Technical guide to network video.

Technologies and factors to consider for the successful deployment of IP-based security surveillance and remote monitoring applications.




AXIS COMMUNICATIONS

Welcome to the Axis technical guide to network video

The move to open video systems—combined with the benefits of networking, digital imaging, and camera intelligence—constitutes a far more effective means of security surveillance and remote monitoring than has ever been reached before. Network video provides everything that analog video offers, plus a wide range of innovative functions and features that are only possible with digital technology.

Before setting up your own system, you need to consider what features are required. It is equally important to consider factors such as performance, interoperability, scalability, flexibility and future-proof functionality. This guide will walk you through these factors, helping you to achieve a solution that fully takes advantage of the potential of network video technology.

The best in network video

Axis is the global market leader in network video. We were first to bring the benefits of network video technology to professional video surveillance and remote monitoring applications, introducing the world's first network camera in 1996. With more than two decades of experience in networking technologies, the largest installed base of network video products, as well as strong partnerships with leading players across all continents, Axis is the partner of choice in network video.

Flexible, scalable solutions

Using open technology standards that enable easy integration and scalability, Axis offers a full range of network video solutions for surveillance and remote monitoring applications in a broad spectrum of industry segments. Our cutting-edge portfolio comprises network cameras that redefine the categories they represent, as well as video encoders that enable cost-effective migration to the best in network video technology. Our offering also includes comprehensive video management software solutions and a full range of accessories.

Table of contents

Network video: overview, benefits and applications 7

1.1 Overview of a network video system 7
1.2 Benefits 8
1.3 Applications 12
1.3.1 Retail 12
1.3.2 Transportation 12
1.3.3 Education 12
1.3.4 Industrial 13
1.3.5 City surveillance 13
1.3.6 Government 13
1.3.7 Healthcare 13
1.3.8 Banking and finance 14

Network cameras 15

2.1 What is a network camera? 15
2.2 Types of network cameras 16
2.2.1 Fixed network cameras 17
2.2.2 Fixed dome network cameras 17
2.2.3 PTZ cameras and PTZ dome cameras 18
2.3 Day and night network cameras 21
2.4 Megapixel network cameras 23
2.5 Guidelines for selecting a network camera 24

Camera elements 27

3.1 Light sensitivity 27
3.2 Lens elements 28
3.2.1 Field of view 28
3.2.2 Matching lens and sensor 30
3.2.3 Lens mount standards 31
3.2.4 F-number and exposure 31
3.2.5 Manual or automatic iris 32
3.2.6 Depth of field 33
3.3 Image sensors 34
3.3.1 CCD technology 34
3.3.2 CMOS technology 34
3.3.3 Megapixel sensors 35
3.4 Image scanning techniques 35
3.4.1 Interlaced scanning 35
3.4.2 Progressive scanning 36
3.5 Image processing 37
3.5.1 Backlight compensation 37
3.5.2 Exposure zones 37
3.5.3 Wide dynamic range 37
3.6 Installing a network camera 38

Camera protection and housings 39
4.1 Camera enclosures in general 39
4.2 Transparent covering 40
4.3 Positioning a fixed camera in a housing 40
4.4 Environmental protection 41
4.5 Vandal and tampering protection 41
4.5.1 Camera/housing design 41
4.5.2 Mounting 42
4.5.3 Camera placement 43
4.5.4 Intelligent video 43
4.6 Types of mounting 43
4.6.1 Ceiling mounts 43
4.6.2 Wall mounts 44
4.6.3 Pole mounts 44
4.6.4 Parapet mounts 44

Video encoders 45
5.1 What is a video encoder? 45
5.1.1 Video encoder components and considerations 46
5.1.2 Event management and intelligent video 47
5.2 Standalone video encoders 47
5.3 Rack-mounted video encoders 48
5.4 Video encoders with PTZ cameras and PTZ domes 48
5.5 Deinterlacing techniques 49
5.6 Video decoder 50

Resolutions 51
6.1 NTSC and PAL resolutions 51
6.2 VGA resolutions 52
6.3 Megapixel resolutions 53
6.4 High-definition television (HDTV) resolutions 54

Video compression 55
7.1 Compression basics 55
7.1.1 Video codec 55
7.1.2 Image compression vs. video compression 56
7.2 Compression formats 59
7.2.1 Motion JPEG 59
7.2.2 MPEG-4 60
7.2.3 H.264 or MPEG-4 Part 10/AVC 60
7.3 Variable and constant bit rates 61
7.4 Comparing standards 61

Audio 63
8.1 Audio applications 63
8.2 Audio support and equipment 64
8.3 Audio modes 65
8.3.1 Simplex 65
8.3.2 Half duplex 66
8.3.3 Full duplex 66

8.4 Audio detection alarm 66
8.5 Audio compression 66
8.5.1 Sampling frequency 67
8.5.2 Bit rate 67
8.5.3 Audio codecs 67
8.6 Audio and video synchronization 67

Network technologies 69
9.1 Local area network and Ethernet 69
9.1.1 Types of Ethernet networks 70
9.1.2. Switch 71
9.1.3 Power over Ethernet 73
9.2 The Internet 75
9.2.1 IP addressing 76
9.2.2 Data transport protocols for network video 80
9.3 VLANs 82
9.4 Quality of Service 82
9.5 Network Security 84
9.5.1 Username and password authentication 84
9.5.2 IP address filtering 84
9.5.3 IEEE 802.1X 84
9.5.4 HTTPS or SSL/TLS 85
9.5.5 VPN (Virtual Private Network) 85

Wireless technologies 87
10.1 802.11 WLAN standards 88
10.2 WLAN security 88
10.2.1 WEP (Wired Equivalent Privacy) 89
10.2.2 WPA/WPA2 (WiFi Protected Access) 89
10.2.3 Recommendations 89
10.3 Wireless bridges 89

Video management systems 91
11.1 Hardware platforms 91
11.1.1 PC server platform 91
11.1.2 NVR platform 92
11.2 Software platforms 93
11.2.1 Built-in functionality 93
11.2.2 Windows client-based software 93
11.2.3 Web-based software 94
11.2.4 Scalability of video management software 94
11.2.5 Open vs. vendor-specific software 94
11.3 System features 94
11.3.1 Viewing 95
11.3.2 Multi-streaming 95
11.3.3 Video recording 96
11.3.4 Recording and storage 97
11.3.5 Event management and intelligent video 97
11.3.6 Administration and management features 102
11.3.7 Security 103

11.4 Integrated systems 104
11.4.1 Application programming interface 104
11.4.2 Point of Sale 104
11.4.3 Access control 105
11.4.4 Building management 105
11.4.5 Industrial control systems 106
11.4.6 RFID 106

Bandwidth and storage considerations 107
12.1 Bandwidth and storage calculations 107
12.1.1 Bandwidth needs 107
12.1.2 Calculating storage needs 108
12.2 Server-based storage 110
12.3 NAS and SAN 110
12.4 Redundant storage 112
12.5 System configurations 113

Tools and resources 115

Axis Communications' Academy 117

Contact information 118

Network video: overview, benefits and applications

Network video, like many other kinds of communications such as e-mail, web services and computer telephony, is conducted over wired or wireless IP (Internet Protocol) networks. Digital video and audio streams, as well as other data, are communicated over the same network infrastructure. Network video provides users, particularly in the security surveillance industry, with many advantages over traditional analog CCTV (closed-circuit television) systems.

This chapter provides an overview of network video, as well as its benefits and applications in various industry segments. Comparisons with an analog video surveillance system are often made to provide a better understanding of the scope and potential of a digital, network video system.

1.1 Overview of a network video system

Network video, often also called IP-based video surveillance or IP-Surveillance as it is applied in the security industry, uses a wired or wireless IP network as the backbone for transporting digital video, audio and other data. When Power over Ethernet (PoE) technology is applied, the network can also be used to carry power to network video products.

A network video system allows video to be monitored and recorded from anywhere on the network, whether it is, for instance, on a local area network (LAN) or a wide area network (WAN) such as the Internet.

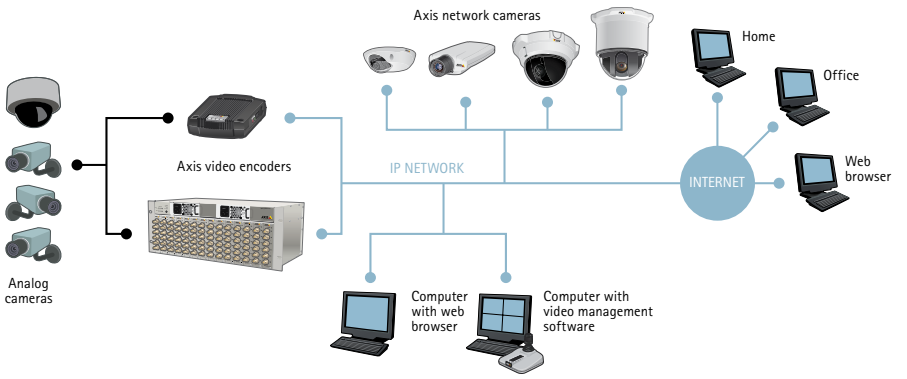


Figure 1.1a *A network video system comprises many different components, such as network cameras, video encoders and video management software. The other components including the network, storage and servers are all standard IT equipment.*

The core components of a network video system consist of the network camera, the video encoder (used to connect to analog cameras), the network, the server and storage, and video management software. As the network camera and the video encoder are computer-based equipment, they have capabilities that cannot be matched by an analog CCTV camera. The network camera, the video encoder and the video management software are considered the cornerstones of an IP-Surveillance solution.

The network, the server and storage components are all standard IT equipment. The ability to use common off-the-shelf equipment is one of the main benefits of network video. Other components of a network video system include accessories, such as camera housings and PoE midspans and active splitters. Each network video component is covered in more detail in other chapters.

1.2 Benefits

The digital, network video surveillance system provides a host of benefits and advanced functionalities that cannot be provided by an analog video surveillance system. The advantages include remote accessibility, high image quality, event management and intelligent video capabilities, easy integration possibilities and better scalability, flexibility and cost-effectiveness.

> **Remote accessibility:** Network cameras and video encoders can be configured and accessed remotely, enabling multiple, authorized users to view live and recorded video at any time and from virtually any networked location in the world. This is advantageous if users would like a third-party company, such as a security firm, to also gain access to the video. In a traditional analog CCTV system, users would need to be at a specific, on-site monitoring

location to view and manage video, and off-site video access would not be possible without such equipment as a video encoder or a network digital video recorder (DVR). A DVR is the digital replacement for the video cassette recorder.

> **High image quality:** In a video surveillance application, high image quality is essential to be able to clearly capture an incident in progress and identify persons or objects involved. With progressive scan and megapixel technologies, a network camera can deliver better image quality and higher resolution than an analog CCTV camera. *For more on progressive scan and megapixel, see chapters 2, 3 and 6.*

Image quality can also be more easily retained in a network video system than in an analog surveillance system. With analog systems today that use a DVR as the recording medium, many analog-to-digital conversions take place: first, analog signals are converted in the camera to digital and then back to analog for transportation; then the analog signals are digitized for recording. Captured images are degraded with every conversion between analog and digital formats and with the cabling distance. The further the analog video signals have to 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 over a network. In addition, digital images can be more easily stored and retrieved than in cases where analog video tapes are used.

> **Event management and intelligent video:** There is often too much video recorded and lack of time to properly analyze them. Advanced network cameras and video encoders with built-in intelligence or analytics take care of this problem by reducing the amount of uninteresting recordings and enabling programmed responses. Such functionalities are not available in an analog system.

Axis network cameras and video encoders have built-in features such as video motion detection, audio detection alarm, active tampering alarm, I/O (input/output) connections, and alarm and event management functionalities. These features enable the network cameras and video encoders to constantly analyze inputs to detect an event and to automatically respond to an event with actions such as video recording and sending alarm notifications.

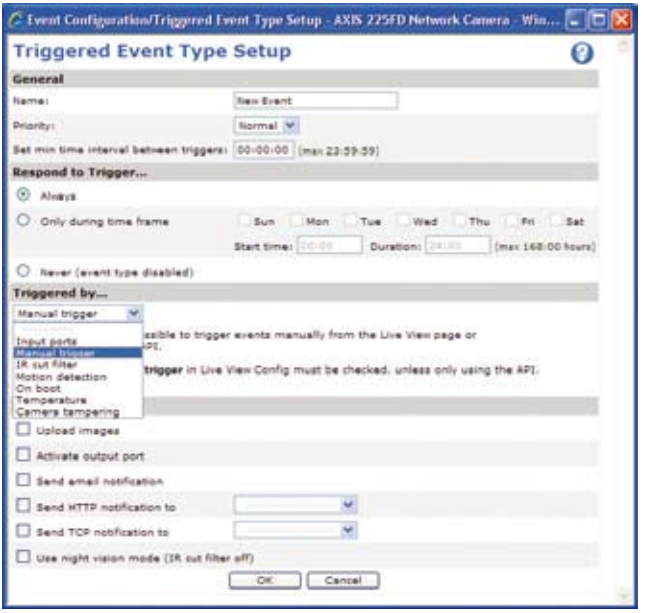


Figure 1.2a *Setting up an event trigger using a network camera's user interface.*

Event management functionalities can be configured using the network video product's user interface or a video management software program. Users can define the alarms or events by setting the type of triggers to be used and when. Responses can also be configured (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 sending notification messages to users). *For more on video management, see Chapter 11.*

> **Easy, future-proof integration:** Network video products based on open standards can be easily integrated with computer and Ethernet-based information systems, audio or security systems and other digital devices, in addition to video management and application software. For instance, video from a network camera can be integrated into a Point of Sales system or a building management system. *For more on integrated systems, see Chapter 11.*

> **Scalability and flexibility:** A network video system can grow with a user's needs. IP-based systems provide a means for many network cameras and video encoders, as well as other types of applications, to share the same wired or wireless network for communicating data; so any number of network video products can be added to the system without significant or costly changes to the network infrastructure. This is not the case with an analog system. In an analog video system, a dedicated coaxial cable must run directly from each camera to a

viewing/recording station. Separate audio cables must also be used if audio is required. Network video products can also be placed and networked from virtually any location, and the system can be as open or as closed as desired.

> **Cost-effectiveness:** An IP-Surveillance system typically has a lower total cost of ownership than a traditional analog CCTV system. An IP network infrastructure is often already in place and used for other applications within an organization, so a network video application can piggyback off the existing infrastructure. IP-based networks and wireless options are also much less expensive alternatives than traditional coaxial and fiber cabling for an analog CCTV system. In addition, digital video streams can be routed around the world using a variety of interoperable infrastructure. Management and equipment costs are also 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.

Furthermore, Power over Ethernet technology, which cannot be applied in an analog video system, can be used in a network video system. PoE enables networked devices to receive power from a PoE-enabled switch or midspan through the same Ethernet cable that transports data (video). PoE provides substantial savings in installation costs and can increase the reliability of the system. *For more on PoE, see Chapter 9.*

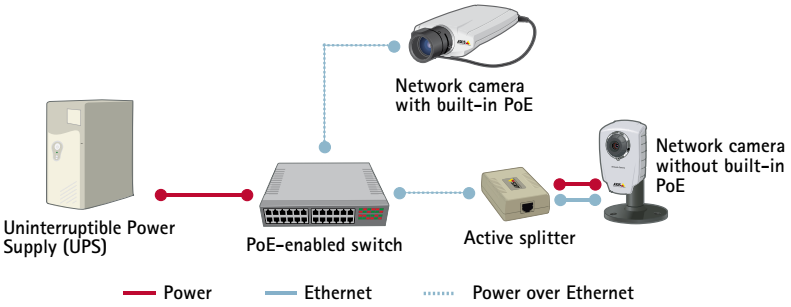


Figure 1.2b *A system that uses Power over Ethernet.*

1.3 Applications

Network video can be used in an almost unlimited number of applications; however, most of its uses fall under security surveillance or remote monitoring of people, places, property and operations. The following are some typical application possibilities in key industry segments.

1.3.1 Retail

Network video systems in retail stores can significantly reduce theft, improve staff security and optimize store management. A major benefit of network video is that it can be integrated with a store's EAS (electronic article surveillance) system or a POS (point of sale) system to provide a picture and a record of shrinkage-related activities. The system can enable rapid detection of potential incidents, as well as any false alarms. Network video offers a high level of interoperability and gives the shortest return on investment.

Network video can also help identify the most popular areas of a store and provide a record of consumer activity and buying behaviors that will help optimize the layout of a store or display. It can also be used to identify when shelves need to be restocked and when more cash registers need to be opened because of long queues.

1.3.2 Transportation

Network video can enhance personal safety and overall security at airports, highways, train stations and other transit systems, as well as in mobile transport such as in buses, trains and cruise ships. Network video can also be used to monitor traffic conditions to reduce congestion and improve efficiency. Many installations in the transportation sector require only the best systems, involving high image quality (which can be provided by progressive scan technology in network cameras), high frame rates and long retention times. In some demanding environments such as on buses and trains, Axis offers network cameras that can withstand varying temperatures, humidity, dust, vibrations and vandalism.

1.3.3 Education

From daycare centers to universities, network video systems have helped deter vandalism and increase the safety of staff and students. In education facilities where an IT infrastructure is already in place, network video presents a more favorable and cost-effective solution than an analog system because new cabling is often not required. In addition, event management features in network video can generate alarms and give security operators accurate, real-time images on

which to base their decisions. Network video can also be used for remote learning; for example, for students who are unable to attend lectures in person.

1.3.4 Industrial

Network video can be used to monitor and increase efficiencies in manufacturing lines, processes and logistic systems, and for securing warehouses and stock control systems. Network video can also be used to set up virtual meetings and get technical support at a distance.

1.3.5 City surveillance

Network video is one of the most useful tools for fighting crime and protecting citizens. It can be used to detect and deter. The use of wireless networks has enabled effective city-wide deployment of network video. The remote surveillance capabilities of network video have enabled police to respond quickly to crimes being committed in live view.

1.3.6 Government

Network video products are used to secure all kinds of public buildings, from museums and offices to libraries and prisons. Cameras placed at building entrances and exits can record who comes in and out, 24 hours a day. They are used to prevent vandalism and increase security of staff. With intelligent video applications such as people counting, network video can provide statistical information, such as the number of visitors to a building.

1.3.7 Healthcare

Network video enables cost-effective, high-quality patient monitoring and video surveillance solutions that increase the safety and security of staff, patients and visitors, as well as property. Authorized hospital staff can, for example, view live video from multiple locations, detect activity and provide remote assistance.

1.3.8 Banking and finance

Network video is used in security applications in bank branches, headquarters and ATM (automated teller machine) locations. Banks have been using surveillance for a long time, and while most installations are still analog, network video is starting to make inroads, especially in banks that value high image quality and want to be able to easily identify people in a surveillance video.

Network video is a proven technology and the shift from analog systems to IP-Surveillance is rapidly taking place in the video surveillance industry. *For case studies, visit www.axis.com/success_stories/*

Network cameras

There is a wide range of network cameras to meet a variety of requirements. This chapter describes what a network camera is and explains the different camera types. Information is also provided about day and night, and megapixel network cameras. A camera selection guide is included at the end of the chapter. *For more on camera elements, see Chapter 3.*

2.1 What is a network camera?

A network camera, often also called an IP camera, can be described as a camera and computer combined in one unit. The main components of a network camera include a lens, an image sensor, one or several processors, and memory. The processors are used for image processing, compression, video analysis and networking functionalities. The memory is used for storing the network camera's firmware (computer program) and for local recording of video sequences.

Like a computer, the network camera has its own IP address, is connected directly to a network and can be placed wherever there is a network connection. This differs from a web camera, which can only operate when it is connected to a personal computer (PC) via the USB or IEEE 1394 port, and to use it, software must be installed on the PC. A network camera provides web server, FTP (File Transfer Protocol), and e-mail functionalities, and includes many other IP network and security protocols.

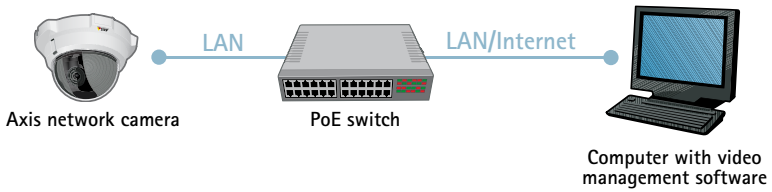


Figure 2.1a *A network camera connects directly to the network.*

A network camera can be configured to send video over an IP network for live viewing and/or recording either continuously, at scheduled times, on an event or on request from authorized users. Captured images can be streamed as Motion JPEG, MPEG-4 or H.264 video using various networking protocols, or uploaded as individual JPEG images using FTP, e-mail or HTTP (Hypertext Transfer Protocol). *For more on video compression formats and networking protocols, see chapters 7 and 9, respectively.*

In addition to capturing video, Axis network cameras provide event management and intelligent video functionalities such as video motion detection, audio detection, active tampering alarm and auto-tracking. Most network cameras also offer input/output (I/O) ports that enable connections to external devices such as sensors and relays. Other features may include audio capabilities and built-in support for Power over Ethernet (PoE). Axis network cameras also support advanced security and network management features.

Figure 2.1b *Front and back of a network camera.*

2.2 Types of network cameras

Network cameras can be classified in terms of whether they are designed for indoor use only or for indoor and outdoor use. Outdoor network cameras often have an auto iris lens to regulate the amount of light the image sensor is exposed to. An outdoor camera will also require an external, protective housing unless the camera design already incorporates 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. In some camera designs, vandal and tamper-proof features are already built-in and no external housing is required. *For more on camera protection and housings, see Chapter 4.*

Network cameras, whether for indoor or outdoor use, can be further categorized into fixed, fixed dome, PTZ, and PTZ dome network cameras.

2.2.1 Fixed network cameras

A fixed network camera, which may come with a fixed or varifocal lens, is a camera that has a fixed field of view (normal/telephoto/wide-angle) once it is mounted. A fixed camera is the traditional camera type where the camera and the direction in which it is pointing are clearly visible. This type of camera represents the best choice in applications where it is advantageous to make the camera very visible. A fixed camera usually enables its lens to be changed. Fixed cameras can be installed in housings designed for indoor or outdoor installation.

Figure 2.2a *Fixed network cameras including wireless and megapixel versions.*

2.2.2 Fixed dome network cameras

A fixed dome network camera, also called a mini dome, essentially involves a fixed camera that is pre-installed in a small dome housing. The camera can be 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.

One of the limitations of a fixed dome camera is that it rarely comes with an exchangeable lens, and even if it is exchangeable, the choice of lenses is limited by the space inside the dome housing. To compensate for this, a varifocal lens is often provided to enable the camera's field of view to be adjusted.

Axis fixed dome cameras are designed with different types of enclosures such as vandal-resistant and/or IP66-rated for outdoor installations. No external housing is required. The mounting of such a camera is usually on a wall or ceiling.

Figure 2.2b *Fixed dome network cameras. From left to right: AXIS 209FD and AXIS 216FD (also available in ruggedized and megapixel versions), AXIS P3301 and AXIS 225FD.*

2.2.3 PTZ cameras and PTZ dome cameras

A PTZ camera or a PTZ dome camera can manually or automatically pan, tilt and zoom in and out of an area or object. All PTZ commands are sent over the same network cable as for video transmission; no RS-485 wires need to be installed as is the case with an analog PTZ camera.

Some of the features that can be incorporated in a PTZ camera or a PTZ dome camera include:

> **Electronic image stabilization (EIS).** In outdoor installations, PTZ dome cameras with zoom factors above 20x are sensitive to vibrations and motion caused by traffic or wind. EIS helps reduce the affects of vibration in a video. In addition to getting more useful video, EIS will reduce the file size of the compressed image, thereby saving valuable storage space.

> **Privacy masking.** Privacy masking, which allows certain areas of a scene to be blocked or masked from viewing and recording, can be made available in various network video products. In a PTZ camera or PTZ dome camera, the functionality has the ability to maintain the privacy masking even as the camera's field of view changes since the masking moves with the coordinate system.

