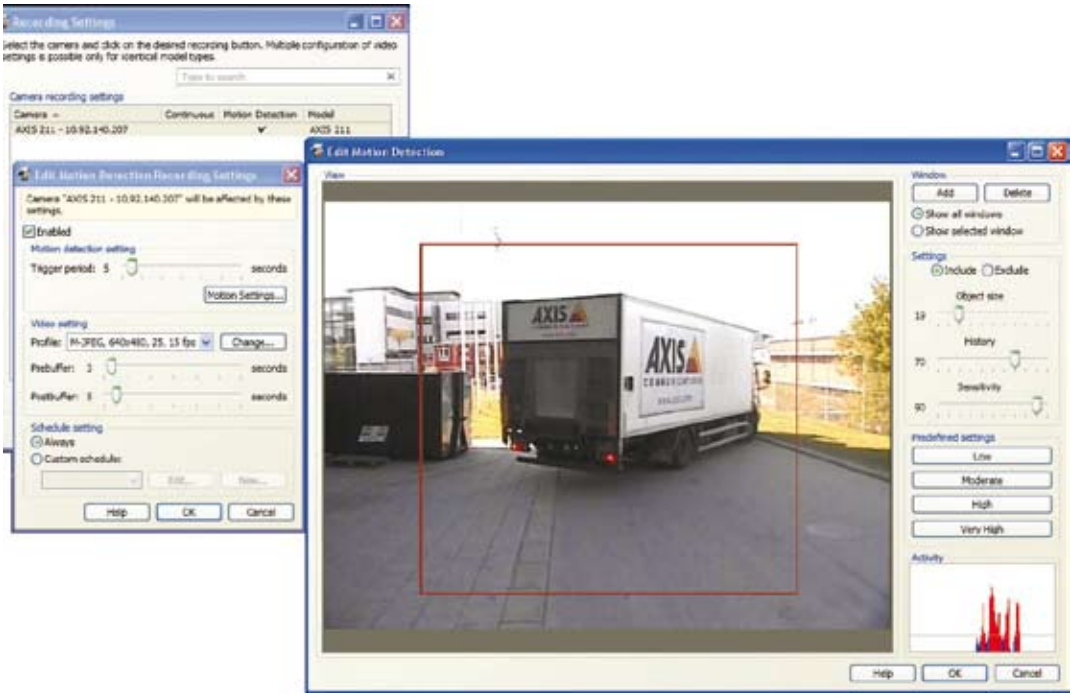


Figure 6a. *Setting recording instructions using the network camera's or video encoder's video motion detection functionality.*

When configuring for video motion detection, you can adjust the size of the window where you want motion to be detected and drag the window to the desired position. You can then adjust sliders for the object size (how large the object should be in order for the trigger to activate), history (how far back in time the reference point for motion detection should be), and sensitivity (how big the pixel changes should be in order to trigger an alarm).

Any detected motion within an active window is then indicated by red peaks in the activity window (the active window has a red frame).

Once the video motion detection is configured, AXIS Camera Station will monitor the function and start recording when the motion flag is raised by the network camera/video encoder. This is a very efficient way of doing video motion detection as all the image processing is done by the network camera/video encoder and not by the AXIS Camera Station server.

7. Daily operation

This chapter describes the functions in the AXIS Camera Station that may be used on a daily basis: events search, live image viewing, log files and configuration check, as well as remote connections.

7.1. Events search

AXIS Camera Station offers easy ways to search for recorded events. The Event Search function pulls up recordings that are triggered by alarms or by manual recordings. The 4-camera Playback function plays simultaneous recordings from up to four cameras, enabling users to obtain a comprehensive picture of events.

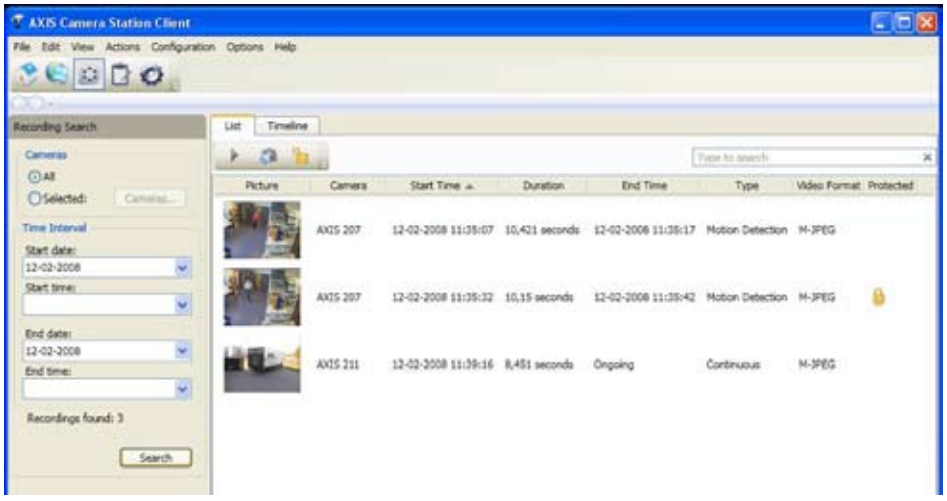


Figure 7.1a. *By selecting the camera and the date, AXIS Camera Station will search for and display the recordings.*

To search, simply select a camera and the date and time, and you will get sample images of all events found. Double-clicking on the image plays the recorded sequence. Another option is to view the recorded events on a timeline. This will show when recordings are present during a selected period of time, as well as the type of recording (manual, continuous or triggered).

