Technical guide to network video

June 2025

Introduction

We created this *Technical guide to network video* to support you in your work with Axis network video surveillance systems and to help you keep up with the changing technology landscape. Our guide is intended as a comprehensive resource for anyone involved in developing, implementing, and maintaining Axis video surveillance systems. It provides a complete overview of network video surveillance, and covers recent developments in cloud, analytics, and video management systems (VMS).

We hope you find *Technical guide to network video* useful!

Table of Contents

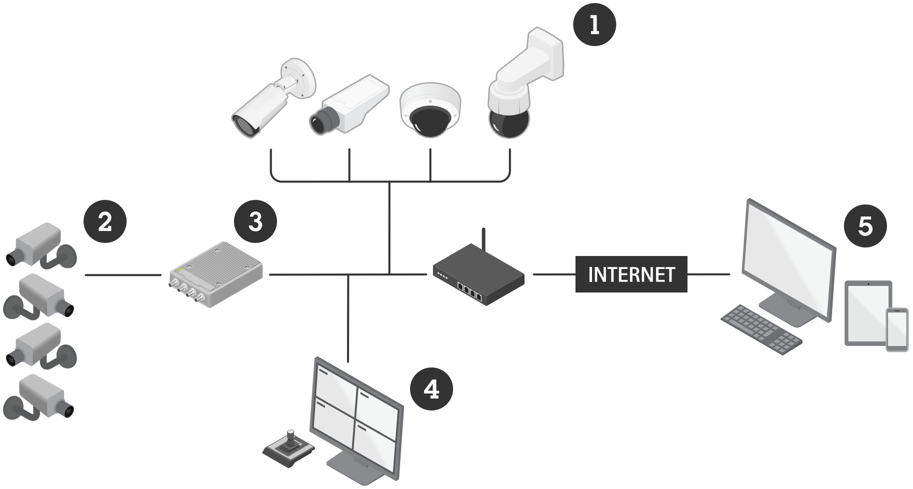
1. Network video: overview, benefits, and applications

A network video system uses standard IP-based networks for transporting video and audio. Digitized video and audio streams are sent over wired or wireless IP networks, enabling video monitoring and recording from anywhere on the network. With a multitude of advanced functionalities, network video has a lot to offer in security surveillance. The high-quality video, scalability, and built-in intelligence of network video enhance security personnel's ability to protect people, property, and assets.

1.1 Overview of a network video system

Network video, often also called *IP-based video surveillance* or *IP surveillance* as applied in the security industry, uses a wired or wireless IP network as the backbone for transporting digital video, audio, and other data. The network also carries power to the network video devices through Power over Ethernet (PoE) technology.

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



A network video system with network cameras (1), analog cameras (2) connected through video encoders (3), and video management software (4). Other components, including the network, storage, and servers, are all standard IT equipment. Remote access is possible from a computer or a mobile device (5).

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

The network, the server, and storage components are all common off-the-shelf equipment — one of the main benefits of network video. Other components include accessories, such as mounts, PoE midspans, and joysticks. Each network video component is covered in more detail in other chapters.

1.2 Benefits

A fully digital, network video surveillance system provides a host of advanced functionalities. Network video comes with high image quality, remote accessibility, analytics, easy integration possibilities, scalability, flexibility, cost-effectiveness, and secure communication.

> **High image quality.** In video surveillance, high image quality is essential to clearly capture an incident and to identify the persons or objects involved. With progressive scan and HDTV/

megapixel technologies, a network camera can deliver high image quality and high resolution. For more on image quality, see chapters , , and .

> **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. This is advantageous if you need a third party, such as an alarm monitoring center or law enforcement, to also have access to the video.

> **Analytics**. In network video, a camera can be much more than just a source of video. Analytics in the camera are used to extract the useful information from massive amounts of video and trigger instant, automatic actions when necessary. This may include notifying security staff or starting a video recording upon detection of specific events. Analytics that use deep learning algorithms for object detection and classification can extract very detailed information about people and vehicles in a scene, enabling extremely accurate and efficient searches. For more on analytics, see chapter .

> **Easy, future-proof integration**. Network video products based on open standards can be easily integrated into a wide array of video management systems. Video from a network camera can also be integrated into other systems, such as point-of-sales, access control, or a building management system. For more on integrated systems, see chapter .

> **Scalability and flexibility**. A network video system can grow with the user's needs. Video products and other types of applications share the same wired or wireless IP network for communicating data. Video, audio, PTZ and I/O commands, other data, and power are carried over the same cable, and any number of devices can be added to the system with no significant or costly changes to the network infrastructure. Devices can be placed and networked in virtually any location, and the system can be as open or as closed as desired. Since a network video system is based on standard IT equipment and protocols it can benefit from those technologies as the system grows. For instance, video can be stored on redundant servers placed in separate locations for greater reliability and security, and tools can be used for automatic load sharing, network management, and system maintenance.

> **Cost-effectiveness**. An IP surveillance system typically has a low total cost of ownership. The 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. Management and equipment costs are also low, since back-end applications and storage run on industry-standard, open systems-based servers, and not on proprietary hardware such as DVRs in the case of an analog CCTV system. Many network video devices are powered by Power over Ethernet (PoE) technology, which provides power through the same Ethernet cable that transports the data (video). PoE keeps installation costs down and facilitates backup. For more on PoE, see chapter .

> **Secure communication**. Network video devices, as well as their video streams, can be secured in many ways. These include user name and password authentication, IP address filtering, authentication using IEEE 802.1X, data encryption using HTTPS (SSL/TLS), and by using multiple user access levels. For more on network security, see chapter .

> **Increased security**. Axis devices are safeguarded by the hardware-based cybersecurity platform Axis Edge Vault, which minimizes a device's exposure to cybersecurity risks and enables it to be a trusted and reliable unit within the network. Axis Edge Vault enables cybersecurity features such as signed OS (guaranteeing that AXIS OS has not been compromised), secure boot (ensuring that unauthenticated or altered code is rejected during the boot process), and signed video (verifying video authenticity through a signature in the video stream).

Existing analog video installations can migrate to a network video system and take advantage of some of the digital benefits with the help of video encoders and devices such as Ethernet-over-coax adapters, which make use of legacy coax cables. For more on video encoders and decoders, see chapter .

1.3 Applications

Network video can be used in an almost unlimited number of applications. Most uses fall under security surveillance or remote monitoring of people, places, property, and operations. Increasingly, network video is also being used to improve business efficiency, as the number of analytics applications grows. The following are some typical application possibilities in key industry segments.

> **Retail**. Network video systems in retail stores can significantly reduce theft, improve staff security, and optimize store management.

> **Transportation**. Network video helps to protect passengers, staff, and assets in all types of transport.

> **Banking and finance**. Network video systems enable a bank to efficiently monitor its headquarters, branch offices, and ATM machines from a central location.

> **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.

> **Education**. From day-care centers to universities, network video systems help to deter vandalism and increase the safety of staff and students.

> **Government**. Network video can be used by law enforcement, the military, and border control. It is also an efficient means to secure all kinds of public buildings.

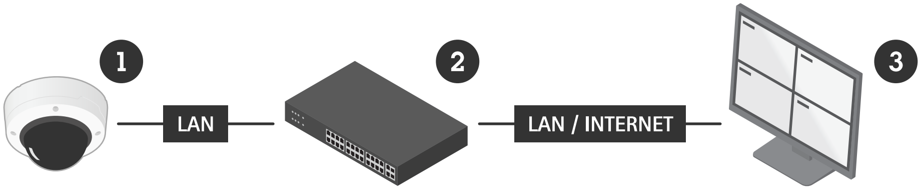
- **Healthcare**. Network video enables hospitals and healthcare facilities to improve the overall safety and security of staff, patients, and visitors.
- **Industrial**. Network video is not only an efficient tool for securing perimeters and premises, it can also be used to monitor and increase efficiency in manufacturing lines, processes, and logistics systems.
- **Critical infrastructure**. Whether a solar plant, an electrical substation, or a waste management facility, network video can help ensure safe, secure, and uninterrupted activity. Production data from remote sites can be enhanced with visual information.

2. Network cameras

Network cameras, or IP cameras, offer a wide variety of features and capabilities to meet the requirements of almost any surveillance system. This chapter provides a description of what a network camera is, the options and features it may have, and the various types of cameras available: fixed cameras, PTZ (pan-tilt-zoom) cameras, modular cameras, thermal cameras, and explosion-protected cameras.

2.1 What is a network camera?

A network camera, also known as an IP camera, is used primarily to send video/audio over an IP network such as a local area network (LAN) or the internet. A network camera enables live viewing and/or recording, either continuously, at scheduled times, on request, or when triggered by an event. Video can be saved locally and/or at a remote location, and authorized access to video can be made wherever there is access to an IP network.



A network camera (1) connects to a network switch (2) and video can be accessed (3) over the network.

A network camera can be described as a camera and computer combined in a single unit. The main components include a lens, an image sensor, one or more processors, and memory. The processors are used for image processing, compression, video analysis, and networking functionalities. The memory is used mainly for storing the device software, but also for storing video.

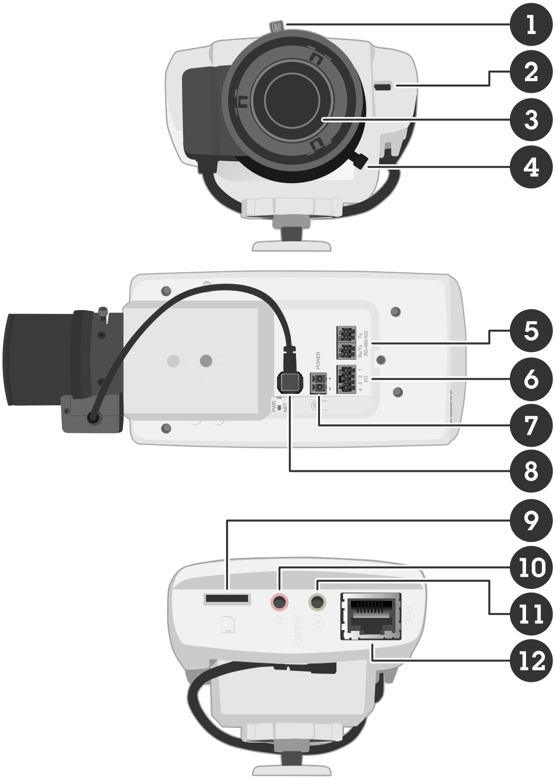
Like a computer, the camera has its own IP address, is connected directly to a wired or wireless network, and can be placed wherever there is a network connection. This differs from a web camera, which can only operate when connected to a PC.

In addition to capturing video, network cameras provide event management that enables you to program automatic responses to predefined events. Typical responses include sending live video and email alerts, activating devices such as doors and lights, and initiating video recordings. By recording only when something specific happens in the scene, you make more efficient use of network bandwidth and storage space.

Network cameras support analytics, which automatically extract what is important in the video stream and uses that to provide actionable insights. Analytics that are embedded in the camera (edge analytics) come with several advantages, such as reduced network transmission needs and low latency for scenarios that require a quick response. Axis Scene Intelligence technology combines advanced image processing technology with analytics on the edge and deep learning to create a superior foundation for consistent analytics performance. It also enables the camera to adapt automatically when circumstances change.

Many network cameras have support for audio. They can have audio input/output ports, or the possibility to connect audio devices through portcast technology or edge-to-edge technology (both of which provide seemingly camera-integrated audio). Network cameras also often offer input/output (I/O) ports that enable connections to other external devices such as motion sensors, door lock relays, and audio/visual alerters.

Most network video cameras are powered by Power over Ethernet (PoE) technology, which means that power is supplied through the network cable. They also have a memory card slot for local storage of recordings.



Front, underside, and back of a typical network camera.

1. Zoom puller

2. Internal microphone

3. P-Iris lens

4. Focus puller

5. Serial port

6. I/O terminal block

7. Power connector

8. Iris connector

9. Memory card slot

10. Audio in

11. Audio out

12. Network connector

Axis cameras are installed on a network through AXIS Camera Station Edge or AXIS Camera Station Pro, video management systems (VMS) that automatically detect and configure the camera. Advanced customers with large installations can use AXIS Device Manager to configure the cameras. It is also possible to access a camera directly through its built-in web pages by entering its IP address in a browser. Configuration concerns, for example, user access, camera settings, resolution, frame rate, compression format (H.264/H.265/AV1), as well as rules for events.

Axis cameras also support a host of accessories that extend their abilities. For example, cameras can be connected to a fiber optic network using a media converter switch, or to coax cables using an Ethernet-over-coax adapter with support for PoE.

2.1.1 AXIS Camera Application Platform (ACAP)

Most Axis cameras (and speakers, intercoms, and radar products) are supported by AXIS Camera Application Platform (ACAP). ACAP is an open application platform for a broad range of industries and use cases and it enables analytics applications, accessible from Axis website or from thirdparty suppliers. These applications can be downloaded and installed on the devices. ACAP also makes it possible to develop customized applications, and run applications on the edge (completely or partially) by combining advanced edge analytics and cloud or server-based technologies. For more on ACAP, see *www.axis.com/developer-community/acap*

2.1.2 Application programming interface

All Axis network video products have an application programming interface (API) called VAPIX®. VAPIX enables developers to easily integrate Axis video products and their built-in functionalities into other software solutions.

2.1.3 ONVIF

Most Axis network video products are ONVIF conformant. ONVIF®[1] is a global, open industry forum founded by Axis, Bosch, and Sony in 2008, and its aim is to standardize the network interface of network video and access control products of different manufacturers to ensure greater interoperability. It gives users the flexibility to use ONVIF conformant products from different manufacturers in a multi-vendor, IP-based physical security system. ONVIF is today endorsed by the majority of the world's largest manufacturers of IP-based physical security products, and has more than 500 member companies. For more information, visit *www.onvif.org*

[1] ONVIF is a trademark of ONVIF, Inc.

2.2 Camera features for handling difficult scenes

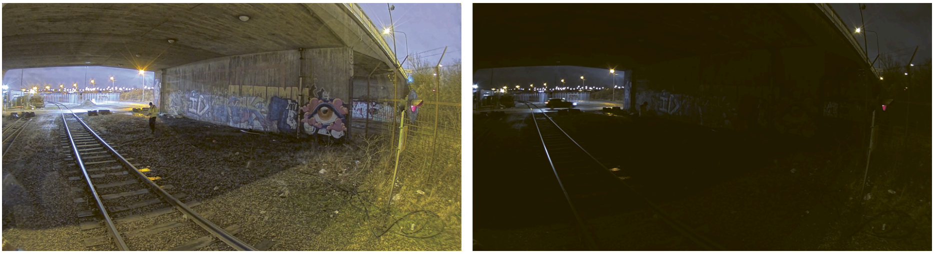
The video quality of security cameras may be negatively affected by challenging weather conditions or low or wide-ranging light levels. This chapter lists camera factors and features that impact the camera's ability to handle difficult scenes.

2.2.1 WDR

When the light level changes in the scene, an Axis camera automatically adjusts to ensure optimal exposure. For challenging situations with scenes that contain both bright and darker parts, the WDR (wide dynamic range) option is recommended. This is enabled by default and is the best way to use Axis cameras because it does not need adjustments over time. WDR often enables the camera to combine short exposure times in the bright parts of the scene with long exposure times in the dark areas. The resulting image is correctly exposed in all areas. For more details on WDR imaging, see section .

2.2.2 Lightfinder technology

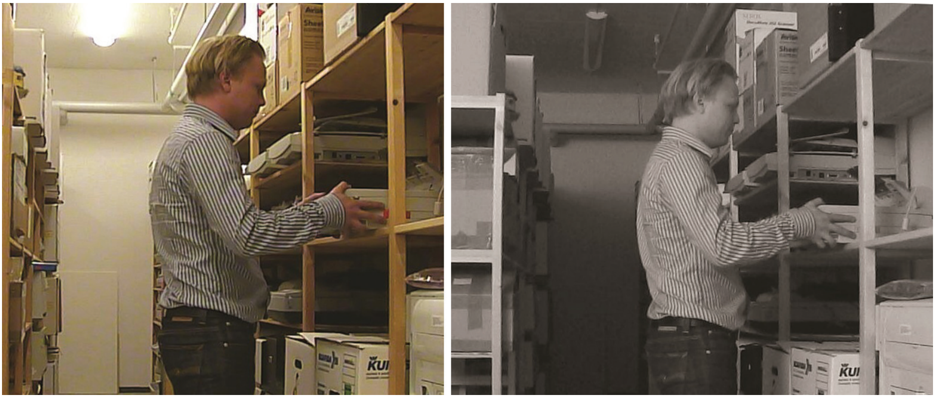
Surveillance video with color greatly enhances the possibility to effectively identify people, vehicles, and incidents. Cameras with Axis Lightfinder technology have extreme light sensitivity, and can deliver day-mode color images in as little light as 0.08 lux, or lower. This is achieved through the optimal selection of image sensor and lens, Axis image-processing know-how, and in-house ASIC chip development. As these building blocks of Lightfinder regularly improve, Lightfinder, too, is constantly evolving. Lightfinder 2.0, which is suitable even for cameras with resolutions up to 4K, represents a step change in this evolution, with increased light sensitivity, a more life-like color reproduction, and customized tuning for advanced users.



Left: a sharp, bright color image delivered by a Lightfinder 2.0 camera, even though the light intensity was only 0.05 lux under the bridge. Right: a snapshot of the same scene manipulated to visualize how the scene appeared to the human eye.

2.2.3 Day/night functionality

A network camera with day/night functionality has an automatically removable infrared-cut filter. The filter is on during daytime, enabling the camera to produce colors as the human eye sees them. At night, the filter is removed to enable the camera to take advantage of near-infrared light and produce good quality black and white images. This is one way of extending a network camera's usefulness in low-light conditions.

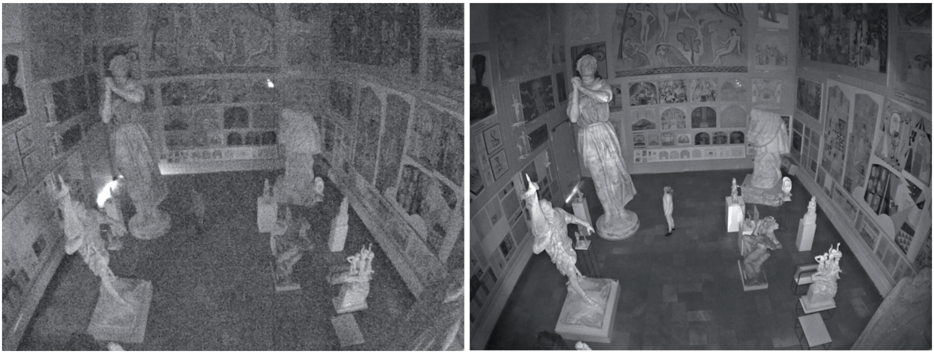


Left: day mode. Right: night mode.