Figure 2.2c *With built-in privacy masking (gray rectangle in image), the camera can guarantee privacy for areas that should not be covered by a surveillance application.*

> **Preset positions.** Many PTZ cameras and PTZ dome cameras enable a number of preset positions, normally between 20 and 100, to be programmed. Once the preset positions have been set in the camera, it is very quick for the operator to go from one position to the next.

> **E-flip.** When a PTZ dome camera is mounted on a ceiling and is used to follow a person in, for example, a retail store, there will be situations when a person will pass just under the camera. When following through on the person, images would be seen upside down without the E-flip functionality. E-flip electronically rotates images 180 degrees in such cases. It is performed automatically and will not be noticed by an operator.

> **Auto-flip.** PTZ cameras, unlike PTZ dome cameras, do not normally have a full 360-degree continuous pan due to a mechanical stop that prevents the cameras from making a continuous circular movement. However, with the Auto-flip functionality, a PTZ network camera 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 in any direction.

> **Auto-tracking.** Auto-tracking is an intelligent video functionality that will automatically detect a moving person or vehicle and follow it within the camera's area of coverage. Auto-tracking is particularly beneficial in unmanned video surveillance situations where the occasional presence of people or vehicles requires special attention. The functionality cuts down substantially the cost of a surveillance system since fewer cameras are needed to cover a scene. It also increases the effectiveness of the solution since it allows a PTZ camera or PTZ dome camera to record areas of a scene with activity.

Although PTZ cameras and PTZ dome cameras may share similar functionalities, there are differences between them:

> PTZ network cameras do not have a full 360-degree continuous pan due to a mechanical stop. It means that the camera cannot follow a person walking continuously in a full circle around the camera. Exceptions are PTZ cameras that have the Auto-flip functionality; for example, AXIS 215 PTZ Network Camera.

> PTZ network cameras are not made for continuous automatic operation or so-called guard tours where the camera automatically moves from one preset position to the next.

More on PTZ network cameras, which are available in mechanical or non-mechanical versions, and PTZ dome network cameras is provided in the next sections.

Mechanical PTZ network cameras

Mechanical PTZ cameras are mainly used indoors and in applications where an operator is employed. The optical zoom on PTZ cameras typically ranges from 10x to 26x. A PTZ camera can be mounted on a ceiling or wall.

Figure 2.2d *PTZ network cameras. From left to right: AXIS 212 PTZ-V (non-mechanical), AXIS 213 PTZ, AXIS 214 PTZ and AXIS 215 PTZ.*

Non-mechanical PTZ network cameras

A non-mechanical PTZ network camera, such as the AXIS 212 PTZ and its vandal-resistant version (seen above), offers instant pan, tilt, zoom capabilities with no moving parts, so there is no wear and tear. Using a wide-angle lens, it offers a wider field of view than a mechanical PTZ network camera.

Figure 2.2e *Images from a non-mechanical PTZ network camera. At left, a 140-degree overview image in VGA resolution; at right, image when making a 3x zoom.*

A non-mechanical PTZ camera uses a megapixel image sensor and allows an operator to instantly zoom in on any part of a scene without any loss in image resolution. This is achieved by presenting an overview image in VGA resolution (640x480 pixels) even though the camera captures a much higher resolution image. When the camera is instructed to zoom in on any part of the overview image, the camera uses the original megapixel resolution to provide a full 1:1 ratio in VGA resolution. The resulting close-up image offers good details with maintained sharpness. With a normal

digital zoom, the zoomed-in image often loses detail and sharpness. A non-mechanical PTZ camera is ideal for discreet, wall-mounted installations.

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), 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 automatically moves from one preset position to the next in a pre-determined order or at random. Normally up to 20 guard tours can be set up and activated during different times of the day. In guard tour mode, one PTZ dome network camera can cover an area where 10 fixed network 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 of a PTZ dome typically ranges between 10x and 35x. A PTZ dome 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 wall of a building in outdoor installations.

Figure 2.2f *PTZ dome network cameras. From left to right: AXIS 231D+, AXIS 232D+, AXIS 233D.*

2.3 Day and night network cameras

All types of network cameras—fixed, fixed dome, PTZ, and PTZ dome—can offer day and night functionality. A day and night camera is designed to be used in outdoor installations or in indoor environments with poor lighting.

A day and night, color network camera delivers color images during the day. As light diminishes below a certain level, the camera can automatically switch to night mode to make use of near-infrared (IR) light to deliver high-quality, black and white images.

Near-infrared light, which spans from 700 nanometers (nm) up to about 1000 nm, is beyond what the human eye can see, but most camera sensors can detect it and make use of it. During the day, a day and night camera uses an IR-cut filter. IR light is filtered out so that it does not distort the colors of images as the human eye sees them. When the camera is in night (black and white) mode, the IR-cut filter is removed, allowing the camera's light sensitivity to reach down to 0.001 lux or lower.

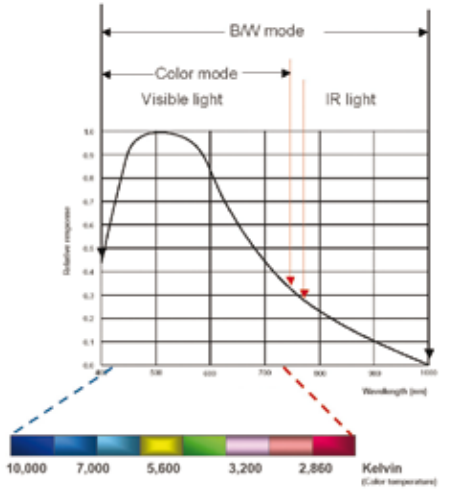


Figure 2.3a *The graph shows how an image sensor responds to visible and near-IR light. Near-IR light spans the 700 nm to 1000 nm range.*

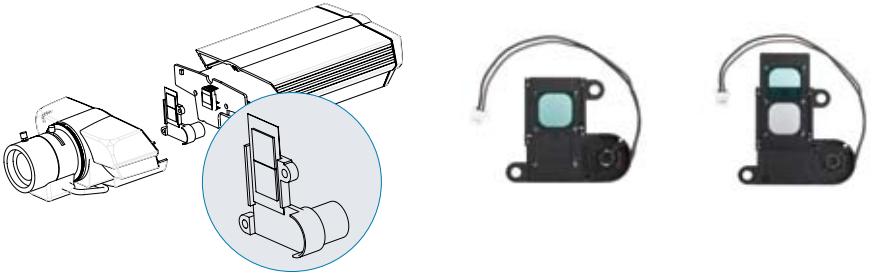


Figure 2.3b *Image at left, IR-cut filter in a day/night network camera; middle, position of IR-cut filter during daytime; at right, position of IR-cut filter during nighttime.*

Day and night cameras are useful in environments that restrict the use of artificial light. They include low-light video surveillance situations, covert surveillance and discreet applications, for example, in a traffic surveillance situation where bright lights would disturb drivers at night.

An IR illuminator that provides near-infrared light can also be used in conjunction with a day and night camera to further enhance the camera's ability to produce high-quality video in low-light or nighttime conditions. *For more information on IR illuminators, visit Axis' website at www.axis.com/products/cam_irillum*

Figure 2.3c *At left, image without an IR illuminator; at right, image with an IR illuminator.*

2.4 Megapixel network cameras

Megapixel network cameras, available in Axis' fixed cameras and fixed dome cameras, incorporate a megapixel image sensor to deliver images with one million or more pixels. This is at least two times better pixel resolution than what can be provided by analog cameras.

A megapixel, fixed network camera can be used in one of two ways: it can enable viewers to see greater details in a higher resolution image, which would be helpful in identifying people and objects, or it can be used to cover a larger part of a scene if the image resolution is kept the same as a non-megapixel camera.

Megapixel cameras today are normally less light sensitive than a non-megapixel network camera. The higher-resolution video streams generated by a megapixel camera also put higher demands on the network bandwidth and storage space for recordings, although this can be mitigated by using the H.264 video compression standard. *For more on H.264 , see Chapter 7.*

2.5 Guidelines for selecting a network camera

With the variety of network cameras available, it is useful to have some guidelines when selecting a network camera.

> **Define the surveillance goal: overview or high detail.** Overview images aim to view a scene in general or view the general movements of people. High detail images are important for identification of persons or objects (e.g., face or license plate recognition, point-of-sales monitoring). The surveillance goal will determine the field of view, the placement of the camera, and the type of camera/lens required. *For more on lenses, see Chapter 3.*

> **Area of coverage.** For a given location, determine the number of interest areas, how much of these areas should be covered and whether the areas are located relatively close to each other or spread far apart. The area will determine the type of camera and number of cameras required.

- *Megapixel or non-megapixel.* For instance, if there are two, relatively small areas of interest that are close to each other, a megapixel camera with a wide-angle lens can be used instead of two non-megapixel cameras.

- *Fixed or PTZ.* (In the following context, fixed cameras refer also to fixed domes and PTZ cameras refer also to PTZ domes.) An area may be covered by several fixed cameras or a few PTZ cameras. Consider that a PTZ camera with high optical zoom capabilities can provide high detail images and survey a large area. However, a PTZ camera may provide a brief view of one part of its area of coverage at a time, while a fixed camera will be able to provide full coverage of its area all the time. To make full use of the capabilities of a PTZ camera, an operator is required or an automatic tour needs to be set up.

> **Indoor or outdoor environment.**

- *Light sensitivity and lighting requirements.* In outdoor environments, consider the use of day and night cameras. Consider the light sensitivity of the camera required and whether additional lighting or specialized light such as IR lamps is needed. Keep in mind that lux measurements on network cameras are not comparable among different network video product vendors as there is no industry standard for measuring light sensitivity.

- *Housing.* If the camera is to be placed outdoors or in environments that require protection from dust, humidity or vandalism, housings are required. *For more on housing, see Chapter 4.*

> **Overt or covert surveillance**. This will help in selecting cameras, in addition to housing and mounts, that offer a non-discreet or discreet installation.

Other important feature considerations that may be required of a camera include:

> **Image quality.** Image quality is one of the most important aspects of any camera, but it is difficult to quantify and measure it. The best way to determine image quality is to install different cameras and look at the video. If capturing moving objects clearly is a priority, it is important that the network camera uses progressive scan technology. *For more on progressive scan, see Chapter 3.*

> **Resolution**. For applications that require detailed images, megapixel cameras may be the best option. *For more on megapixel resolution, see Chapter 6.*

> **Compression.** The three video compression standards offered in Axis network video products are H.264, MPEG-4 and Motion JPEG. H.264 is the latest standard and offers the greatest savings in bandwidth and storage. *For more on compression, see Chapter 7.*

> **Audio.** If audio is required, consider whether one- or two-way audio is needed. Axis network cameras with audio support come with a built-in microphone and/or an input for an external microphone and a speaker or a line out for external speakers. *For more on audio, see Chapter 8.*

> **Event management and intelligent video.** Event management functionalities are often configured using a video management software program and are supported by input/output ports and intelligent video features in a network camera or video encoder. Making recordings based on event triggers from input ports and intelligent video features in a network video product provides savings in bandwidth and storage use, and allows operators to take care of more cameras since not all cameras require live monitoring unless an alarm/event takes place. *For more on event management functions, see Chapter 11.*

> **Networking functionalities.** Considerations include PoE; HTTPS encryption for encrypting video streams before they are sent over the network; IP address filtering, which gives or denies access rights to defined IP addresses; IEEE802.1X to control access to a network; IPv6; and wireless functionality. *For more on networking and security technologies, see Chapter 9.*

> **Open interface and application software.** A network video product with an open interface enables better integration possibilities with other systems. It is also important that the product is supported by a good selection of application software, and management software that enable easy installation and upgrades of network video products. Axis products are supported by both in-house video management software and a wide variety of video management software solutions from more than 550 of its Application Development Partners. *For more on video management systems, see Chapter 11.*

Another important consideration, outside of the network camera itself, is the selection of the network video product vendor. Since needs grow and change, the vendor should be seen as a partner, and a long-term one. This means that it is important to select a vendor that offers a full product line of network video products and accessories that can meet the needs now and well into the future. The vendor should also provide innovation, support, upgrades and product path for the long term.

Once a decision has been made as to the required camera, it is a good idea to purchase one and test its quality before setting out to order quantities of it.

Camera elements

There are a number of camera elements that have an impact on image quality and field of view and are, therefore, important to understand when choosing a network camera. The elements include the light sensitivity of a camera, the type of lens, type of image sensor and scanning technique, as well as image processing functionalities, all of which are discussed in this chapter. Some guidelines on installation considerations are also provided at the end.

3.1 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 specification, the better light sensitivity the camera has. Normally, at least 200 lux is needed to illuminate an object so that a good quality image can be obtained. In general, the more light on the subject, the better the image. With too little light, focusing will be difficult and the image will be noisy and/or dark. To capture good quality images in low light or dark conditions, a day and night camera that takes advantage of near-infrared light is required. *For more on day and night cameras, see Chapter 2.*

Different light conditions offer different illuminance. 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 important, therefore, to keep in mind that one lux reading does not indicate the light condition for a scene as a whole.

Illuminance	Lighting condition
100,000 lux	Strong sunlight
10,000 lux	Full daylight
500 lux	Office light
100 lux	Poorly lit room

Table 3.1a *Examples of different levels of illuminance.*

Many manufacturers specify the minimum level of illumination needed for a network camera to produce an acceptable image. While such specifications are helpful in making light sensitivity comparisons for cameras produced by the same manufacturer, it may not be helpful to use such numbers to compare cameras from different manufacturers. This is because different manufacturers use different methods and have different criteria for what is an acceptable image. To properly compare the low light performance of two different cameras, the cameras should be placed side by side and be viewing a moving object in low light.

3.2 Lens elements

A lens or lens assembly on a network camera performs several functions. They include:

> Defining the field of view; that is, defining how much of a scene and level of detail are to be captured.

> Controlling the amount of light passing through to the image sensor so that an image is correctly exposed.

> Focusing by adjusting either elements within the lens assembly or the distance between the lens assembly and the image sensor.

3.2.1 Field of view

A consideration to take into account when selecting a camera is the field of view required; that is, the area of coverage and the degree of detail to be viewed. The field of view is determined by the focal length of the lens and the size of the image sensor; both are specified in a network camera's datasheet.

A len's focal length is defined as the distance between the entrance lens (or a specific point in a complicated lens assembly) and the point where all the light rays converge to a point (normally the camera's image sensor). The longer the focal length, the narrower the field of view.

The fastest way to find out what focal length lens is required for a desired field of view is to use a rotating lens calculator or an online lens calculator (*www.axis.com/tools*), both of which are available from Axis. The size of a network camera's image sensor, typically 1/4", 1/3", 1/2" and 2/3", must also be used in the calculation. (The drawback of using a lens calculator is that it does not take into account any possible geometrical distortion of a lens.)

The field of view can be classified into three types:

> **Normal view:** offering the same field of view as the human eye.

> **Telephoto:** a narrower field of view, providing, in general, finer details than a human eye can deliver. A telephoto lens is used when the surveillance object is either small or located far away from the camera. A telephoto lens generally has less light gathering capability than a normal lens.

> **Wide angle:** a larger field of view with less detail than in normal view. A wide-angle lens generally provides good depth of field and fair, low-light performance. Wide-angle lenses sometimes produce geometrical distortions such as the "fish-eye" effect.

Figure 3.2a *Different fields of view: wide-angle view (at left); normal view (middle); telephoto (at right).*

Figure 3.2b *Network camera lenses with different focal lengths: wide-angle (at left); normal (middle); telephoto (at right).*

There are three main types of lenses:

> **Fixed lens:** Such a lens offers a focal length that is fixed; that is, only one field of view (either normal, telephoto or wide angle). A common focal length of a fixed network camera lens is 4 mm.

> **Varifocal lens:** This type of lens offers a range of focal lengths, and hence, different fields of view. The field of view can be manually adjusted. Whenever the field of view is changed, the user has to manually refocus the lens. Varifocal lenses for network cameras often provide focal lengths that range from 3 mm to 8 mm.

> **Zoom lens:** Zoom lenses are like varifocal lenses in that they enable the user to select different fields of view. However, with zoom lenses, there is no need to refocus the lens if the field of view is changed. Focus can be maintained within a range of focal lengths, for example, 6 mm to 48 mm. Lens adjustments can be either manual or motorized for remote control. When a lens states, for example, 3x-zoom capability, it is referring to the ratio between the lens' longest and shortest focal length.

3.2.2 Matching lens and sensor

If a network camera offers an exchangeable lens, it is important to select a lens suitable for the camera. A lens made for a 1/2-inch image sensor will work with 1/2-inch, 1/3-inch and 1/4-inch image sensors, but not with a 2/3-inch image sensor.

If a lens is made for a smaller image sensor than the one that is actually fitted inside the camera, the image will have black corners (s*ee left-hand illustration in Figure 3.2c below*). If a lens is made for a larger image sensor than the one that is actually fitted inside the camera, the field of view will be smaller than the lens' capability since part of the information will be "lost" outside the image sensor (*see right-hand illustration in Figure 3.2c*). This situation creates a telephoto effect as it makes everything look zoomed in.

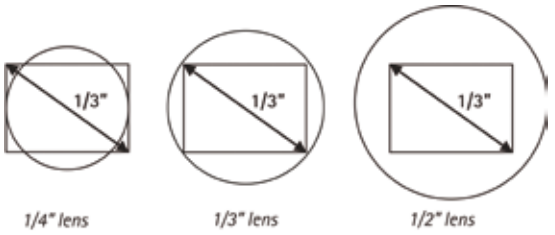


Figure 3.2c *Examples of different lenses mounted onto a 1/3-inch image sensor.*

When replacing a lens on a megapixel camera, a high quality lens is required since megapixel sensors have pixels that are much smaller than those on a VGA sensor (640x480 pixels). It is best to match the lens resolution to the camera resolution in order to fully use the camera's capability.

3.2.3 Lens mount standards

When changing a lens, it is also important to know what type of lens mount the network camera has. There are two main standards used on network cameras: CS-mount and C-mount. They both have a 1-inch thread and they look the same. What differs is the distance from the lenses to the sensor when fitted on the camera:

> **CS-mount.** The distance between the sensor and the lens should be 12.5 mm.
> **C-mount.** The distance between the sensor and the lens should be 17.526 mm.

It is possible to mount a C-mount lens to a CS-mount camera body by using a 5 mm spacer (C/CS adapter ring). If it is impossible to focus a camera, it is likely that the wrong type of lens is used.

3.2.4 F-number and exposure

In low-light situations, particularly in indoor environments, an important factor to look for in a network camera is the lens' light-gathering ability. This can be determined by the lens' f-number, also known as f-stop. An f-number defines how much light can pass through a lens.

An f-number is the ratio of the lens' focal length to the diameter of the aperture or iris diameter; that is, f-number = focal length/aperture.

The smaller the f-number (either short focal length relative to the aperture, or large aperture relative to the focal length), the better the lens' light gathering ability; i.e. more light can pass through the lens to the image sensor. In low-light situations, a smaller f-number generally produces a better image quality. (There may be some sensors, however, that may not be able to take advantage of a lower f-number in low-light situations due to the way they are designed.) A higher f-number, on the other hand, increases the depth of field, which is explained in section 3.2.6. A lens with a lower f-number is normally more expensive than a lens with a higher f-number.

F-numbers are often written as F/x. The slash indicates division. An F/4 means the iris diameter is equal to the focal length divided by 4; so if a camera has an 8 mm lens, light must pass through an iris opening that is 2 mm in diameter.

While lenses with automatically adjustable iris (DC-iris) have a range of f-numbers, often only the maximum light gathering end of the range (smallest f-number) is specified.

A lens' light-gathering ability or f-number, and the exposure time (i.e., the length of time an image sensor is exposed to light) are the two main elements that control how much light an image sensor receives. A third element, the gain, is an amplifier that is used to make the image brighter. However, increasing the gain also increases the level of noise (graininess) in an image, so adjusting the exposure time or iris opening is preferred.

Limits to the exposure time and gain can be set in some Axis cameras. The longer the exposure time, the more light an image sensor receives. Bright environments require shorter exposure time, while low-light conditions require longer exposure time. It is important to be aware that increasing the exposure time also increases motion blur, while increasing the iris opening has the downside of reducing the depth of field, which is explained in section 3.2.6 below.

When deciding upon the exposure, a shorter exposure time is recommended when rapid movement or when a high frame rate is required. A longer exposure time will improve image quality in poor lighting conditions, but it may increase motion blur and lower the total frame rate since a longer time is required to expose each frame. In some 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 artificial light or prioritized frame rate or image quality is important to consider.

Figure 3.2d *A camera user interface with options for setting, among other things, exposure in low-light conditions.*

3.2.5 Manual or automatic iris

In indoor environments where light levels may be constant, a manual iris lens can be used. This type of lens either provides a ring to adjust the iris, or the iris is fixed at a certain f-number. The latter is what Axis uses on its indoor network cameras.

A lens with automatically adjustable iris is recommended for outdoor applications and where the scene illumination is constantly changing. The iris aperture is controlled by the camera and is used to maintain the optimum light level to the image sensor if exposure and gain settings are not available or used in the network camera. The iris can also be used to control the depth of field (explained in the section below) and to obtain sharper images. Most automatic iris lenses are controlled by the camera's processor via a direct current (DC) and are, therefore, called "DC-iris" lenses. All Axis outdoor cameras, whether fixed, fixed dome, PTZ or PTZ dome, use DC-iris or auto-iris lenses.

3.2.6 Depth of field

A criterion that may be important to a video surveillance application is depth of field. Depth of field refers to the distance in front of and beyond the point of focus where objects appear to be sharp simultaneously. Depth of field may be important, for instance, in monitoring a parking lot, where there may be a need to identify license plates of cars at 20, 30 and 50 meters (60, 90 and 150 feet) away.

Depth of field is affected by three factors: focal length, iris diameter and distance of the camera to the subject. A long focal length, a large iris opening or a short distance between the camera and the subject will limit the depth of field.

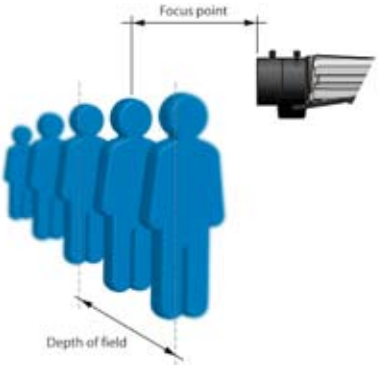


Figure 3.2e *Depth of field: Imagine a line of people standing behind each other. If the focus is in the middle of the line and it is possible to identify the faces of all in front and behind the mid-point more than 15 meters (45 feet) away, the depth of field is good.*

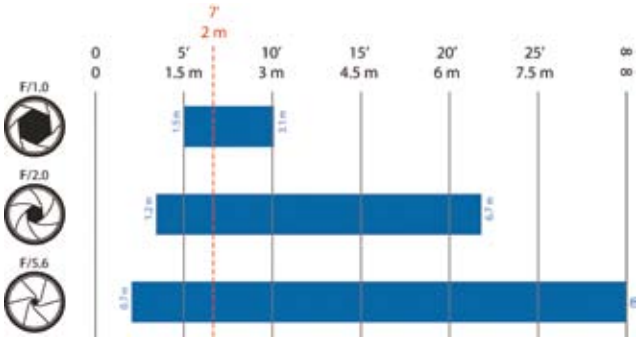


Figure 3.2f *Iris opening and depth of field. The above illustration is an example of the depth of field for different f-numbers with a focal distance of 2 meters (7 feet). A large f-number (smaller iris opening) enables objects to be in focus over a longer range. (Depending on the pixel size, very small iris openings may blur an image due to diffraction.)*

3.3 Image sensors

As light passes through a lens, it is focused on the camera's image sensor. An image sensor is made up of many photosites and each photosite corresponds to a picture element, more commonly known as "pixel", on an image sensor. Each pixel on an image sensor registers the amount of light it is exposed to and converts it into a corresponding number of electrons. The brighter the light, the more electrons are generated.