Each recorded event can be locked from the log search window. This means that the event recording will not be deleted even if the AXIS Camera Station engine detects that the event is older than the configured days to keep recordings. The event recording will remain on the hard drive until it is unlocked.

During playback, you can zoom into the video and continue to playback the stream in zoomed-in mode.

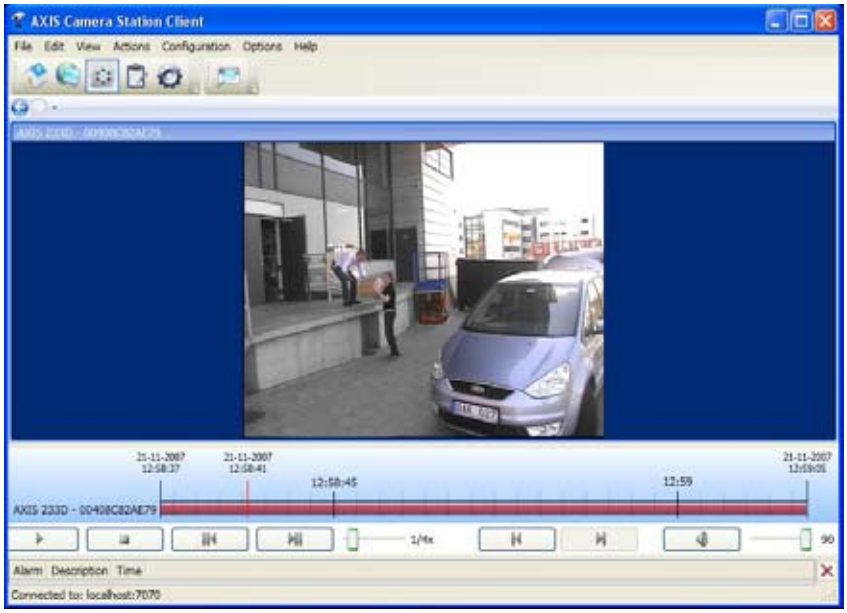


Figure 7.1.b. *Recording playback with timeline*

Single or multiple event recordings can be exported to ASF files from the event list. The ASF files include the selected streaming format's decoder and are playable from Windows Media Player, so any Windows client with Media Player installed should be able to view the recording.

7.2. Live images, PTZ and audio controls

The AXIS Camera Station provides four different ways to view live images:

1) Split view

2) Single camera view

3) Monitor mode (full screen)

4) Sequence/salvos (A camera sequence is a pre-defined "tour" that automatically switches to all of the cameras included in the tour.)

AXIS Camera Station also enables pan/tilt/zoom (PTZ) control when working with a PTZ or dome network camera. The software allows you to control the PTZ function of the camera by 1) clicking on a display keypad, 2) using a mouse (you can click in the image to move the camera or zoom in using the mouse scroll wheel), or 3) using the AXIS 295 Video Surveillance Joystick.

In live view, you can also do digital pan/tilt/zoom. This means that when you are using a fixed camera, you can zoom and steer within the camera's view.