2.2.4 Built-in IR illumination

In low light or complete darkness, built-in infrared (IR) LEDs in a camera (or a separately installed IR illuminator) will increase the camera's ability to use near-infrared light to deliver quality black and white images. Near-infrared light from the moon, street lamps, or IR illuminators is not visible to the human eye, but a camera's image sensor detects it.

The built-in IR LEDs in Axis cameras can be adjusted to match the viewing angle and can be activated automatically in darkness, upon an event, or upon request by a user.



Left: night mode snapshot captured without illuminators (a small amount of light was admitted under a door in the left-hand corner of the room). Right: night mode snapshot captured using IR illuminators.

2.2.5 OptimizedIR

Axis cameras with OptimizedIR provide a unique and powerful combination of camera intelligence and sophisticated LED technology using Axis most advanced camera-integrated IR solutions. Examples include a patented technology for assuring an even illumination in the camera's variable field of view, extremely efficient heat management, and the use of long-range, high-quality LEDs that are fine tuned to the camera. OptimizedIR is in constant development, with new advanced features being added.

2.2.6 Lenses with low f-number

Camera lenses with a lower f-number have a better light gathering ability. In general, the lower the f-number, the better its performance in low-light settings. Sometimes a higher f-number is preferable for handling certain types of lighting. A camera's light sensitivity depends not only on its lens, but also on the image sensor and image processing. More details on lenses and image sensors are provided in Chapter .

2.2.7 Automatic iris control

For scenes with changing light levels, an automatically adjustable iris (DC-iris, P-Iris, or i-CS lens) is recommended to provide the right level of exposure. Cameras with a P-Iris lens or i-CS lens have better iris control for optimal image quality in all lighting conditions. More details are covered in Chapter .

2.2.8 The right resolution

A camera's resolution is defined by the number of pixels on the image sensor. A camera with a *megapixel* sensor delivers images with one million pixels or more.

A high resolution is generally desired. When using a wide view angle, a camera with higher resolution provides a wider area of coverage. When using a narrow view angle, a camera with higher resolution provides greater detail, which is useful in identifying people and objects.

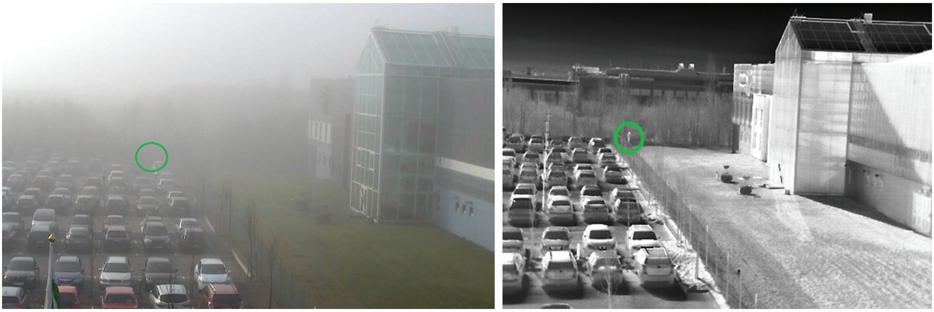
But as the surveillance industry has continued to move to higher resolutions, manufacturers have usually tried to keep the same sensor size to avoid the higher cost of using a larger sensor. This means that each pixel must be smaller, and smaller pixels are able to capture less light. By simply increasing the number of pixels in a sensor of the same size you get better resolution, but your image may also have lower quality, especially in a low-light scene. A camera with a sensor of around 4 megapixels generally strikes a balance between resolution and light sensitivity because it provides a large enough pixel size without having to use a larger, more expensive sensor.

Cameras supporting HDTV 720p (1280x720 pixels), HDTV 1080p (1920x1080 pixels), WQHD (2560x1440 pixels), and 4K Ultra HD (3840x2160 pixels), which are approximately 1, 2, 4, and 8.5 megapixels, respectively, follow standards that guarantee full frame rate, high color fidelity and a 16:9 aspect ratio.

2.2.9 Thermal imaging

Besides sunlight, artificial light, and near-infrared light, thermal radiation can also be used to generate images. A thermal camera requires no light source, but instead detects the thermal radiation emitted by any object warmer than absolute zero (0 K).

Thermal cameras can be used to detect subjects in complete darkness, in smoke or fog, or when subjects are obscured by shadows or a complex background. Nor are such cameras blinded by strong lights. Thermal cameras are ideal for detection purposes and can be used to complement conventional cameras in enhancing the effectiveness of a surveillance system. For more information about thermal cameras, see section .



Left: image from a conventional camera on a foggy scene. Right: image from a thermal camera on the same foggy scene.

2.2.10 Image stabilization

A surveillance camera mounted in an exposed location, such as on a high pole or a street sign near a busy road, can be shaken by winds or passing traffic. This could blur the video, especially when a powerful zoom lens is used. Having cameras that are less sensitive to vibrations makes installation more flexible and allows for multiple mounting options, even though vibration shall be avoided if possible. Because stabilized video will contain comparatively less movement, it requires less bandwidth and storage resources than shaky video.

Real-time image stabilization techniques can make the video output less sensitive to vibration and maintain image quality.

- **Optical image stabilization** (OIS) usually relies on gyroscopes or accelerometers to detect and measure camera vibrations. This method is particularly useful with long focal lengths and works well also in low light conditions. The main disadvantage of an optical solution is the price.
- **Electronic image stabilization** (EIS) relies on algorithms for modeling camera motion, which then are used to correct the images. This method is cost-efficient, but sometimes fails to distinguish between physical motion induced by vibrations and perceived motion caused by fast-moving objects in front of the camera.

Axis employs a stabilization method that is a hybrid of the two techniques. The Axis feature is called *electronic image stabilization* (EIS), but combines advanced gyroscopes together with optimized algorithms to make a robust and reliable system. It covers a wide band of vibration frequencies and copes with high and low amplitudes. EIS from Axis can always distinguish between physically induced vibrations and perceived motion. The system performs very well even in poor lighting since it relies on gyroscopic information, rather than video content, for its motion calculations. For the same reason, the system can always distinguish between perceived motion and physically induced vibrations.

2.3 Camera features for ease of installation

Axis cameras incorporate features that make the products easy to install and use, as well as more reliable, by minimizing installation errors.

2.3.1 Outdoor-ready

Axis outdoor-ready products are prepared for outdoor installation out of the box. No separate housing is required and the products come with captive screws that will not fall out of their screw holes. The products are designed to run in a range of operating temperatures and offer protection against dust, rain, and snow. Some even meet military standards for operation in harsh climates.

2.3.2 Focused at delivery

To make installation faster and simpler, Axis cameras with a fixed focal lens are ready-focused at the factory, eliminating the need to focus them during installation. This is possible because fixed focal cameras with a wide or mid-range field of view usually have a wide depth of field (the range in which objects both near and far are in focus). For more on focal length, f-numbers and depth of field, see chapter .

2.3.3 Remote focus and zoom

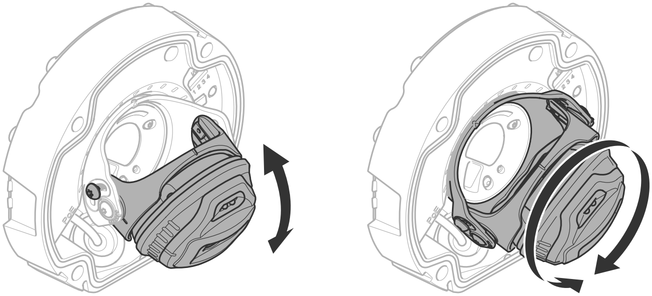
A varifocal camera with remote focus and zoom eliminates the need to manually, on site, adjust the focus and the field of view when the camera is installed. Thanks to the camera's lens motor, this can be done remotely from a computer on the network.

2.3.4 Remote back focus

A CS-mount varifocal camera with remote back focus allows the focus to be fine-tuned remotely from a computer, by making tiny adjustments to the position of the image sensor. This functionality also works with optional lenses.

2.3.5 3-axis camera angle adjustment

An Axis dome camera is designed with a 3-axis angle adjustment that allows the lens holder (comprising the lens and image sensor) to pan, tilt, and rotate. This allows the camera to be mounted on a wall or ceiling. Users can then easily adjust the camera's direction and level the image. The flexibility of the camera adjustment, together with the ability to rotate the image using the camera web interface, also means it is possible to get a vertically oriented video stream (corridor format).



3-axis camera angle adjustment

2.3.6 Corridor format

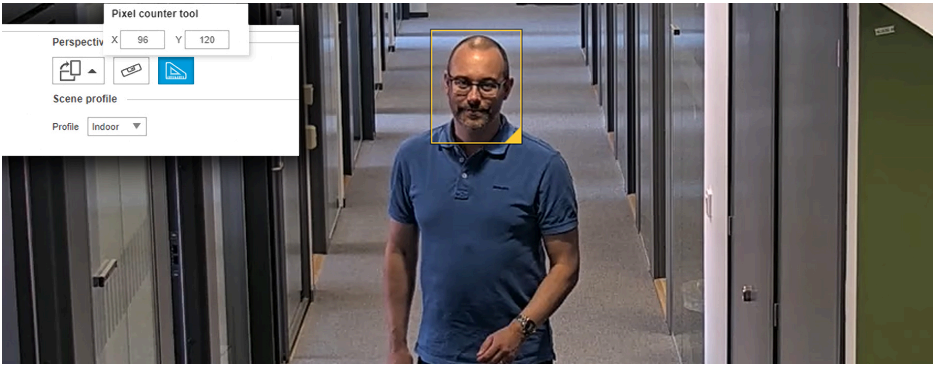
Corridor format enables a fixed camera to provide vertically oriented video. The vertical format optimizes the coverage of areas such as corridors, hallways, and aisles, maximizing image quality while minimizing bandwidth and storage requirements. It enables, for example, HDTV network cameras to deliver video with a 9:16 aspect ratio. With a dome camera, this is achieved by first rotating the lens 90° (or with a bullet or box camera, by rotating the entire camera), and then rotating the video image back 90° in the camera's web page.

2.3.7 Straighten image

Straighten image is an image processing tool which makes it possible to digitally correct slight mechanical skews in image rotation (around the longitudinal axis). The goal is to level the image with the horizon.

2.3.8 Pixel counter

Axis pixel counter is a visual aid shaped as a frame with a corresponding counter to show the frame's width and height. The pixel counter helps ensure that the video resolution has sufficient quality to meet goals such as facial identification, and also to verify that the resolution of an object fulfills regulatory or customer requirements. For details about recommended pixel densities for different surveillance purposes, see chapter .



Pixel counter tool

Perspectiv X 96 Y 120

Scene profile

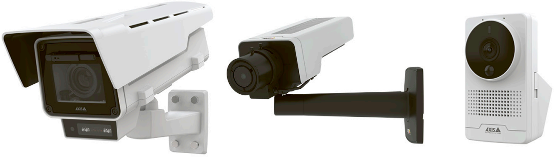
Profile Indoor

Axis pixel counter showing the pixel resolution of a face.

2.4 Types of network cameras

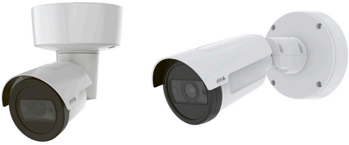
Network cameras may be designed for indoor use only, or for both indoor and outdoor use. An outdoor-ready camera is supplied with an external, protective housing. For more on protection, see section .

2.4.1 Box cameras



A box camera is a traditional surveillance camera type. Both the camera and its viewing direction are readily apparent, making this camera type the best choice for deterrence purposes. Most box cameras come with an interchangeable lens, which may be fixed, varifocal, or with motorized zoom. This type of camera is available for both indoor and outdoor use. Axis box cameras for outdoor use come in protective housings.

2.4.2 Bullet cameras



Bullet cameras have a small and slim design, compared with box cameras. They are outdoor-ready, which means that they can be placed both indoors and outdoors, without any additional protective enclosure. All bullet cameras from Axis are equipped with built-in IR light which enables surveillance in low light or complete darkness. As with box cameras, the camera's viewing direction is obvious. On bullet cameras, however, it is not possible to switch lenses.

2.4.3 Dome cameras

Dome cameras consist of a fixed camera preinstalled in a small dome-shaped housing. This camera's main benefit lies in its discreet, unobtrusive design. In addition, people in the camera's field of view find it difficult to see in which direction the camera is pointing. There is a wide selection of accessories that enable even more discreet installation, such as black casings, recessed mounts, and smoked domes. The dome camera is also more resistant to tampering than other fixed cameras. It may come with a fixed, varifocal, or motorized zoom lens.

Dome cameras are designed with different types and levels of protection, such as vandal and dust resistance, and IP66, IP67, and NEMA 4X ratings for outdoor installations. No external housing is required. These cameras are usually mounted on a wall, ceiling, or pole.

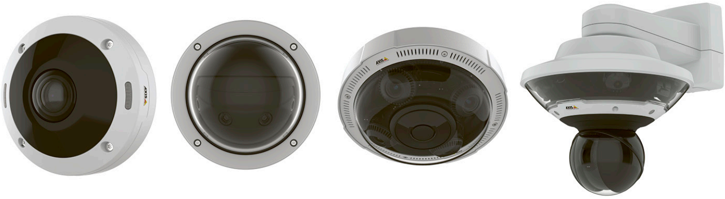
2.4.3.1 Onboard dome cameras

The onboard camera category consists of modular cameras, dome cameras, and panoramic cameras.

Onboard cameras are specially designed for surveillance on rolling stock, busses, and other vehicles. The conditions in onboard surveillance vary depending on the type of vehicle the camera is used in. In some usage areas, such as on trains, there are specific protocols and regulations to follow, and only products tested specifically for these environments should be used. However, common for all onboard surveillance is the need for a particularly rugged design. This means cameras must withstand harsh conditions such as vibrations, shocks, and bumps, as well as dust, water, and temperature fluctuations. An onboard camera's discreet appearance is often combined with an active tampering alarm that helps detect and prevent attempts to redirect and defocus the camera.

An onboard dome camera mounted in the ceiling of a bus.

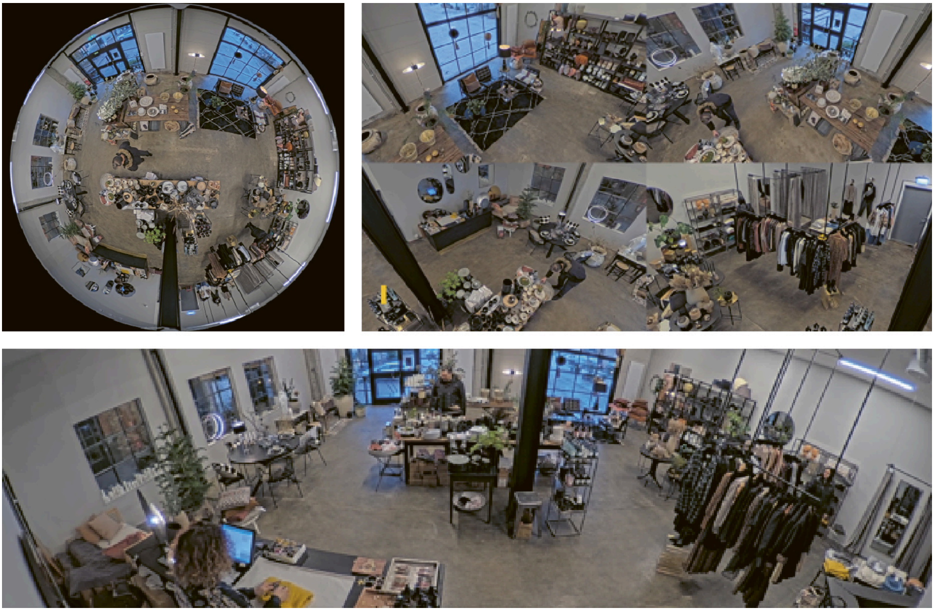
2.4.3.2 Panoramic cameras



Panoramic cameras: single-sensor, multisensor, multidirectional, and a solution combining a multidirectional camera with a PTZ camera.

A panoramic camera is a dome camera that provides wide area coverage and excellent image detail at the same time, in an efficient one-camera installation. The camera can be single-sensor, multisensor, or multidirectional.

A single-sensor panoramic camera has one wide-angle lens that gives a 360° fisheye view. The view can be transformed, either live or on recorded material, into various rectangular views, including panoramic, double panoramic, or quad-view format (simulating four different cameras).



A single-sensor panoramic camera offers multiple viewing modes such as 360° overview, quad view, and panorama.

A multisensor camera provides seamless 180° coverage with great detail and minimal distortion. Because it has multiple sensors, it combines wide coverage with high image quality and high pixel density. It uses a universal white balance setting and synchronized exposure for all the sensors. With its seamlessly stitched image, a multisensor camera also eliminates blind spots.

180° view from a multisensor camera.

A multidirectional camera with 360° coverage is a panoramic camera with individually adjustable camera heads. It is ideal in, for example, retail stores, hallways, and warehouses.

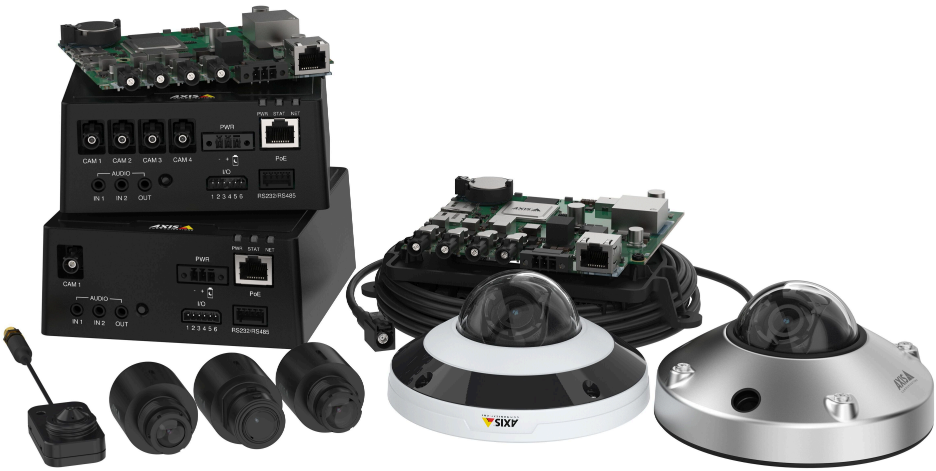
A solution that combines a multidirectional panoramic camera with a PTZ camera is especially useful in, for example, intersections.

2.4.4 Modular cameras

Modular cameras including main units and sensor units.