When building a camera, there are two main technologies that can be used for the camera's image sensor:

> **CCD** (charge-coupled device)
> **CMOS** (complementary metal-oxide semiconductor)

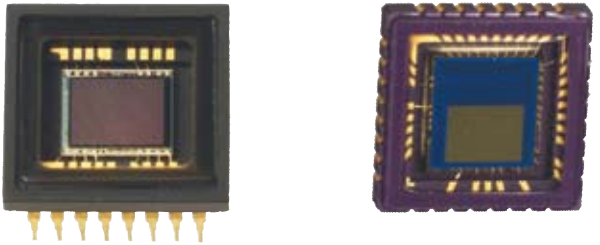


Figure 3.3a *Images sensors: CCD (at left); CMOS (at right).*

While CCD and CMOS sensors are often seen as rivals, each has unique strengths and weaknesses that make it appropriate for different applications. CCD sensors are produced using a technology that has been developed specifically for the camera industry. Early CMOS sensors were based on standard technology already extensively used in memory chips inside PCs, for example. Modern CMOS sensors use a more specialized technology and the quality of the sensors is rapidly increasing.

3.3.1 CCD technology

CCD sensors have been used in cameras for more than 30 years and present many advantageous qualities. Generally, they still offer slightly better light sensitivity and produce somewhat less noise than CMOS sensors. Higher light sensitivity translates into better images in low light conditions. CCD sensors, however, are more expensive and more complex to incorporate into a camera. A CCD can also consume as much as 100 times more power than an equivalent CMOS sensor.

3.3.2 CMOS technology

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. In comparison with CCDs, CMOS sensors enable more integration

possibilities and more functions. CMOS sensors also have a faster readout (which is advantageous when high-resolution images are required), lower power dissipation at the chip level, as well as a smaller system size. Megapixel CMOS sensors are more widely available and are less expensive than megapixel CCD sensors.

3.3.3 Megapixel sensors

For cost reasons, many megapixel sensors (i.e., sensors containing a million or more pixels) in megapixel cameras are the same size as or only slightly larger than VGA sensors that provide a resolution of 640x480 (307,200) pixels. This means that the size of each pixel on a megapixel sensor is smaller than on a VGA sensor. For instance, a megapixel sensor such as a 1/3-inch, 2-megapixel sensor has pixel sizes measuring 3 µm (micrometers/microns) each. By comparison, the pixel size of a 1/3-inch VGA sensor is 7.5 µm. So while the megapixel camera provides higher resolution and greater detail, it is less light sensitive than its VGA counterpart since the pixel size is smaller and light reflected from an object is spread to more pixels.

3.4 Image scanning techniques

Interlaced scanning and progressive scanning are the two techniques available today for reading and displaying information produced by image sensors. Interlaced scanning is used mainly in CCDs. Progressive scanning is used in either CCD or CMOS sensors. Network cameras can make use of either scanning technique. (Analog cameras, however, can only make use of the interlaced scanning technique for transferring images over a coaxial cable and for displaying them on analog monitors.)

3.4.1 Interlaced scanning

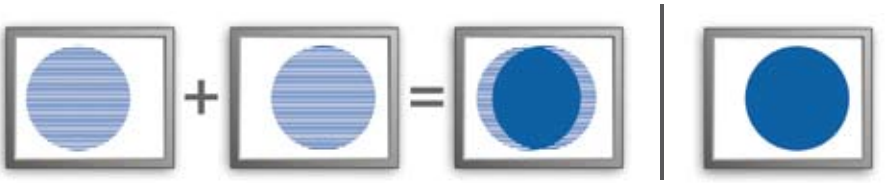
When an interlaced image from a CCD is produced, two fields of lines are generated: a field displaying the odd lines, and a second field displaying the even lines. However, to create the odd field, information from both the odd and even lines on a CCD sensor is combined. The same goes for the even field, where information from both the even and odd lines is combined to form an image on every other line.

When transmitting an interlaced image, only half the number of lines (alternating between odd and even lines) of an image is sent at a time, which reduces the use of bandwidth by half. The monitor, for example, a traditional TV, must also use the interlaced technique. First the odd lines and then the even lines of an image are displayed and then refreshed alternately at 25 (PAL) or 30 (NTSC) frames per second so that the human visual system interprets them as complete images. All analog video formats and some modern HDTV formats are interlaced. Although the interlacing technique creates artifacts or distortions as a result of 'missing' data, they are not very noticeable on an interlaced monitor.

However, when interlaced video is shown on progressive scan monitors such as computer monitors, which scan lines of an image consecutively, the artifacts become noticeable. The artifacts, which can be seen as "tearing", are caused by the slight delay between odd and even line refreshes as only half the lines keep up with a moving image while the other half waits to be refreshed. It is especially noticeable when the video is stopped and a freeze frame of the video is analyzed.

3.4.2 Progressive scanning

With a progressive scan image sensor, values are obtained for each pixel on the sensor and each line of image data is scanned sequentially, producing a full frame image. In other words, captured images are not split into separate fields as with interlaced scanning. With progressive scan, an entire image frame is sent over a network and when displayed on a progressive scan computer monitor, each line of an image is put on the screen one at a time in perfect order. Moving objects are, therefore, better presented on computer screens using the progressive scan technique. In a video surveillance application, it can be critical in viewing details of a moving subject (e.g., a person running away). Most Axis network cameras use the progressive scan technique.



1st field: Odd lines | *2nd field: Even lines [17/20 ms (NTSC/PAL) later]* | *Freeze frame on moving dot using interlaced scan* | *Freeze frame on moving dot using progressive scan*

Figure 3.4a *At left, an interlaced scan image shown on a progressive (computer) monitor. At right, a progressive scan image on a computer monitor.*

Figure 3.4b *At left, a full-sized JPEG image (704x576 pixels) from an analog camera using interlaced scanning. At right, a full-sized JPEG image (640x480 pixels) from an Axis network camera using progressive scan technology. Both cameras used the same type of lens and the speed of the car was the same at 20 km/h (15 mph). The background is clear in both images. However, the driver is clearly visible only in the image using progressive scan technology.*

3.5 Image processing

Three features that may be supported in network cameras to improve image quality are backlight compensation, exposure zones and wide dynamic range.

3.5.1 Backlight compensation

While a camera's automatic exposure tries to get the brightness of an image to appear as the human eye would see a scene, it can be easily fooled. Strong backlight can cause objects in the foreground to be dark. Network cameras with backlight compensation strive to ignore limited areas of high illumination, just as if they were not present. It enables objects in the foreground to be seen, although the bright areas will be overexposed. Such lighting situations can also be handled by increasing the dynamic range of the camera, which is discussed in section 3.5.3 below.

3.5.2 Exposure zones

Besides dealing with limited areas of high illumination, a network camera's automatic exposure must also decide what area of an image should determine the exposure value. For instance, the foreground (usually the bottom section of an image) may hold more important information than the background; for example, the sky (usually the top section of an image). The less important areas of a scene should not determine the overall exposure. In advanced Axis network cameras, the user is able to use exposure zones to select the area of a scene—center, left, right, top or bottom—that should be more correctly exposed.

3.5.3 Wide dynamic range

Some Axis network cameras offer wide dynamic range to handle a wide range of lighting conditions in a scene. In a scene with extremely bright and dark areas or in backlight situations where a person is in front of a bright window, a typical camera will produce an image where objects in the dark areas will hardly be visible. Wide dynamic range solves this by applying techniques, such as using different exposures for different objects in a scene, to enable objects in both bright and dark areas to be visible.

Figure 3.5a *At left, image without wide dynamic range. At right, image with wide dynamic range applied.*

3.6 Installing a network camera

Once a network camera has been purchased, the way it is installed is just as important. Below are some recommendations on how to best achieve high-quality video surveillance based on camera positioning and environmental considerations.

> **Surveillance objective.** If the aim is to get an overview of an area to be able to track the movement of people or objects, make sure a camera that is suitable for the task is placed in a position that achieves the objective. If the intention is to be able to identify a person or object, the camera must be positioned or focused in a way that will capture the level of detail needed for identification purposes. Local police authorities may also be able to provide guidelines on how best to position a camera.

> **Use lots of light or add light if needed.** It is normally easy and cost-effective to add strong lamps in both indoor and outdoor situations to provide the necessary light conditions for capturing good images.

> **Avoid direct sunlight** as it will "blind" the camera and can reduce the performance of the image sensor. If possible, position the camera with the sun shining from behind the camera.

> **Avoid backlight.** This problem typically occurs when attempting to capture an object in front of a window. To avoid this problem, reposition the camera or use curtains and close blinds if possible. If it is not possible to reposition the camera, add frontal lighting. Cameras with support for wide dynamic range are better at handling a backlight scenario.

> **Reduce the dynamic range of the scene.** In outdoor environments, viewing too much sky results in too high a dynamic range. If the camera does not support wide dynamic range, a solution is to mount the camera high above the ground, using a pole if needed.

> **Adjust camera settings.** It may be necessary at times to adjust settings for white balance, brightness and sharpness to obtain an optimal image. In low light situations, users must also prioritize either frame rate or image quality.

> **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 the local region before installing a video surveillance system. It may be necessary, for instance, to register or get a license for video surveillance, particularly in public areas. Signage may be required. Video recordings may require time and date stamping. There may be rules regulating how long video should be retained. Audio recordings may or may not be permitted.

Camera protection and housings

Surveillance cameras are often placed in environments that are very demanding. Cameras may require protection from rain, hot and cold environments, dust, corrosive substances, vibrations and vandalism. Manufacturers of cameras and camera accessories employ various methods to meet such environmental challenges. Solutions include placing cameras in separate, protective housings, designing built-in special-purpose camera enclosures, and/or using intelligent algorithms that can detect and alert users of a change in a camera's operating conditions.

The sections below cover such topics as coverings, positioning of fixed cameras in enclosures, environmental protection, vandal and tampering protection, and types of mounting.

4.1 Camera enclosures in general

When the demands of the environment are beyond a camera's operating conditions, protective housings are required. Camera housings come in different sizes and qualities and with different features. Housings are made of either metal or plastic and can be generally classified into two types: fixed camera housings and dome camera housings. When selecting an enclosure, several things need to be considered, including:

> Side or slide opening (for fixed camera housings)
> Mounting brackets
> Clear or smoked bubble (for dome camera housings)
> Cable management
> Temperature and other ratings (consider the need for heater, sunshield, fan and wipers)
> Power supply (12 V, 24 V, 110 V, etc.)
> Level of vandal resistance

Some housings also have peripherals such as antennas for wireless applications. An external antenna is only required if the housing is made of metal. A wireless camera inside a plastic housing will work without the use of an external antenna.

4.2 Transparent covering

The "window" or transparent covering of an enclosure is usually made of high-quality glass or durable, polycarbonate plastic. As windows act like optical lenses, they should be of high quality to minimize its effect on image quality. When there are built-in imperfections in the clear material, clarity is compromised.

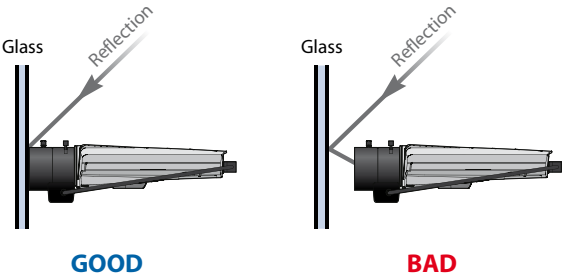
Higher demands are placed on the windows of housings for PTZ cameras and PTZ dome cameras. Not only do the windows have to be specially shaped in the form of a bubble, but they must also have high clarity since imperfections such as dirt particles can be magnified, particularly when cameras with high zoom factors are installed. In addition, if the thickness of the window is uneven, a straight line may appear curved in the resulting image. A high-quality bubble should have very little impact on image quality, irrespective of the camera's zoom level and lens position.

The thickness of a bubble can be increased to withstand heavy blows, but the thicker a covering is, the higher the chances of imperfections. Increased thickness may also create unwanted reflections and refraction of light. Therefore, thicker coverings should meet higher requirements if the effect on image quality is to be minimized.

A variety of dome coverings or bubbles are available, such as clear or smoked versions. While smoked versions enable a more discrete installation, they also act much like sunglasses do in reducing the amount of light available to the camera. It will, therefore, have an affect on the camera's light sensitivity.

4.3 Positioning a fixed camera in a housing

When installing a fixed camera in an enclosure, it is important that the lens of the camera is positioned right up against the window to prevent any glare. 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.



igure 4.3a *When installing a camera behind a glass, correct positioning of the camera becomes important to avoid reflections.*

4.4 Environmental protection

The main environmental threats to a camera—particularly one that is installed outdoors—are cold, heat, water and dust. Housings with built-in heaters and fans (blowers) can be used in environments with low and high temperatures. In hot environments, cameras can be placed in enclosures that have active cooling with a separate heat exchanger.

To withstand water and dust, housings (often with an IP66 rating) are carefully sealed. In situations where cameras may be exposed to acids, such as in the food industry, housings made of stainless steel are required. Some specialized housings can be pressurized, submersible, bullet-proofed or built for installation in potentially explosive locations. Special enclosures may also be required for aesthetic considerations.

Other environmental elements include wind and traffic. To minimize vibrations, particularly on pole-mounted camera installations, the housing should ideally be small and securely mounted.

The terms "indoor housing" and "outdoor housing" often refer to the level of environmental protection. An indoor housing is mostly used to prevent the entry of dust and does not include a heater and/or fan. The terms are misleading since the location, whether indoor or outdoor, does not always correspond to the conditions at an installation site. A camera placed in a freezer room, for example, will need an "outdoor housing" that has a heater.

The level of protection provided by enclosures, whether built-in or separate from a camera, is often indicated by classifications set by such standards as IP, which stands for Ingress Protection (also sometimes known as International Protection) and applicable worldwide; NEMA (National Electrical Manufacturers Association) in the U.S.; and IK ratings for external mechanical impacts, which apply in Europe. When a camera is to be installed in a potentially explosive environment, other standards—such as IECEx, which is a global certification, and ATEX, a European certification—come into play. *More on IP ratings can be found here: www.axis.com/products/cam_housing/ip66.htm*

4.5 Vandal and tampering protection

In some surveillance applications, cameras are at risk of hostile and violent attacks. While a camera or housing can never guarantee 100% protection from destructive behavior in every situation, vandalism can be mitigated by considering various aspects: camera/housing design, mounting, placement and use of intelligent video alarms.

4.5.1 Camera/housing design

Casings and related components that are made of metal provide better vandal protection than ones made of plastic. The shape of the housing or camera is another factor. A housing or a traditional fixed camera that protrudes from a wall or ceiling is more vulnerable to attacks (e.g., kick-

ing or hitting) than more discretely designed housings or casings for a fixed dome or PTZ dome camera. The smooth, rounded covering of a fixed dome or PTZ dome makes it more difficult, for example, to block the camera's view by trying to hang a piece of clothing over the camera. The more a housing or camera blends into an environment or is disguised as something other than a camera—for example, an outdoor light—the better the protection against vandalism.

Figure 4.5a *Examples of fixed camera housings. Only the middle and right housings are classified as vandal-resistant.*

Figure 4.5b *Examples of vandal-resistant housings for a small or compact fixed network camera (at left), for a fixed dome network camera (middle) and for a PTZ camera (at right).*

4.5.2 Mounting

The way cameras and housings are mounted is also important. A traditional fixed network camera and a PTZ dome camera that is mounted on the surface of a ceiling are more vulnerable to attacks than a fixed dome or PTZ dome camera that is mounted flush to a ceiling or wall, where only the transparent part of the camera or housing is visible.

Figures 4.5c *Examples of flush ceiling-mounted housings for fixed network cameras.*

Another important consideration is how the cabling to a camera is mounted. Maximum protection is provided when the cable is pulled directly through the wall or ceiling behind the camera. In this way, there are no visible cables to tamper with. If this is not possible, a metal conduit tube should be used to protect cables from attacks.

4.5.3 Camera placement

Camera placement is also an important factor in deterring vandalism. By placing a camera out of reach on high walls or in the ceiling, many spur-of-the-moment attacks can be prevented. The downside may be the angle of view, which to some extent can be compensated by selecting a different lens.

4.5.4 Intelligent video

Axis' active tampering alarm feature helps protect cameras against vandalism. It can detect if a camera has been redirected, obscured or tampered with, and can send alarms to operators. This is especially useful in installations with hundreds of cameras in demanding environments where keeping track of the proper functioning of all cameras is difficult. It is also useful in situations where no live viewing takes place and operators can be notified when cameras have been tampered with.

4.6 Types of mounting

Cameras need to be placed in all kinds of locations and this requires a large number of variations in the type of mounting.

4.6.1 Ceiling mounts

Ceiling mounts are mainly used in indoor installations. The enclosure itself can be:

- **A surface mount:** mounted directly on the surface of a ceiling and, therefore, completely visible.
- **A flush mount:** mounted inside the ceiling with only parts of a camera and housing (usually the bubble) visible.
- **A pendant mount:** housing that is hung from a ceiling like a pendant.

Figure 4.6a *An example of a surface mount (left), a flush mount (middle) and a pendant mount (right).*

4.6.2 Wall mounts

Wall mounts are often used to mount cameras inside or outside a building. The housing is connected to an arm, which is mounted on a wall. Advanced mounts have an inside cable gland to protect the cable. To install an enclosure at a corner of a building, a normal wall mount, together with an additional corner adapter, can be used. Other special mounts include a pendant kit mount, which allows a fixed network camera to be mounted in a style that is similar to a PTZ dome enclosure.

Figure 4.6b *An example of a wall mount with a pendent mount kit for a fixed dome camera.*

4.6.3 Pole mounts

A pole mount is often used together with a PTZ camera in locations such as a parking lot. This type of mount usually takes into consideration the impact of wind. The dimensions of the pole and the mount itself should be designed to minimize vibrations. Cables are often enclosed inside the pole and outlets must be properly sealed. More advanced PTZ dome cameras have built-in electronic image stabilization to limit the effects of wind and vibrations.

4.6.4 Parapet mounts

Parapet mounts are used for roof-mounted housings or to raise the camera for a better angle of view.

Figure 4.6c *An example of a parapet mount.*

Axis provides an online tool that can help users identify the right housing and mounting accessories needed. *Visit www.axis.com/products/video/accessories/configurator/*

Video encoders

Video encoders, also known as video servers, enable an existing analog CCTV video surveillance system to be integrated with a network video system. Video encoders play a significant role in installations where many analog cameras are to be maintained. This chapter describes what a video encoder is and its benefits, and provides an overview of its components and the different types of video encoders available. A brief discussion on deinterlacing techniques is also included, in addition to a section on video decoders.

5.1 What is a video encoder?

A video encoder makes it possible for an analog CCTV system to migrate to a network video system. It enables users to gain the benefits of network video without having to discard existing analog equipment such as analog CCTV cameras and coaxial cabling.

A video encoder connects to an analog video camera via a coaxial cable and converts analog video signals into digital video streams that are then sent over a wired or wireless IP-based network (e.g., LAN, WLAN or Internet). To view and/or record the digital video, computer monitors and PCs can be used instead of DVRs or VCRs and analog monitors.

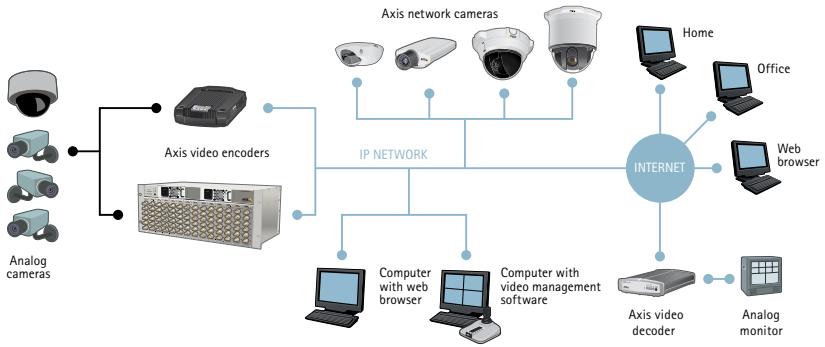


Figure 5.1a *An illustration of how analog video cameras and analog monitors can be integrated with a network video system using video encoders and decoders.*

By using video encoders, analog video cameras of all types, such as fixed, indoor/outdoor, dome, pan/tilt/zoom, and specialty cameras such as highly sensitive thermal cameras and microscope cameras can be remotely accessed and controlled over an IP network.

A video encoder also offers other benefits such as event management and intelligent video functionalities, as well as advanced security measures. In addition, it provides scalability and ease of integration with other security systems.

Figure 5.1b *A one-channel, standalone video encoder with audio, I/O (input/output) connectors 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.*

5.1.1 Video encoder components and considerations

Axis video encoders offer many of the same functions that are available in network cameras. Some of the main components of a video encoder include:

> Analog video input for connecting an analog camera using a coaxial cable.

> Processor for running the video encoder's operating system, networking and security functionalities, for encoding analog video using various compression formats and for video analysis. The processor determines the performance of a video encoder, normally measured in frames per second in the highest resolution. Advanced video encoders can provide full frame rate (30 frames per second with NTSC-based analog cameras or 25 frames per second with PAL-based analog cameras) in the highest resolution for every video channel. Axis video encoders also have auto sensing to automatically recognize if the incoming analog video signal is an NTSC or PAL standard. *For more on NTSC and PAL resolutions, see Chapter 6.*

> Memory for storing the firmware (computer program) using Flash, as well as buffering of video sequences (using RAM).

> Ethernet/Power over Ethernet port to connect to an IP network for sending and receiving data, and for powering the unit and the attached camera if Power over Ethernet is supported. *For more on Power over Ethernet, see Chapter 9.*

> Serial port (RS-232/422/485) often used for controlling the pan/tilt/zoom functionality of an analog PTZ camera.

> Input/output connectors for connecting external devices; for example, sensors to detect an alarm event, and relays to activate, for instance, lights in response to an event.

> Audio in for connecting a microphone or line-in equipment and audio out for connecting to speakers.

Video encoders for professional systems should meet high demands for reliability and quality. When selecting a video encoder, other considerations include the number of supported analog channels, image quality, compression formats, resolution, frame rate and features such as pan/tilt/zoom support, audio, event management, intelligent video, Power over Ethernet and security functionalities.

5.1.2 Event management and intelligent video

One of the main benefits of Axis video encoders is the ability to provide event management and intelligent video functionalities, capabilities that cannot be provided in an analog video system. Built-in intelligent video features such as multi-window video motion detection, audio detection and active tampering alarm, as well as input ports for external sensors, enable a network video surveillance system to be constantly on guard to detect an event. Once an event is detected, the system can automatically respond with actions that may include video recording, sending alerts such as e-mails and SMS, activating lights, opening/closing doors and sounding alarms. *For more on event management and intelligent video, see Chapter 11.*

5.2 Standalone video encoders

The most common type of video encoders is the standalone version, which offers one or multi-channel (often four) connections to analog cameras. A multi-channel video encoder is ideal in situations where there are several analog cameras located in a remote facility or a place that is a fair distance from a central monitoring room. Through the multi-channel video encoder, video signals from the remote cameras can then share the same network cabling, thereby reducing cabling costs.

In situations where investments have been made in analog cameras but coaxial cables have not yet been installed, it is best to use and position standalone video encoders close to the analog cameras. It reduces installation costs as it eliminates the need to run new coaxial cables to a central location since the video can be sent over an Ethernet network. It also eliminates the loss in image quality that would occur if video were to be sent over long distances through coaxial cables. With coaxial cables, the video quality decreases the further the signals have to travel. A video encoder produces digital images, so there is no reduction in image quality due to the distance traveled by a digital video stream.

Figure 5.2a *An illustration of how a small, single-channel video encoder can be positioned next to an analog camera in a camera housing.*

5.3 Rack-mounted video encoders

Rack-mounted video encoders are beneficial in instances where there are many analog cameras with coaxial cables running to a dedicated control room. They enable many analog cameras to be connected and managed from one rack in a central location. A rack allows a number of different video encoder blades to be mounted and thereby offers a flexible, expandable, high-density solution. A video encoder blade may support one, four or six analog cameras. A blade can be seen as a video encoder without a casing, although it cannot function on its own; it has to be mounted in a rack to operate.