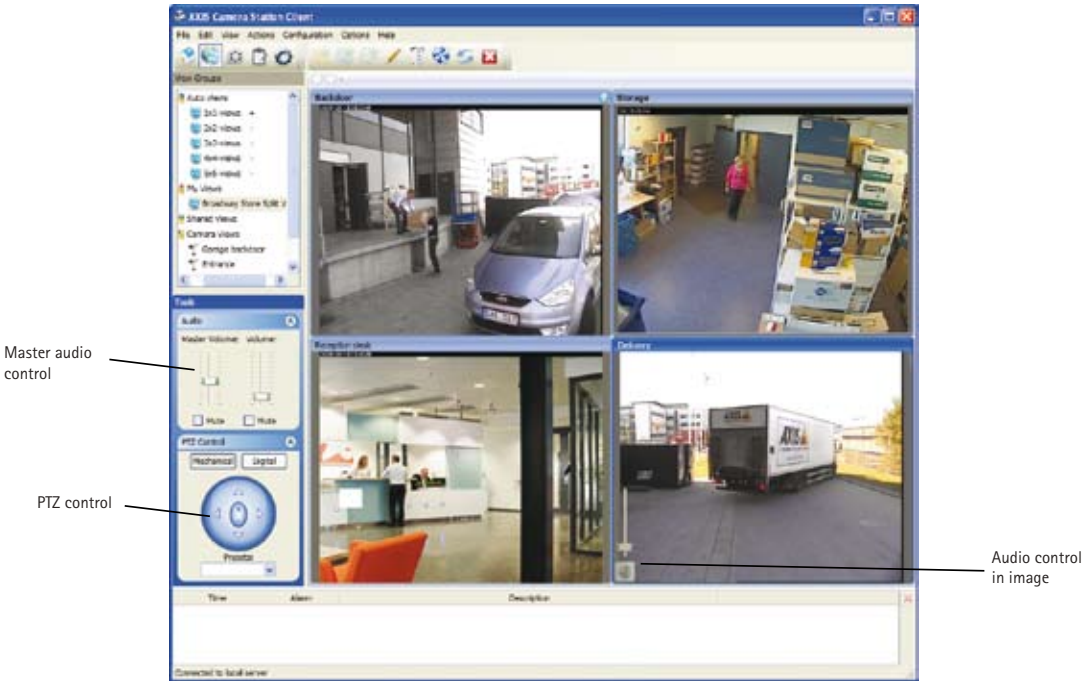


Figure 7.2.a. *Screenshot of live view with PTZ and audio controls.*

If the camera is equipped with audio capability, the audio controls will be automatically shown in the AXIS Camera Station program.

7.3. Log files

The AXIS Camera Station provides three types of log files: alarm, event and audit. The alarm log shows customer-configured alarms as defined in the event configuration, as well as some system-related messages. The event log provides a list of camera and server events based on date, time, type and source of the events. You can sort or search, for example, for a list of errors or when motion is detected.

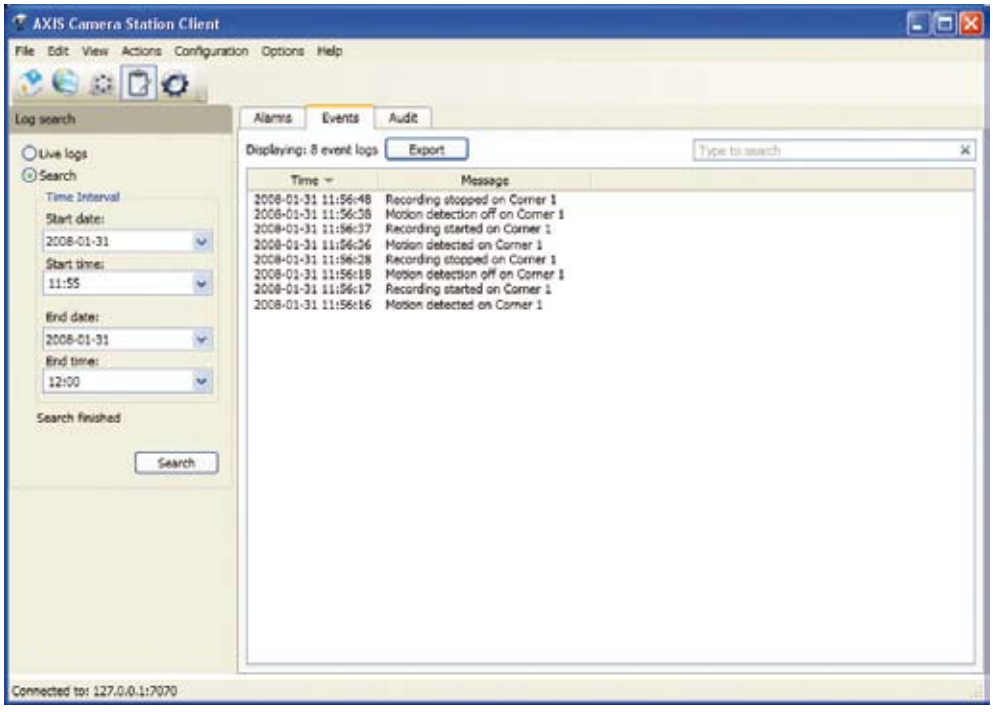


Figure 7.3.a. *The event log provides a list of events such as errors or change in motion detection status.*

The audit log allows you to generate a list of user actions based on the user, time, type of activity and camera. All user activities are logged in AXIS Camera Station. All fields in the generated list can be filtered and sorted.