Axis modular cameras are designed to provide a flexible and discreet installation. Blending in with the environment, they can be used practically anywhere. The sensor units can be installed in tight spaces, used in buses and police cars, integrated with machines such as ATMs, and placed at eye level at exits for optimal face captures. They are ideal for highly discreet video and audio surveillance and analytics applications.

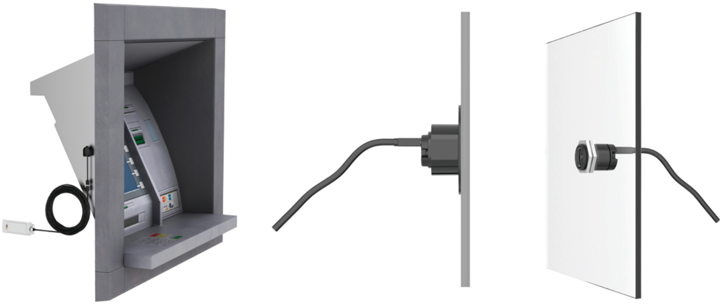
A modular camera is a divided camera concept, where the main unit can be installed up to 30 m (98 ft) from the sensor unit. The sensor unit contains the lens and the image sensor, and the main unit processes the image. This divided concept provides flexibility in the choice of hardware, as well as in installation. The main and sensor units can easily be exchanged or relocated after the initial installation and the detachable cables ensure easy maintenance or upgrading. A discreet installation also reduces the risk of tampering.



AXIS F Modular Cameras series offers a range of high-performance modular cameras designed for indoor, outdoor, and onboard surveillance. The series includes two rugged main units, two UL-recognized barebone main units, multiple cable options and sensor units for a wide range of applications.

Modular cameras are also cost-effective when you need multiple cameras installed in one area. There are one- and four-channel main units, and a four-channel main unit connects to up to four sensor units. Thanks to maximum cable lengths up to 30 m (98 ft), one main unit with four sensor units can cover both larger and smaller areas. Four connected sensor units also enable simultaneous, multiple video streaming and quad view streaming using a single IP address. One main unit, whether it supports one or four video channels, requires a single VMS license and one switch port for cost-effective surveillance.

Quad-view streaming from a four-channel modular camera system in a bus.



At left, a pinhole modular camera in an ATM application. At right, a sensor unit mounted on a wall, and on a glass panel.

A wide range of sensor units with different form factors and different lens types, such as standard, varifocal, mini-dome, and pinhole are available.

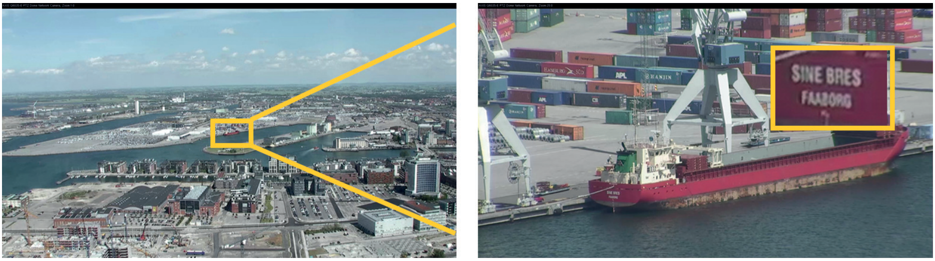
Designed to be placed near building exits, a height strip housing enables extremely discreet installation of pinhole sensors. The camera is positioned to look straight at a person's face for more reliable identification.

2.4.5 PTZ cameras

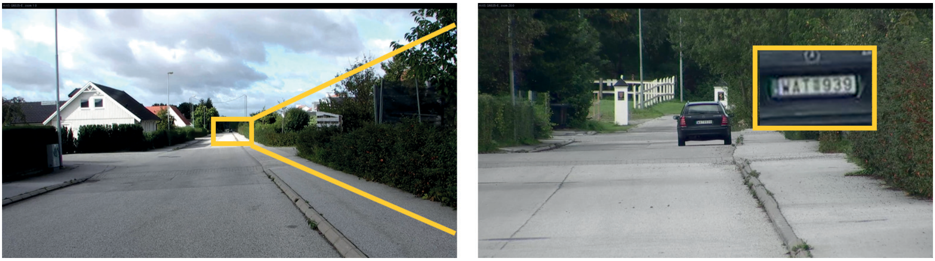
PTZ camera models with features such as: (from left) HDTV 1080p resolution with Sharpdome technology, active cooling, a solution combining a multi-sensor camera and a PTZ camera, and (far right) a combination of a visual and a thermal camera in one unit.

A PTZ camera provides pan, tilt, and zoom functions (using manual or automatic control), enabling wide area coverage and great detail when zooming in. Axis PTZ cameras usually have the ability to pan 360°, to tilt 180° or 220°, and are often equipped with a zoom lens. A true zoom lens provides optical zoom that maintains image resolution, as opposed to digital zoom, which enlarges the image at the expense of image quality.

In operations with live monitoring, PTZ cameras can be used to follow an object, and to zoom in for closer inspection. In unmanned operations, automatic guard tours on PTZ cameras can be used to monitor different areas of a scene. In guard tour mode, one PTZ camera can cover an area that would require many fixed cameras to do the same job.



Wide view (left) and zoomed-in view (right) in an HDTV 1080p PTZ camera, making the text on the cargo ship readable at 1.6 km (1 mile).



Wide view (left) and zoomed view (right) in an HDTV 1080p PTZ camera, allowing the license plate to be read at 275 m (900 ft.).

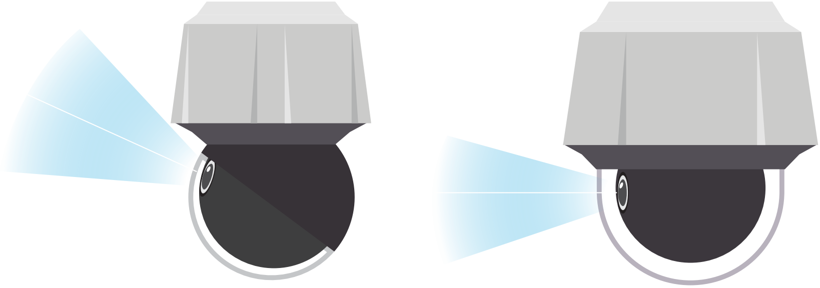
Axis PTZ cameras can be equipped with a variety of intelligent functionalities, for example:

> **Guard tour (preset positions)**. PTZ cameras usually allow multiple (up to 100) preset positions to be programmed. Once these positions have been set in the camera, the operator can quickly move from one position to the next, simply by selecting a position. In guard tour mode, the camera can be programmed to automatically move from one preset position to the next in a pre-determined order or at random. Normally up to 20 guard tours can be configured and activated at different times of the day.

- **Guard tour (recorded)**. The tour recording functionality in PTZ cameras enables easy setup of an automatic tour using a device such as a joystick to record an operator's pan-tilt-zoom movements and the time spent at each position. The recorded tour can then be activated at the touch of a button or at a scheduled time.
- **Autotracking**. This analytics application will automatically detect a moving person or vehicle and follow it within the camera's area of coverage. Autotracking is particularly beneficial in unmanned video surveillance situations where the occasional presence of people or vehicles requires special attention. The functionality reduces the cost of a surveillance system substantially, as fewer cameras are needed to cover a scene. It also increases the effectiveness of the solution, as it allows a PTZ camera to record the parts of a scene where there is activity.
- **AXIS Radar Autotracking for PTZ**. This software application uses motion data from Axis radar devices to find objects of interest on a site, and automatically controls the direction and zoom level of one or more PTZ cameras. The radar device acts as a complement to the PTZ camera, and the application enables visual confirmation of detected objects even outside of the camera's current field of view. AXIS Radar Autotracking for PTZ also minimizes the need for manual, joystick control of the camera.
- **AXIS Perimeter Defender PTZ Autotracking**. When installed on a PTZ camera, this application allows a fixed thermal or fixed visual camera running AXIS Perimeter Defender analytics to automatically steer the PTZ camera for close-up views of alarm objects in the fixed camera's detection zone. The PTZ camera automatically adjusts the zoom level to keep in view all alarm objects, including new ones that appear in the fixed camera's detection zone.
- **Advanced/active gatekeeper**. Advanced gatekeeper enables a PTZ camera to pan, tilt, and zoom in to a preset position when motion is detected in a predefined area, and to then return to the home position after a set time. When this is combined with the ability to continue to track the detected object, the function is called active gatekeeper.

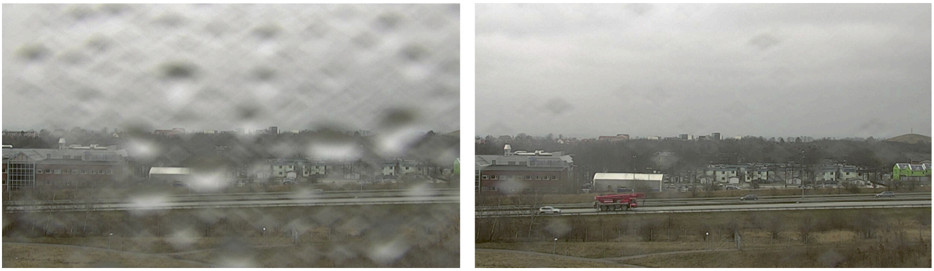
2.4.5.1 Sharpdome technology

With Axis Sharpdome technology, a PTZ camera can see above its horizon. Sharpdome offers innovative mechanics that makes the entire dome rotate, in contrast to a conventional dome where the camera rotates inside the dome. The mechanics and the placement of the camera module together with the unique design of the outdoor dome enable the same optimal image sharpness and full scene fidelity in all pan and tilt positions. This provides clear identification of objects as much as 20° above the camera horizon.



A camera with Sharpdome (left) and a conventional dome camera (right)

Sharpdome includes the speed dry function, which helps to provide sharp images in rainy weather. When visibility through the dome is impaired by water drops, speed dry rotates the dome in alternating directions at high speed, effectively shaking off the water.



Two snapshots of the same rainy scene, before shaking (left) and after shaking off the water (right) using speed dry.

2.4.6 Thermal cameras

Thermal cameras in bullet (left) and fixed box mounted on positioning unit (center) form factors. The bispectral PTZ camera (right) combines a visual and a thermal camera in one unit for mission-critical surveillance.

Thermal cameras detect the thermal radiation (heat) that all objects with a non-zero temperature emit. With the ability to pick up small temperature differences and convert them into a visual image, these cameras can distinguish persons and vehicles at great distances. They perform even in complete darkness and regardless of lighting conditions, camouflaging, vegetation, difficult weather, or other conditions where a visual camera might be found lacking.

Thermal cameras are widely used in perimeter protection systems. Live video from a thermal camera can detect activity around critical locations long before a visual camera has seen anything unusual. The thermal images are analyzed automatically, directly in the camera, and the security system can be set up to respond in various ways. It can trigger automatic audio alerts in loudspeakers to actively deter intruders, it can email alerts to security personnel, and can and pan and zoom the system's visual cameras to capture and record video footage in which the intruders can be identified. Thermal images alone are typically not enough to identify individuals. This makes thermal cameras a valuable option for surveillance in locations where privacy is especially important. Thermal cameras are also installed to monitor the temperature of industrial processes. They can be used, for example, to find heat leaks in buildings, or to determine whether a vehicle was recently used.

A thermometric camera is a thermal camera designed to monitor objects or processes to detect if temperatures rise above or fall below a set of user-defined limits. This type of camera is used in order to prevent damage, failure, fire, or other hazardous situations.

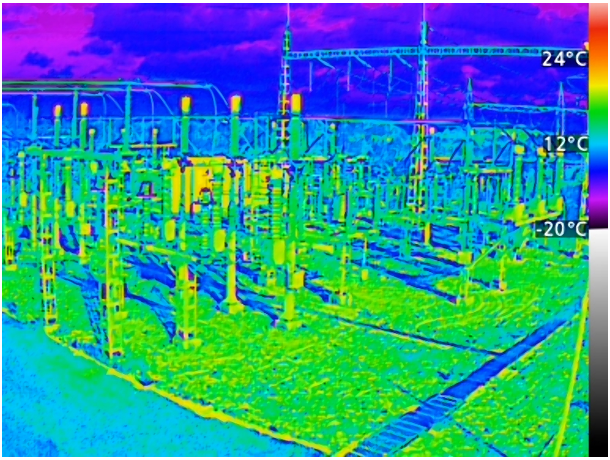


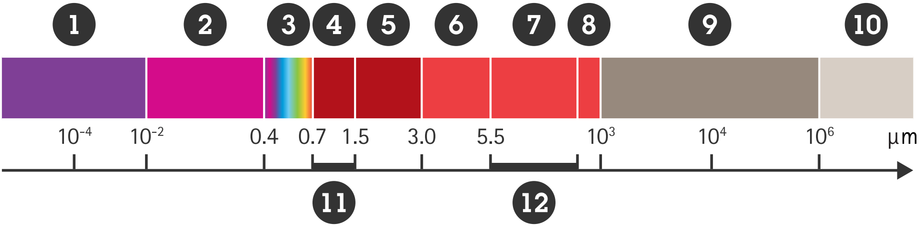
Image from a thermometric camera. Different temperatures are visualized using a color palette.

A thermal camera requires special optics, since regular glass will block the thermal radiation. Most thermal camera lenses are made of germanium, which enables infrared light and thermal radiation to pass through. How much or how far a thermal camera can "see" or detect depends on the lens. A wide-angle lens gives a thermal camera a wider field of view, but a shorter detection range than a telephoto lens, which provides a longer detection range with a narrower field of view.

A thermal camera also requires a special image sensor. Sensors for thermal imaging can be broadly divided in two types:

Uncooled thermal image sensors operate at or close to the ambient temperature, at 8–14 µm in the long-wave infrared range. Uncooled sensors are often based on microbolometer technology, and are smaller and more affordable than cooled image sensors.

Cooled thermal image sensors are usually contained in a vacuum-sealed case and cooled to temperatures as low as -210 °C (-346 °F) to reduce noise created by their own thermal radiation at higher temperatures. It allows the sensors to operate in the mid-wave infrared band, approximately 3–5 µm, which provides better spatial resolution and higher thermal contrast since such sensors can distinguish smaller temperature differences and produce crisp, high resolution images. The disadvantages of such detectors are that they are bulky, expensive, energy-consuming and the coolers must be rebuilt every 8,000 to 10,000 hours.



The spectrum of electromagnetic radiation. Axis thermal cameras work in the long-wavelength IR region (7) at about 8–14 µm.
1. X-rays
2. Ultraviolet light
3. Visible light
4. Near-infrared (NIR) radiation (approximately 0.75–1.4 µm)
5. Short-wavelength infrared (SWIR) radiation (1.4–3 µm)
6. Mid-wavelength infrared (MWIR) radiation (3–5 µm)
7. Long-wavelength infrared (LWIR) radiation (8–14 µm) — used by Axis thermal cameras
8. Far-infrared (FIR) radiation at approximately 15–1,000 µm
9. Microwave radiation
10. Radio/TV wavelengths
11. IR illumination
12. Axis thermal cameras

A thermal sensor's ability to detect very small differences in thermal radiation can be characterized by its NETD (noise equivalent temperature difference) value. In general, the smaller the NETD, the better the sensor. However, cameras should not be rated by comparison of NETD specifications only, due to the lack of a standardized measurement protocol.

Products and technologies that can be used both for military and commercial purposes are called dual-use goods. Exports of such items are regulated in the international Wassenaar Arrangement from 1996, which, among other things, aims to promote transparency and greater responsibility in transfers of conventional arms, as well as dual-use goods and technologies. For a thermal camera to be freely exported, its maximum frame rate cannot exceed 9 frames per second (fps). Thermal cameras with a frame rate up to 60 fps can be sold in most 42 Wassenaar Arrangement member countries on the condition that the buyer is registered and can be traced and that the seller fulfills all country-specific export requirements, including license or license exception. Thermal cameras may never be sold to any embargoed or sanctioned destination.

2.4.7 Explosion-protected cameras

Explosion-protected cameras.
Left and middle: Fixed and PTZ cameras designed and certified for Zone/Division 1 hazardous areas.
Right: Fixed camera designed and certified for the less potentially combustible Zone/Division 2 areas in hazardous locations.

Explosion-protected cameras are ideal for health and safety applications as well as operational efficiency. You can use them to monitor operations and processes with remote visual verification of readings from gauges and sensors across your sites. They can help increase efficiency, maintain peak operability, and maximize uptime. Cameras used in hazardous locations can be integrated with a system of sensors and safe-area cameras already in place on an existing network. Thermometric cameras can monitor potential overheating of equipment, which enables informed decisions about the ongoing process, helping to keep production up-and-running and as efficient as possible.

With explosion-protected cameras, you can improve the safety of employees and minimize unnecessary human exposure to hazardous areas. You can use analytics that monitor the use of personal protection equipment, such as hard hats, or that detect signs of smoke or fire in potentially combustible environments.

Typical industry segments for explosion-protected equipment are processing industries, oil and gas installations, and grain handling and storage. Hazardous areas can, however, also be found in a *wide range of other industries, such as chemical plants, pharmaceuticals, mining, and water and waste treatment.*

Explosion-protected network cameras offer many advantages over analog versions, the major ones being built-in intelligence, analytics, recording and storage possibilities, superior image quality, and a modern, future-proof camera technology.

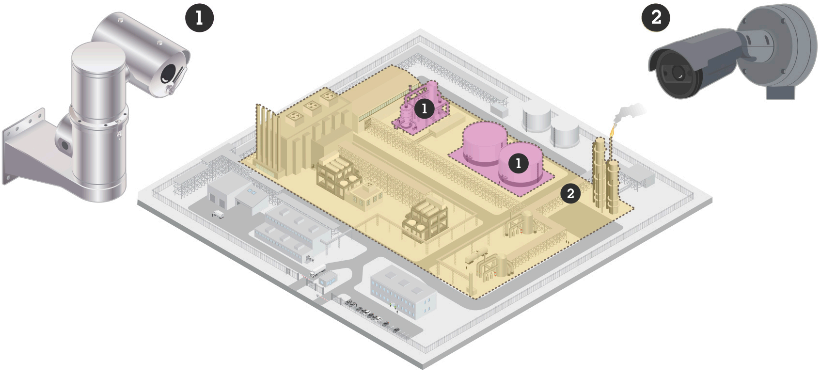
When an electrical device is installed in a potentially combustible environment, such as in chemical processing plants, or near gas valves or vents, it must meet very specific safety standards. It is the potentially combustible environment that must be protected from ignition.