Figure 5.3a *When the AXIS Q7900 Rack (shown here) is fully outfitted with 6-channel video encoder blades, it can accommodate as many as 84 analog cameras.*

Axis video encoder racks support features such as hot swapping of blades; that is, blades can be removed or installed without having to power down the rack. The racks also provide serial communication and input/output connectors for each video encoder blade, in addition to a common power supply and shared Ethernet network connection(s).

5.4 Video encoders with PTZ cameras and PTZ dome cameras

In a network video system, pan/tilt/zoom commands from a control board are carried over the same IP network as for video transmission and are forwarded to the analog PTZ camera or PTZ dome camera through the video encoder's serial port (RS-232/422/485). Video encoders, therefore,

enable analog PTZ cameras to be controlled over long distances, even through the Internet. (In an analog CCTV system, each PTZ camera would require separate and dedicated serial wiring from the control board—with joystick and other control buttons—all the way to the camera.)

To control a specific PTZ camera, a driver must be uploaded to the video encoder. Many manufacturers of video encoders provide PTZ drivers for most analog PTZ cameras and PTZ dome cameras. A PTZ driver can also be installed on the PC that runs the video management software program if the video encoder's serial port is set up as a serial server that simply passes on the commands.

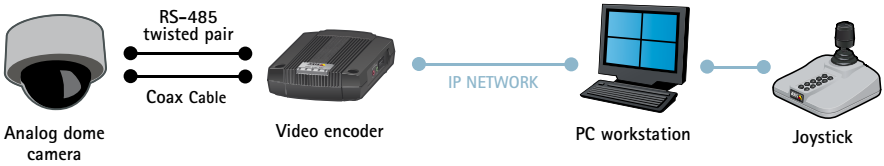


Figure 5.4a *An analog PTZ dome camera can be controlled via the video encoder's serial port (e.g., RS-485), making it possible to remotely control it over an IP network.*

The most commonly used serial port for controlling PTZ functions is RS-485. One of the benefits that RS-485 allows is the possibility to control multiple PTZ cameras using twisted pair cables in a daisy chain connection from one dome camera to the next. The maximum distance of an RS-485 cable, without using a repeater, is 1,220 meters (4,000 feet) at baud rates up to 90 kbit/s.

5.5 Deinterlacing techniques

Video from analog cameras is designed to be viewed on analog monitors such as traditional TV sets, which use a technique called interlaced scanning. With interlaced scanning, two consecutive interlaced fields of lines are shown to form an image. When such video is shown on a computer screen, which uses a different technique called progressive scanning, interlacing effects (i.e., tearing or comb effect) from moving objects can be seen. In order to reduce the unwanted interlacing effects, different deinterlacing techniques can be employed. In advanced Axis video encoders, users can choose between two different deinterlacing techniques: adaptive interpolation and blending.

Figure 5.5a *At left, a close-up of an interlaced image shown on a computer screen; at right, the same interlaced image with deinterlacing technique applied.*

Adaptive interpolation offers the best image quality. The technique involves using only one of the two consecutive fields and using interpolation to create the other field of lines to form a full image.

Blending involves merging two consecutive fields and displaying them as one image so that all fields are present. The image is then filtered to smooth out the motion artifacts or 'comb effect' caused by the fact that the two fields were captured at slightly different times. The blending technique is not as processor intensive as adaptive interpolation.

5.6 Video decoder

A video decoder decodes digital video and audio coming from a video encoder or a network camera into analog signals, which can then be used by analog monitors, such as regular TV sets, and video switches. A typical case could be in a retail environment where the user may want to have traditional monitors in public spaces to demonstrate that video surveillance is used.

Another common application for video decoders is to use them in an analog-to-digital-to-analog configuration for transporting video over long distances. The quality of digital video is not affected by the distance traveled, which is not the case when sending analog signals over long distances. The only downside may be some level of latency, from 100 ms to a few seconds, depending on the distance and the quality of the network between the end points.

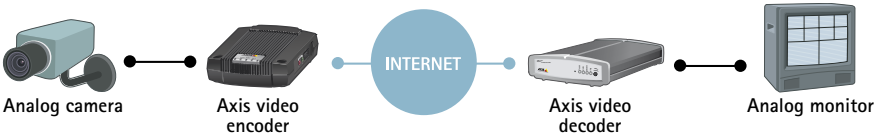


Figure 5.6a *An encoder and decoder can be used to transport video over long distances, from an analog camera to an analog monitor.*

A video decoder has the ability to decode and display video from many cameras sequentially; that is, decoding and showing video from one camera for some seconds before changing to another and so on.

Resolutions

Resolution in an analog or digital world is similar, but there are some important differences in how it is defined. In analog video, an image consists of lines or TV-lines since analog video technology is derived from the television industry. In a digital system, an image is made up of square pixels.

The sections below describe the different resolutions that network video can provide. They include NTSC, PAL, VGA, megapixel and HDTV.

6.1 NTSC and PAL resolutions

NTSC (National Television System Committee) and PAL (Phase Alternating Line) resolutions are analog video standards. They are relevant to network video since video encoders provide such resolutions when they digitize signals from analog cameras. Current PTZ network cameras and PTZ dome network cameras also provide NTSC and PAL resolutions since such cameras today use a camera block (which incorporates the camera, zoom, auto-focus and auto-iris functions) made for analog video cameras, in conjunction with a built-in video encoder board.

In North America and Japan, the NTSC standard is the predominant analog video standard, while in Europe and many Asian and African countries, the PAL standard is used. Both standards originate from the television industry. NTSC has a resolution of 480 lines and uses a refresh rate of 60 interlaced fields per second (or 30 full frames per second). A new naming convention, which defines the number of lines, type of scan and refresh rate, for this standard is 480i60 ("i" stands for interlaced scanning). PAL has a resolution with 576 lines and uses a refresh rate of 50 interlaced fields per second (or 25 full frames per second). The new naming convention for this standard is 576i50. The total amount of information per second is the same in both standards.

When analog video is digitized, the maximum amount of pixels that can be created is based on the number of TV lines available to be digitized. The maximum size of a digitized image is typically D1 and the most commonly used resolution is 4CIF.

When shown on a computer screen, digitized analog video may show interlacing effects such as tearing and shapes may be off slightly since the pixels generated may not conform to the square pixels on the computer screen. Interlacing effects can be reduced using deinterlacing techniques (*see Chapter 5*), while aspect ratio correction can be applied to video before it is displayed to ensure, for instance, that a circle in an analog video remains a circle when shown on a computer screen.

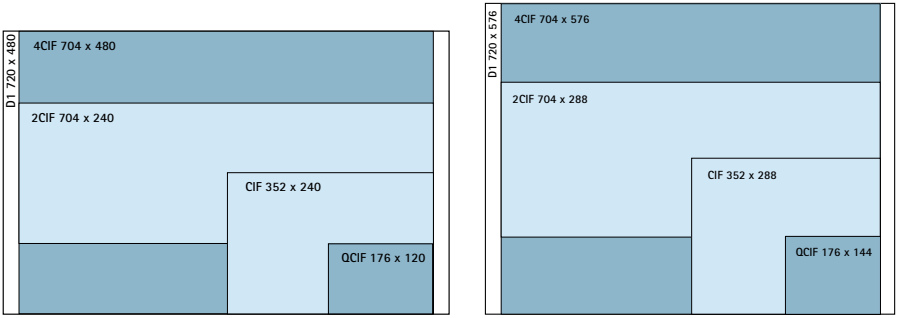


Figure 6.1a *At left, different NTSC image resolutions. At right, different PAL image resolutions.*

6.2 VGA resolutions

With 100% digital systems based on network cameras, resolutions that are derived from the computer industry and that are standardized worldwide can be provided, allowing for better flexibility. The limitations of NTSC and PAL become irrelevant.

VGA (Video Graphics Array) is a graphics display system for PCs originally developed by IBM. The resolution is defined as 640x480 pixels, which is a common format used by non-megapixel network cameras. The VGA resolution is normally better suited for network cameras since VGA-based video produces square pixels that match with those on computer screens. Computer monitors can handle resolutions in VGA or multiples of VGA.

Display format	Pixels
QVGA (SIF)	320x240
VGA	640x480
SVGA	800x600
XVGA	1024x768
4x VGA	1280x960

Table 6.2 *VGA resolutions.*

6.3 Megapixel resolutions

A network camera that offers megapixel resolution uses a megapixel sensor to deliver an image that contains one million or more pixels. The more pixels a sensor has, the greater the potential it has for capturing finer details and for producing a higher quality image. Megapixel network cameras can be used to allow users to see more details (ideal for identification of people and objects) or to view a larger area of a scene. This benefit is an important consideration in video surveillance applications.

Display format	No. of megapixels	Pixels
SXGA	1.3 megapixels	1280x1024
SXGA+ (EXGA)	1.4 megapixels	1400x1050
UXGA	1.9 megapixels	1600x1200
WUXGA	2.3 megapixels	1920x1200
QXGA	3.1 megapixels	2048x1536
WQXGA	4.1 megapixels	2560x1600
QSXGA	5.2 megapixels	2560x2048

Table 6.3 *Above are some megapixel formats.*

Megapixel resolution is one area in which network cameras excel over analog cameras. The maximum resolution a conventional analog camera can provide after the video signal has been digitized in a digital video recorder or a video encoder is D1, which is 720x480 pixels (NTSC) or 720x576 pixels (PAL). The D1 resolution corresponds to a maximum of 414,720 pixels or 0.4 megapixel. By comparison, a common megapixel format of 1280x1024 pixels gives a 1.3-megapixel resolution. This is more than 3 times the resolution that can be provided by analog CCTV cameras. Network cameras with 2-megapixel and 3-megapixel resolutions are also available, and even higher resolutions are expected in the future.

Megapixel resolution also provides a greater degree of flexibility in terms of being able to provide images with different aspect ratios. (Aspect ratio is the ratio of the width of an image to its height.) A conventional TV monitor displays an image with an aspect ratio of 4:3. Axis megapixel network cameras can offer the same ratio, in addition to others, such as 16:9. The advantage of a 16:9 aspect ratio is that unimportant details, usually located in the upper and lower part of a conventional-sized image, are not present and therefore, bandwidth and storage requirements can be reduced.

Figure 6.3a *Illustration of 4:3 and 16:9 aspect ratios.*

6.4 High-definition television (HDTV) resolutions

HDTV provides up to five times higher resolution than standard analog TV. HDTV also has better color fidelity and a 16:9 format. Defined by SMPTE (Society of Motion Picture and Television Engineers), the two most important HDTV standards are SMPTE 296M and SMPTE 274M.

SMPTE 296M (HDTV 720P) defines a resolution of 1280x720 pixels with high color fidelity in a 16:9 format using progressive scanning at 25/30 Hertz (Hz), which corresponds to 25 or 30 frames per second depending on the country, and at 50/60 Hz (50/60 frames per second).

SMPTE 274M (HDTV 1080) defines a resolution of 1920x1080 pixels with high color fidelity in a 16:9 format using either interlaced or progressive scanning at 25/30 Hz and 50/60Hz.

A camera that complies with the SMPTE standards indicates adherence to HDTV quality and should provide all the benefits of HDTV in resolution, color fidelity and frame rate.

The HDTV standard is based on square pixels—similar to computer screens, so HDTV video from network video products can be shown on either HDTV screens or standard computer monitors. With progressive scan HDTV video, no conversion or deinterlacing technique needs to be applied when the video is to be processed by a computer or displayed on a computer screen.

Video compression

Video compression technologies are about reducing and removing redundant video data so that a digital video file can be effectively sent over a network and stored on computer disks. With efficient compression techniques, a significant reduction in file size can be achieved with little or no adverse effect on the visual quality. The video quality, however, can be affected if the file size is further lowered by raising the compression level for a given compression technique.

Different compression technologies, both proprietary and industry standards, are available. Most network video vendors today use standard compression techniques. Standards are important in ensuring compatibility and interoperability. They are particularly relevant to video compression since video may be used for different purposes and, in some video surveillance applications, needs to be viewable many years from the recording date. By deploying standards, end users are able to pick and choose from different vendors, rather than be tied to one supplier when designing a video surveillance system.

Axis uses three different video compression standards. They are Motion JPEG, MPEG-4 Part 2 (or simply referred to as MPEG-4) and H.264. H.264 is the latest and most efficient video compression standard. This chapter covers the basics of compression and provides a description of each of the three standards mentioned earlier.

7.1 Compression basics

7.1.1 Video codec

The process of compression involves applying an algorithm to the source video to create a compressed file that is ready for transmission or storage. To play the compressed file, an inverse algorithm is applied to produce a video that shows virtually the same content as the original source video. The time it takes to compress, send, decompress and display a file is called latency. The more advanced the compression algorithm, the higher the latency.

A pair of algorithms that works together is called a video codec (encoder/decoder). Video codecs of different standards are normally not compatible with each other; that is, video content that is compressed using one standard cannot be decompressed with a different standard. For instance, an MPEG-4 decoder will not work with an H.264 encoder. This is simply because one algorithm cannot correctly decode the output from another algorithm but it is possible to implement many different algorithms in the same software or hardware, which would then enable multiple formats to coexist.

7.1.2 Image compression vs. video compression

Different compression standards utilize different methods of reducing data, and hence, results differ in bit rate, quality and latency. Compression algorithms fall into two types: image compression and video compression.

Image compression uses intraframe coding technology. Data is reduced within an image frame simply by removing unnecessary information that may not be noticeable to the human eye. Motion JPEG is an example of such a compression standard. Images in a Motion JPEG sequence is coded or compressed as individual JPEG images.

Figure 7.1a *With the Motion JPEG format, the three images in the above sequence are coded and sent as separate unique images (I-frames) with no dependencies on each other.*

Video compression algorithms such as MPEG-4 and H.264 use interframe prediction to reduce video data between a series of frames. This involves techniques such as difference coding, where one frame is compared with a reference frame and only pixels that have changed with respect to the reference frame are coded. In this way, the number of pixel values that is coded and sent is reduced. When such an encoded sequence is displayed, the images appear as in the original video sequence.

Figure 7.1b *With difference coding, only the first image (I-frame) is coded in its entirety. In the two following images (P-frames), references are made to the first picture for the static elements, i.e. the house. Only the moving parts, i.e. the running man, are coded using motion vectors, thus reducing the amount of information that is sent and stored.*

Other techniques such as block-based motion compensation can be applied to further reduce the data. Block-based motion compensation takes into account that much of what makes up a new frame in a video sequence can be found in an earlier frame, but perhaps in a different location. This technique divides a frame into a series of macroblocks (blocks of pixels). Block by block, a new frame can be composed or 'predicted' by looking for a matching block in a reference frame. If a match is found, the encoder codes the position where the matching block is to be found in the reference frame. Coding the motion vector, as it is called, takes up fewer bits than if the actual content of a block were to be coded.

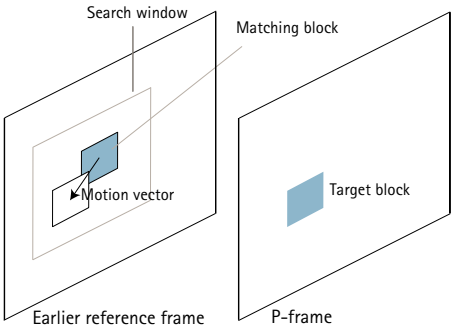


Figure 7.1c *Illustration of block-based motion compensation.*

With interframe prediction, each frame in a sequence of images is classified as a certain type of frame, such as an I-frame, P-frame or B-frame.

An I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. The first image in a video sequence is always an I-frame. I-frames are needed as starting points for new viewers or resynchronization points if the transmitted bit stream is damaged. I-frames can be used to implement fast-forward, rewind and other random access functions. An encoder will automatically insert I-frames at regular intervals or on demand if new clients are expected to join in viewing a stream. The drawback of I-frames is that they consume much more bits, but on the other hand, they do not generate many artifacts, which are caused by missing data.

A P-frame, which stands for predictive inter frame, makes references to parts of earlier I and/or P frame(s) to code the frame. P-frames usually require fewer bits than I-frames, but a drawback is that they are very sensitive to transmission errors because of the complex dependency on earlier P and/or I frames.

A B-frame, or bi-predictive inter frame, is a frame that makes references to both an earlier reference frame and a future frame. Using B-frames increases latency.

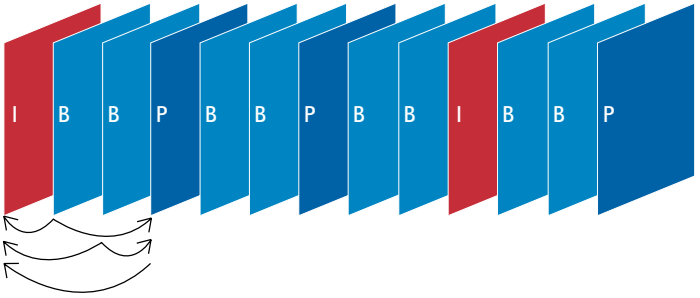


Figure 7.1d *A typical sequence with I-, B- and P-frames. A P-frame may only reference preceding I- or P-frames, while a B-frame may reference both preceding and succeeding I- or P-frames.*

When a video decoder restores a video by decoding the bit stream frame by frame, decoding must always start with an I-frame. P-frames and B-frames, if used, must be decoded together with the reference frame(s).

Axis network video products allow users to set the GOV (group of video) length, which determines how many P-frames should be sent before another I-frame is sent. By decreasing the frequency of I-frames (longer GOV), the bit rate can be reduced. To reduce latency, B-frames are not used.

Besides difference coding and motion compensation, other advanced methods can be employed to further reduce data and improve video quality. H.264, for example, supports advanced techniques that include prediction schemes for encoding I-frames, improved motion compensation down to sub-pixel accuracy, and an in-loop deblocking filter to smooth block edges (artifacts). *For more information on H.264 techniques, see Axis' white paper on H.264 at www.axis.com/corporate/corp/tech_papers.htm*

7.2 Compression formats

7.2.1 Motion JPEG

Motion JPEG or M-JPEG is a digital video sequence that is made up of a series of individual JPEG images. (JPEG stands for Joint Photographic Experts Group.) When 16 image frames or more are shown per second, the viewer perceives motion video. Full motion video is perceived at 30 (NTSC) or 25 (PAL) frames per second.

One of the advantages of Motion JPEG is that each image in a video sequence can have the same guaranteed quality that is determined by the compression level chosen for the network camera or video encoder. The higher the compression level, the lower the file size and image quality. In some situations, such as in low light or when a scene becomes complex, the image file size may become quite large and use more bandwidth and storage space. To prevent an increase in the bandwidth and storage used, Axis network video products allow the user to set a maximum file size for an image frame.

Since there is no dependency between the frames in Motion JPEG, a Motion JPEG video is robust, meaning that if one frame is dropped during transmission, the rest of the video will not be affected.

Motion JPEG is an unlicensed standard. It has broad compatibility and is popular in applications where individual frames in a video sequence are required—for example, for analysis—and where lower frame rates, typically 5 frames per second or lower, are used. Motion JPEG may also be needed for applications that require integration with systems that support only Motion JPEG.

The main disadvantage of Motion JPEG is that it makes no use of any video compression techniques to reduce the data since it is a series of still, complete images. The result is that it has a relatively high bit rate or low compression ratio for the delivered quality compared with video compression standards such as MPEG-4 and H.264.

7.2.2 MPEG-4

When MPEG-4 is mentioned in video surveillance applications, it is usually referring to MPEG-4 Part 2, also known as MPEG-4 Visual. Like all MPEG (Moving Picture Experts Group) standards, it is a licensed standard, so users must pay a license fee per monitoring station. MPEG-4 supports low-bandwidth applications and applications that require high quality images, no limitations in frame rate and with virtually unlimited bandwidth.

7.2.3 H.264 or MPEG-4 Part 10/AVC

H.264, also known as MPEG-4 Part 10/AVC for Advanced Video Coding, is the latest MPEG standard for video encoding. H.264 is expected to become the video standard of choice in the coming years. This is because an H.264 encoder can, without compromising image quality, reduce the size of a digital video file by more than 80% compared with the Motion JPEG format and as much as 50% more than with the MPEG-4 standard. This means that much less network bandwidth and storage space are required for a video file. Or seen another way, much higher video quality can be achieved for a given bit rate.

H.264 was jointly defined by standardization organizations in the telecommunications (ITU-T's Video Coding Experts Group) and IT industries (ISO/IEC Moving Picture Experts Group), and is expected to be more widely adopted than previous standards. In the video surveillance industry, H.264 will most likely find the quickest traction in applications where there are demands for high frame rates and high resolution, such as in the surveillance of highways, airports and casinos, where the use of 30/25 (NTSC/PAL) frames per second is the norm. This is where the economies of reduced bandwidth and storage needs will deliver the biggest savings.

H.264 is also expected to accelerate the adoption of megapixel cameras since the highly efficient compression technology can reduce the large file sizes and bit rates generated without compromising image quality. There are tradeoffs, however. While H.264 provides savings in network bandwidth and storage costs, it will require higher performance network cameras and monitoring stations.

Axis' H.264 encoders use the baseline profile, which means that only I- and P-frames are used. This profile is ideal for network cameras and video encoders since low latency is achieved because B-frames are not used. Low latency is essential in video surveillance applications where live monitoring takes place, especially when PTZ cameras or PTZ dome cameras are used.

7.3 Variable and constant bit rates

With MPEG-4 and H.264, users can allow an encoded video stream to have a variable or a constant bit rate. The optimal selection depends on the application and network infrastructure.

With VBR (variable bit rate), a predefined level of image quality can be maintained regardless of motion or the lack of it in a scene. This means that bandwidth use will increase when there is a lot of activity in a scene and will decrease when there is no motion. This is often desirable in video surveillance applications where there is a need for high quality, particularly if there is motion in a scene. Since the bit rate may vary, even when an average target bit rate is defined, the network infrastructure (available bandwidth) must be able to accommodate high throughputs.

With limited bandwidth available, the recommended mode is normally CBR (constant bit rate) as this mode generates a constant bit rate that can be predefined by a user. The disadvantage with CBR is that when there is, for instance, increased activity in a scene that results in a bit rate that is higher than the target rate, the restriction to keep the bit rate constant leads to a lower image quality and frame rate. Axis network video products allow the user to prioritize either the image quality or the frame rate if the bit rate rises above the target bit rate.

7.4 Comparing standards

When comparing the performance of MPEG standards such as MPEG-4 and H.264, it is important to note that results may vary between encoders that use the same standard. This is because the designer of an encoder can choose to implement different sets of tools defined by a standard. As long as the output of an encoder conforms to a standard's format and decoder, it is possible to make different implementations. An MPEG standard, therefore, cannot guarantee a given bit rate or quality, and comparisons cannot be properly made without first defining how the standards are implemented in an encoder. A decoder, unlike an encoder, must implement all the required parts of a standard in order to decode a compliant bit stream. A standard specifies exactly how a decompression algorithm should restore every bit of a compressed video.

The graph on the following page provides a bit rate comparison, given the same level of image quality, among the following video standards: Motion JPEG, MPEG-4 Part 2 (no motion compensation), MPEG-4 Part 2 (with motion compensation) and H.264 (baseline profile).

Figure 7.4a *Axis' H.264 encoder generated up to 50% fewer bits per second for a sample video sequence than an MPEG-4 encoder with motion compensation. The H.264 encoder was at least three times more efficient than an MPEG-4 encoder with no motion compensation and at least six times more efficient than with Motion JPEG.*

Audio

While the use of audio in video surveillance systems is still not widespread, having audio can enhance a system's ability to detect and interpret events, as well as enable audio communication over an IP network. The use of audio, however, can be restricted in some countries, so it is a good idea to check with local authorities.

Topics covered in this chapter include application scenarios, audio equipment, audio modes, audio detection alarm, audio compression and audio/video synchronization.