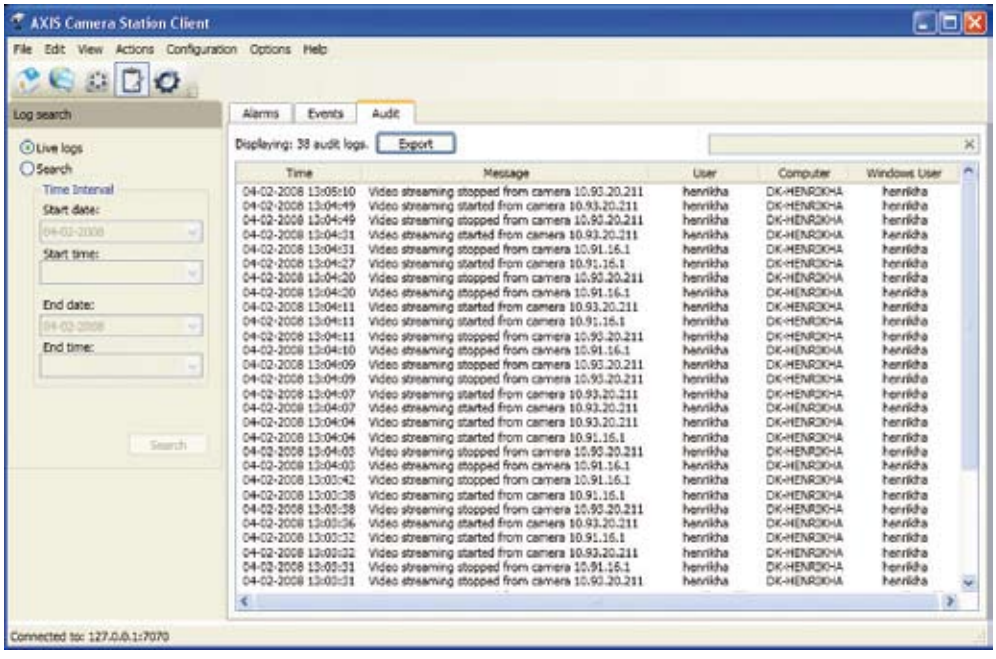


Figure 7.3.b. *The audit log notes all user activities.*

7.4. Configuration overview

For maintenance purposes, the AXIS Camera Station's configuration sheet enables you to obtain, in one place, an overview of all camera and recording configurations. The sheet is accessible from the Help menu.

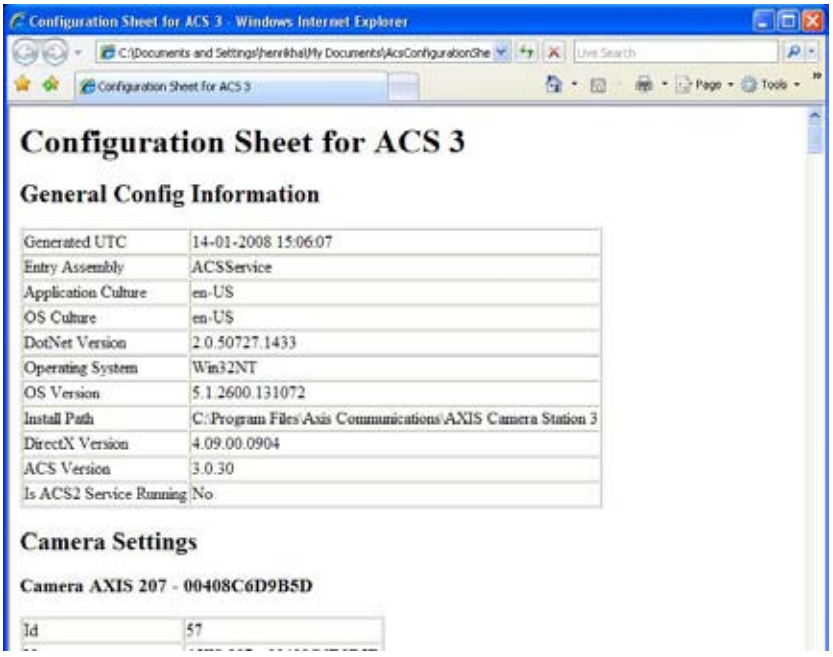


Figure 7.4.a. *AXIS Camera Station's configuration sheet provides an overview of all camera and recording configurations.*