Explosion-protected cameras are certified for use in hazardous locations because the cameras are designed to comply with an explosion-protection method, which could be, for example, containment or prevention. The term explosion-protected **does not imply** that the camera itself will withstand an external explosion.

> **Containment:** These cameras utilize a heavy-duty enclosure to confine the energy of a potential internal combustion. In case of explosion caused by sparks or high temperatures in these cameras, the explosion will be limited to within the enclosure and not spread to the possibly flammable atmosphere outside of it. This type of explosion-protected camera can be certified for use in *Zone/Division 1 hazardous areas*, where there is a relatively large likelihood that the atmosphere is flammable due to its concentration of explosive vapors, gases, dust, or fibers.

> **Prevention:** These cameras are designed so that they cannot provide sufficient energy to ignite a flammable atmosphere. They can be certified for use in *Zone/Division 2 hazardous areas*, which are less potentially combustible areas in a hazardous location.

In hazardous locations, Zone/Division 2 areas are typically significantly larger than Zone/Division 1 areas. Cameras certified for Zone/Division 1 areas can also be used in Zone/Division 2 areas, but cameras specifically designed and certified for Zone/Division 2 areas are a more cost-efficient alternative in these areas.



The right camera for the right type of hazardous area.
1. In Zone/Division 1 areas you must use a camera specifically certified for Zone/Division 1 areas.
2. In the large, less potentially combustible (Zone/Division 2) areas of a hazardous area site, it is also possible to use a substantially lighter and more cost-efficient camera certified for Zone/ Division 2 areas.

Explosion-protected cameras must be certified according to the industry standards applicable in the country where the camera will be used.

3. Camera elements

Image quality and field of view may be the most important aspects of any camera. They are affected by a number of camera elements, including the camera's light sensitivity, the lens it uses, the image sensor, and image-processing functionalities.

3.1 Light sensitivity

A camera's light sensitivity, often specified in lux, is the lowest illuminance level at which the camera produces an acceptable image. Illuminance is a measure of how much the incident light illuminates a surface, per area unit. The light sensitivity depends mainly on the lens and the image sensor, and the lower the specified lux value, the better the light sensitivity of the camera.

Illuminance (lux)	Light condition
100,000	Strong sunlight
10,000	Full daylight
500	Office light
100	Family living room
10	Candle at a distance of 30 cm (1 ft.)
0.1	Full moon on a clear night
0.01	Quarter moon

Table 3.1a *Example levels of illuminance in various light conditions.*

Many natural scenes have fairly complex illumination, with both shadows and highlights that give different lux readings in different parts of the scene. It is important, therefore, to keep in mind that a single lux reading does not indicate the light condition for the scene as a whole.

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 might not be so helpful when comparing cameras from different manufacturers. This is because different manufacturers use different measurement methods and have different criteria for what makes an acceptable image. To properly compare the low light performance of two different cameras, the cameras should be placed side by side and view a moving object in low light.

To capture good quality images in low light or at night, Axis provides a variety of solutions such as cameras with day/night functionality, or day/night cameras with Axis Lightfinder technology or with built-in infrared (IR) LED. Cameras with day/night functionality take advantage of near-infrared light to produce quality black and white video, and day/night cameras with Lightfinder enable color video in very little light. External IR illuminators enhance the quality of black and white video in low light or complete darkness. Thermal cameras that make use of infrared radiation (at longer wavelengths than visible light) emanating from objects are the most reliable tools to detect incidents, 24/7.

For more information on Axis Lightfinder technology, cameras with built-in IR LED, and thermal cameras, see chapter . For more information on day/night functionality and illuminators, see section .

3.2 Lenses

A lens (or a lens assembly) on a camera performs several functions.

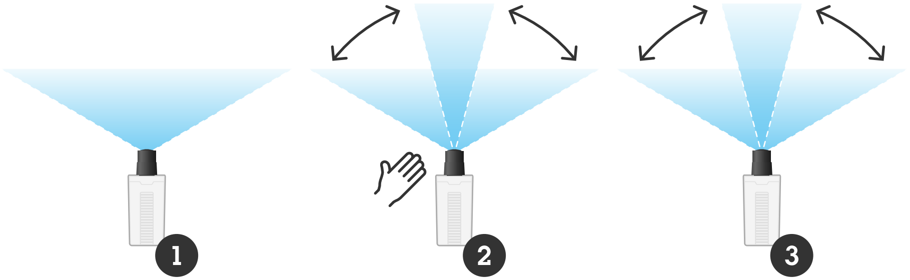
- It defines the field of view, which determines how much of a scene can be seen in the image.
- It preserves the details of the scene by matching the lens resolution to the sensor resolution.
- It controls the amount of light reaching the image sensor so that the image is correctly exposed.
- It focuses the image, either by adjusting elements within the lens assembly itself or by changing the distance between the lens assembly and the image sensor.

The lens is the eye of the camera and its capabilities and features are therefore very important. Field of view, resolution, light sensitivity, and depth of field should be carefully considered and matched to your needs when choosing the camera.

3.2.1 Lens types

Depending on the use there are different types of lenses to choose from:

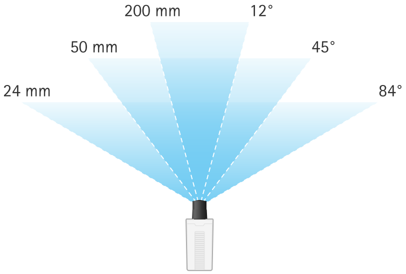
- **Fixed focal length lens**. Also called fixed lens. The focal length is fixed and provides a single field of view.
- **Varifocal lens**. Offers a variable focal length and thus different fields of view. The field of view can be adjusted on the lens or through the camera's web interface. Adjusting the focal length in a varifocal lens also requires the lens to be refocused.
- **Zoom lens**. Is like a varifocal lens in that it offers adjustable field of view, but here there is no need to refocus if the field of view is changed. Focus is maintained when changing focal length. This lens type is very uncommon in the security industry, but the function can be mimicked by motorized lenses.



Camera with a fixed lens (1), a varifocal lens (2), and a zoom lens (3).

3.2.2 Field of view

The field of view describes the angle that the camera can capture. It is determined by the focal length of the lens and the size of the image sensor. The longer the focal length, the narrower the field of view. Field of view is sometimes labeled HFoV, VFoV, or DFoV, representing the horizontal, vertical, or diagonal field of view.



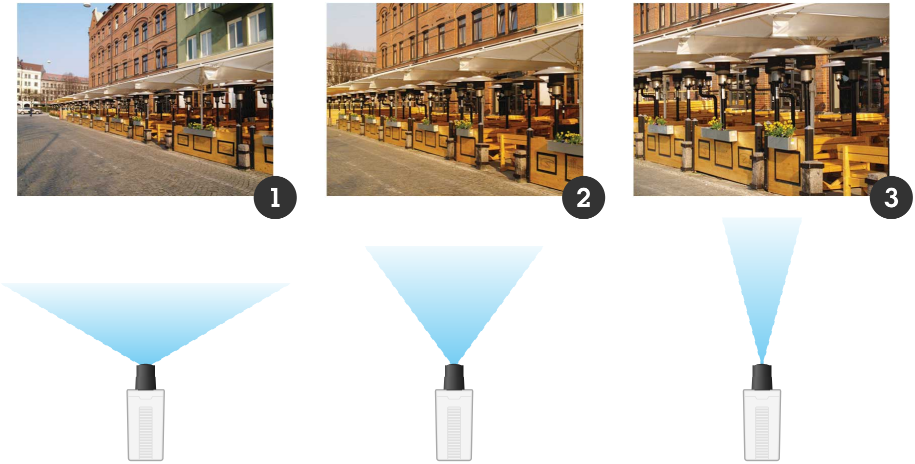
A larger focal length (in mm) provides a narrower field of view (in degrees).

A lens can be classified in one of three categories depending on which angles the lens can reproduce.

> **Wide angle lens**. Gives a much larger field of view than what is normal for the human eye. Generally also provides a large depth of field.

> **Normal view lens**. Gives a similar field of view as the human eye's central field of view.

> **Telephoto lens**. Gives a narrower field of view and provides a magnifying effect when compared to human vision. Can sometimes result in a small depth of field.



Field of view with wide angle lens (1), normal view lens (2), and telephoto lens (3).

The easiest way to find the required focal length for a specific field of view is to use Axis online tools *Lens calculator* or *Product selector*, both available at *www.axis.com/tools*.

3.2.3 F-number and exposure

The light gathering ability of a camera is specified by the f-number (also known as the f-stop) of the lens. The f-number defines how much light can pass through the lens and reach the image sensor. It is the ratio of the lens's focal length to the diameter of the lens's entrance pupil.

The smaller the f-number, the better the light gathering ability, that is, more light can pass to the image sensor. In low-light situations, a lower f-number generally produces better image quality, while a higher f-number increases the depth of field. A lens with a low f-number is normally more expensive than a lens with a higher f-number.

In some lenses the size of the aperture can be changed. This is done by the iris, which can be manual or controlled by the camera. When using a varifocal or zoom lens, the f-number changes when the focal length is changed. The longer the focal length, the higher the f-number. The f-number that is printed on the lens is normally valid only for the wide setting.

The light gathering ability of a camera is higher when the f-number is lower.

3.2.4 Iris types

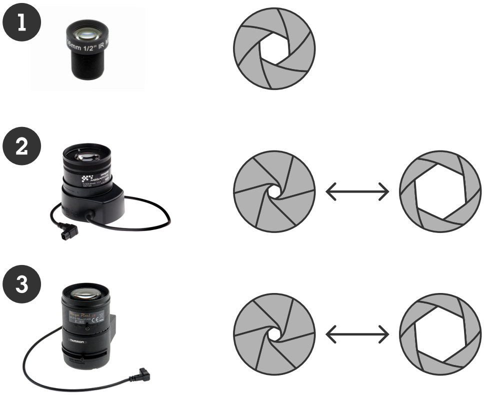
The iris of a lens works in similar ways to the iris of the human eye. It controls the amount of light that passes through so that the camera image is correctly exposed. It can also be used to optimize image quality aspects, such as resolution, contrast, and depth of field.

Three types of iris are common in the security industry:

> In a **fixed iris** lens the size of the iris opening cannot be changed. This is used by the M12 (S-mount) lens. Lenses with this type of iris are mostly used in environments with controlled light levels, typically indoors.

> In a **DC-iris** lens the camera can automatically change the size of the iris opening in response to the light level and thereby control the amount of light that reaches the image sensor. Lenses with this type of iris can be used in environments with more challenging light conditions, typically outdoors.

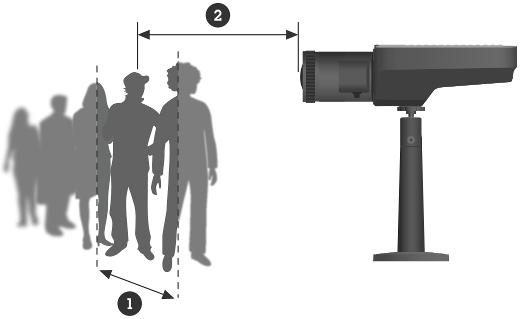
> In a **P-Iris** lens the camera can control the size of the iris opening much more precisely than with a DC-iris lens. The camera can not only optimize the amount of light reaching the image sensor but also adjust for better sharpness, contrast, and a more suitable depth of field.



Iris types common in the security industry: fixed (1), DC-iris (2), P-Iris (3).

3.2.5 Depth of field

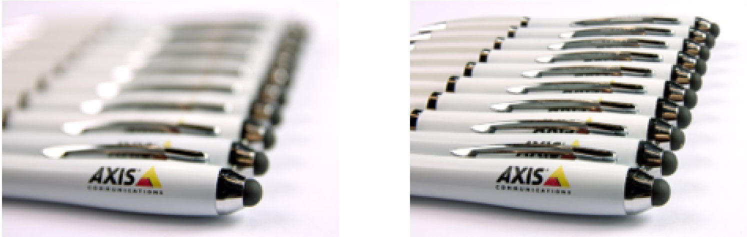
Depth of field refers to the distance between the closest and farthest objects that appear sharp simultaneously. This is important in applications such as the monitoring of a parking lot, where you may need to read license plates at 20, 30, and 50 meters (60, 90, and 150 feet) distance.



This illustration marks out the depth of field (1) and the focal distance (2) which is the distance from the camera to its focal point. Having a larger depth of field means that objects appear sharp at a longer range around the focal point.

Depth of field is affected by four factors: focal length, f-number, distance between the camera and the subject, and how the image is viewed. The part about how the image is viewed relates to aspects like the pixel size, the distance between the monitor and the observer, the observer's eyesight, and so on.

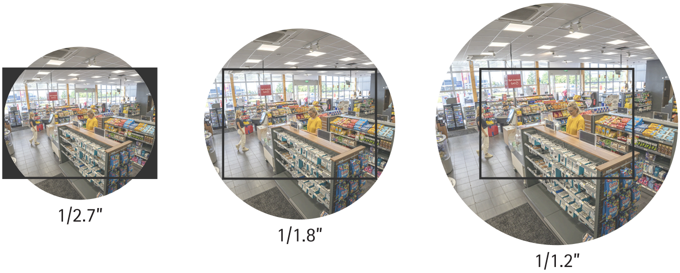
A longer focal length, a lower f-number, a shorter distance between the camera and the subject, and a shorter distance between the monitor and the observer will all decrease the depth of field.



Left: photo with small depth of field – only the pens in the front are in focus. Right: photo with larger depth of field – all the pens are in acceptably sharp focus.

3.2.6 Matching lens and sensor

When exchanging lenses it is important to match the lens to the camera's image sensor. If the lens is intended for a smaller sensor than the one in the camera, the image will have black corners. If the lens is intended for a larger sensor than the one in the camera, the field of view will be smaller than the lens's capability, because part of the information outside the image sensor will be lost. This situation creates a telephoto effect as it makes everything look zoomed in.



The effect of different lenses on a 1/1.8" sensor. Right: a 1/2.7" lens is too small for the sensor and the image has black corners. Center: a 1/1.8" lens matches the sensor size. Left: a 1/1.2" lens is too large for the sensor and the information outside the image sensor will be lost.

The lens product pages on axis.com usually provide information about which sensor sizes are supported, and which cameras are compatible with each lens.

3.2.7 Lens types in surveillance

	A block lens uses motors to adjust the focus and zoom remotely as well as providing some possibilities for an optimized image quality. It is commonly used in PTZ, dome, and bullet cameras. This type of lens is built into the camera and cannot be exchanged.
	An M12 lens usually has a fixed focal length and no iris control. Because of its small form factor it is used in modular cameras, some dome cameras, body worn cameras, and intercoms. In some cameras this lens is exchangeable. This lens is also known as S-mount lens.
	A C/CS lens has a specific mounting thread, making it easy to exchange. This type of lens is used in box cameras. It exists in a variety of varifocal lengths with DC or P-Iris control. This lens offers great flexibility and is suitable for various surveillance applications.
	An i-CS lens has the same thread as a C/CS lens, but has extra intelligence due to built-in motors for adjusting zoom and focus remotely. It offers similar benefits as the block lens, but it is exchangeable. It is compatible with box cameras that have i-CS support.

3.2.8 Focusing

Focusing a network camera often requires making fine adjustments to the lens. With the less sophisticated auto-iris lenses, it is best to adjust the focus in low-light conditions or by using a darkening filter such as a neutral density filter. In low-light conditions the iris automatically opens, which shortens the depth of field and helps the user focus more precisely.

Autofocus

Autofocus means that the camera automatically adjusts the lens mechanically so that the image is focused. The autofocus feature is a requirement in pan-tilt cameras where the camera direction is constantly changing. Some fixed cameras also have autofocus, but because focusing a fixed camera is normally only needed at installation, it is difficult to justify the additional cost.

Some cameras include full remote focus capabilities, eliminating the need for manual adjustment on-site. The computer software gives live feedback so that the user sees that the focus is correct. With a built-in pixel counter, users can also make sure that they get enough pixels across the subject to be able to identify it, whether it is a person's face or a license plate.

The autofocus feature requires neither setting nor programming to work. In Axis PTZ cameras, it is enabled as default and starts working as soon as the camera is turned on.

In scenes with low light or contrast, or that contain a lot of noise, the autofocus may need some time to find focus, and sometimes will even focus on the wrong object. When the scene changes, focus may be lost for a moment until the autofocus feature finds it again. This can give the impression that the camera is continually being focused.

Focus recall

A focus recall area in the desired view is a quick and easy way to regain focus immediately. The main difference between autofocus and focus recall is that autofocus will adjust focus every time the scene changes. Focus recall instead memorizes an area with a fixed focus, eliminating the need for repeated adjustments.

The user sets a focus recall area by clicking the focus recall button in the camera user interface when the view has the desired focus. The camera saves its focus setting. Focus recall is then activated as soon as the user pans or tilts to the focus recall area using the joystick, and the camera automatically focuses using the saved setting.

Laser focus

Some lighting conditions can pose a challenge to the autofocus feature. There may be difficulties finding focus in scenes with low light or low contrast, and in scenes with reflections or pinpoint light sources.

The laser focus feature makes it possible to focus on bright objects and objects that reflect a lot of light, for example window panes. Autofocus may find these challenging since the reflecting light blurs or hides the sharp edges that autofocus needs to be able to focus. With moving objects and scenes that change quickly, laser focus will find focus instantly, making it possible to focus, for example, on the license plate of a moving vehicle.

Laser focus focusing on a license plate in low light conditions with pinpoint light sources

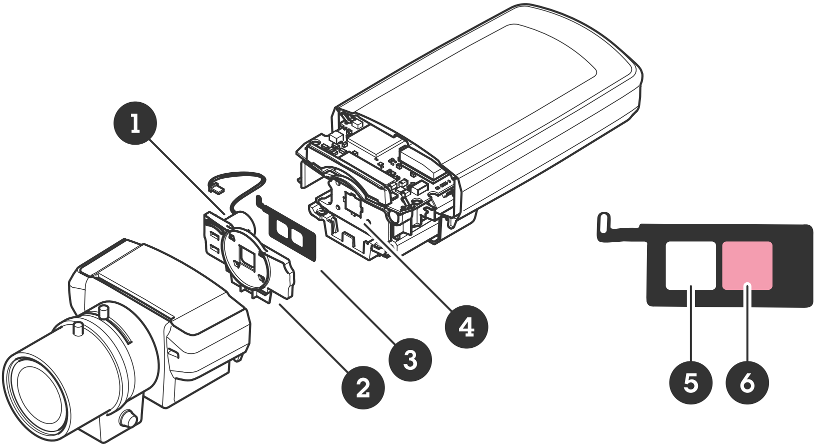
Laser focus is especially useful for PTZ cameras, since the view changes dynamically when the PTZ function is used.