8.1 Audio applications

Having audio as an integrated part of a video surveillance system can be an invaluable addition to a system's ability to detect and interpret events and emergency situations. The ability of audio to cover a 360-degree area enables a video surveillance system to extend its coverage beyond a camera's field of view. It can instruct a PTZ camera or a PTZ dome camera (or alert the operator of one) to visually verify an audio alarm.

Audio can also be used to provide users with the ability to not only listen in on an area, but also communicate orders or requests to visitors or intruders. For instance, if a person in a camera's field of view demonstrates suspicious behavior, such as loitering near a bank machine, or is seen to be entering a restricted area, a remote security guard can send a verbal warning to the person. In a situation where a person has been injured, being able to remotely communicate with and notify the victim that help is on the way can also be beneficial. Access control—that is, a remote 'doorman' at an entrance—is another area of application. Other applications include a remote helpdesk situation (e.g., an unmanned parking garage), and video conferencing. An audiovisual surveillance system increases the effectiveness of a security or remote monitoring solution by enhancing a remote user's ability to receive and communicate information.

8.2 Audio support and equipment

Audio support can be more easily implemented in a network video system than in an analog CCTV system. In an analog system, separate audio and video cables must be installed from end-point to endpoint; that is, from the camera and microphone location to the viewing/recording location. If the distance between the microphone and the station is too long, balanced audio equipment must be used, which increases installation costs and difficulty. In a network video system, a network camera with audio support processes the audio and sends both audio and video over the same network cable for monitoring and/or recording. This eliminates the need for extra cabling, and makes synchronizing the audio and video much easier.

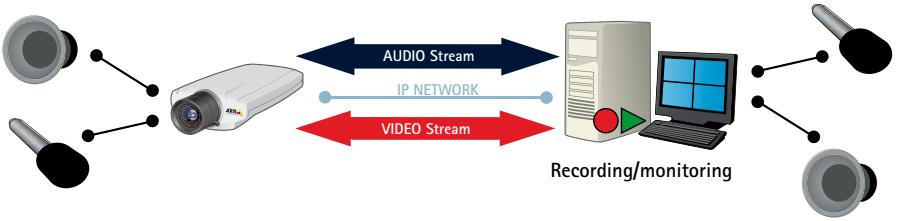


Figure 8.2a *A network video system with integrated audio support. Audio and video streams are sent over the same network cable.*

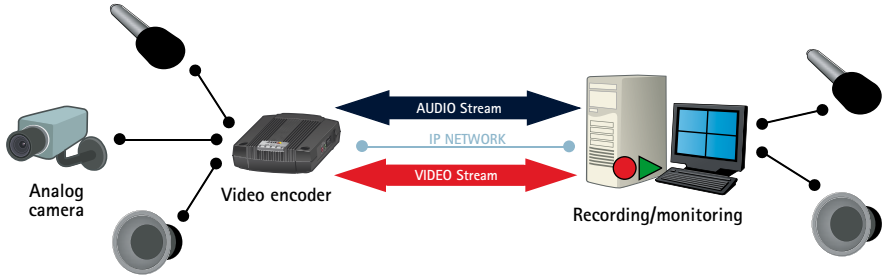


Figure 8.2b *Some video encoders have built-in audio, making it possible to add audio even if analog cameras are used in an installation.*

A network camera or video encoder with an integrated audio functionality often provides a built-in microphone, and/or mic-in/line-in jack. With mic-in/line-in support, users have the option of using another type or quality of microphone than the one that is built into the camera or video encoder. It also enables the network video product to connect to more than one microphone, and the microphone can be located some distance away from the camera. The microphone should always be placed as close as possible to the source of the sound to reduce noise. In two-way, full-duplex mode, a microphone should face away and be placed some distance from a speaker to reduce feedback from the speaker.

Many Axis network video products do not come with a built-in speaker. An active speaker—a speaker with a built-in amplifier—can be connected directly to a network video product with audio support. If a speaker has no built-in amplifier, it must first connect to an amplifier, which is then connected to a network camera/video encoder.

To minimize disturbance and noise, always use a shielded audio cable and avoid running the cable near power cables and cables carrying high frequency switching signals. Audio cables should also be kept as short as possible. If a long audio cable is required, balanced audio equipment—that is, cable, amplifier and microphone that are all balanced—should be used to reduce noise.

8.3 Audio modes

Depending on the application, there may be a need to send audio in only one direction or both directions, which can be done either simultaneously or in one direction at a time. There are three basic modes of audio communication: simplex, half duplex and full duplex.

8.3.1 Simplex

Figure 8.3a *In simplex mode, audio is sent in one direction only. In this case, audio is sent by the camera to the operator. Applications include remote monitoring and video surveillance.*

Figure 8.3b *In this example of a simplex mode, audio is sent by the operator to the camera. It can be used, for instance, to provide spoken instructions to a person seen on the camera or to scare a potential car thief away from a parking lot.*

8.3.2 Half duplex

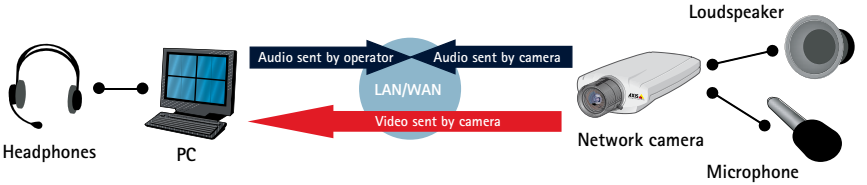


Figure 8.3c *In half-duplex mode, audio is sent in both directions, but only one party at a time can send. This is similar to a walkie-talkie.*

8.3.3 Full duplex

Figure 8.3d *In full-duplex mode, audio is sent to and from the operator simultaneously. This mode of communication is similar to a telephone conversation. Full duplex requires that the client PC has a sound card with support for full-duplex audio.*

8.4 Audio detection alarm

Audio detection alarm can be used as a complement to video motion detection since it can react to events in areas too dark for the video motion detection functionality to work properly. It can also be used to detect activity in areas outside of the camera's view.

When sounds, such as the breaking of a window or voices in a room, are detected, they can trigger a network camera to send and record video and audio, send e-mail or other alerts, and activate external devices such as alarms. Similarly, alarm inputs such as motion detection and door contacts can be used to trigger video and audio recordings. In a PTZ camera or a PTZ dome camera, audio alarm detection can trigger the camera to automatically turn to a preset location such as a specific window.

8.5 Audio compression

Analog audio signals must be converted into digital audio through a sampling process and then compressed to reduce the size for efficient transmission and storage. The conversion and compression is done using an audio codec, an algorithm that codes and decodes audio data.

8.5.1 Sampling frequency

There are many different audio codecs supporting different sampling frequencies and levels of compression. Sampling frequency refers to the number of times per second a sample of an analog audio signal is taken and is defined in hertz (Hz). In general, the higher the sampling frequency, the better the audio quality and the greater the bandwidth and storage needs.

8.5.2 Bit rate

The bit rate is an important setting in audio since it determines the level of compression and, thereby, the quality of the audio. In general, the higher the compression level (the lower the bit rate), the lower the audio quality. The differences in the audio quality of codecs may be particularly noticeable at high compression levels (low bit rates), but not at low compression levels (high bit rates). Higher compression levels may also introduce more latency or delay, but they enable greater savings in bandwidth and storage.

The bit rates most often selected with audio codecs are between 32 kbit/s and 64 kbit/s. Audio bit rates, as with video bit rates, are an important consideration to take into account when calculating total bandwidth and storage requirements.

8.5.3 Audio codecs

Axis network video products support three audio codecs. The first is AAC-LC (Advanced Audio Coding - Low Complexity), also known as MPEG-4 AAC, which requires a license. AAC-LC, particularly at a sampling rate of 16 kHz or higher and at a bit rate of 64 kbit/s, is the recommended codec to use when the best possible audio quality is required. The other two codecs are G.711 and G.726, which are non-licensed technologies.

8.6 Audio and video synchronization

Synchronization of audio and video data is handled by a media player (a computer software program used for playing back multimedia files) or by a multimedia framework such as Microsoft DirectX, which is a collection of application programming interfaces that handles multimedia files.

Audio and video are sent over a network as two separate packet streams. In order for the client or player to perfectly synchronize the audio and video streams, the audio and video packets must be time-stamped. The timestamping of video packets using Motion JPEG compression may not always be supported in a network camera. If this is the case and if it is important to have synchronized video and audio, the video format to choose is MPEG-4 or H.264 since such video streams, along with the audio stream, are sent using RTP (Real-time Transport Protocol), which timestamps the video and audio packets. There are many situations, however, where synchronized audio is less important or even undesirable; for example, if audio is to be monitored but not recorded.

Network technologies

Different network technologies are used to support and provide the many benefits of a network video system. This chapter begins with a discussion about the local area network, in particular, Ethernet networks and the components that support it. The use of Power over Ethernet is also covered.

Internet communication is then addressed with discussions on IP (Internet Protocol) addressing—what they are and how they work, including how network video products can be accessed over the Internet. An overview of the data transport protocols used in network video is also provided.

Other areas covered in the chapter include virtual local area networks and Quality of Service, and the different ways of securing communication over IP networks. *For more on wireless technologies, see Chapter 10.*

9.1 Local area network and Ethernet

A local area network (LAN) is a group of computers that are connected together in a localized area to communicate with one another and share resources such as printers. Data is sent in the form of packets and to regulate the transmission of the packets, different technologies can be used. The most widely used LAN technology is the Ethernet and it is specified in a standard called IEEE 802.3. (Other types of LAN networking technologies include token ring and FDDI.)

Ethernet uses a star topology in which the individual nodes (devices) are networked with one another via active networking equipment such as switches. The number of networked devices in a LAN can range from two to several thousand.

The physical transmission medium for a wired LAN involves cables, mainly twisted pair or fiber optics. A twisted pair cable consists of eight wires, forming four pairs of twisted copper wires and is used with RJ-45 plugs and sockets. The maximum cable length of a twisted pair is 100 m (328 ft.) while for fiber, the maximum length ranges from 10 km to 70 km, depending on the

type of fiber. Depending on the type of twisted pair or fiber optic cables used, data rates today can range from 100 Mbit/s to 10,000 Mbit/s.

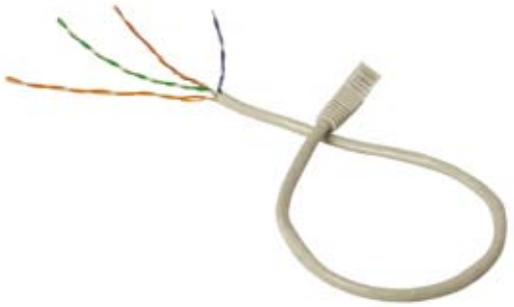


Figure 9.1a *Twisted pair cabling includes four pairs of twisted wires, normally connected to a RJ-45 plug at the end.*

A rule of thumb is to always build a network with greater capacity than is currently required. To future-proof a network, it is a good idea to design a network such that only 30% of its capacity is used. Since more and more applications are running over networks today, higher and higher network performance is required. While network switches (discussed below) are easy to upgrade after a few years, cabling is normally much more difficult to replace.

9.1.1 Types of Ethernet networks

Fast Ethernet

Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s. It can be based on a twisted pair or fiber optic cable. (The older 10 Mbit/s Ethernet is still installed and used, but such networks do not provide the necessary bandwidth for some network video applications.)

Most devices that are connected to a network, such as a laptop or a network camera, are equipped with a 100BASE-TX/10BASE-T Ethernet interface, most commonly called a 10/100 interface, which supports both 10 Mbit/s and Fast Ethernet. The type of twisted pair cable that supports Fast Ethernet is called a Cat-5 cable.

Gigabit Ethernet

Gigabit Ethernet, which can also be based on a twisted pair or fiber optic cable, delivers a data rate of 1,000 Mbit/s (1 Gbit/s) and is becoming very popular. It is expected to soon replace Fast Ethernet as the de facto standard.

The type of twisted pair cable that supports Gigabit Ethernet is a Cat-5e cable, where all four pairs of twisted wires in the cable are used to achieve the high data rates. Cat-5e or higher cable

categories are recommended for network video systems. Most interfaces are backwards compatible with 10 and 100 Mbit/s Ethernet and are commonly called 10/100/1000 interfaces.

For transmission over longer distances, fiber cables such as 1000BASE-SX (up to 550 m/1,639 ft.) and 1000BASE-LX (up to 550 m with multimode optical fibers and 5,000 m with single-mode fibers) can be used.

Figure 9.1b *Longer distances can be bridged using fiber optic cables. Fiber is typically used in the backbone of a network and not in nodes such as a network camera.*

10 Gigabit Ethernet

10 Gigabit Ethernet is the latest generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s), and a fiber optic or twisted pair cable can be used. 10GBASE-LX4, 10GBASE-ER and 10GBASE-SR based on an optical fiber cable can be used to bridge distances of up to 10,000 m (6.2 miles). With a twisted pair solution, a very high quality cable (Cat-6a or Cat-7) is required. 10 Gbit/s Ethernet is mainly used for backbones in high-end applications that require high data rates.

9.1.2. Switch

When only two devices need to communicate directly with one another via a twisted pair cable, a so-called crossover cable can be used. The crossover cable simply crosses the transmission pair on one end of the cable with the receiving pair on the other end and vice versa.

To network multiple devices in a LAN, however, network equipment such as a network switch is required. When using a network switch, a regular network cable is used instead of a crossover cable.

The main function of a network switch is to forward data from one device to another on the same network. It does it in an efficient manner since data can be directed from one device to another without affecting other devices on the same network.

How it works is that a switch registers the MAC (Media Access Control) addresses of all devices that are connected to it. (Each networking device has a unique MAC address, which is made up of a series of numbers and letters that is set by the manufacturer and the address is often found on the product label.) When a switch receives data, it forwards it only to the port that is connected to a device with the appropriate destination MAC address.

Switches typically indicate their performance in per port rates and in backplane or internal rates (both in bit rates and in packets per second). The port rates indicate the maximum rates on specific ports. This means that the speed of a switch, for example 100 Mbit/s, is often the performance of each port.

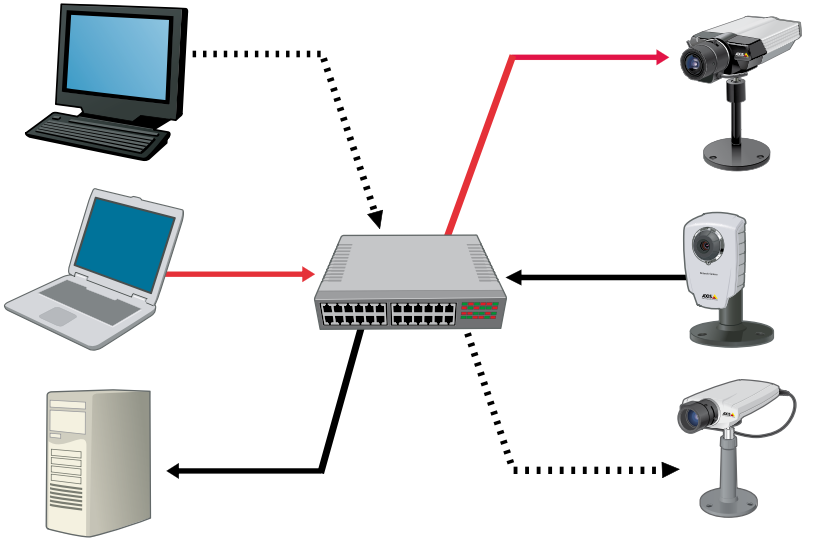


Figure 9.1c *With a network switch, data transfer is managed very efficiently as data traffic can be directed from one device to another without affecting any other ports on the switch.*

A network switch normally supports different data rates simultaneously. The most common rates used to be 10/100, supporting 10 Mbit/s as well as Fast Ethernet. However, 10/100/1000 are quickly taking over as the standard switch, thus supporting 10 Mbit/s, Fast Ethernet and Gigabit Ethernet simultaneously. The transfer rate and mode between a port on a switch and a connected device are normally determined through auto-negotiation, whereby the highest common data rate and best transfer mode are used. A switch also allows a connected device to function in full-duplex mode, i.e. send and receive data at the same time, resulting in increased performance.

Switches may come with different features or functions. Some switches include the function of a router (*see section 9.2*). A switch may also support Power over Ethernet or Quality of Service (*see section 9.4*), which controls how much bandwidth is used by different applications.

9.1.3 Power over Ethernet

Power over Ethernet (PoE) provides the option of supplying devices connected to an Ethernet network with power using the same cable as for data communication. Power over Ethernet is widely used to power IP phones, wireless access points and network cameras in a LAN.

The main benefit of PoE is the inherent cost savings. Hiring a certified electrician and installing a separate power line are not needed. This is advantageous, particularly in difficult-to-reach areas. The fact that no power cable has to be installed can save, depending on the camera location, up to a few hundred dollars per camera. Having PoE also makes it easier to move a camera to a new location, or add cameras to a video surveillance system.

Additionally, PoE can make a video system more secure. A video surveillance system with PoE can be powered from the server room, which is often backed up with a UPS (Uninterruptible Power Supply). This means that the video surveillance system can be operational even during a power outage.

Due to the benefits of PoE, it is recommended for use with as many devices as possible. The power available from the PoE-enabled switch or midspan should be sufficient for the connected devices and the devices should support power classification. These are explained in more detail in the sections below.

802.3af standard and High PoE

Most PoE devices today conform to the IEEE 802.3af standard, which was published in 2003. The IEEE 802.3af standard uses standard Cat-5 or higher cables, and ensures that data transfer is not affected. In the standard, the device that supplies the power is referred to as the power sourcing equipment (PSE). This can be a PoE-enabled switch or midspan. The device that receives the power is referred to as a powered device (PD). The functionality is normally built into a network device like a network camera, or provided in a standalone splitter (*see section below*).

Backward compatibility to non PoE-compatible network devices is guaranteed. The standard includes a method for automatically identifying if a device supports PoE, and only when that is confirmed will power be supplied to the device. This also means that the Ethernet cable that is connected to a PoE switch will not supply any power if it is not connected to a PoE-enabled device. This eliminates the risk of getting an electrical shock when installing or rewiring a network.

In a twisted pair cable, there are four pairs of twisted wires. PoE can use either the two 'spare' wire pairs, or overlay the current on the wire pairs used for data transmission. Switches with built-in PoE often supply electricity through the two pairs of wires used for transferring data, while midspans normally use the two spare pairs. A PD supports both options.

According to IEEE 802.3af, a PSE provides a voltage of 48 V DC with a maximum power of 15.4 W per port. Considering that power loss takes place on a twisted pair cable, only 12.95 W is guaranteed for a PD. The IEEE 802.3af standard specifies various performance categories for PDs.

PSE such as switches and midspans normally supply a certain amount of power, typically 300 W to 500 W. On a 48-port switch, that would mean 6 W to 10 W per port if all ports are connected to devices that use PoE. Unless the PDs support power classification, the full 15.4 W must be reserved for each port that uses PoE, which means a switch with 300 W can only supply power on 20 of the 48 ports. However, if all devices let the switch know that they are Class 1 devices, the 300 W will be enough to supply power to all 48 ports.

Class	Minimum power level at PSE	Maximum power level used by PD	Usage
0	15.4 W	0.44 W - 12.95 W	default
1	4.0 W	0.44 W - 3.84 W	optional
2	7.0 W	3.84 W - 6.49 W	optional
3	15.4 W	6.49 W - 12.95 W	optional
4	treat as Class 0		reserved for future use

Table 9.1a *Power classifications according to IEEE 802.3af.*

Most fixed network cameras can receive power via PoE using the IEEE 802.3af standard and are normally identified as Class 1 or 2 devices.

With IEEE 802.3at pre-standard or PoE+, the power limit will be raised to at least 30 W via two pairs of wires from a PSE. The final specifications are still to be determined and the standard is expected to be ratified in mid-2009.

In the meantime, IEEE 802.3at pre-standard (High PoE) midspans and splitters can be used for devices such as PTZ cameras and PTZ dome cameras with motor control, as well as cameras with heaters and fans, which require more power than can be delivered by the IEEE 802.3af standard.

Midspans and splitters

Midspans and splitters (also known as active splitters) are equipment that enable an existing network to support Power over Ethernet.

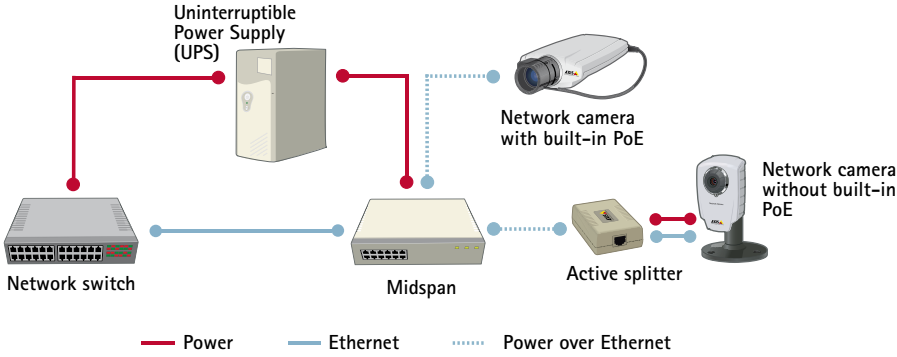


Figure 9.1d *An existing system can be upgraded with PoE functionality using a midspan and splitter.*

The midspan, which adds power to an Ethernet cable, is placed between the network switch and the powered devices. To ensure that data transfer is not affected, it is important to keep in mind that the maximum distance between the source of the data (e.g., switch) and the network video products is not more than 100 m (328 ft.). This means that the midspan and active splitter(s) must be placed within the distance of 100 m.

A splitter is used to split the power and data in an Ethernet cable into two separate cables, which can then be connected to a device that has no built-in support for PoE. Since PoE or High PoE only supplies 48 V DC, another function of the splitter is to step down the voltage to the appropriate level for the device; for example, 12 V or 5 V.

PoE and High PoE midspans and splitters are available from Axis.

9.2 The Internet

To send data between a device on one local area network to another device on another LAN, a standard way of communicating is required since local area networks may use different types of technologies. This need led to the development of IP addressing and the many IP-based protocols for communicating over the Internet, which is a global system of interconnected computer networks. (LANs may also use IP addressing and IP protocols for communicating within a local area network, although using MAC addresses is sufficient for internal communication.) Before IP addressing is discussed, some of the basic elements of Internet communication such as routers, firewalls and Internet service providers are covered below.

Routers

To forward data packages from one LAN to another LAN via the Internet, a networking equipment called a network router must be used. A router routes information from one network to

another based on IP addresses. It forwards only data packages that are to be sent to another network. A router is most commonly used for connecting a local network to the Internet. Traditionally, routers were referred to as gateways.

Firewalls
A firewall is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks that are connected to the Internet. Messages entering or leaving the Internet pass through the firewall, which examines each message, and blocks those that do not meet the specified security criteria.

Internet connections
In order to connect a LAN to the Internet, a network connection via an Internet service provider (ISP) must be established. When connecting to the Internet, terms such as upstream and downstream are used. Upstream describes the transfer rate with which data can be uploaded from the device to the Internet; for instance, when video is sent from a network camera. Downstream is the transfer speed for downloading files; for instance, when video is received by a monitoring PC.

In most scenarios—for example, a laptop that is connected to the Internet—downloading information from the Internet is the most important speed to consider. In a network video application with a network camera at a remote site, the upstream speed is more relevant since data (video) from the network camera will be uploaded to the Internet.

9.2.1 IP addressing
Any device that wants to communicate with other devices via the Internet must have a unique and appropriate IP address. IP addresses are used to identify the sending and receiving devices. There are currently two IP versions: IP version 4 (IPv4) and IP version 6 (IPv6). The main difference between the two is that the length of an IPv6 address is longer (128 bits compared with 32 bits for an IPv4 address). IPv4 addresses are most commonly used today.

9.2.1.1 IPv4 addresses
IPv4 addresses are grouped into four blocks, and each block is separated by a dot. Each block represents a number between 0 and 255; for example, 192.168.12.23.