7.5. Remote connections

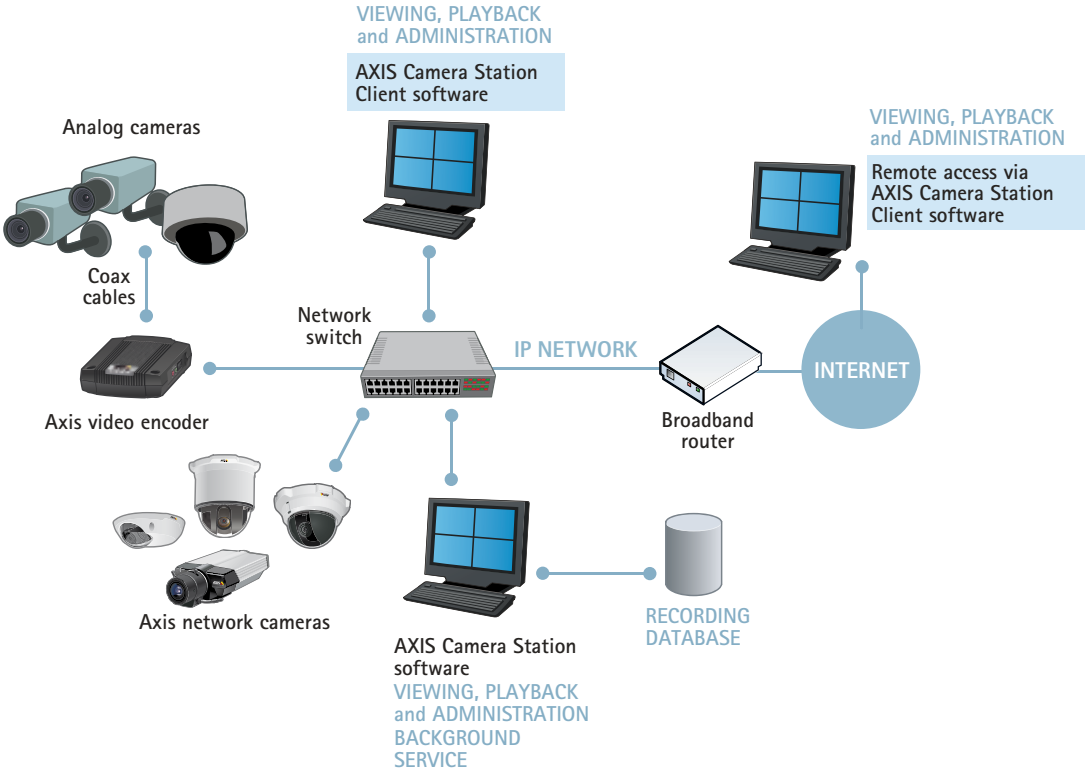


Figure 7.5.a. *Using AXIS Camera Station's Windows client software*

The AXIS Camera Station Client program enables local as well as remote operations on client workstations using the same user interface. The client application lets you work as if you are operating directly on the AXIS Camera Station recording server. Once the Client program is installed, you simply enter the IP address or host name of the server PC where AXIS Camera Station is installed and, if required, enter the user name and password. The Client will download and inherit the camera settings from the AXIS Camera Station server. From the same client, you can also switch between different AXIS Camera Station servers.

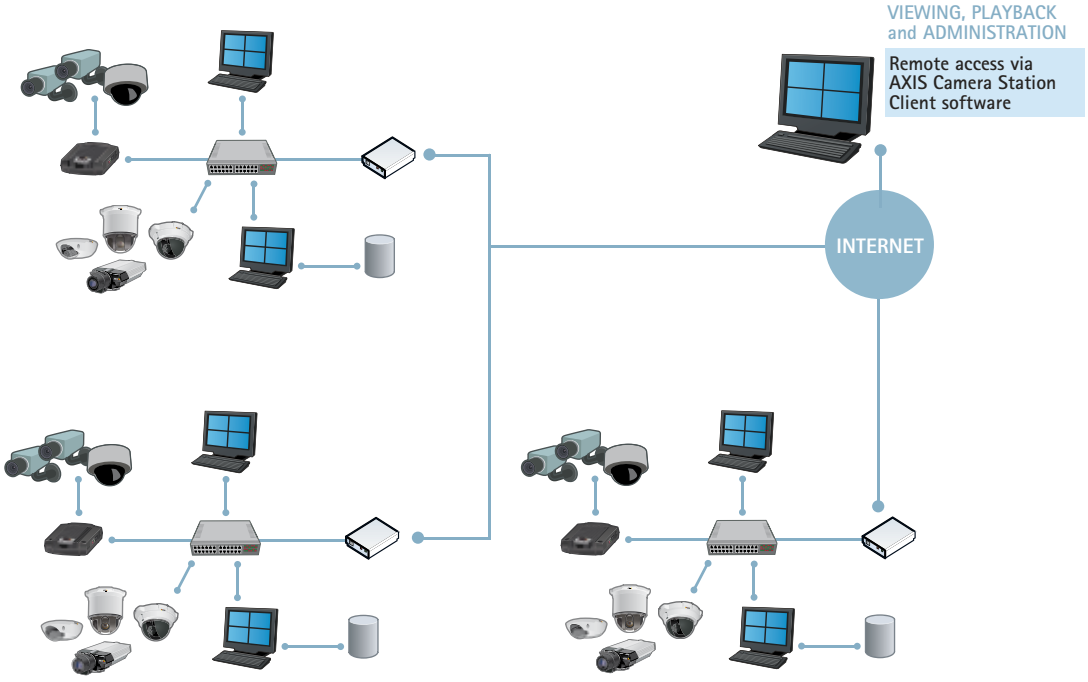


Figure 7.5.b. *You can also switch between different AXIS Camera Station servers using the client software*

8. Scaling up your surveillance system

AXIS Camera Station enables you to easily add more cameras to the system, while the client application allows you to work with multiple AXIS Camera Station servers.

8.1. Adding more cameras

AXIS Camera Station allows you to easily add cameras to the system simply by using the Add function. You can add as many cameras to the system as the purchased license allows. If the number of cameras exceeds the number allowed under license, simply purchase an add-on license.