3.2.9 PTRZ precision

Remote PTRZ (pan-tilt-roll-zoom) is a feature that makes it possible to adjust the camera view from afar, without pausing the recording. The camera can rotate around its vertical (up-and-down), lateral (side-to-side), and longitudinal (front-to-back) axes, and also change its focal length to achieve a narrower (zoom in) or wider (zoom out) field of view.

3.3 Removable IR-cut filter (day/night functionality)

Many cameras have an automatically removable infrared-cut filter between the lens and the image sensor. This filter blocks the incoming infrared (IR) light, to allow the camera to produce the colors that the human eye can see. However, when the filter is removed in low light or at night, the camera sensor can then take advantage of the ambient near-infrared (NIR) light and is able to deliver black and white images in scenes with insufficient visible light.



IR-cut (day/night) filter on an optical holder that, in this camera, slides sideways. The red-hued filter is used during the day and the clear part at night.

1. Solenoid

2. Front guard

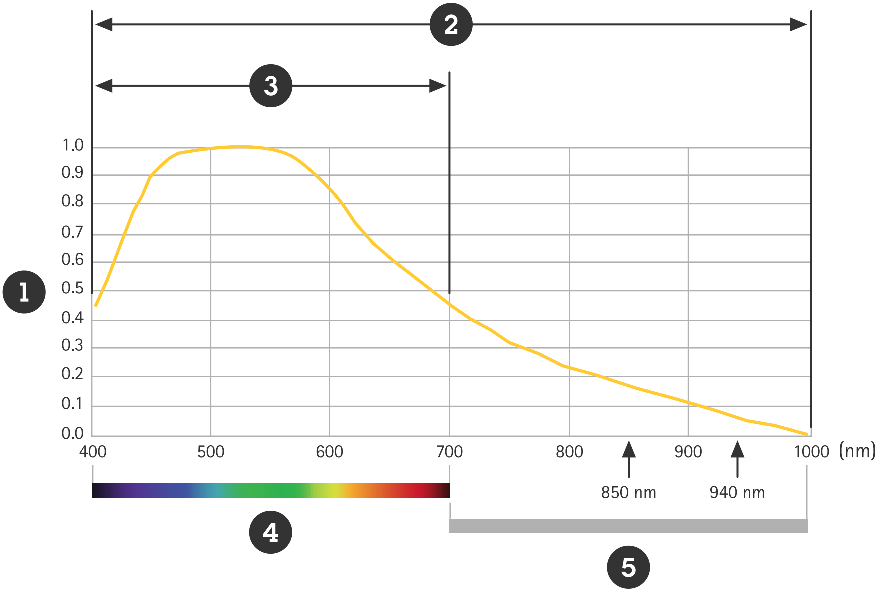
3. Optical holder

4. Image sensor

5. Night filter

6. Day filter

The human eye cannot see NIR light, which is in the approximate range 700–1000 nanometers (nm), but most camera sensors can detect and use it.



Graph showing how an image sensor responds to visible and NIR light.
1. Relative sensor sensitivity
2. Wavelengths used in night mode
3. Wavelengths used in day mode
4. Visible light
5. Near-infrared light

Cameras with a removable IR-cut filter have day/night functionality, as they deliver color video during the day, and black and white video at night. They are useful in low-light situations, covert surveillance, and in environments that restrict the use of artificial light.

IR illuminators that provide NIR light can be used together with day/night cameras to further enhance the camera's ability to produce high-quality video in low light or complete darkness. Some day/night cameras have built-in IR illumination using IR LED lights. IR illumination normally provides IR light with a wavelength of 850 nm or 940 nm.

External IR illuminators and a camera with built-in IR illuminators.

Built-in IR LEDs in Axis cameras can be adjusted to match the viewing angle and can be activated automatically in darkness, upon an event, or upon request by a user. Axis cameras with built-in IR LEDs simplify installation and provide a cost-effective option compared with using external IR illuminators. External illuminators, on the other hand, allow installers to freely choose the IR illuminator– for instance, a long range model–and place the light where it is needed and not necessarily in the same location as the camera.

3.4 Image sensors

The image sensor is a key component of any digital camera. The image sensor registers the light coming through the lens from all parts of the scene and converts it to electric signals. These signals provide the information that is needed for the camera to, after additional amplification and processing, reproduce a digital image of the scene.

The camera's image sensor is made up of millions of photodetectors (photosensitive diodes), commonly known as pixels. Each pixel captures light (photons) throughout a defined period of time, which is the camera's exposure time, or exposure interval. After that period of time, the pixel is read out and its charge is measured. A new exposure interval begins and the pixel can capture new photons.

The quality of sensors has undergone dramatic improvements and megapixel, HDTV, and 4K sensors are widely available. But although the surveillance industry has continued to move to higher resolutions, manufacturers have often kept the same sensor size to avoid the higher cost of using a larger sensor. This means they need to fit more photodetectors in the same sensor area, making each pixel smaller and able to capture less light. The charge after each exposure interval will consequently be lower and the electric signal from each pixel will need more amplification and be noisier.

Thus, by simply increasing the number of pixels in a sensor of the same size you will get better resolution, but you may also get images with lower quality. This is especially true in low light scenes, where image noise tends to be more disturbing. If you instead increase the size of the sensor, each photodetector can capture more photons and generate a stronger signal with less noise.

Axis offers cameras with various sensor sizes, including several that combine 4K resolution with a large sensor. With pixels that are more than four times larger than those in most other 4K cameras, these cameras with large sensors effortlessly produce high-resolution footage that is clear and crisp even in low light.

3.5 Exposure control

The two main elements that control how much light an image sensor receives are the lens's light-gathering ability, or f-number, and the exposure time. A third element - gain - is an image level 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.

Exposure time will always have an effect on images, and the settings related to exposure can be changed in a number of ways. The most important ones, exposure priority, exposure zones, WDR and dynamic range, and backlight compensation, are explained in this section.

3.5.1 Exposure priority

Bright environments require shorter exposures. Low-light conditions require longer exposures so that the image sensor can take in more light and thus improve the image quality. However, increasing the exposure time also increases motion blur and lowers the total frame rate, since more time is required to expose each image frame.

In low-light conditions, Axis cameras allow users to prioritize video quality in terms of either movement or low noise (graininess). For rapid movement or when a high frame rate is required, a shorter exposure/faster shutter speed is recommended, but image quality may be reduced.

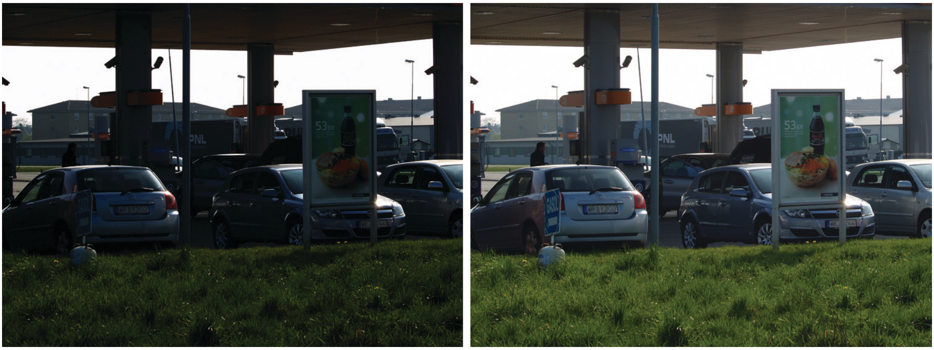
When low noise is prioritized, the gain (amplification) should be kept as low as possible to improve image quality, but the frame rate may be reduced as a result. Keep in mind that in dark conditions, setting a low gain can result in a very dark image. A high gain value makes it possible to view a dark scene, but with increased noise.

3.5.2 Exposure zones

A camera's automatic exposure must decide which part of the image should determine the exposure value. In many Axis cameras, the user can also employ exposure zones to make sure that the most important part of the scene is optimally exposed.

3.5.3 Backlight compensation

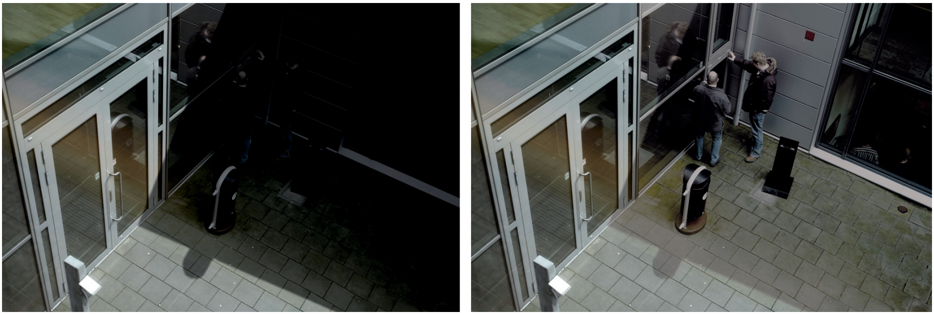
Network cameras with backlight compensation strive to ignore limited areas of high illumination (typically the sky), as if they were not present. Backlight compensation enables objects in the foreground to be seen, although the bright areas will be overexposed.



Strong backlight, without backlight compensation (left). With backlight compensation applied, the foreground is more visible (right).

3.5.4 Dynamic range

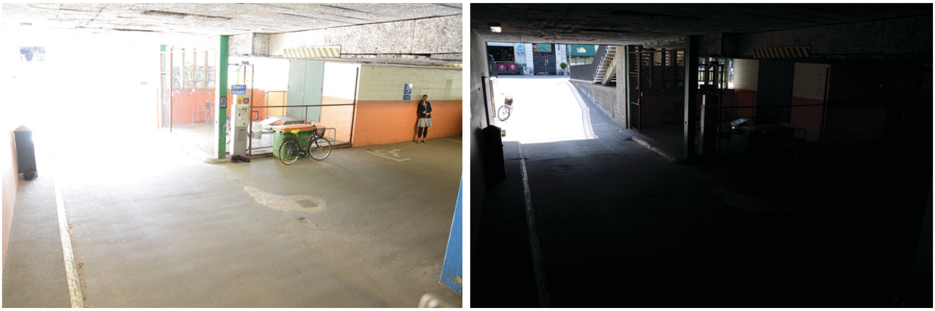
Dynamic range, as it relates to light, is the ratio between the highest and lowest illumination values in an image. Many scenes have high dynamic range, with areas that are very bright and very dark. This is a problem for standard cameras, which can only handle a limited dynamic range. In such scenes, or in backlit situations where a person is in front of a bright window, a standard camera will produce an image in which objects in the dark areas will hardly be visible. To increase a camera's dynamic range capability and enable objects in dark and light areas to be seen, various techniques can be applied. Exposure can be controlled and tone mapping can be used to increase the gain in dark areas.



Two images of the same scene. The image on the right handles the dynamic range in the scene better, and details in both the bright and dark areas are visible.

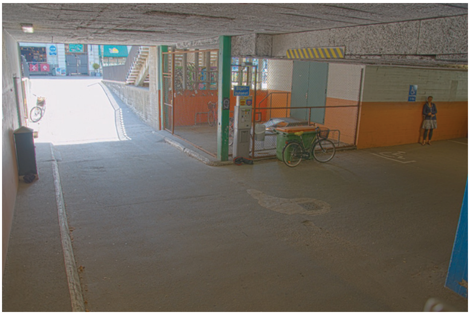
3.5.5 WDR imaging

Wide dynamic range (WDR) imaging is a way to recreate the full dynamic range of a WDR scene in one single image. For example, see the parking garage scene below. A conventional camera cannot capture its full dynamic range, and visibility must be sacrificed either in the dark or the bright areas.



Parking garage with a challenging light situation. To the left, the image is overexposed. To the right, the image is underexposed.

With a WDR-capable camera, all areas can be made visible in one single image.



Parking garage with a challenging light situation, as captured by a WDR-capable surveillance camera.

Axis has several solutions for WDR imaging:

- **Forensic WDR** is a combination of a dual-exposure method and a local contrast enhancement method. It provides images that are tuned for maximal forensic usability. Employing the latest generation of image processing algorithms, this technology effectively reduces visible noise and anomalies. Forensic WDR is suitable also in scenes with motion and in ultra high resolution cameras.

- **WDR – forensic capture** is a combination of dual exposure and a local contrast enhancement method. It provides an image that is tuned for maximal forensic usability.
- **WDR – dynamic capture** uses a dual-exposure method for merging images with different exposure times. The dynamic range is limited by visual anomalies, for example related to motion and flickering in the scene.
- **WDR – dynamic contrast** uses a contrast enhancement method with fairly limited dynamic range but with very few visual anomalies. Since only one exposure is used, this solution performs well in scenes with a lot of motion.

The dynamic range capability of a camera is usually specified as a dB value. However, actual WDR performance is not easily measured, since it depends on many factors, including scene complexity, scene movements, and camera image processing capability. Axis prioritizes forensic usability and a high image quality instead of a high dB value. Therefore, an Axis camera with a certain specified dynamic range could very well outperform a competing camera that has a higher dB value.

3.6 Active tampering alarm

The active tampering alarm automatically alerts the operator when a camera is manipulated, enabling security staff to quickly detect disrupted camera operation. The application is especially useful where there is a risk of vandalism, such as in schools, prisons, public transportation, and in harsh environments where weather, vibration, or dirt can affect the camera performance. The active tampering alarm detects incidents such as redirection, blocking, or defocusing of cameras, and reacts when the camera is attacked, spray-painted, or intentionally covered.

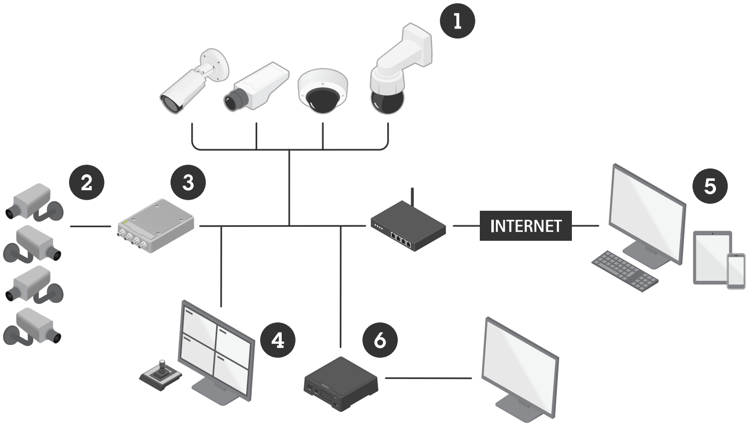
3.7 Sound detection

Sound detection can be used to detect noise, such as voices or the breaking of a window, and trigger the transmission and recording of video or audio or alert operators to suspicious activities. Sound detection is a powerful complement to video because it can detect activity beyond the camera's field of view or in areas that are too dark for video motion detection. For sound detection to work, the camera needs to include audio support and either have a built-in microphone or an external microphone attached.

4. Video encoders

Video encoders enable an existing analog CCTV video surveillance system to be integrated with a network video system. Video encoders play a significant role in installations with many analog cameras.

4.1 What is a video encoder?



Video encoders and decoders can be used to integrate analog video cameras and live view monitors in a network video system. Network cameras (1) are here supplemented by analog cameras (2) and a video encoder (3). The system is managed through a video management system (4) and can be remotely accessed from a computer or mobile device (5). A decoder (6) enables the use of monitors for displaying live video without a computer.

Video encoders allow security managers to keep using their analog CCTV cameras while at the same time constructing a video surveillance system that provides the benefits of network video. If a video encoder is included in the system, analog cameras can be controlled and accessed over an IP network, such as a local area network or the internet. This also means that old video recording equipment such as DVRs and monitors can be replaced with standard computer monitors and servers.

4.1.1 Video encoder components and considerations

Axis video encoders offer many of the same functions available in network cameras. When selecting a video encoder, key considerations for professional systems are reliability and quality. Other considerations include the number of supported analog channels, image quality, compression formats, frame rate, and resolution. Some encoders support HD analog cameras as well as standard resolution analog cameras. Features such as PTZ support, audio, event management, analytics, Power over Ethernet, and security functionalities may also be crucial.

If the video encoder needs to withstand conditions such as vibrations, shocks, and extreme temperatures, a protective enclosure or a rugged video encoder should be considered.

Video encoders supporting four channels and 16 channels.

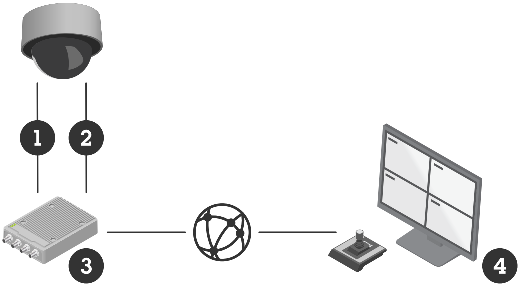
Through a multi-channel video encoder, video signals from remote cameras can share the same network cabling, thereby reducing cabling costs. If investments have been made in analog cameras but coaxial cables have not yet been installed, it is best to use and position video encoders close to the analog cameras. This reduces installation costs as it eliminates the need to run new coaxial cables to a central location – the video can be sent over an Ethernet network instead.

4.1.2 Event management and analytics

One of the main benefits of Axis video encoders is the ability to provide event management and analytics – capabilities that cannot be provided in an analog video system. Built-in analytics, such as multi-window video motion detection, sound detection, and an active tampering alarm, as well as input ports for external sensors, all enable a network video surveillance system to be constantly on alert for events. Once an event is detected the system can automatically respond with actions that may include video recording, sending email alerts, activating lights, opening/closing doors, and sounding alarms.

4.2 Video encoders with analog PTZ cameras

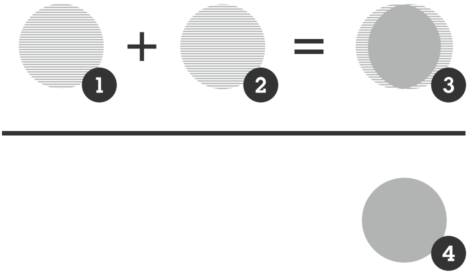
In a network video system, pan-tilt-zoom commands from a control board are carried over the same IP network as the video transmission and are forwarded to the analog PTZ camera through the video encoder's serial port (RS-422/RS-485). Video encoders, therefore, enable analog PTZ cameras to be controlled over long distances, even over the internet.



An analog PTZ dome camera can be controlled via the video encoder's serial port (for example, RS-485) making it possible to remotely control it over an IP network.
1. RS–485 twisted pair cable
2. Coax cable
3. Video encoder
4. Workstation with joystick

4.3 De-interlacing techniques

Analog cameras use interlaced scanning to form an image. This means that two fields of lines are generated: one field displaying the odd lines, and a second field displaying the even lines. When transmitting an interlaced image, the odd and even lines in the image are transmitted alternately, which reduces the use of bandwidth by half. Network cameras instead use progressive scanning, in which all lines in the image are captured, transmitted, and displayed in a single frame.