Certain blocks of IPv4 addresses have been reserved exclusively for private use. These private IP addresses are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255. Such addresses can only be used on private networks and are not allowed to be forwarded through a router to the Internet. All devices that want to communicate over the Internet must have its own individual, public IP address. A public IP address is an address allocated by an Internet service provider. An ISP can allocate either a dynamic IP address, which can change during a session, or a static address, which normally comes with a monthly fee.

Ports

A port number defines a particular service or application so that the receiving server (e.g., network camera) will know how to process the incoming data. When a computer sends data tied to a specific application, it usually automatically adds the port number to an IP address without the user's knowledge.

Port numbers can range from 0 to 65535. Certain applications use port numbers that are pre-assigned to them by the Internet Assigned Numbers Authority (IANA). For example, a web service via HTTP is typically mapped to port 80 on a network camera.

Setting IPv4 addresses

In order for a network camera or video encoder to work in an IP network, an IP address must be assigned to it. Setting an IPv4 address for an Axis network video product can be done mainly in two ways: 1) automatically using DHCP (Dynamic Host Configuration Protocol), and 2) manually by either entering into the network video product's interface a static IP address, a subnet mask and the IP address of the default router, or using a management software tool such as AXIS Camera Management.

DHCP manages a pool of IP addresses, which it can assign dynamically to a network camera/video encoder. The DHCP function is often performed by a broadband router, which in turn gets its IP addresses from an Internet service provider. Using a dynamic IP address means that the IP address for a network device may change from day to day. With dynamic IP addresses, it is recommended that users register a domain name (e.g., *www.mycamera.com*) for the network video product at a dynamic DNS (Domain Name System) server, which can always tie the domain name for the product to any IP address that is currently assigned to it. (A domain name can be registered using some of the popular dynamic DNS sites such as *www.dyndns.org*. Axis also offers its own called AXIS Internet Dynamic DNS Service at *www.axiscam.net*, which is accessible from an Axis network video product's web interface.)

Using DHCP to set an IPv4 address works as follows. When a network camera/video encoder comes online, it sends a query requesting configuration from a DHCP server. The DHCP server replies with an IP address and subnet mask. The network video product can then update a dynamic DNS server with its current IP address so that users can access the product using a domain name.

With AXIS Camera Management, the software can automatically find and set IP addresses and show the connection status. The software can also be used to assign static, private IP addresses for Axis network video products. This is recommended when using video management software to access network video products. In a network video system with potentially hundreds of cameras, a software program such as AXIS Camera Management is necessary in order to effectively manage the system. *For more on video management, see Chapter 11.*

NAT (Network address translation)

When a network device with a private IP address wants to send information via the Internet, it must do so using a router that supports NAT. Using this technique, the router can translate a private IP address into a public IP address without the sending host's knowledge.

Port forwarding

To access cameras that are located on a private LAN via the Internet, the public IP address of the router should be used together with the corresponding port number for the network camera/video encoder on the private network.

Since a web service via HTTP is typically mapped to port 80, what happens then when there are several network cameras/video encoders using port 80 for HTTP in a private network? Instead of changing the default HTTP port number for each network video product, a router can be configured to associate a unique HTTP port number to a particular network video product's IP address and default HTTP port. This is a process called port forwarding.

Port forwarding works as follows. Incoming data packets reach the router via the router's public (external) IP address and a specific port number. The router is configured to forward any data coming into a predefined port number to a specific device on the private network side of the router. The router then replaces the sender's address with its own private (internal) IP address. To a receiving client, it looks like the packets originated from the router. The reverse happens with outgoing data packets. The router replaces the private IP address of the source device with the router's public IP address before the data is sent out over the Internet.

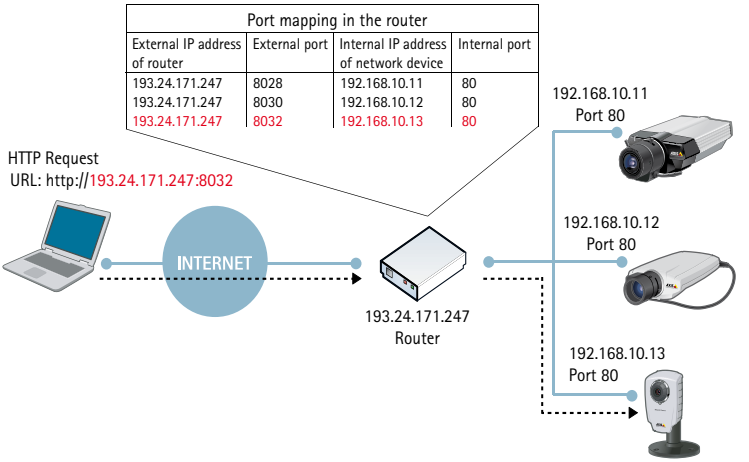


Figure 9.2a *Thanks to port forwarding in the router, network cameras with private IP addresses on a local network can be accessed over the Internet. In this illustration, the router knows to forward data (request) coming into port 8032 to a network camera with a private IP address of 192.168.10.13 port 80. The network camera can then begin to send video.*

Port forwarding is traditionally done by first configuring the router. Different routers have different ways of doing port forwarding and there are web sites such as *www.portfoward.com* that offer step-by-step instruction for different routers. Usually port forwarding involves bringing up the router's interface using an Internet browser, and entering the public (external) IP address of the router and a unique port number that is then mapped to the internal IP address of the specific network video product and its port number for the application.

To make the task of port forwarding easier, Axis offers the NAT traversal feature in many of its network video products. NAT traversal will automatically attempt to configure port mapping in a NAT router on the network using UPnP™. In the network video product interface, users can manually enter the IP address of the NAT router. If a router is not manually specified, then the network video product will automatically search for NAT routers on the network and select the default router. In addition, the service will automatically select an HTTP port if none is manually entered.

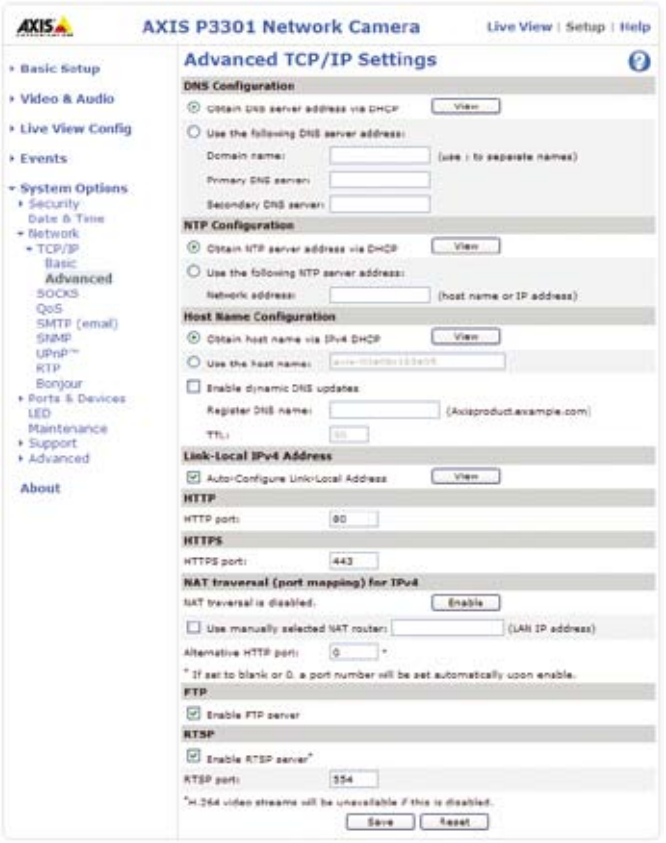


Figure 9.2b *Axis network video products enable port forwarding to be set using NAT traversal.*

9.2.1.2 IPv6 addresses

An IPv6 address is written in hexadecimal notation with colons subdividing the address into eight blocks of 16 bits each; for example, 2001:0da8:65b4:05d3:1315:7c1f:0461:7847

The major advantages of IPv6, apart from the availability of a huge number of IP addresses, include enabling a device to automatically configure its IP address using its MAC address. For communication over the Internet, the host requests and receives from the router the necessary prefix of the public address block and additional information. The prefix and host's suffix is then used, so DHCP for IP address allocation and manual setting of IP addresses are no longer required with IPv6. Port forwarding is also no longer needed. Other benefits of IPv6 include renumbering to simplify switching entire corporate networks between providers, faster routing, point-to-point encryption according to IPSec, and connectivity using the same address in changing networks (Mobile IPv6).

An IPv6 address is enclosed in square brackets in a URL and a specific port can be addressed in the following way: http://[2001:0da8:65b4:05d3:1315:7c1f:0461:7847]:8081/

Setting an IPv6 address for an Axis network video product is as simple as checking a box to enable IPv6 in the product. The product will then receive an IPv6 address according to the configuration in the network router.

9.2.2 Data transport protocols for network video

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are the IP-based protocols used for sending data. These transport protocols act as carriers for many other protocols. For example, HTTP (Hyper Text Transfer Protocol), which is used to browse web pages on servers around the world using the Internet, is carried by TCP.

TCP provides a reliable, connection-based transmission channel. It handles the process of breaking large chunks of data into smaller packets and ensures that data sent from one end is received on the other. TCP's reliability through retransmission may introduce significant delays. In general, TCP is used when reliable communication is preferred over transport latency.

UDP is a connectionless protocol and does not guarantee the delivery of data sent, thus leaving the whole control mechanism and error-checking to the application itself. UDP provides no transmissions of lost data and, therefore, does not introduce further delays.

Protocol	Transport protocol	Port	Common usage	Network video usage
FTP (File Transfer Protocol)	TCP	21	Transfer of files over the Internet/ intranets	Transfer of images or video from a network camera/video encoder to an FTP server or to an application
SMTP (Send Mail Transfer Protocol	TCP	25	Protocol for sending e-mail messages	A network camera/video encoder can send images or alarm notifications using its built-in e-mail client.
HTTP (Hyper Text Transfer Protocol	TCP	80	Used to browse the web, i.e. to retrieve web pages from web servers	The most common way to transfer video from a network camera/video encoder where the network video device essentially works as a web server making the video available for the requesting user or application server.
HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)	TCP	443	Used to access web pages securely using encryption technology	Secure transmission of video from network cameras/video encoders.
RTP (Real Time Protocol)	UDP/TCP	Not defined	RTP standardized packet format for delivering audio and video over the Internet—often used in streaming media systems or video conferencing	A common way of transmitting H.264/MPEG-based network video, and for synchronizing video and audio since RTP provides sequential numbering and timestamping of data packets, which enable the data packets to be reassembled in the correct sequence. Transmission can be either unicast or multicast.
RTSP (Real Time Streaming Protocol)	TCP	554	Used to set up and control multimedia sessions over RTP	

Table 9.2a *Common TCP/IP protocols and ports used for network video.*

9.3 VLANs

When a network video system is designed, there is often a desire to keep the network separate from other networks, both for security as well as performance reasons. At first glance, the obvious choice would be to build a separate network. While the design would be simplified, the cost of purchasing, installing and maintaining the network would often be higher than using a technology called virtual local area network (VLAN).

VLAN is a technology for virtually segmenting networks, a functionality that is supported by most network switches. It can be achieved by dividing network users into logical groups. Only users in a specific group are capable of exchanging data or accessing certain resources on the network. If a network video system is segmented into a VLAN, only the servers located on that VLAN can access the network cameras. VLANs normally provide a better and more cost-efficient solution than a separate network. The primary protocol used when configuring VLANs is IEEE 802.1Q, which tags each frame or packet with extra bytes to indicate which virtual network the packet belongs to.

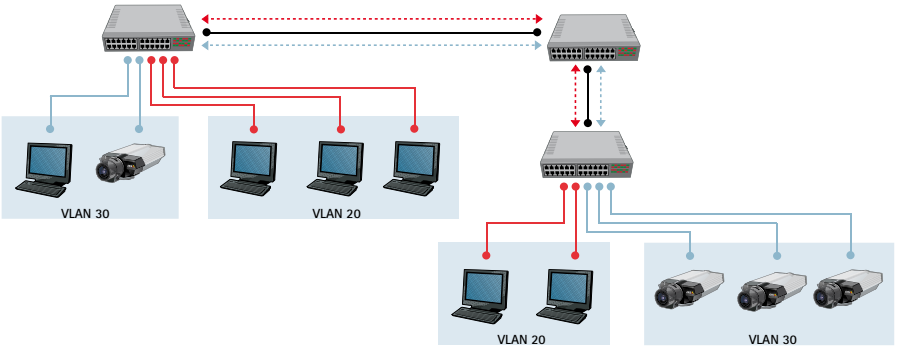


Figure 9.3a *In this illustration, VLANs are set up over several switches. First, each of the two different LANs are segmented into VLAN 20 and VLAN 30. The links between the switches transport data from different VLANs. Only members of the same VLAN are able to exchange data, either within the same network or over different networks. VLANs can be used to separate a video network from an office network.*

9.4 Quality of Service

Since different applications—for example, telephone, e-mail and surveillance video—may be using the same IP network, there is a need to control how network resources are shared to fulfill the requirements of each service. One solution is to let network routers and switches operate differently on different kinds of services (voice, data, and video) as traffic passes through the network. By using Quality of Service (QoS), different network applications can co-exist on the same network without consuming each other's bandwidth.

The term, Quality of Service, refers to a number of technologies such as Differentiated Service Codepoint (DSCP), which can identify the type of data in a data packet and so divide the packets into traffic classes that can be prioritized for forwarding. The main benefits of a QoS-aware network include the ability to prioritize traffic to allow critical flows to be served before flows with lesser priority, and greater reliability in a network by controlling the amount of bandwidth an application may use and thus controlling bandwidth competition between applications. PTZ traffic, which is often regarded as critical and requires low latency, is a typical case where QoS can be used to guarantee fast responses to movement requests. The prerequisite for the use of QoS within a video network is that all switches, routers and network video products must support QoS.

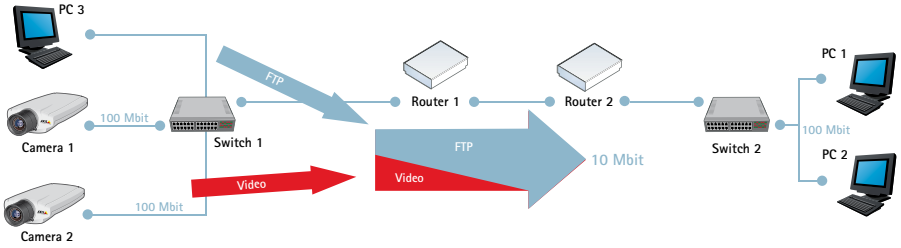


Figure 9.4a *Ordinary (non-QoS aware) network. In this example, PC1 is watching two video streams from cameras 1 and 2, with each camera streaming at 2.5 Mbit/s. Suddenly, PC2 starts a file transfer from PC3. In this scenario, the file transfer will try to use the full 10 Mbit/s capacity between the routers 1 and 2, while the video streams will try to maintain their total of 5 Mbit/s. The amount of bandwidth given to the surveillance system can no longer be guaranteed and the video frame rate will probably be reduced. At worst, the FTP traffic will consume all the available bandwidth.*

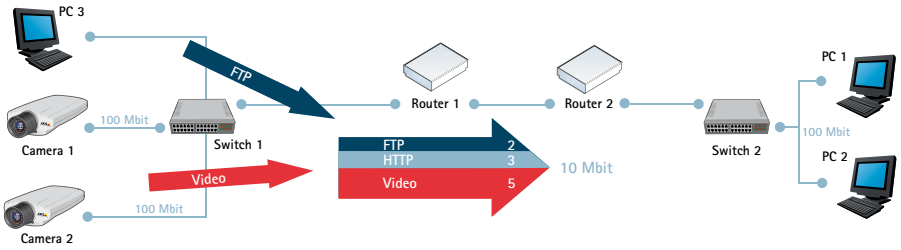


Figure 9.4b *QoS aware network. Here, Router 1 has been configured to devote up to 5 Mbit/s of the available 10 Mbit/s for streaming video. FTP traffic is allowed to use 2 Mbit/s, and HTTP and all other traffic can use a maximum of 3 Mbit/s. Using this division, video streams will always have the necessary bandwidth available. File transfers are considered less important and get less bandwidth, but there will still be bandwidth available for web browsing and other traffic. Note that these maximums only apply when there is congestion on the network. If there is unused bandwidth available, this can be used by any type of traffic.*

9.5 Network Security

There are different levels of security when it comes to securing information being sent over IP networks. The first is authentication and authorization. The user or device identifies itself to the network and the remote end by a username and password, which are then verified before the device is allowed into the system. Added security can be achieved by encrypting the data to prevent others from using or reading the data. Common methods are HTTPS (also known as SSL/TLS), VPN and WEP or WPA in wireless networks. *(For more on wireless security, see Chapter 10.)* The use of encryption can slow down communications, depending on the kind of implementation and encryption used.

9.5.1 Username and password authentication

Using a username and password authentication is the most basic method of protecting data on an IP network and may be sufficient where high levels of security are not required, or where the video network is segmented off from the main network and unauthorized users would not have physical access to the video network. The passwords can be encrypted or unencrypted when they are sent; the former provides the best security.

Axis network video products provide multi-level password protection. Three levels are available: Administrator (full access to all functionalities), Operator (Access to all functionalities except the configuration pages), Viewer (Access only to live video).

9.5.2 IP address filtering

Axis network video products provide IP address filtering, which gives or denies access rights to defined IP addresses. A typical configuration is to configure the network cameras to allow only the IP address of the server that is hosting the video management software to access the network video products.

9.5.3 IEEE 802.1X

Many Axis network video products support IEEE 802.1X, which provides authentication to devices attached to a LAN port. IEEE 802.1X establishes a point-to-point connection or prevents access from the LAN port if authentication fails. IEEE 802.1X prevents what is called "port hi-jacking"; that is, when an unauthorized computer gets access to a network by getting to a network jack inside or outside a building. IEEE 802.1X is useful in network video applications since network cameras are often located in public spaces where an openly accessible network jack can pose a security risk. In today's enterprise networks, IEEE 802.1X is becoming a basic requirement for anything that is connected to a network.

In a network video system, IEEE 802.1X can work as follows: 1) A network camera sends a request for network access to a switch or access point; 2) the switch or access point forwards the query to an authentication server; for instance, a RADIUS (remote authentication dial-in user service) server such as a Microsoft Internet Authentication Service server; 3) if authentication is successful, the

server instructs the switch or access point to open the port to allow data from the network camera to pass through the switch and be sent over the network.

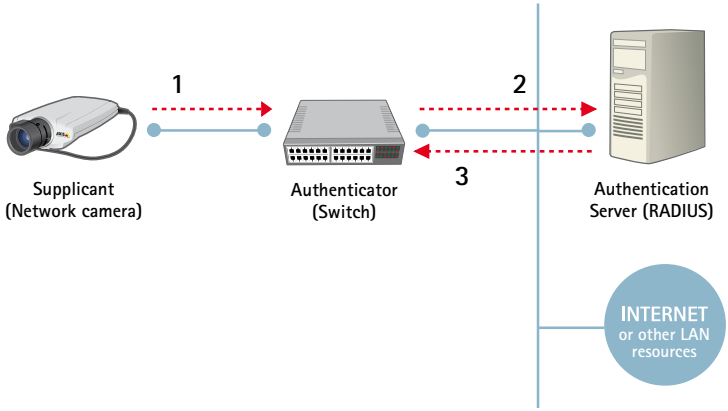


Figure 9.5a *IEEE 802.1X enables port-based security and involves a supplicant (e.g., a network camera), an authenticator (e.g., a switch) and an authentication server. Step 1: network access is requested; step 2: query forwarded to an authentication server; step 3: authentication is successful and the switch is instructed to allow the network camera to send data over the network.*

9.5.4 HTTPS or SSL/TLS

HTTPS (Hyper Text Transfer Protocol Secure) is identical to HTTP but with one key difference: the data transferred is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). This security method applies encryption to the data itself. Many Axis network video products have built-in support for HTTPS, which makes it possible for video to be securely viewed using a web browser. The use of HTTPS, however, can slow down the communication link and, therefore, the frame rate of the video.

9.5.5 VPN (Virtual Private Network)

With VPN, a secure "tunnel" between two communicating devices can be created, enabling safe and secure communication over the Internet. In such a set up, the original packet, including the data and its header, which may contain information such as the source and destination addresses, the type of information being sent, the packet number in the sequence of packets and the packet length, is encrypted. The encrypted packet is then encapsulated in another packet that shows only the IP addresses of the two communicating devices (i.e., routers). This set up protects the traffic and its contents from unauthorized access, and only devices with the correct "key" will be able to work within the VPN. Network devices between the client and the server will not be able to access or view the data.

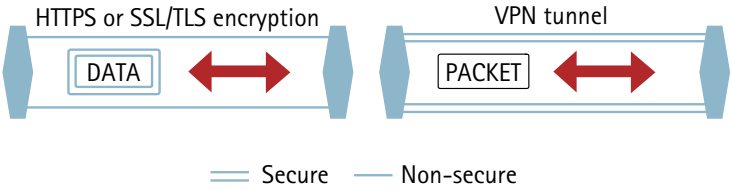


Figure 9.5b *The difference between HTTPS (SSL/TLS) and VPN is that in HTTPS only the actual data of a packet is encrypted. With VPN, the entire packet can be encrypted and encapsulated to create a secure "tunnel". Both technologies can be used in parallel, but it is not recommended since each technology will add overhead and decrease the performance of the system.*

Wireless technologies

For video surveillance applications, wireless technology offers a flexible, cost-efficient and quick way to deploy cameras, particularly over a large area as in a parking lot or a city center surveillance application. There would be no need to pull a cable through the ground. In older, protected buildings, wireless technology may be the only alternative if standard Ethernet cables may not be installed.

Axis offers cameras with built-in wireless support. Network cameras without built-in wireless technology can still be integrated into a wireless network if a wireless bridge is used.

Figure 10a *An Axis wireless network camera using 802.11b/g.*

Figure 10b *By using a wireless bridge, any network camera can be used in a wireless network.*

10.1 802.11 WLAN standards

The most common wireless standard for wireless local area networks (WLAN) is the 802.11 standard by IEEE. While there are also other standards as well as proprietary technologies, the benefit of 802.11 wireless standards is that they all operate in a license-free spectrum, which means there is no license fee associated with setting up and operating the network. The most relevant extensions of the standards are 802.11b, 802.11g, 802.11a and 802.11n.

.

802.11b, which was approved in 1999, operates in the 2.4 GHz range and provides data rates up to 11 Mbit/s. Until 2004, most WLAN products sold were based on 802.11b.

802.11g, which was approved in 2003, is the most common 802.11 variant on the market. It operates in the 2.4 GHz range and provides data rates of up to 54 Mbit/s. WLAN products are usually 802.11b/g compliant.

802.11a, which was approved in 1999, operates in the 5 GHz frequency range and provides data rates of up to 54 Mbit/s. An issue with the 5 GHz frequency range is that it is not available for use in parts of Europe where it is allocated for military radar systems. In such areas, 5 GHz WLAN components should conform to 802.11a/h standard. Another disadvantage with 802.11a is that its signal range is shorter than 802.11g's because it operates on a higher frequency; consequently, many more access points are required for transmission in the 5 GHz range than in the 2.4 GHz range.

802.11n, which is not yet completed and ratified, is the next generation standard that will enable data rates of up to 600 Mbit/s. Products supporting 802.11n are based on a draft of the standard.

When setting up a wireless network, the bandwidth capacity of the access point and the bandwidth requirements of the network devices should be considered. In general, the useful data throughput supported by a particular WLAN standard is about half the bit rate stipulated by a standard due to signaling and protocol overhead. With network cameras that support 802.11g, no more than four to five of such cameras should be connected to a wireless access point.

10.2 WLAN security

Due to the nature of wireless communications, anyone with a wireless device that is present within the area covered by a wireless network can share the network and intercept data being transferred over it unless the network is secured.

To prevent unauthorized access to the data transferred and to the network, some security technologies such as WEP and WPA/WPA2 have been developed to prevent unauthorized access and encrypt data sent over the network.