8.2. Network considerations

When implementing 10 cameras or more, try to estimate the load on the network using a few rules of thumb:

> A camera will use approx. 2 to 3 megabits of bandwidth when configured to deliver high-quality images at high frame rates. The bandwidth usage will be significantly lowered using H.264 or MPEG-4 streaming compared with Motion JPEG.

> In a system with more than 12-15 cameras, consider using a switch with a gigabit backbone. If a gigabit-supporting switch is used, the server that runs the video management software should have a gigabit network adapter installed.

Consider also using Quality of Service (QoS) on your network. Quality of Service enables reservation of network capacity and prioritization of mission-critical surveillance. Some Axis network video products support QoS.

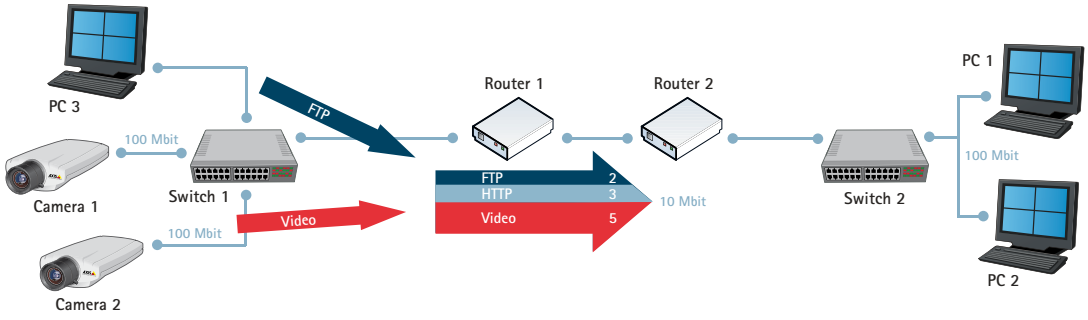


Figure 8.2.a. *The above is an example of a QoS aware network, where Router 1 has been configured to devote a certain amount of maximum bandwidth usage to streaming video, FTP traffic, and HTTP and all other traffic. The maximum usage applies only when there is congestion on the network. If there is unused bandwidth available, any type of traffic can take advantage of it. (In an ordinary or non-QoS network, there is no reserved bandwidth usage for different types of traffic, so when there is network congestion, there is no guarantee that video streams will be able to maintain the desired frame rate.)*

8.3. Server considerations

If you are adding more cameras, you should monitor the server's CPU usage so that it does not exceed its limitations. One hard disk is suitable for storing recordings from six to eight cameras. With more than 12-15 cameras, at least two hard disks should be used to split the load. For 50 or more cameras, the use of a second server is recommended. The AXIS Camera Station Client will be able to switch between different AXIS Camera Station servers.

Number of cameras	Considerations
1 to 15	1 disk
15 to 30	2 disks
30 to 40	3 disks
40 to 50	4 disks
50+	2 servers

For more information, please refer to the hardware recommendation sheet on page 31.

8.4. Storage considerations

When the amount of stored data and management requirements exceed the limitations of a direct attached storage, a network-attached storage (NAS) or storage area network (SAN) allows for increased storage space, flexibility and recoverability.

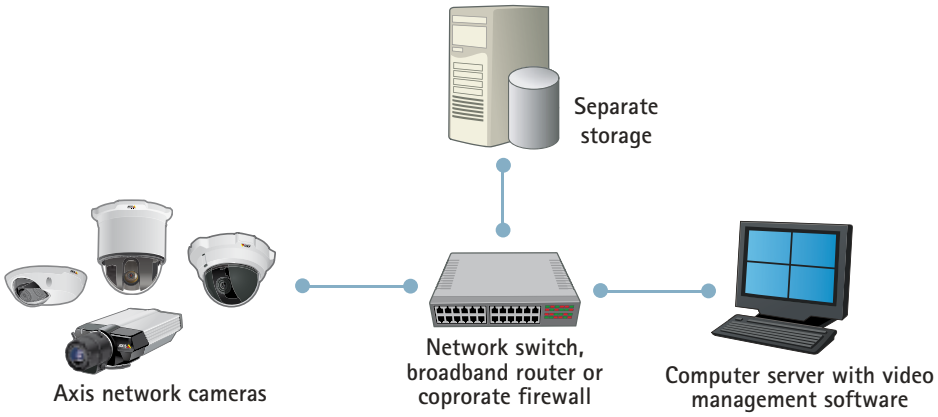


Figure 8.4.a. *Network-attached storage*

NAS provides a single storage device that is directly attached to a 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 can become problematic in high-performance systems.

SANs are high-speed, special-purpose networks for storage, typically connected to one or more servers via fiber. 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. Technologies such as Fiber Channel are commonly used, providing data transfers at four gigabits per second. This type of hard disk configuration allows for very large and scalable solutions where large amounts of data can be stored with a high level of redundancy.