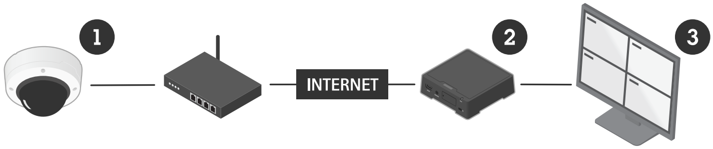
Top: an interlaced scan image, with odd and even lines transmitted alternately, and its appearance on a computer monitor. Bottom: the appearance of a progressive scan image on the same monitor.
1. First field: odd lines.
2. Second field: even lines, 17/20 (NTSC/PAL) milliseconds later.
3. Freeze frame on moving object using interlaced scanning.
4. Freeze frame on moving object using progressive scanning.

Video from analog cameras is designed to be viewed on analog monitors such as traditional TV sets, which use interlaced scanning. When such video is instead shown on a computer screen, which uses progressive scanning, interlacing effects (i.e., tearing or comb effect) from moving objects can be seen. To reduce the unwanted interlacing effects, different de-interlacing techniques can be employed. In advanced Axis video encoders, users can choose one of two de-interlacing techniques: adaptive interpolation or blending.

Adaptive interpolation offers the best image quality, and 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.

4.4 Video decoders

Axis video decoders enable digital monitors to connect to and display live video from Axis cameras. This is a cost-effective solution for video monitoring where multiple live video streams can be displayed on a public view monitor or security monitor without the use of connection via a PC.



A video decoder (2) makes it possible to display live video from an Axis camera (1) on a monitor (3) without using a computer.

5. Video resolutions

The more pixels a sensor has, the greater its potential for capturing finer details and for producing a higher-quality image. Several new, world-wide standardized resolutions have been introduced, originating from the computer and digital television industry.

5.1 Megapixel resolutions

A megapixel sensor delivers an image that contains millions of pixels (one million or more). Megapixel cameras are used in surveillance where details are critical, such as when people and objects need to be identified or a large area needs to be monitored.

According to best practice in video surveillance, an overview image needs about 70–100 pixels to represent 1 m (20-30 pixels per foot). For situations that require detailed images, such as identification of individuals, you may need as much as 250 pixels per meter (80 pixels per foot). For example, this means that if it is necessary to identify people passing through an area that is 4 m wide and 4m high, the camera must be able to provide a resolution of at least one megapixel (1000 × 1000 pixels). For details about recommended pixel densities, see chapter .

5.2 High-definition television (HDTV) resolutions

The two most important HDTV standards are SMPTE 296M, which defines the HDTV 720p format and SMPTE 274M, which defines the HDTV 1080 format.

A camera that complies with the SMPTE standards indicates adherence to HDTV quality and should provide all the benefits of HDTV regarding 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 de-interlacing technique needs to be applied when the video is to be processed by a computer or displayed on a computer screen.

Size	Aspect ratio	Scan	Frame rate (fps/ Hz)	Label
1280 × 720	16:9	Progressive	50	720p50
1920 × 1080	16:9	Interlaced	25[a]	1080i50
1920 × 1080	16:9	Progressive	25	1080p25
1920 × 1080	16:9	Progressive	50	1080p50

Table 5.2a *Basic HDTV image sizes in the European Broadcasting Union. [a] 50 Hz field rate. Note that other frame rates can be used. The most common are 24, 25, 30, 50, and 60 fps.*

Size	Aspect ratio	Scan	Frame rate (fps/ Hz)	Label
1280 × 720	16:9	Progressive	60	720p60
1920 × 1080	16:9	Interlaced	30[a]	1080i60
1920 × 1080	16:9	Progressive	30	1080p30
1920 × 1080	16:9	Progressive	60	1080p60

Table 5.2b *Basic HDTV image sizes in the National Television System Committee countries. [a] 60 Hz field rate. Note that other frame rates can be used. The most common are 24, 25, 30, 50, and 60 fps.*

5.3 Ultra-HD resolutions

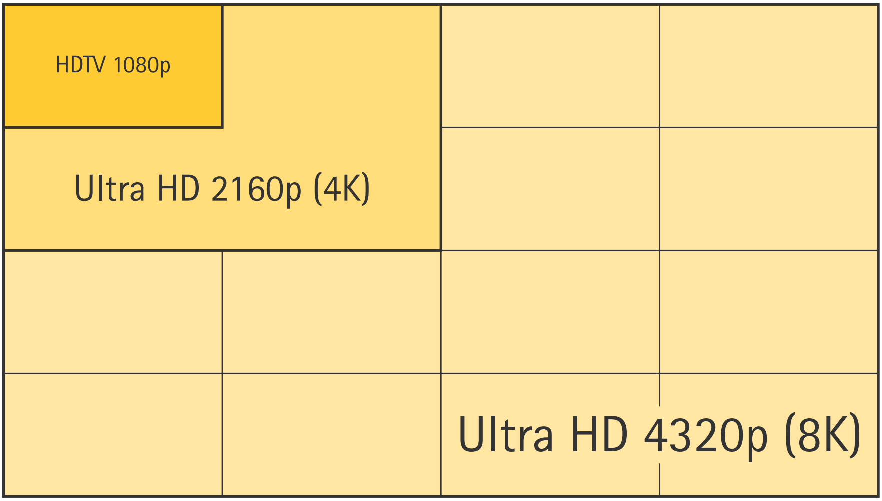
Like HDTV, Ultra-HD is a standard that guarantees a certain video quality, whereas megapixel is merely a statement of the camera's resolution. Ultra-HD television (UHDTV) has two digital video formats:

> Ultra-HD 2160p is commonly referred to as 4K, with a resolution of 3840x2160 pixels giving 8.3 megapixels, four times more than HDTV 1080p.

> Ultra-HD 4320p is commonly referred to as 8K, with a resolution of 7680x4320 pixels giving 33.2 megapixels, sixteen times more than HDTV 1080p.

Both formats feature extra high color fidelity, progressive scanning, up to 100/120 frames per second, and H.265 compression.

In video surveillance, the unmatched resolution of Ultra-HD means exceptional digital zoom capabilities and extended field of view. These powers make Ultra-HD cameras ideal for capturing facial features and other details. However, Ultra-HD demands high-quality lenses, lots of pixels, and large sensors that can capture enough light, as well as significant expansions in bandwidth and storage capacity. In other words, the increased resolution may come with very high costs.



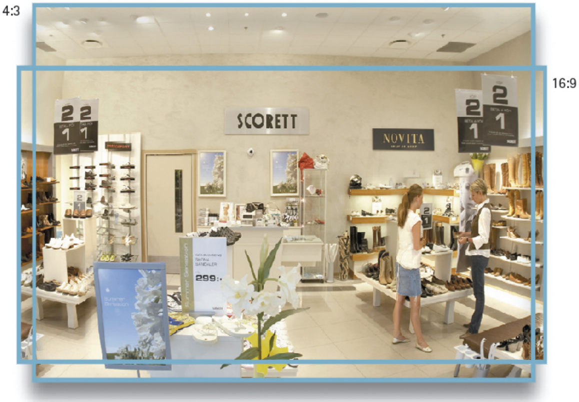
Ultra-HD 4320p (8K) has 16 times the resolution of HDTV 1080p. Ultra-HD 2160p (4K) has 4 times the resolution of HDTV 1080p.

5.4 Aspect ratios

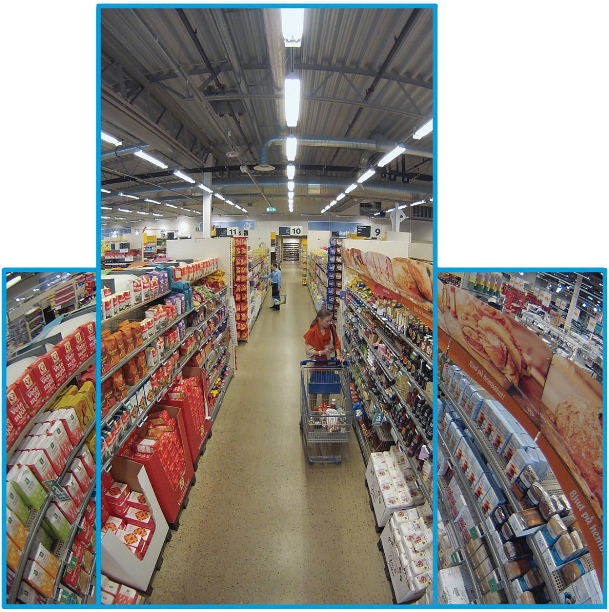
Aspect ratio is the ratio of the image's width to its height. An old-fashioned TV monitor, traditionally used to view analog surveillance video, displays an image with an aspect ratio of 4:3. Network video can offer the same ratio but also other ratios such as 16:9.

The advantage of a 16:9 aspect ratio is that unimportant details usually located in the upper and lower parts of the scene are not part of the image. Therefore, bandwidth and storage requirements can be reduced.

The aspect ratio 9:16 is simply a 16:9 image that has been rotated 90°. The 9:16 aspect ratio is popular in video surveillance, because the full view of the camera can be used to monitor narrow scenes such as retail store aisles, roads, school hallways, and train station platforms. This aspect ratio is sometimes referred to as corridor format.



4:3 and 16:9 aspect ratios



Corridor format is often used in retail environments.

6. Video compression

Most network video vendors today use standardized compression techniques that ensure compatibility and interoperability. Industry standards are particularly relevant to video surveillance because the video material may be used for many different purposes and, in some cases, must be viewable many years after the recording date. Because of technologies like Axis Zipstream, a surveillance system can combine the use of high-resolution cameras with reasonable system costs, while preserving the forensic value of the video. This is because unnecessary data is removed, keeping storage requirements down, while the important details and motion are preserved.

6.1 Compression basics

Video compression technologies are about reducing and removing redundant video data so that digital video can be effectively viewed over a network and stored on computer disks. With efficient compression techniques, significant reductions in file size can be achieved with little or no adverse effect on the video quality. But if the compression level of a given compression technique is increased too much, it may have negative effects on the quality.

6.1.1 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 decompress the video and produce 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 work together is called a video codec (encoder/decoder).

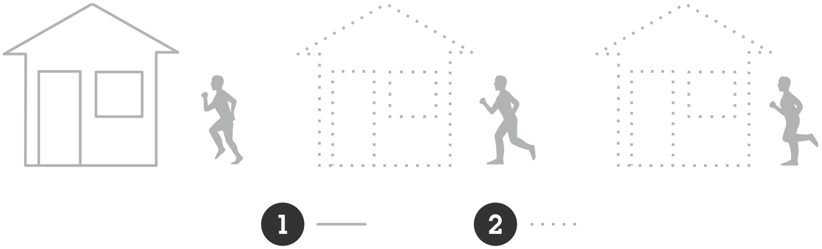
Video codecs of different standards are normally not compatible with each other; that is, video content that is compressed using one standard cannot be decompressed with a different standard. For instance, an H.264 decoder will not work with an H.265 encoder. This is simply because one algorithm cannot 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.

6.1.2 Image compression vs. video compression

Different compression standards utilize different methods to reduce 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 might not be noticeable to the human eye. Motion JPEG is an example of such a compression standard. Images in a Motion JPEG sequence are coded or compressed as individual JPEG images.

In the Motion JPEG format, the three images in the above sequence are coded and sent as separate unique images, with no dependencies on each other.

Video compression algorithms such as H.264, H.265, and AV1 use interframe prediction to reduce video data over a series of frames. This involves techniques such as difference coding, where one frame is compared with an earlier sent reference frame and only the pixels that have changed with respect to the reference frame are coded. This way, the number of pixel values coded and sent is reduced. When such an encoded sequence is displayed, the images appear as in the original video sequence.



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 image for the static elements, i.e., the house.

Only the moving parts, i.e., the running person, are coded, thus reducing the amount of information sent and stored.
1. Transmitted
2. Not transmitted

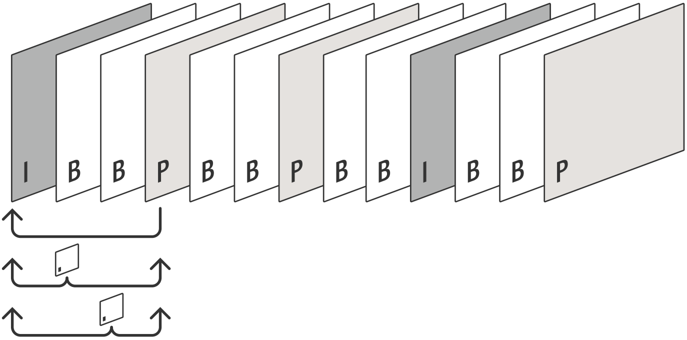
Other techniques can be applied to further reduce the data. An example is block-based motion compensation, which takes into account that much of what makes up a new frame in a video sequence can be found in an earlier frame, but perhaps in a different location. This technique divides a frame into a series 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.

In 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 reference to any other frames. The first image in a video sequence is always an I-frame and is needed as a starting point for new viewers or a re-synchronization point if the 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 when new clients start to view the stream. The drawback of I-frames is that they consume many more bits. 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). P-frames usually require fewer bits than I-frames, but one 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.



A typical sequence of 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 decoder restores a video by decoding the bit stream frame by frame, decoding must always start at an I-frame. If used, P-frames and B-frames must be decoded together with the reference frame(s).

Axis video products allow users to set the GOP (group of pictures) length, which determines how many P-frames should be sent before another I-frame is sent. By lowering the frequency of I-frames (a longer GOP), the bit rate can be reduced. However, if there is congestion on the network, the video quality may drop, due to network packets being lost.

Besides difference coding and motion compensation, other advanced methods can be employed to further reduce data and improve video quality. H.264 and the other video compression standards support 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).

6.2 Compression formats

Axis uses four video compression standards: H.264, H.265, AV1, and Motion JPEG. AV1 is the newest and most advanced video compression standard, with very attractive bitrate. MPEG-4 Part 2 (simply referred to as MPEG-4) has been phased out.

6.2.1 H.264

H.264, also known as MPEG-4 Part 10 or ISO/IEC 14496-10 Advanced Video Coding, is the MPEG standard for video encoding. It 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).

H.264 is the most widely adopted standard and it is compatible with a vast number of operating systems, softwares, and mobile clients. H.264 has helped accelerate the adoption of megapixel/ HDTV cameras since the highly efficient compression technology can reduce the large file sizes and bitrates generated without compromising image quality.

While still being a dependable choice for video compression, H.264 was introduced over two decades ago and is no longer the standard with the best bitrate. Its aging technology struggles to meet the growing demands for high-resolution video transmission and storage and H.264 does not support video wider than 8K.

The Baseline profile for H.264 uses only I- and P- frames, while the Main profile may also use B-frames in addition to I- and P-frames. Without B-frames, latency is lower. Axis video products use the H.264 Baseline or Main profile. In video products with more powerful processors, Axis uses the Main profile without B-frames, to enable higher compression and at the same time low latency and maintained video quality.

6.2.2 H.265

H.265 is the ITU approved High Efficiency Video Coding standard, ISO/IEC 23008-5. Compared with H.264, H.265 improves compression by 15–40% for the same video quality. The standard is tuned for higher video resolutions, higher frame rates, and more motion.

H.265 encoding does not yet entirely fulfill the requirements of surveillance type video. Most surveillance equipment supports H.265, but there are limitations in decoder support and browser support. Many users must continue using H.264 to be able to view video on their preferred clients, but this should not be a problem since Zipstream with H.264 is very bitrate efficient. The newer standard AV1 is likely to challenge H.265 as preferred successor to H.264, given the superior performance and broad industry support of AV1 compared to H.265.

6.2.3 AV1

AV1 is a modern video encoding standard that is optimized for video transmission over the internet. AV1 provides high-resolution, hassle-free, and cost-efficient streaming and storage.

AV1 is expected to become the dominant codec in the video surveillance industry thanks to low bitrate, new features, and wide client decoder support. It is already supported by major browsers, operating systems, cloud platforms, and mobile devices.

AV1 was standardized in the Alliance for Open Media (AOM) as *AOMedia Video 1 video coding* according to *AV1 Bitstream & Decoding Process Specification v1.0.0* by aomedia.org. AOM was founded by the world's main IT companies and AV1 is freely accessible without licensing fees to AOM.

AV1 has gained widespread support across the IT industry. It is widely used in cloud streaming technologies, such as WebRTC, enabling efficient real-time communication and video streaming. Seamless cloud integration allows developers to directly use security video in IT applications, such as logistics systems, to enhance business intelligence and operational efficiency.

6.2.4 Zipstream for H.264, H.265, and AV1

Optimized for video surveillance, Axis Zipstream technology is a radically more efficient video encoder implementation, further lowering bandwidth and storage requirements by an average of 50% or more, on top of the already received reduction. Zipstream is in no way a replacement for H.264/H.265/AV1 but an improvement that is 100% standard-compliant.

Zipstream works by including a module in the camera's video compression engine to ensure that important details in the image (regions of interest) get enough attention, while unnecessary data can be removed. Zipstream cuts storage requirements without any complicated integration, and no costly changes are required in the rest of the surveillance system. Details of interest and motion are preserved at the specified video quality, while the Axis-unique module compresses the other areas much more, to make optimum use of the available bandwidth. Zipstream is supported by the latest Axis cameras, including PTZ cameras and 4K Ultra HD cameras.

The solution that is used to compress video according to H.264, H.265, and AV1 is not part of the standards, since only the syntax and the method to perform playback is standardized. This enables improved standard-compatible H.264/H.265/AV1 encoders, such as Zipstream, to be created while preserving the file format for interoperability (decoder compatibility).

Zipstream is a collection of different algorithms that reduce bandwidth:

- **Dynamic Region-Of-Interest (ROI) algorithm**. Automatic full frame rate method to select important areas to reduce size of all frames.
- **Dynamic Frames-Per-Second (FPS) algorithm**. Additional method to reduce frame rate in order to reduce the storage needed for P-frames.
- **Dynamic Group-Of-Pictures (GOP) algorithm**. Additional method to change GOP length in order to reduce the amount of storage needed for I-frames.

Zipstream adapts the compressed video stream based on scene motion, scene content, ambient light level, and configuration options, such as, compression parameters, frame rate, and a strength parameter that defines the effort level.

Strength parameter	Effort level	Visible effect
Off	Off	None
10	Low	No visible effect in most scenes
20	Medium	Visible effect in some scenes: less noise, and slightly lower level of detail in regions of lower interest
30	High	Visible effect in many scenes: less noise, and lower level of detail in regions of lower interest
40	Higher	Visible effect in even more scenes: less noise, and lower level of detail in regions of lower interest
50	Extreme	Visible effect in most scenes: less noise, and lower level of detail in regions of lower interest

Table 6.2a *Zipstream strength parameter values and effort levels.*

You can configure the different parts of the Zipstream algorithm individually or use storage profile, which automatically configures Zipstream to optimize the video for storage.