10.2.1 WEP (Wired Equivalent Privacy)

WEP prevents people without the correct key from accessing the network. There are, however, weaknesses in WEP. They include keys that are relatively short and other flaws that allow keys to be reconstructed from a relatively small amount of intercepted traffic. WEP today is no longer considered to provide adequate security as there are a variety of utilities freely available on the web that can be used to crack what is meant to be a secret WEP key.

10.2.2 WPA/WPA2 (WiFi Protected Access)

WPA significantly increases security by taking care of the shortcomings in the WEP standard. WPA adds a standard way for distributing encrypted keys.

10.2.3 Recommendations

Some security guidelines when using wireless cameras for surveillance:

> Enable the user/password login in the cameras.

> Enable the encryption (HTTPS) in the wireless router/cameras. This should be done before the keys or credentials are set for the WLAN to prevent unauthorized access to the network with stolen credentials.

> Ensure that wireless cameras support security protocols such as IEEE 802.1X and WPA/WPA2.

10.3 Wireless bridges

Some solutions may use other standards than the dominating IEEE 802.11, providing increased performance and much longer distances in combination with very high security. Two commonly used technologies are microwave and laser, which can be used to connect buildings or sites with a point-to-point high-speed data link.

Video management systems

An important aspect of a video surveillance system is managing video for live viewing, recording, playback and storage. If the system consists of only one or a few cameras, viewing and some basic video recording can be managed via the built-in web interface of the network cameras and video encoders. When the system consists of more than a few cameras, using a network video management system is recommended.

Today, several hundred different video management systems are available, covering different operating systems (Windows, UNIX, Linux and Mac OS), market segments and languages. Considerations include choice of hardware platform (PC server-based or one based on a network video recorder); software platform; system features, including installation and configuration, event management, intelligent video, administration and security; and integration possibilities with other systems such as point of sale or building management.

11.1 Hardware platforms

There are two different types of hardware platforms for a network video management system: a PC server platform involving one or more PCs that run a video management software program, and one based on a network video recorder (NVR), which is a proprietary hardware with pre-installed video management software.

11.1.1 PC server platform

A video management solution based on a PC server platform involves PC servers and storage equipment that can be selected off the shelf to obtain the maximum performance for the specific design of the system. Such an open platform makes it easier to add functionality to the system, such as increased or external storage, firewalls, virus protection and intelligent video algorithms, in parallel with a video management software program.

A PC server platform is also fully scalable, enabling any number of network video products to be added to the system as needed. The system hardware can be expanded or upgraded to meet increased performance requirements. An open platform also enables easier integration with

other systems such as access control, building management, and industrial control. This allows users to manage video and other building controls through a single program and user interface. *For more on servers and storage, see Chapter 12.*

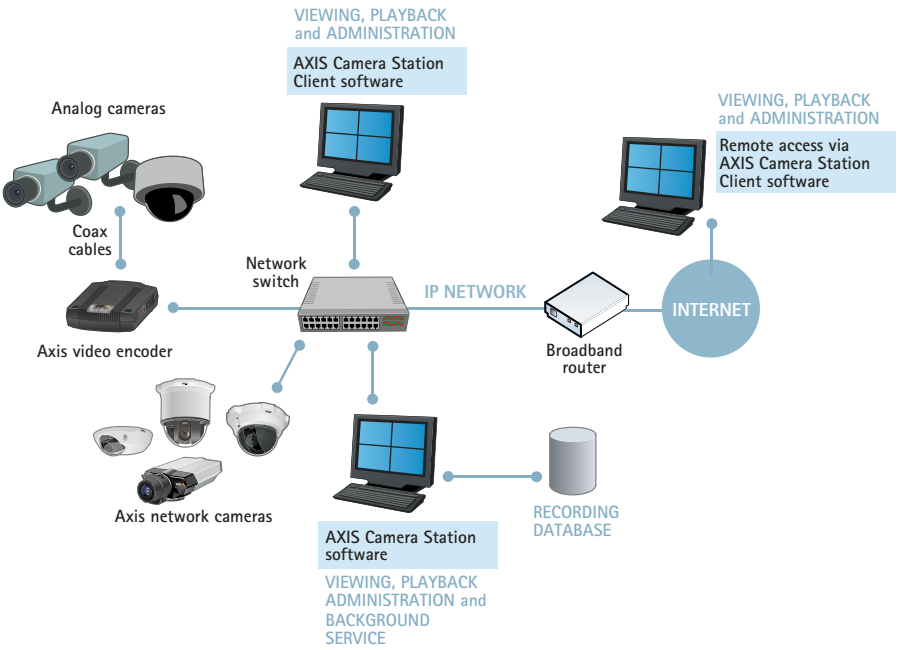


Figure 11.1a *A network video surveillance system based on a open, PC server platform with AXIS Camera Station video management software.*

11.1.2 NVR platform

A network video recorder comes as a hardware box with preinstalled video management functionalities. In this sense, an NVR is similar to a DVR. (Some DVRs, often called hybrid DVRs, also include an NVR function; i.e., the ability to also record network-based video.)

An NVR hardware is often proprietary and specifically designed for video management. It is dedicated to its specific tasks of recording, analyzing and playing back network video, and often does not allow for any other applications to reside on them. The operating system can be Windows, UNIX/Linux or proprietary.

An NVR is designed to offer optimal performance for up to a set number of cameras, and is normally less scalable than a PC server-based system. This makes the unit suitable for smaller

systems where the number of cameras stays within the limits of an NVR's designed capacity. An NVR is normally easier to install than a system based on a PC server platform.

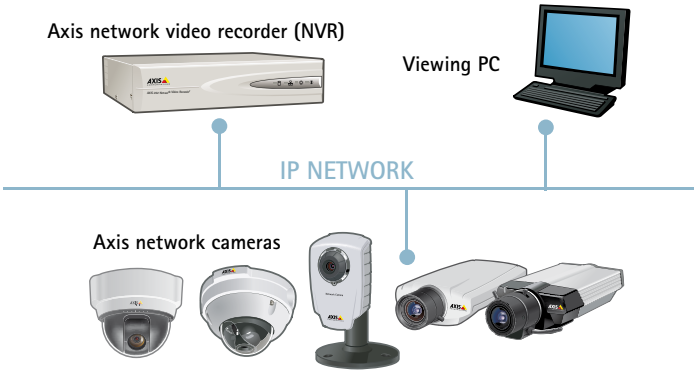


Figure 11.1b *A network video surveillance system that uses an NVR.*

11.2 Software platforms

Different software platforms can be used to manage video. They include using the built-in web interface, which exists in many network video products, or using a separate video management software program that is either a Windows-based or a web-based interface.

11.2.1 Built-in functionality

Axis network cameras and video encoders can be accessed over a network simply by typing the product's IP address in the Address/Location field of a web browser on a computer. Once a connection is made with the network video product, the product's 'start page', along with links to the product's configuration pages, is automatically displayed in the web browser.

The built-in web interface of Axis network video products provides simple recording functions; that is, manual recording of video streams (H.264, MPEG-4, Motion JPEG) to a server by clicking an icon, or event-triggered recording of individual JPEG images to one or several locations. Event-triggered recording of video streams is possible with network video products that support local storage. In such cases, the video streams are recorded onto the products' SD/SDHC card. For greater recording flexibility in terms of modes (e.g., continuous or scheduled recordings) and functionalities, a separate video management software program is required. Configuring and managing a network video product through its built-in web interface works when only a small number of cameras are involved in a system.

11.2.2 Windows client-based software

When it comes to separate software programs for video management, Windows client-based programs are the most popular. Web-based software programs are also available.

With a Windows client-based program, the video management software must first be installed on the recording server. Then a viewing client software program can be installed on the same recording server or any other PC, whether locally on the same network where the recording server resides, or remotely at a viewing station located on a separate network. In some cases, the client application also enables users to switch between different servers that have the video management software installed, thus making the management of video in a large system or at many remote sites possible.

11.2.3 Web-based software

A web-based video management software program must be installed first on a PC server that serves as both a web and recording server. It then allows users on any type of networked computer anywhere in the world, to access the video management server and thereby, the network video products it manages, simply by using a web browser.

11.2.4 Scalability of video management software

The scalability of most video management software, in terms of the number of cameras and frames per second that can be supported, is in most cases limited by the hardware capacity rather than the software. Storing video files puts new strains on the storage hardware because it may be required to operate on a continual basis, as opposed to only during normal business hours. In addition, video by nature generates large amounts of data, which put high demands on the storage solution. *For more on servers and storage, see Chapter 12.*

11.2.5 Open vs. vendor-specific software

Video management software programs are available from vendors of network video products. They often support only the network video devices of the vendor. Software programs that support multiple brands of network video products also exist, often from independent companies. A variety of software solutions are available from more than 550 Axis' Application Development Partners. *See www.axis.com/partner/adp*

11.3 System features

A video management system can support many different features. Some of the more common ones are listed below:

> Simultaneous viewing of video from multiple cameras
> Recording of video and audio
> Event management functions including intelligent video such as video motion detection
> Camera administration and management
> Search options and playback
> User access control and activity (audit) logging

11.3.1 Viewing

A key function of a video management system is enabling live and recorded video to be viewed in efficient and user-friendly ways. Most video management software applications enable multiple users to view in different modes such as split view (to view different cameras at the same time), full screen or camera sequence (where views from different cameras are displayed automatically, one after the other).

Figure 11.3a *AXIS Camera Station's live view screen.*

Many video management software programs also offer a multi-camera playback feature, which enables users to view simultaneous recordings from different cameras. This provides users with an ability to obtain a comprehensive picture of an event, which is helpful in an investigation. Additional features may be multi-monitor viewing and mapping, which overlays camera icons that represent the locations of cameras on a map of a building or area.

11.3.2 Multi-streaming

Axis' advanced network video products enable multi-streaming, where multiple video streams from a network camera or video encoder can be individually configured with different frame rates, compression formats and resolutions, and sent to different recipients. This capability optimizes the use of network bandwidth.

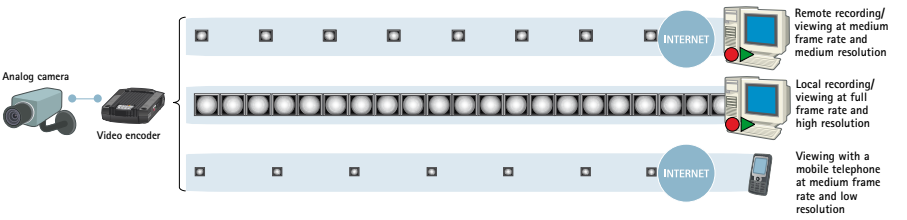


Figure 11.3b *Multiple, individually configurable video streams enable different frame rate video and resolution to be sent to different recipients.*

11.3.3 Video recording

With video management software such as AXIS Camera Station, video can be recorded manually, continuously and on trigger (by motion or alarm), and continuous and triggered recordings can be scheduled to run at selected times during each day of the week.

Continuous recording normally uses more disk space than an alarm-triggered recording. An alarm-triggered recording may be activated by, for example, video motion detection or external inputs through a camera's or video encoder's input port. With scheduled recordings, timetables for both continuous and alarm/motion-triggered recordings can be set.

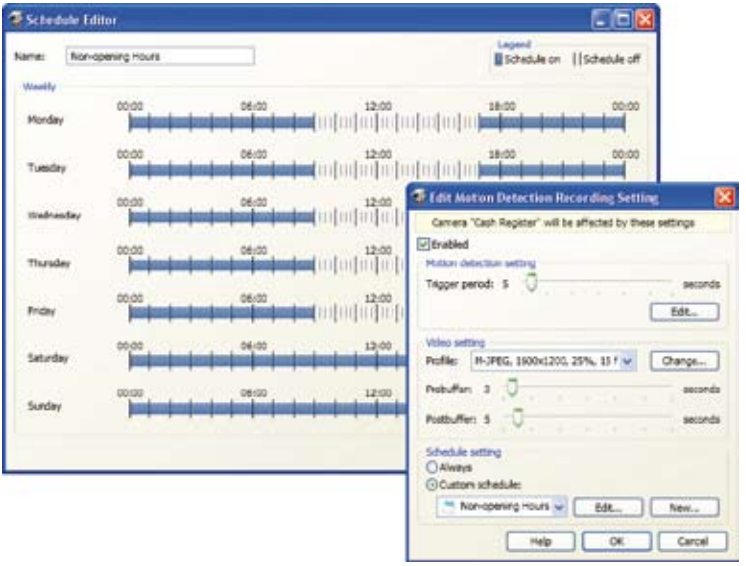


Figure 11.3c *Scheduled recording settings with a combination of continuous and alarm/motion-triggered recordings applied using AXIS Camera Station video management software.*

Once the type of recording method is selected, the quality of the recordings can be determined by selecting the video format (e.g., H.264, MPEG-4, Motion JPEG), resolution, compression level and frame rate. These parameters will affect the amount of bandwidth used, as well as the size of storage space required.

Network video products may have varying frame rate capabilities depending on the resolution. Recording and/or viewing at full frame rate (considered as 30 frames per second in NTSC standard and 25 frames per second in PAL standard) on all cameras at all times is more than what is required for most applications. Frame rates under normal conditions can be set lower—for example, 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 separate stream with a higher recording frame rate can be sent.

11.3.4 Recording and storage

Most video management software use the standard Windows file system for storage, so any system drive or network-attached drive can be used for storing video. A video management software program may enable more than one level of storage; for instance, recordings are made on a primary hard drive (the local hard disk) and archiving takes place on either local disks, network-attached drive or remote hard drive. Users may be able to specify how long images should remain on the primary hard drive before they are automatically deleted or moved to the archive drive. Users may also be able to prevent event-triggered video from being deleted automatically by specially marking or locking them in the system.

11.3.5 Event management and intelligent video

Event management is about identifying or creating an event that is triggered by inputs, whether from built-in features in the network video products or from other systems such as point-of-sale terminals or intelligent video software, and configuring the network video surveillance system to automatically respond to the event by, for example, recording video, sending alert notifications and activating different devices such as doors and lights.

Event management and intelligent video functionalities can work together to enable a video surveillance system to more efficiently use network bandwidth and storage space. Live camera monitoring is not required all the time since alert notifications to operators can be sent when an event occurs. All configured responses can be activated automatically, improving response times. Event management helps operators cover more cameras.

Both event management and intelligent video functionalities can be built-in and conducted in a network video product or in a video management software program. It can also be handled by both in the sense that a video management software program can take advantage of an intelligent video functionality that is built into a network video product. In such a case, the intelligent video functionality, such as video motion detection and camera tampering, can be performed by the

network video product and flagged to the management software program for further actions to be taken. This process offers a number of benefits:

> It enables a more efficient use of bandwidth and storage space since there is no need for a camera to continuously send video to a video management server for analysis of any potential events. Analysis takes place at the network video product and video streams are sent for recording and/or viewing only when an event occurs.

> It does not require the video management server to have a fast processing capability, thereby providing some cost-savings. Conducting intelligent video algorithms is CPU intensive.

> Scalability can be achieved. If a server were to perform intelligent video algorithms, only a few cameras can be managed at any given time. Having the intelligent functionality "at the edge", i.e. in the network camera or video encoder, enables a fast response time and a very large number of cameras to be managed proactively.

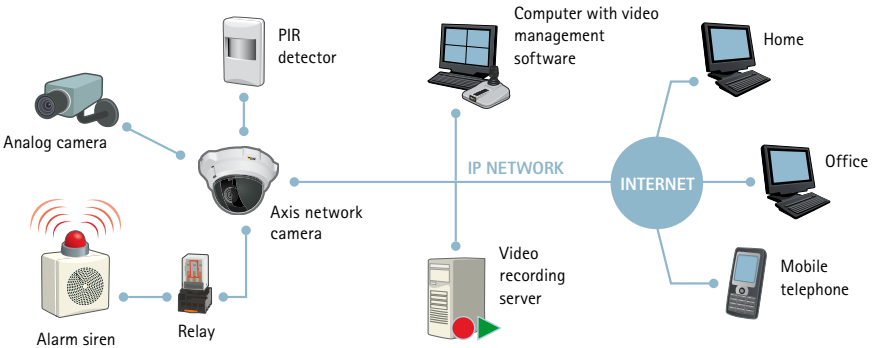


Figure 11.3d *Event management and intelligent video enable a surveillance system to be constantly on guard in analyzing inputs to detect an event. Once an event is detected, the system can automatically respond with actions such as video recording and sending alerts.*

Event triggers

An event can be scheduled or triggered. Events can be triggered by, for example:

> **Input port(s)**: The input port(s) on a network camera or video encoder can be connected to external devices such as a motion sensor or a door switch.

> **Manual trigger**: An operator can make use of buttons to manually trigger an event.

> **Video motion detection**: When a camera detects certain movement in a camera's motion detection window, an event can be triggered. *For more on video motion detection see page 102.*

> **Camera tampering**: This feature, which allows a camera to detect when it has been intentionally covered, moved or is no longer in focus, can be used to trigger an event. *For more on active tampering alarm, see page 102.*

> **Audio trigger**: This enables a camera with built-in audio support to trigger an event if it detects audio below or above a certain threshold. *For more on audio detection, see Chapter 8.*

> **Temperature**: If the temperature rises or falls outside of the operating range of a camera, an event can be triggered.

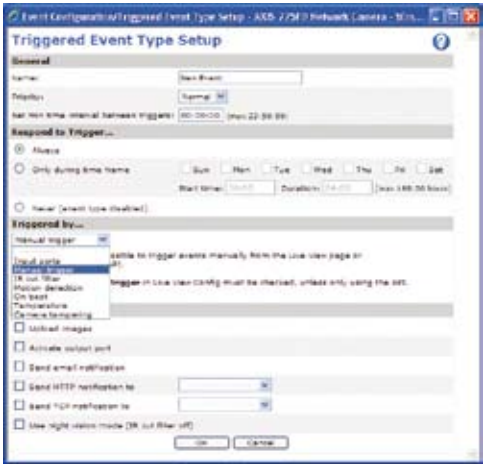


Figure 11.3e *Setting event triggers using an Axis network video product web interface.*

Responses

Network video products or a video management software program can be configured to respond to events all the time or at certain set times. When an event is triggered, some of the common responses that can be configured include the following:

> Upload images or recording of video streams to specified location(s) and at a certain frame rate. When using the event-triggered functionality in Axis network video products' web interface, only JPEG images can be uploaded. When using a video management software program, a video stream with a specified compression format (H.264/MPEG-4/Motion JPEG) and compression level can be requested from the network video product.

> Activate output port: The output port(s) on a network camera or video encoder can be connected to external devices such as alarms. (More details are provided below on output ports.)

> Send e-mail notification: This notifies users that an event has occurred. An image can also be attached in the e-mail.

> Send HTTP/TCP notification: This is an alert to a video management system, which can then, for example, initiate recordings.

> Go to a PTZ preset: This feature may be available with PTZ cameras or PTZ domes. It enables the camera to point to a specified position such as a window when an event takes place.

> Send an SMS (Short Message Service) with text information about the alarm or an MMS (Multimedia Messaging Service) with an image showing the event.

> Activate an audio alert on the video management system.

> Enable on-screen pop-up, showing views from a camera where an event has been activated.

> Show procedures that the operator should follow.

In addition, pre-alarm and post-alarm image buffers can be set, enabling a network video product to send a set length and frame rate of video captured before and after an event is triggered. This can be beneficial in helping to provide a more complete picture of an event.

Input/Output ports

A unique feature to network cameras and video encoders, in comparison with analog cameras, is their integrated input and output (I/O) ports. These ports enable a network video product to connect to external devices and enable the devices to be manageable over a network. For instance, a network camera or video encoder that is connected to an external alarm sensor via its input port can be instructed to only send video when the sensor triggers.

The range of devices that can be connected to a network video product's input port is almost infinite. The basic rule is that any device that can toggle between an open and closed circuit can be connected to a network camera or a video encoder. The main function of a network video product's output port is to trigger external devices, either automatically or by remote control from an operator or a software application.

Device type	Description	Usage
Door contact	Simple magnetic switch that detects the opening of doors or windows.	When the circuit is broken (door is opened), images/video as well as notifications can be sent from the camera.
Passive infrared detector (PIR)	A sensor that detects motion based on heat emission.	When motion is detected, the PIR breaks the circuit and images/video as well as notifications can be sent from the camera.
Glass break detector	An active sensor that measures air pressure in a room and detects sudden pressure drops. (The sensor can be powered by the camera.)	When a drop in air pressure is detected, the detector breaks the circuit, and images/video as well as notifications can be sent from the camera.

Table 11.3a *Example of devices that can be connected to the input port.*

Device type	Description	Usage
Door relay	A relay (solenoid) that controls the opening and closing of door locks.	The locking/unlocking of a door can be controlled by a remote operator (over a network) or be an automatic response to an alarm event.
Siren	Alarm siren configured to sound when alarm is detected.	The network video product can activate the siren either when motion is detected using the built-in video motion detection or using "information" from the digital input.
Alarm/intrusion system	An alarm security system that continuously monitors a normally closed or open alarm circuit.	The network video product can act as an integrated part of the alarm system that serves as a sensor, enhancing the alarm system with event-triggered video transfers.

Table 11.3b *Example of devices that can be connected to the output port.*

Video motion detection

Video motion detection (VMD) is a common feature in video management systems. It is a way of defining activity in a scene by analyzing image data and differences in a series of images. With VMD, motion can be detected in any part of a camera's view. Users can configure a number of "included" windows (a specific area in a camera's view where motion is to be detected), and "excluded" windows (areas within an "included" window that should be ignored). Using VMD helps to prioritize recordings, decrease the amount of recorded video and make searching for events easier.

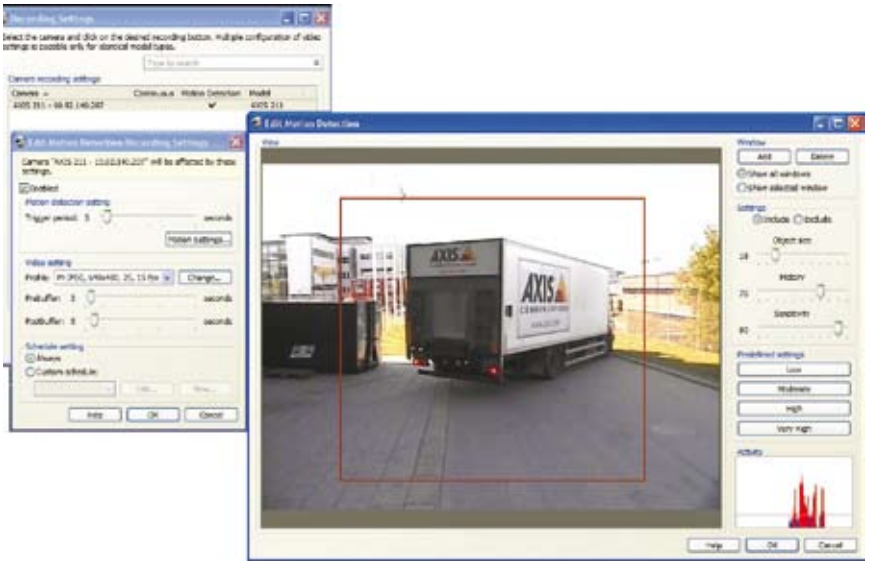


Figure 11.3f *Setting video motion detection in AXIS Camera Station video management software.*

Active tampering alarm

This intelligent video functionality, embedded in many Axis network video products, can be used as an event trigger when a camera is manipulated in any way; for instance, through accidental redirection, blocking, defocusing or being spray-painted, covered or damaged. Without such detection, surveillance cameras can become of limited use.

11.3.6 Administration and management features

All video management software applications provide the ability to add and configure basic camera settings, frame rate, resolution and compression format, but some also include more advanced functionalities, such as camera discovery and complete device management. The larger a video surveillance system becomes, the more important it is to be able to efficiently manage networked devices.