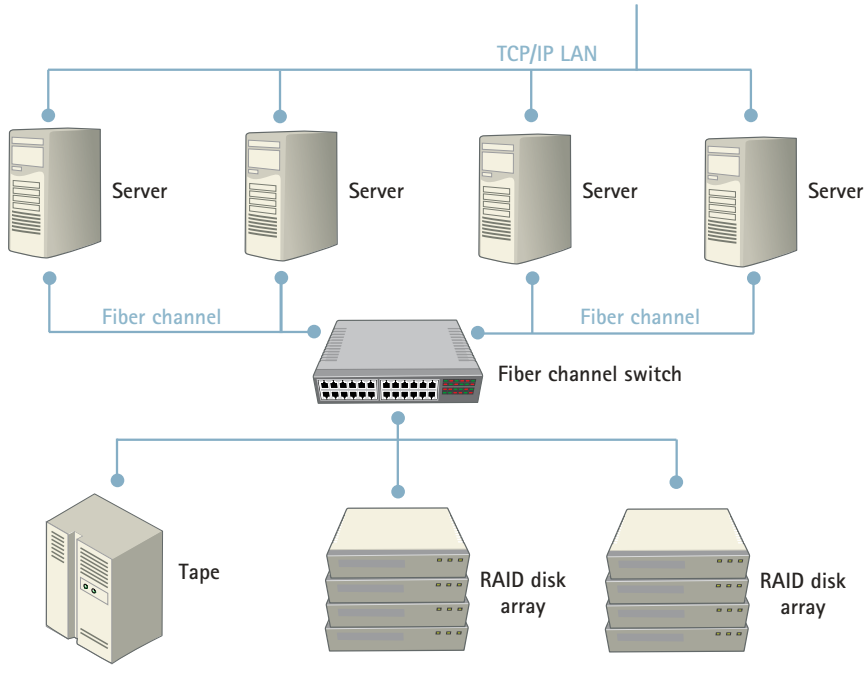
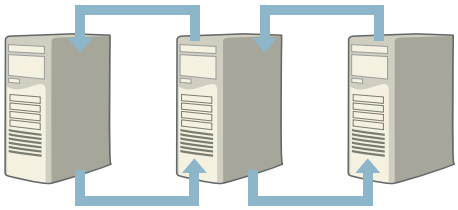


Figure 8.4.b. *A typical SAN architecture where a fiber channel network ties all storage devices together and lets the servers share the storage capacity.*

Redundant Storage
SAN systems build redundancy into the storage device. Redundancy in a storage system allows 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, 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 so 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 loss of data in the event of a hard disk failure.

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



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, such as in mass-transit installations or industrial facilities.

The variety of storage options available for IP-Surveillance systems makes it crucial to consider the different ways the information will be used and stored for the long term. As hard drive technology continues to advance, it is important to utilize open standards to ensure that storage is scalable and future proof. In addition, advances in IP-Surveillance, such as intelligent video algorithm, will make it even more critical to select open storage devices that can handle combinations of data from different sources. Storage systems should be able to accommodate new and upcoming applications so that equipment investments are not lost as technology advances.

9. Conclusion

We hope this document has been helpful in providing guidelines for implementing an IP-Surveillance system. While there are many considerations to take into account, it is relatively easy to set up and operate an Axis IP-Surveillance system once you have defined your application requirements and determined the components you require.

Setting up an Axis IP-Surveillance system – Quick checklist:

> Define your surveillance needs
  - Draw a plan of your installation
  - Select points of interest to view (area of coverage)
  - Position each camera: define what you want to be able to capture with each camera
  - Consider environment: light conditions
  - Consider cabling to cameras
  - Position the recording server

> Network camera and/or video encoder selection
  - Image quality requirements: resolution, compression and frame rate
  - Light sensitivity and lens selection (re: camera)
  - Outdoor/indoor, fixed/fixed dome/PTZ/PTZ dome network camera
  - Consider needs such as Power over Ethernet (PoE), video motion detection, audio...
  - Housing, mounting and other accessories
  - Buy and try: Buy one camera to test its quality