> **Classic profile**: The default profile, which lets you control major parts of the Zipstream algorithm individually. Initially, the strength parameter is set to 10, and dynamic GOP and dynamic FPS are off. This setting is compatible with all existing applications, while still reducing the bitrate. For even lower bitrate, you can choose a higher strength parameter value and activate dynamic GOP and/or dynamic FPS.

> **Storage profile**: This profile configures Zipstream so that the video is optimized for storage and later access, which is the main use case of Axis video products. Storage profile minimizes the bitrate while maximizing the evidence value for that use case. With storage profile, the camera automatically enables the specific Zipstream algorithm that is most suitable for the camera, and uses more advanced video encoding tools. The profile is different in different cameras depending on their capabilities, and the result can differ between camera types.

6.2.5 Motion JPEG

Motion JPEG or M-JPEG is a digital video sequence that is made up of a series of individual JPEG images. Since there is no dependency between the frames, a Motion JPEG video is robust, meaning that if a 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 may be needed when integrating with systems that only support Motion JPEG. It is also popular in applications where individual frames in a video sequence are required–for example, in analytics–and where low frame rates are used, for example in a VMS overview.

Because it is a series of still, complete images, Motion JPEG cannot use video compression techniques to reduce data. This leads to a relatively high bitrate or low compression ratio for the delivered quality compared with other video compression standards.

For video products with resolution above 1080p, Motion JPEG may not be usable, since the images may become too big to transfer over a 100 Mbit/s network in full fps. Upgrading to a gigabit network will only move the bottleneck to the image processing steps in the camera before and after network transportation, and greatly reduce usability. If JPEG images are required, the system frame rate must be reduced accordingly.

6.2.6 JPEG

Still images follow the JPEG standard, which is supported by all cameras. Still images are sometimes used in video cameras as icons or for overview.

6.3 Average, variable, and maximum bitrates

H.264, H.265, and AV1 can all be configured to use encoded video streams with average, variable, or maximum bitrate. The optimal selection depends on the application and the network infrastructure.

With ABR (average bitrate), a specified amount of storage is used over a given period of time. A video stream is assigned a certain amount of storage and the ABR controller in the camera will adapt the video quality to make sure to fit the video from the whole period into the bitrate budget. Unused storage from earlier, idler, periods can be used for maintaining high video quality in later, busier, periods and the bitrate budget is kept. This is meant to improve the video quality and simultaneously avoid overshooting the storage limits of the system. ABR is optimal for continuously recorded streams without scheduled pause periods.

With VBR (variable bitrate), a predefined image quality is maintained regardless of whether the scene contains motion, or not. This means that bandwidth use will increase when there is a lot of activity in a scene and decrease when there is less motion. This is often desirable in video surveillance where there is a need for high quality, particularly if there is motion in the scene. Since the bitrate may vary, even when an average target bitrate is defined, the network infrastructure (available bandwidth) must be able to accommodate high throughputs.

With limited bandwidth available, the recommended mode is normally MBR (maximum bitrate), setting a limit on how high the bitrate is allowed to be. The disadvantage is that when there is, for instance, increased activity in a scene that results in a bitrate higher than the target rate, the restriction on the bitrate leads to a lower image quality and frame rate. Axis video products allow the user to prioritize either the image quality or the frame rate if/when the bitrate rises above the target rate.

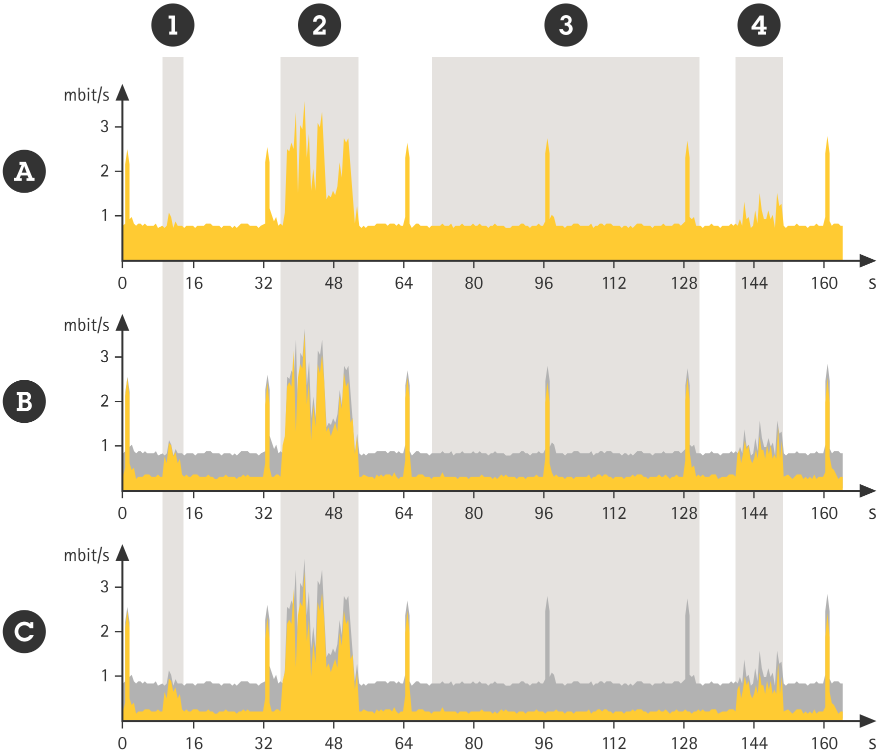
6.4 Comparing standards

When comparing the performance of video compression standards, it is important to note that results may vary between encoders that use the same standard, as different subsets can be implemented. As long as the output of an encoder conforms to a standard's format and decoder, it is possible to make different implementations. This helps to optimize the technology and reduce the complexity in implementations.

However, it also means that a standard cannot guarantee a given bitrate or quality and comparisons cannot be properly made without first defining how the standards are implemented in an encoder.

Unlike an encoder, a decoder must implement all the required parts of a standard to decode a compliant bitstream. This means that only the decoder is truly standardized. The standard specifies exactly how a decompression algorithm should restore every bit of a compressed video. If video quality is a concern, the user should test a few products to make sure that the quality matches the purpose.

Given the same level of image quality, the figure below shows a bitrate comparison between H.264 and Axis improved H.264 (Axis Zipstream) at low and high effort levels.



The instantaneous bitrate in four different scenarios (1, 2, 3, 4) for various Zipstream effort levels (A: Zipstream off, B: low, C: high). The bitrate reduction is represented by the areas shaded in grey. Each I-frame update is clearly visible as a spike in bitrate, which can be read on the vertical axes. All streams are variable bitrate (VBR) streams with GOP length=32.

The time periods in the figure highlight the behavior of Zipstream under different conditions:

1. Period with brief, small movements. The small motion is detected, and adding bits in that region can preserve the quality of the moving part of the video.
2. Longer period with larger movement requires more space but still possible to save storage as the dynamic ROI algorithm detects areas where non-prioritized information can be removed.
3. Periods with no motion are detected, and the dynamic GOP algorithm removes unnecessary I-frame updates.
4. Periods with small, long-lasting movement.

AXIS Site Designer can be used to estimate bitrates for various types of scenes.

7. Audio

Using the audio capabilities with a video surveillance system provides invaluable possibilities for detecting and interpreting events and emergencies. Audio analytics can monitor the audio streams and react when something stands out. Combine the system with network speakers, and you can easily communicate with visitors or issue warnings to intruders.

7.1 Sound detection

Sound detection can be deployed as a standalone technology enabling several use cases in crime prevention, protection, and forensics. One example is audio surveillance with direct operator interaction to increase scene awareness. In a hospital or care facility, sound detection can help you perceive if a patient is in distress and needs a nurse. Sound detection can also be about detecting whether an unexpected sound came from the left or the right and point a PTZ camera towards the sound source.

If used in conjunction with video surveillance, audio adds another dimension of information for decision making and has the potential to reinforce a majority of existing video surveillance use cases. For example, security operators can get a significantly better overview of scene events if their video stream is complemented with an audio stream.

7.1.1 Devices and technology for audio-in connectivity

There are several ways to implement sound detecting capability in a camera.

A camera with integrated microphones for high-quality sound detection, a standalone digital microphone with 3.5 mm (1/8 inch) connector, and an audio and I/O interface that uses portcast technology to seamlessly add sound detection capability to a camera.

Integrated microphone: With built-in microphones, audio features such as voice enhancer can be tailored to the specific camera model and its intended use. With two integrated microphones, a camera can deliver stereo sound which makes it possible to distinguish which direction sounds are coming from. With three or more built-in microphones the camera also receives more detailed spatial information. This can be used for automatic audio source localization or beamforming, which is a way of “zooming in” on audio coming from a specific direction.

Integrated audio support and standalone microphone: Cameras often have a mic-in/line-in 3.5 mm (1/8 inch) jack for connecting, for example, a separate microphone. Separate microphones can be placed in the strategically best locations and capture clear and relevant audio. If a camera needs to be placed high up on a wall or in a ceiling to provide a visual overview, a small, separate microphone can be discreetly placed in a lower position, closer to where people are. If connected using a digital audio extension kit, a digital microphone can transport the audio signal with a network cable up to 100 m (358 ft) without losses.

Edge-to-edge technology: Microphone pairing, using edge-to-edge technology, is possible if both devices are on the same network and have edge-to-edge support in their software. After pairing, the microphone’s audio settings can be controlled from the camera’s user interface even if the camera did not originally support audio.

Audio and I/O interface with portcast: Portcast technology is an Axis-unique concept where an audio and I/O interface device is physically connected directly to the camera using a network cable. It can add two-way audio functionality to cameras that do not have audio support on their own. The portcast device uses the camera’s IP address, is controlled from the camera, and allows the camera to provide seemingly camera-integrated audio connectivity with audio and video in one stream over the network. Some portcast devices come with integrated microphone.

Connectivity hub: This device adds audio-in functionality to your system, including two-way communication capabilities and broad microphone compatibility. The connectivity hub has its own IP address and features several I/Os and ports to integrate various non-visual sensors.

7.1.2 Sound detection enhancements

Devices with sound detecting capabilities use various enhancements for improved sound.

- **Voice enhancer:** amplifies voice content relative to other sounds with the purpose of making speech more perceptible.
- **Automatic gain control:** dynamically adapts the gain to changes in the sound.
- **Echo cancellation:** recognizes and removes sounds that are produced by the built-in speaker.
- **Graphic equalizer:** makes it possible for advanced users to filter out specific sound frequencies.

7.1.3 Audio analytics

Just as several types of video analytics can be employed for automatic alarming based on visual detection, audio analytics can monitor the audio streams and react when something stands out. Audio analytics can be set to trigger automatic alarms and other actions when a microphone picks up sounds associated with people shouting or glass breaking, or other anomalous sounds. This provides early warning that enables quick responses and intervention. Audio analytics can also be used to automatically redirect a PTZ camera towards an audible incident or to measure SPL (sound pressure level) to give insights about noise pollution.

Audio analytics in general do not record sound continuously. They typically just buffer it temporarily and process the audio to search for specific patterns, levels, or frequencies. But systems can be set up to record what was buffered just before and after a detection to allow security to verify the detection and, possibly, preserve the audio for forensic evidence.

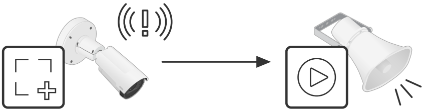
7.2 Audio output

Adding IP-based speakers to a video surveillance system can help you proactively deter crime by responding immediately and intervening remotely with prerecorded or live messages. Speakers can also be used in a multipurpose audio system that enables deterrence, information, safety messages, and background music, all in a single installation.

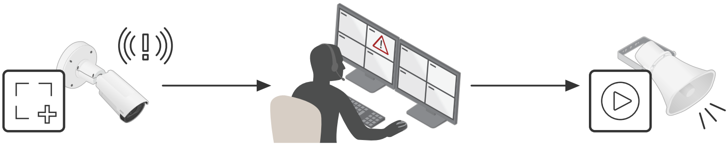
7.2.1 Audio output in video surveillance

Many cameras come with integrated audio capability and an audio output connector for connecting a speaker. But a camera with support for edge-to-edge technology can also be paired with a speaker even if the camera has no audio or line-out capability. After pairing, audio settings can be controlled from the camera's user interface. Many cameras can also connect to speakers by use of a connectivity hub or an audio and I/O interface.

A security solution with audio and video can be monitored or unmonitored with different levels of camera integration.



Unmonitored solution: a camera with analytics detects unauthorized entry or other events in a restricted area and sends a command to a speaker to play a prerecorded audio message.



Monitored solution: a camera with analytics detects unauthorized entry or other events and sends a notification to an operator. The operator can speak live or play a prerecorded audio message.

Cameras can also be connected with audio/visual alerters, such as a strobe siren. This is a fully networked device that can be used to deter intruders or improve operational efficiency with strobe lighting and siren alarms. It can be customized with various white and RGBA light patterns and preconfigured sounds. A strobe siren is especially valuable when connected to a camera with perimeter protection or license plate recognition (LPR) analytics.

7.2.2 Network audio systems for public address

Network speakers and other audio devices can be combined into an IP-based public address (PA) system for live and prerecorded announcements, safety messages, and background music. The use of IP technology makes the system flexible and scalable. It also simplifies integration with other systems as speakers can be integrated directly into a VMS or a Voice over IP (VoIP) phone system.

Axis speakers are complete high-quality audio systems in themselves, with integrated amplifier and digital signal processor for preconfigured sound. They feature an integrated microphone that enables two-way communication and automatic self-checks to ensure optimal sound quality.

Speakers from Axis come with various form factors, sound pressures, and mounting possibilities for different use cases.

You manage the audio content and the devices through audio management software. All Axis audio hardware comes with embedded software for basic use cases in small and midsized systems. Axis also has software options for larger and more advanced systems, even including multisite systems with thousands of sites. With audio management software, every speaker is individually addressable. Speakers can also be grouped into zones, which allows you to target announcements to specific audiences in the relevant areas of a site, without repeating the message across the entire network of speakers. Zones can be easily reconfigured in an instant, without the need for new cabling. Prerecorded messages and background music can be scheduled, and the functionality of the system is automatically monitored.

Read more about network audio systems in Technical guide to network audio, which can be downloaded from *axis.com/learning/technical-guides*.

7.3 Audio communication modes

Depending on the application, there may be a need to send audio in only one direction or both directions. This relates to three basic modes of audio communication:

- **Simplex** means that audio can be sent in one direction only. In network audio, audio is usually sent from an operator to a speaker, for example for communicating warnings or announcements through the speaker. But audio in simplex mode could instead be sent from the speaker to the operator, for example in remote monitoring applications where live audio from a monitored site is sent over a network.
- **Half duplex** means that audio can be sent and received in both directions, but only in one direction at a time. The direction is controlled either through use of a physical push-to-talk button or through voice detection software. This mode of communication is similar to a walkie-talkie conversation. Because speaker and microphone are never active at the same time, there is no risk of echo problems with half duplex.
- **Full duplex** means that users can send and receive audio (talk and listen) at the same time. This mode of communication is similar to a telephone conversation. Full duplex requires both the client (PC, SIP microphone, or VoIP phone) and the speaker to be able to handle full-duplex audio. The implementation must also support acoustic echo cancellation (AEC) in order to avoid echo effects.

Audio devices from Axis work with either half duplex or full duplex for two-way audio.

7.4 Audio codecs

An audio codec (encoder-decoder) is a software system that can digitize and compress data for transmission and decompress the received data. Axis products support various audio codecs:

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 or more, is the recommended codec to use when the best possible audio quality is required.

G.711 and **G.726**, which are non-licensed ITU-T standards. They have lower delay and requires less computing power than AAC-LC. G.711 and G.726 are speech codecs that are primarily used in telephony and have low audio quality. Both have a sampling rate of 8 kHz. G.711 has a bit rate of 64 kbit/s. Axis G.726 implementation supports 24 and 32 kbit/s. With G.711, Axis products support only µ-law, which is one of two sound compression algorithms in the G.711 standard. When using G.711, it is important that the client also uses the µ-law compression.

Axis cameras also support LPCM. In addition, Axis products that support SIP can also use Opus, L16/16000, L16/8000, speex/8000, speex/16000, and G.726-32.

7.5 Synchronization of audio and video

Synchronization of audio and video data is handled by a media player, or by a multimedia framework such as WebRTC.

Audio and video are sent over a network as two separate packet streams. 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 H.264, H.265, or AV1 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.

8. Radar

Radars are ideal for wide-area protection or traffic monitoring. They can be used standalone, for example where privacy concerns restrict camera use, but they are also easy to integrate in a surveillance system.

8.1 A non-visual technology that complements video surveillance

Radar is a non-visual technology and dependable in many situations where other surveillance technologies are inadequate. Radar uses electromagnetic waves to detect movement and is not sensitive to the things that normally trigger false alarms, such as moving shadows or beams of light, raindrops, or insects. It is accurate in any light conditions, 24 hours a day.

Radars also provide crucial information about detected objects that video cameras cannot, such as exact position, and speed and direction of movement. Analytics for detection, tracking, and classification of objects are integrated in the radar.

8.2 Radar devices

Two radars for area and traffic monitoring and a radar-video fusion camera for improved scene intelligence.

Featuring built-in analytics, an Axis radar can accurately detect, classify, and track humans and vehicles. It comes with two detection profiles that are optimized for different scenarios.

The area monitoring profile is for detecting humans and low-speed vehicles. With this profile activated, the radar provides wide area protection 24/7 with low false alarm rate. It is ideal in open outdoor areas with moderate activity, for example, industrial sites or after-hours monitoring of parking lots and loading docks.

The road monitoring profile is for detecting vehicles travelling at higher speeds. With this profile activated, the radar tracks and measures vehicle speeds for traffic flow monitoring. If AXIS Speed Monitor is installed in the radar or in a connected camera, it is easy to extract statistics for more informed decision making and speeds are visualized in the radar's or camera's live view.

A radar-video fusion camera combines two devices in one - a camera with excellent image usability and a fully integrated radar. The radar detects objects over wide areas with little or no light and visualizes the speed and distance of moving objects directly in the application view. The combination of video and radar analytics provides more complete data, with improved scene intelligence combined with the forensic value of video. You can trigger actions based on detection by radar only, camera only, or both, depending on your needs.

8.3 Radars in a surveillance system

Axis radars are powered by PoE and easy to integrate with other devices and video management systems.