Software programs that help simplify the management of network cameras and video encoders in an installation often provide the following functionalities:

> Locating and showing the connection status of video devices on the network
> Setting IP addresses
> Configuring single or multiple units
> Managing firmware upgrades of multiple units
> Managing user access rights
> Providing a configuration sheet, which enables users to obtain, in one place, an overview of all camera and recording configurations.

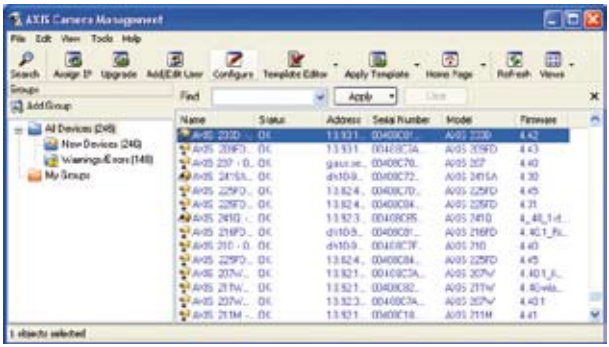


Figure 11.3g *AXIS Camera Management software makes it easy to find, install and configure network video products.*

11.3.7 Security

An important part of video management is security. A network video product or video management software should enable the following to be defined or set:

> Authorized users
> Passwords
> Different user-access levels, for example:
  - Administrator: access to all functionalities (In the AXIS Camera Station software, for instance, an administrator can select which cameras and functionalities a user may have access to.)
  - Operator: access to all functionalities except for certain configuration pages
  - Viewer: access only to live video from selected cameras

11.4 Integrated systems

When video is integrated with other systems such as point-of-sale and building management, 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.

11.4.1 Application programming interface

All Axis network video products have an HTTP-based application programming interface (API) or network interface called VAPIX®, which makes it easier for developers to build applications that support the network video products. A video management software program or building management system that uses VAPIX® will be able to request images from Axis network video products, control network camera functions (e.g., PTZ and relays) and set or retrieve internal parameter values. In effect, it allows a system to do everything that the network video product's web interface provides and more, such as capturing uncompressed images in bitmap file format.

A global, open industry forum called ONVIF was established in early 2008 by Axis, Bosch and Sony to standardize the network interface of network video products. A standard network interface would ensure greater interoperability and more flexibility for end users when building multiple-vendor network video systems. *For more information, visit www.onvif.org.*

11.4.2 Point of Sale

The introduction of network video in retail environments has made the integration of video with point-of-sale (PoS) systems easier.

The integration enables all cash register transactions to be linked to actual video of the transactions. It helps catch and prevent fraud and theft from employees and customers. PoS exceptions such as returns, manually entered values, line corrections, transaction cancellations, co-worker purchases, discounts, specially tagged items, exchanges and refunds can be visually verified with the captured video. A PoS system with integrated video surveillance makes it easier to find and verify suspicious activities.

Event-based recordings can be applied. For instance, a PoS transaction or exception, or the opening of a cash register drawer, can be used to trigger a camera to record and tag the recording. The scene prior to and following an event can be captured using pre- and post-event recording buffers. Event-based recordings increase the quality of the recorded material, as well as reduce storage requirements and the amount of time needed to search for incidents.

Figure 11.4a *An example of a PoS system integrated with video surveillance. This screenshot displays the receipts together with video clips of the event. Picture courtesy of Milestone Systems.*

11.4.3 Access control

Integrating a video management system with a facility's access control system allows for facility and room access to be logged with video. For example, video can be captured at all doors when someone enters or exits a facility. This allows for visual verification when exceptional events occur. In addition, identification of tailgating events can also be made. Tailgating occurs when, for instance, the person who swipes his/her access card knowingly or unknowingly enables others to gain entry without having to swipe a card.

11.4.4 Building management

Video can be integrated into a building management system (BMS) that controls a number of systems ranging from heating, ventilation and air conditioning (HVAC) to security, safety, energy and fire alarm systems.

The following are some application examples:

> An equipment failure alarm can trigger a camera to show video to an operator, in addition to activating alarms at the BMS.

> A fire alarm system can trigger a camera to monitor exit doors and begin recording for security purposes.

> Intelligent video can be used to detect reverse flow of people into a building due to an open or unsecured door from events such as evacuations.

> Information from the video motion detection functionality of a camera that is located in a meeting room can be used with lighting and heating systems to turn the light and heat off once the room is vacated, thereby saving energy.

11.4.5 Industrial control systems

Remote visual verification is often beneficial and required in complex industrial automation systems. By having access to network video using the same interface as for monitoring a process, an operator does not have to leave the control panel to visually check on part of a process. In addition, when an operation malfunctions, the network camera can be triggered to send images. In some sensitive clean-room processes, or in facilities with dangerous chemicals, video surveillance is the only way to have visual access to a process. The same goes for electrical grid systems with a substation in a very remote location.

11.4.6 RFID

Tracking systems that involve RFID (radio-frequency identification) or similar methods are used in many applications to keep track of items. An example is luggage handling at airports that will keep track of the luggage and direct it to the correct destination. If it is integrated with video surveillance, there is visual evidence when luggage is lost or damaged, and search routines can be optimized.

Bandwidth and storage considerations

Network bandwidth and storage requirements are important considerations when designing a video surveillance system. The factors include the number of cameras, the image resolution used, the compression type and ratio, frame rates and scene complexity. This chapter provides some guidelines on designing a system, along with information on storage solutions and various system configurations.

12.1 Bandwidth and storage calculations

Network video products utilize network bandwidth and storage space based on their configuration. As mentioned earlier, this depends on the following:

- Number of cameras
- Whether recording will be continuous or event-based
- Number of hours per day the camera will be recording
- Frames per second
- Image resolution
- Video compression type: Motion JPEG, MPEG-4, H.264
- Scenery: Image complexity (e.g. gray wall or a forest), lighting conditions and amount of motion (office environment or crowded train stations)
- How long data must be stored

12.1.1 Bandwidth needs

In a small surveillance system involving 8 to 10 cameras, a basic 100-megabit (Mbit) network switch can be used without having to consider bandwidth limitations. Most companies can implement a surveillance system of this size using their existing network.

When implementing 10 or more cameras, the network load can be estimated using a few rules of thumb:

> A camera that is configured to deliver high-quality images at high frame rates will use approx. 2 to 3 Mbit/s of the available network bandwidth.

> With more than 12 to 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.

Technologies that enable the management of bandwidth consumption include the use of VLANs on a switched network, Quality of Service and event-based recordings. *For more on these topics, see chapters 9 and 11.*

12.1.2 Calculating storage needs

As mentioned earlier, the type of video compression used is one of the factors affecting storage requirements. 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% compared with the Motion JPEG format and as much as 50% more than with the MPEG-4 (Part 2) standard. This means much less network bandwidth and storage space are required for an H.264 video file.

Sample storage calculations for all three compression formats are provided in the tables below. Because of a number of variables that affect average bit rate levels, calculations are not so clear-cut for H.264 and MPEG-4. With Motion JPEG, there is a clear formula because Motion JPEG consists of one individual file for each image. Storage requirements for Motion JPEG recordings vary depending on the frame rate, resolution and level of compression.

H.264 calculation:
Approx. 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

Camera	Resolution	Approx. 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						

Table 12.1a *The figures above are based on lots of motion in a scene. With fewer changes in a scene, the figures can be 20% lower. The amount of motion in a scene can have a big impact on the amount of storage required.*

MPEG-4 calculation:

Approx. 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	Approx. 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						

Table 12.1b

Motion JPEG calculation:

Image size x frames per second 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

Camera	Resolution	Bit Rate (Kbit/s)	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						

Table 12.1c

A helpful tool in estimating requirements for bandwidth and storage is the AXIS Design Tool, which is accessible from the following web address: *www.axis.com/products/video/design_tool/*

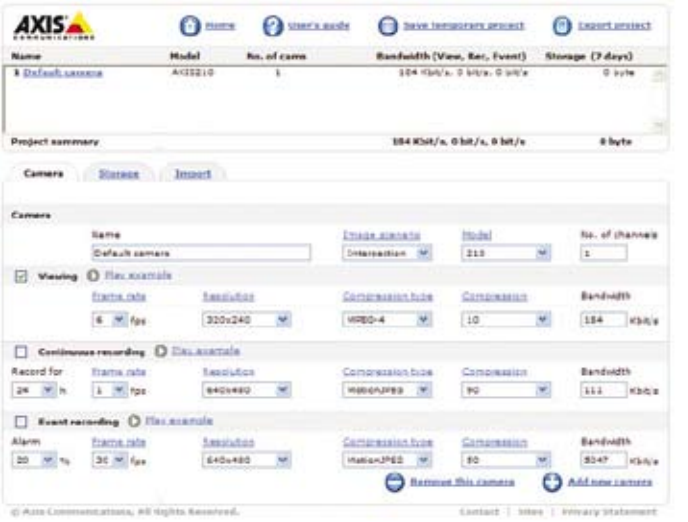


Figure 12.1a *The AXIS Design Tool includes advanced project management functionality that enables bandwidth and storage to be calculated for a large and complex system.*

12.2 Server-based storage

Depending on a PC server's central processing unit (CPU), network card and internal RAM (Random Access Memory), a server can handle a certain number of cameras, frames per second and size of images. Most PCs can hold between two and four hard disks, and each disk can be up to approx. 300 gigabyte (GB). In a small to medium-sized installation, the PC that runs the video management software is also used for video recording. This is called a direct-attached storage.

With the AXIS Camera Station video management software, for instance, one hard disk is suitable for storing recordings from six to eight cameras. With more than 12 to 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.

12.3 NAS and SAN

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.

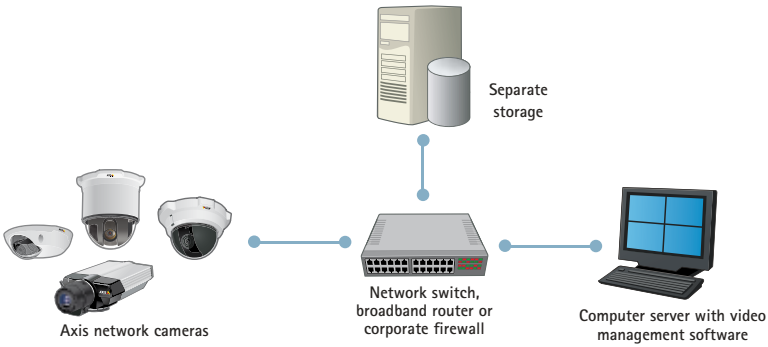


Figure 12.3a *Network-attached storage*

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. Fiber Channel technology is commonly used to provide data transfers at four gigabits per second and to allow large amounts of data to be stored with a high level of redundancy.

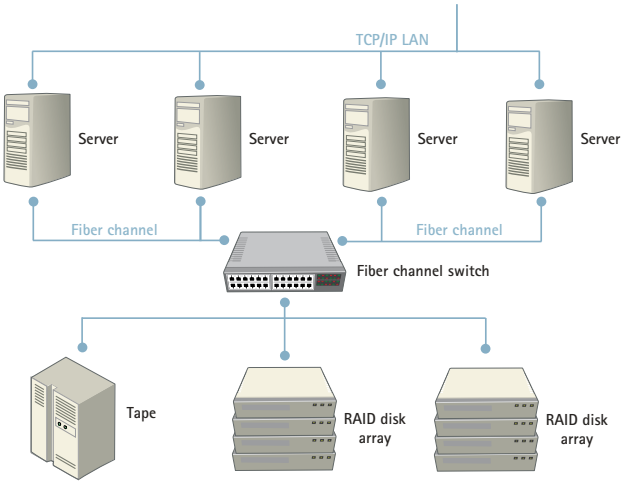


Figure 12.3b *A SAN architecture where storage devices are tied together and the servers share the storage capacity.*

12.4 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 setup 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.

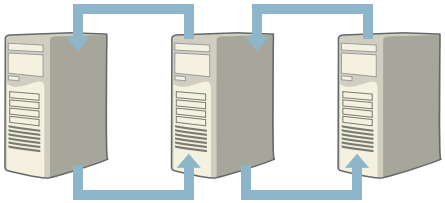


Figure 12.4a *Data replication.*

Data replication. This is a common feature in many network operating systems. File servers in a network are configured to replicate data among each other, providing a backup 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.

12.5 System configurations

Small system (1 to 30 cameras)

A small system usually consists of one server running a surveillance application that records the video to a local hard disk. The video is viewed and managed by the same server. Although most viewing and management will be done at the server, a client (local or remote) can be connected for the same purpose.

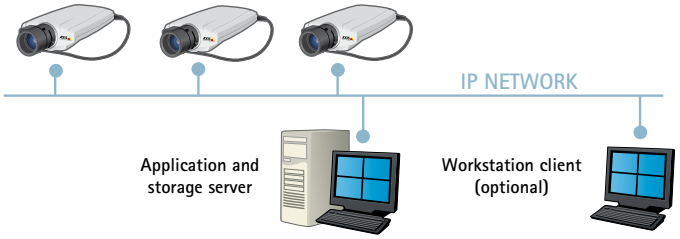


Figure 12.5a *A small system.*

Medium system (25 to 100 cameras)

A typical, medium-sized installation has a server with additional storage attached to it. The storage is usually configured with RAID in order to increase performance and reliability. The video is normally viewed and managed from a client rather than from the recording server itself.

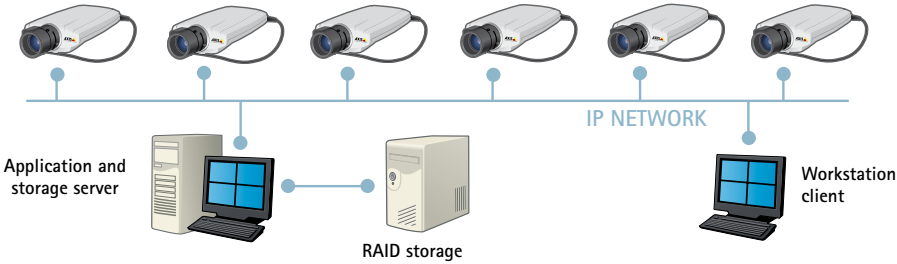


Figure 12.5b *A medium system.*

Large centralized system (50 to +1000 cameras)

A large-sized installation requires high performance and reliability in order to manage the large amount of data and bandwidth. This requires multiple servers with dedicated tasks. A master server controls the system and decides what kind of video is stored at what storage server. As there are dedicated storage servers, it is possible to do load balancing. In such a setup, it is also possible to scale up the system by adding more storage servers when needed and do maintenance without bringing down the entire system.

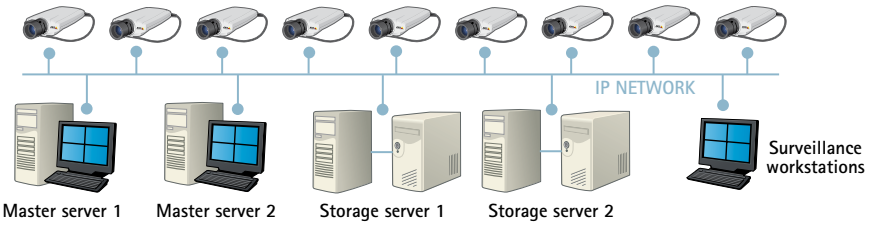


Figure 12.5c *A large centralized system.*

Large distributed system (25 to +1000 cameras)

When multiple sites require surveillance with centralized management, distributed recording systems may be used. Each site records and stores the video from local cameras. The master controller can view and manage recordings at each site.

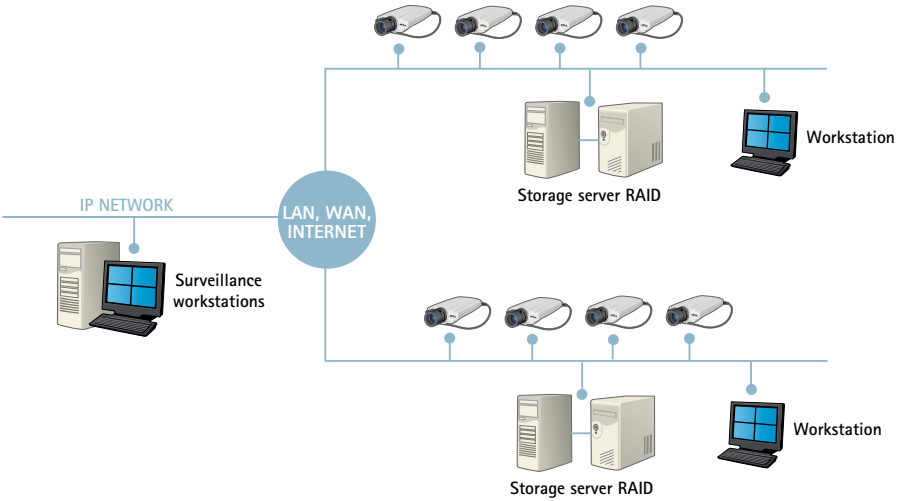


Figure 12.5d *A large distributed system.*

Tools and resources

Axis offers a variety of tools and information resources to help design IP-Surveillance systems. Many are accessible from the Axis website: *www.axis.com/tools*

Lens Calculators
This tool helps you calculate the focal length of the lens you will need in order to capture a specific scene at a certain distance.

Camera Reach Tool
This tool focuses on Axis network cameras' scene capturing and object recognition capabilities at different distances and in combination with alternate lenses. The tool also helps you navigate through the Axis product portfolio to find the most appropriate camera for your application.

AXIS Design Tool
This simulation-based calculation tool, available online or on a DVD, helps determine the bandwidth and storage needs for specific network video projects.

Axis Housing Configurator
This tool helps you find the right housings and complementary accessories such as brackets, power supplies and cables for your specific camera application.

Intelligent Network Video:
Understanding modern surveillance systems
This 390-page hardcover book is authored by Fredrik Nilsson and Axis Communications. It represents the first resource to provide detailed coverage of advanced digital networking and intelligent video capabilities. Published in September 2008, the book is available for purchase through Amazon, Barnes & Noble and CRC Press, or contact your local Axis office.

Axis Communications' Academy

Number one in network video knowledge.

Learn more about network video technologies with Axis' training program.

> Broad course offering
> Hands-on training
> Training from the leading experts
> Gain a competitive edge

The video surveillance market is changing as older analog systems converge towards network video technology. New technologies, applications and integration possibilities are driving the convergence. To succeed in this increasingly competitive market, you need superior skills and expertise on IP-based video solutions. Team up with Axis Communications' Academy to ensure that you are always a step ahead.

Learning the fundamentals
Network Video Fundamentals and Video Solution Fundamentals are the building blocks of the Axis Communications' Academy training program. The fundamentals have been developed and refined to meet the educational requirements of both traditional analog CCTV and IT professionals. Whatever your background, you can achieve the advanced technical proficiency you need to successfully work with and use Axis products and solutions.

For more information, visit www.axis.com/academy

Contact information

www.axis.com/request

CORPORATE HEADQUARTERS, SWEDEN
Axis Communications AB
Emdalavägen 14
SE-223 69 Lund
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

ARGENTINA
Axis Communications
Av. Del Libertador 2442, Piso 4,
CP B1636SR Olivos
Buenos Aires
Tel. +54 11 5368 0569
Fax +54 11 5368 2100 Int. 0569

AUSTRALIA
Axis Communications Pty Ltd.
Level 27, 101 Collins Street
Melbourne VIC 3000
Tel: +613 9221 6133

BRAZIL
Axis Communications
Rua Mario Amaral 172, 13º
Andar, Conjunto 131
04002-020, Sao Paulo
Tel. +55 11 3050 6600

CANADA
Axis Communications, Inc.
117 Lakeshore Road East
Suite 304
Mississauga ON L5G 4T6
Tel: +1 800 444 AXIS (2947)
Fax: +1 978 614 2100
Support: +1 800 444 2947

CHINA
Shanghai Axis Communications
Equipment Trading Co.,Ltd.
Room 6001, Novel Building
887 Huai Hai Zhong Rd.
Shanghai 200020
Tel: +86 21 6431 1690

Beijing Axis Communications
Rm. 2003, Tower B
Tian Yuan Gang Center C2
Dongsanhuan North Road
Chaoyang District
Beijing 100027
Tel: +86 10 8446 4990
Fax: +86 10 8286 2489

FRANCE, BELGIUM, LUXEMBURG
Axis Communications SAS
7–9 avenue Aristide Briand
94230 Cachan, France
Tel: +33 1 49 69 15 50
Fax: +33 1 49 69 15 59
Support: +33 1 49 69 15 50

GERMANY, AUSTRIA, SWITZERLAND
Axis Communications GmbH
Lilienthalstr. 25
DE-85399 Hallbergmoos
Tel: +49 811 555 08 0
Fax: +49 811 555 08 69
Support: +49 1805 2947 78

HONG KONG
Axis Communications Limited
Unit 1801, 18/F
88 Gloucester Road, Wanchai
Hong Kong
Tel: +852 2511 3001
Fax: +852 2511 3280

INDIA
Axis Video Systems India
Private Limited
Kheny Chambers
4/2 Cunningham Road
Bangalore 560002
Karnataka
Tel: +91 (80) 4157 1222
Fax: +91 (80) 4023 9111

ITALY
Axis Communications S.r.l.
Corso Alberto Picco, 73
10131 Torino
Tel: +39 011 819 88 17
Fax: +39 011 811 92 60

JAPAN
Axis Communications K.K.
Shinagawa East 1 Tower 13F
2-16-1 Konan
Minato-ku Tokyo 108-0075
Tel: +81 3 6716 7850
Fax: +81 3 6716 7851

Contact information

www.axis.com/request

KOREA
Axis Communications Korea Co., Ltd.
Rm 407, Life Combi B/D.
61-4 Yoido-dong
Yeongdeungpo-Ku, Seoul
Tel: +82 2 780 9636
Fax: +82 2 6280 9636

MEXICO
AXISNet, S.A. de C.V.
Unión 61, 2º piso
Col. Escandón, Mexico City
México, D.F., C.P. 11800
Tel: +52 55 5273 8474
Fax: +52 55 5272 5358

THE NETHERLANDS
Axis Communications BV
Glashaven 38
NL-3011 XJ Rotterdam
Tel: +31 10 750 46 00
Fax: +31 10 750 46 99
Support: +31 10 750 46 31

RUSSIAN FEDERATION
OOO Axis Communications
Leningradsky prospekt
31/3, of.405
125284, Moscow
Tel: +7 495 940 6682
Fax: +7 495 940 6682

SINGAPORE
Axis Communications
(S) Pte Ltd.
7 Temasek Boulevard
#11-01A Suntec Tower 1
Singapore 038987
Tel: +65 6 836 2777
Fax: +65 6 334 1218

SPAIN
Axis Communications
C/ Yunque 9, 1A
28760 Tres Cantos, Madrid
Tel: +34 91 803 46 43
Fax: +34 91 803 54 52
Support: +34 91 803 46 43

SOUTH AFRICA
Axis Communications SA
Pty Ltd.
Hampton Park, Atterbury
House, 20 Georgian Crescent
Bryanston, Johannesburg
Tel: +27 11 548 6780
Fax: +27 11 548 6799

PO Box 70939
Bryanston 2021

TAIWAN
Axis Communications Ltd.
8F-11,101 Fushing North Road
Taipei
Tel: +886 2 2546 9668
Fax: +886 2 2546 1911

UNITED ARAB EMIRATES
Axis Communications
Middle East
PO Box 293637
DAFZA, Dubai
Tel: +971 4 609 1873

UNITED KINGDOM
Axis Communications (UK) Ltd
Suite 6-7, Ladygrove Court
Hitchwood Lane
Preston, Nr Hitchin
Hertfordshire SG4 7SA
Tel: +44 146 242 7910
Fax: +44 146 242 7911
Support: +44 871 200 2071

UNITED STATES
Axis Communications Inc.
100 Apollo Drive
Chelmsford, MA 01824
Tel: +1 978 614 2000
Fax: +1 978 614 2100
Support: +1 800 444 2947

www.axis.com

33334/EN/R2/0811

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 NASDAQ OMX Stockholm under the ticker AXIS. For more information about Axis, please visit our website at www.axis.com.