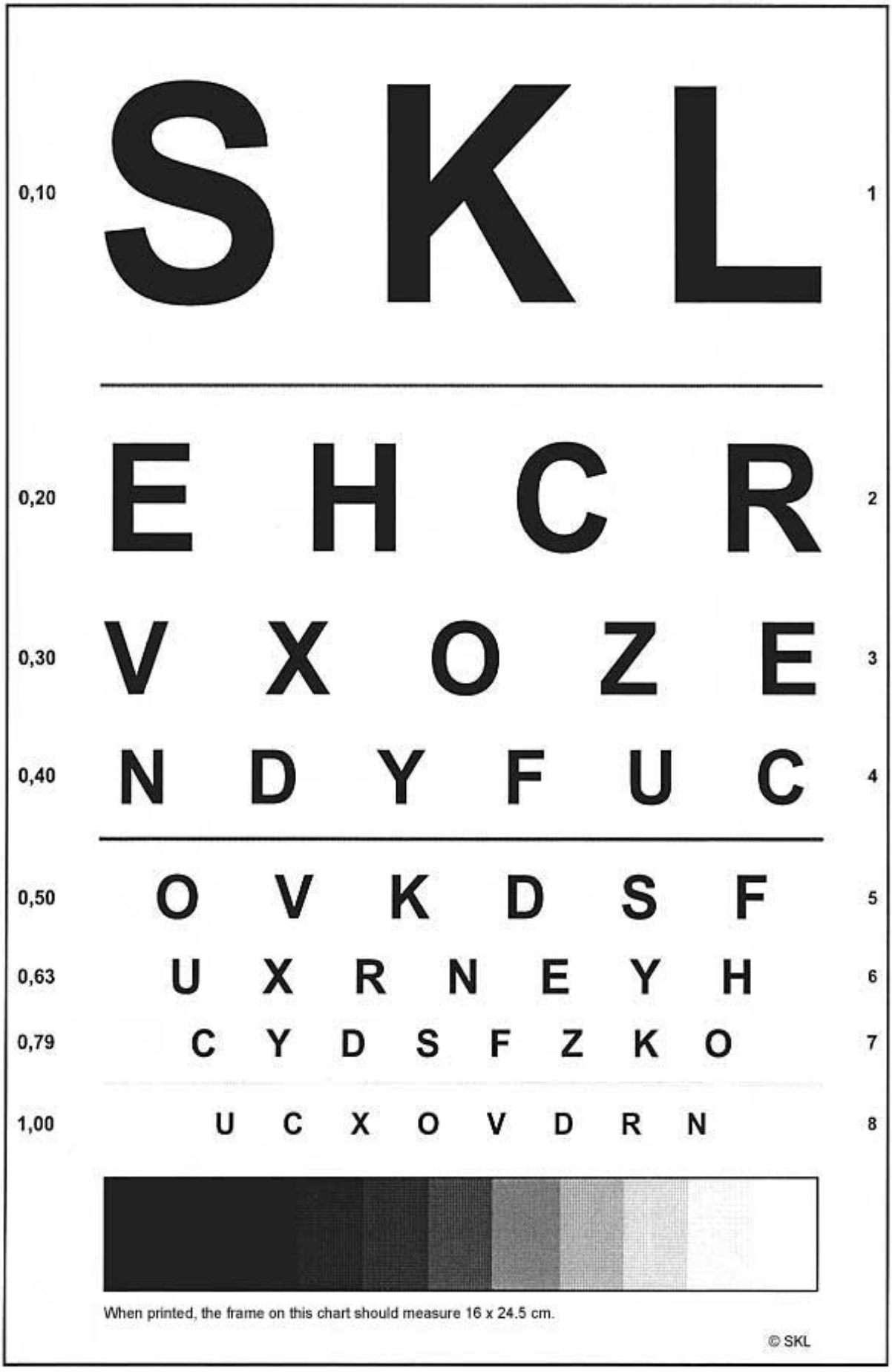
> Hardware components
  - Additional switches (PoE, wireless options)
  - Additional light sources
  - Power supplies and eventually UPS
  - Server for video management software
  - Hard drives (local disks, SAN, RAID, etc.)

> Software
  - Select a software package for your required functionality
  - Purchase licenses that fit the number of cameras
  - Specify image quality and frame rate requirements for each camera
  - IP address range for cameras and servers
  - Calculate hard disk usage
  - Configure your cameras and their recording settings
  - Configure video motion detection settings
  - Grant user access and authentications

> Operations and maintenance
  - Check recorded events for all your cameras
  - Check motion detection settings again
  - Check hard disk free space and eventually adjust recording options

10. Appendix

Letter chart on page 49. (Place the letter chart at the distance where you want an image to be captured. Rows 5 and 6 should be clear for recognition purposes; rows 7 and 8 and most gray shades should be clear for identification purposes.) *Printed with permission from SKL – Statens kriminaltekniska laboratorium*


0,10
S K L
1
0,20
E H C R
2
0,30
V X O Z E
3
0,40
N D Y F U C
4
0,50
O V K D S F
5
0,63
U X R N E Y H
6
0,79
C Y D S F Z K O
7
1,00
U C X O V D R N
8
When printed, the frame on this chart should measure 16 x 24.5 cm.
© SKL

www.axis.com

32568/EN/R3/0807

About Axis Communications

Axis is an IT company offering network video solutions for professional installations. The company is the global market leader in network video, driving the ongoing shift from analog to digital video surveillance. Axis products and solutions focus on security surveillance and remote monitoring, and are based on innovative, open technology platforms.

Axis is a Swedish-based company, operating worldwide with offices in more than 20 countries and cooperating with partners in more than 70 countries. Founded in 1984, Axis is listed on the OMX Nordic Exchange under the ticker AXIS. For more information about Axis, please visit our website at www.axis.com.

AXIS® COMMUNICATIONS