In addition to triggering an alarm when it detects an intruder, the radar can also trigger a video recording for visual verification. Combining radars with cameras is especially effective with PTZ (pan-tilt-zoom) cameras, which can track and identify individuals or vehicles based on their exact geographical position provided by the radar.

In perimeter protection, a radar's wide detection area complements a thermal camera's narrow but further-reaching detection area. You can, for example, mount the radar on a fence facing outwards, to create a buffer zone and detect potential intruders before they even reach the fence line. Radars can also be used together with speakers in scenarios where visual identification is not allowed or not prioritized. An intruder that is detected by the radar can be effectively deterred by an audio message.

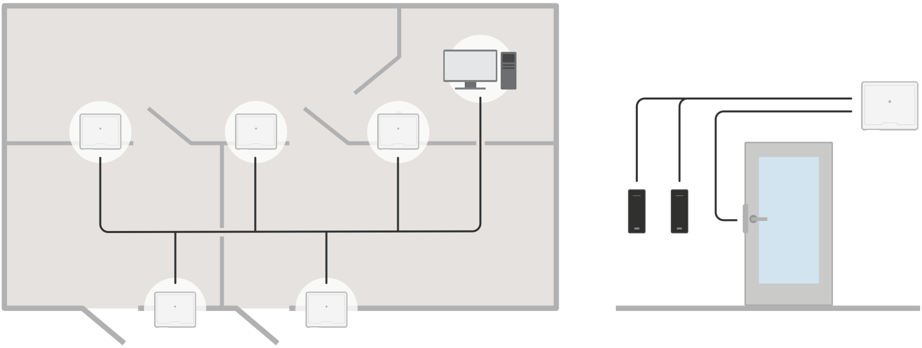
Using a radar in a surveillance system can also save on energy as it can "see" in the dark. For example, you can set triggers that turn on IR lights or floodlights when an object is detected by the radar, which is useful at sites with low activity after working hours. You can also save on storage if you choose to trigger recordings only in certain situations. Furthermore, the low rate of false notifications lets security personnel act only on real threats, allowing them to handle more cameras, thus saving time and money.

9. Access control

Physical access control systems are ubiquitous in factories, hospitals, retail stores, and many other industries throughout the world. Currently, access control is shifting from traditional, proprietary (closed) solutions to open IP technology, which brings major improvements in product and management performance. IP access control can be used as a standalone security system but also as a complement to network video surveillance or integrated with other types of systems.

9.1 What is access control?

In a system for physical access control, devices such as door controllers, card readers, and I/O relay modules are installed next to doors and entry points. Together with access management software, they help manage access for personnel and visitors into specific areas.



Access control system with door controllers, access management software, and card readers.

An example: What happens when an employee presents their access card to the reader at the office entrance? The reader sends the card information to the door controller (connected to the door's electronic lock), which checks the access list (in the door controller's built-in access management system or on a server) to see if the card should be allowed access. If the credentials match an item on the list, the door controller sends a signal to the electronic lock to unlock the door.

Access control can also be integrated with network intercoms to grant visitors access in a controlled and secure manner, with both video identification and two-way communication. Integrating access control systems with video surveillance also adds new dimensions to the security solution, enabling functions such as monitoring, investigation and assistance.

9.2 Why IP in access control?

A traditional access control system is a closed system, designed by vendors who develop the entire product, from controllers and credentials to the software. This ensures system operation but also means a lack of flexibility for the user. As an organization grows, or when its access control needs change, it may have to install an entirely new system and completely remove the old one. And this may need to be done again a few years later if requirements change again.

An IP-based access control system is flexible right from the start, and it is easy to expand it or to add new functionality. It has intelligence all the way out to the door, so that it's possible to make access decisions both locally and centrally. The door controller uses rules that are distributed and updated over the IP network and it can be connected and powered through PoE.

The main benefits can be summarized as:

> **Enhanced security with encryption.** An intelligent, edge-based door controller can guarantee the secure storage of cryptographic keys by using an onboard EAL6+ Certified compute module. An OSDP Secure Channel certification will ensure that communication with the reader is fully encrypted and protected. Such a system can also ensure secure communication with the access control management software.

> **Easy, future-proof integration.** By adhering to open standards and interfaces, IP access control can be integrated with other systems, including surveillance, analytics, intercoms, audio, or time and attendance solutions. The possibilities are endless if the technology is considered an IoT (Internet of things) solution rather than solely access control.

> **Cost-effectiveness.** IP access control solutions can easily be connected to and powered by an existing IP network with no need for special cabling. IP also enables remote management and system health monitoring, which helps lower the total cost of ownership.

> **Scalability.** With IP, you can begin with the solution you need today, and can then easily scale up as the requirements of the business change.

> **Flexibility.** IP access control products are built on open API architecture and are non-proprietary. This means it is possible to use and combine open-standard components from any supplier.

9.3 Access control components

The components of an access control system include everything from the most basic access control management software and hardware to more advanced options.

Access control products including (from the left): a network intercom, a reader, door controller, an I/O relay module, and credentials: key fobs, access cards, and mobile credentials.

9.3.1 Network door controllers

A network door controller can be thought of as the brain of an access control system. It unlocks the door, but it also stores the access control software.

No matter the size of the system, a network door controller can be installed for each door. For installations with basic access requirements, management can be handled by the built-in software, while a more complex system will need third-party software.

A door controller can be integrated with other systems such as video surveillance, intrusion detection, and time and attendance. For example, when someone enters or exits through a door, the door controller can trigger a camera to start recording. Or, if linked with an HVAC system, a door controller's information about building occupancy can be used to adapt heating and cooling of the premises. Door controllers can also be integrated with network intercoms for video and audio communication possibilities.

9.3.2 Readers

Card readers are the most common way to let users identify themselves in an access control system. However, credential types do not have to be limited to cards, especially when you include cameras and network video door stations in an access control solution. Access can be granted based on different factors:

- **Something the user has**, e.g. a smart card, QR code, key fob, or mobile phone.
- **Something the user knows**, e.g. a PIN or the answer to a security question.
- **Biometric factors**, like fingerprints or facial features.
- **Someone verifying the user**, e.g. a receptionist recognizing the user's camera image.

Security is strongest when two or more factor types must be combined to grant access.

9.3.3 Network I/O relay modules

A network I/O relay module provides an easy and cost-efficient way to extend the functionality of any Axis product. It is particularly useful for integrating a network door controller with other systems in a building but can also be used with other facility systems. The module triggers actions when reacting to inputs, such as signals from PIR motion detectors or door position switches. The module can also operate standalone and according to a schedule, for example if you want a gate to unlock at a certain time every day, or if you want specific rules for credentials to regulate an elevator's access to certain floors of a building.

9.3.4 Access management systems

When it comes to overseeing an access control system, there are various software solutions. AXIS Camera Station Secure Entry provides intuitive access management for any need. For a solution based on vehicle access, there is AXIS License Plate Verifier that automatically captures and validates plates for streamlined gate management. There is also an array of third-party software to choose from for access control management.

10.Network intercoms

Network intercoms are used as visitor communication tools at entrances, but also as info points or local emergency phones. They are reliable, easy-to-install devices that increase overall security. Network intercoms are based on open, standardized IP technology that enables easy integration with other systems, such as access control, video surveillance, and IP-based communication systems (VoIP).

10.1 Multifunctional communication devices for increased security

Network video intercoms combine video surveillance, two-way communication, and remote entry control in a single device. They can be placed at entrances and exits for known and unknown visitors, where they enable video calls and allow you to remotely control access through a computer, desk phone, mobile device, or designated answering unit. Intercoms are also widely used as help points or emergency phones within larger areas like cities, parks, or university campuses. Network intercoms can easily be connected to and powered by an existing IP network, so there is no need for special cabling.

Network video intercoms.

Features of network video intercoms from Axis include:

- **High-quality video.** An integrated, high-quality network video camera enables a quality, eye-level view of who is calling. With advanced camera features such as WDR (wide dynamic range), the caller will be clearly visible even in challenging light. Integrated video motion detection analytics can be set up to trigger various kinds of alarms, as well as video recordings. AXIS Camera Application Platform (ACAP) support enables installation of additional analytics applications.

- **Clear, two-way audio.** Communication is clear, uninterrupted, and echo-free thanks to full-duplex audio streaming with noise reduction and echo cancellation. Intercoms may also include accessibility features for hearing-impaired individuals, such as an induction loop for hearing aids. And thanks to audio analytics, intercoms can trigger audio warnings or recordings when, for instance, someone approaches, or if gunshots or aggressive behavior are detected.

- **Entry control.** Some intercoms can function as card and pin code readers for admitting employees and other authorized individuals with no other intervention. Unknown visitors can use the intercom keypad to request access by calling reception, the person they are visiting, or security personnel. Call recipients can then see, talk to, and open the door for those visitors directly or remotely from a cell phone, IP phone, or video management system.

- **Integration.** As IP devices, network intercoms integrate easily with other systems. SIP support allows integration with IP telephony, which makes it possible to forward video and sound from the intercom and answer calls from a desk phone or mobile device. Calls can also be received through most IP-based video management systems, allowing the customer to leverage whatever system solution they prefer. In more complex systems, for instance at logistics centers or airports, intercoms are a useful complement to an integrated solution with network cameras, access control systems, intrusion alarms, and other security applications. Intercoms may feature a multitude of ports, relays, and supported protocols that allow you to connect external sensors, activate lights, open doors, trigger external cameras, or sound alarms.

11. Wearables

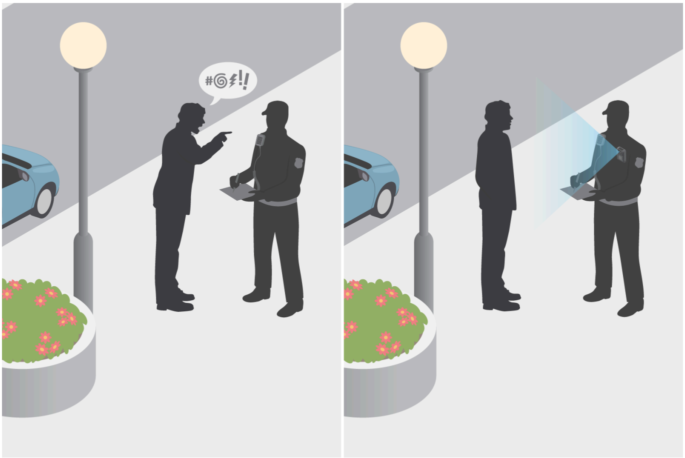
Body worn cameras document events and capture valuable evidence. They are also an effective way to deter bad behavior and to positively influence the actions of both camera wearers and the public. Axis body worn cameras provide superior video and audio quality, to enable evidence that is easy to understand and interpret and which holds up in court. Axis body worn system is based on open standards for flexibility and scalability. It can be used with various content destinations and employs end-to-end encryption for cybersecurity. And with AXIS Body Worn Live it is possible to stream live video, audio, and metadata from Axis body worn cameras. It is secure and reliable, it enables informed decision-making by operators and it provides an added sense of security for camera wearers.

11.1 The purpose of body worn cameras

With a body worn camera, incidents can be recorded wherever they occur. Mounted on the body of, for example, a delivery person, train conductor, clerk, or security guard, the camera is taken where it is needed and can capture events that never would have been caught by cameras in fixed locations.

A recording produced by a body worn camera comprises an item of trusted and secure evidence, showing objectively what happened at the scene of an incident. The footage can be used in internal investigations and in court, but also for discussion and analysis when training personnel on how to respond to situations they are likely to encounter. A body worn camera also makes it easy to document that deliveries or other tasks were handled in accordance with the appropriate procedures.

The use of body worn cameras affects the behavior of both camera wearers and the individuals they interact with. Awareness of being recorded seems to make people feel there is a digital witness to their actions, so they are less likely to misbehave, and camera wearers are more likely to stay calm and comply with regulations.



The use of body worn cameras can help keep situations calm when both the camera wearer and the public know that their behavior and decisions may be witnessed by another party.

11.2 Body worn cameras

Axis body worn cameras come in black, white, or grey, to let them blend in or stand out against clothing. These models are suitable for use in any industry.

Axis body worn cameras deliver sharp images and clear audio. They are lightweight, robust, and water-resistant. They start and stop at a touch and buffer up to 120 seconds before a recording is started. Long battery life, USB charging, and fast offloading make them even easier to use.

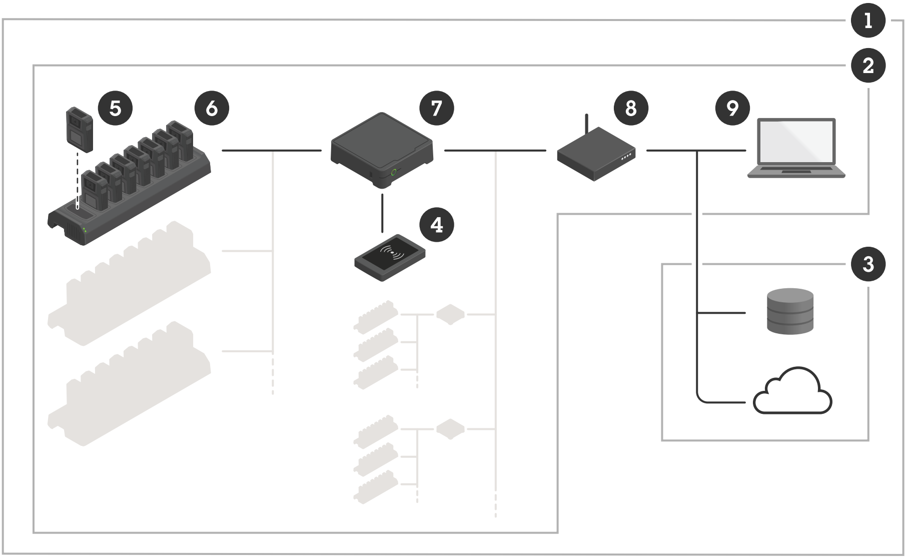
Select a black or white model depending on whether or not you want the camera to stand out against clothing for deterrence. Mini sensors can be attached to the camera and clipped onto headgear or clothing using standard mounts, for convenient and unobtrusive filming.

Body worn cameras store location data obtained from navigational satellites in their recordings. By tying the video material to the geographical coordinates where it was filmed, location tracking is enabled, and the evidentiary value of recordings is significantly enhanced. Axis body worn cameras also feature Axis Zipstream technology, which ensures that you can store a large amount of footage without having to compromise video quality.

With AXIS Body Worn Live, when the wearer starts a recording, they can also immediately activate a live audio and video stream from their camera to the operator, who can then follow events in real-time. For a hands-off solution, organizations can choose the cloud-based Axis-hosted version. Or they can host AXIS Body Worn Live themselves if regulations rule out cloud-based hosting. The operator can make informed decisions about things such as when to send backup, and GPS location coordinates indicate where to send it. The operator can send a notification to the wearer, who will then know that they have support so they can concentrate on the incident rather than on communicating with headquarters. Notifications can be received as a "beep", or, on some models, as a symbol in the camera's LCD display.

11.3 Axis body worn solution

After the body worn camera has been used, you place it in its docking station. The system controller instantly starts to transfer the data from the camera to the content destination of your choice, and the camera's battery starts to charge. The system controller also keeps the cameras up to date with the latest AXIS OS version and other settings, and it monitors the overall health of the Axis body worn solution.



Components of Axis body worn solution.
Axis body worn solution (1) consists of one or more Axis body worn systems (2) connected to a content destination (3). The body worn system functions only when it is connected to a content destination.

Axis body worn system (2) consists of Axis body worn cameras (5), Axis docking stations (6), Axis system controllers (7), and AXIS Body Worn Manager (9).

An optional RFID reader (4) can be connected to the system controller. This lets the user self-assign any available body worn camera, using their self-assign tag.

AXIS Body Worn Manager (9) is a web application in which you can configure and manage your body worn system.

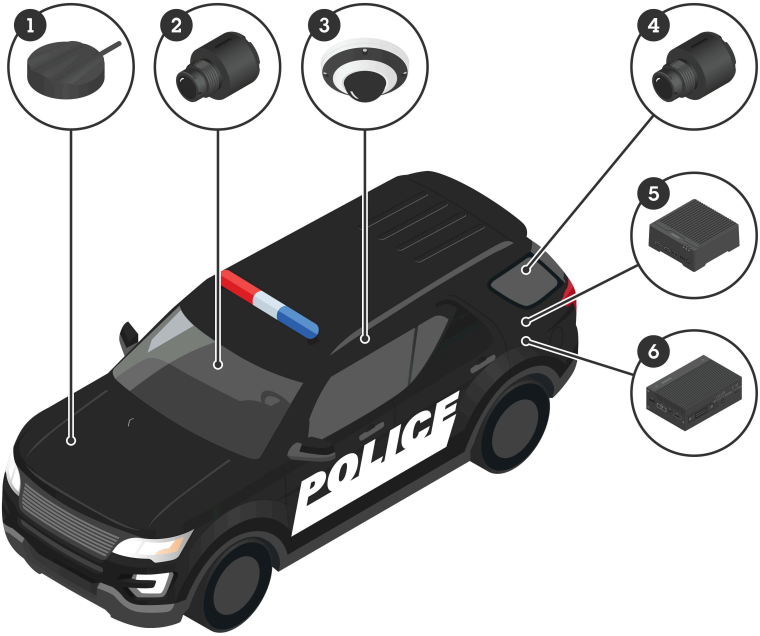
Open standards and the low-cost docking stations with a separate system controller make it easy and cost-efficient to add more cameras and users to the system as needed. The application for mobile devices AXIS Body Worn Assistant connects directly to the body worn camera, and, for example, lets you view recorded video.

Axis body worn solution has support for different types of content destinations: evidence management systems (EMS), video management systems (VMS), and media servers. You can use an end-to-end Axis solution that includes AXIS Camera Station or Axis Case Insight, or any third party VMS or EMS — on-site or in the cloud.

Axis body worn cameras support official FBI standards for cybersecurity, with end-to-end encryption.

11.4 In-vehicle solution

Axis in-vehicle solution for law enforcement integrates rugged and reliable in-vehicle surveillance with Axis wearable cameras. The cameras and microphones in this solution deliver video and audio for forensic usability, and they provide comprehensive situational awareness inside vehicles and outside. All recorded material and information is safeguarded by built-in cybersecurity features.



A typical vehicle installation, including: 1) Antenna, 2) Windshield camera, 3) Box camera, 4) Rear window camera, 5) Main unit, 6) Ruggedized computer.

12.Analytics

A camera can be much more than just a source of video. Analytics turn video, audio, and other data into actionable insights. And because of the development of artificial intelligence (AI), analytics have become a major differentiator in video surveillance and monitoring, which helps facilitate security, safety, and operational efficiency.

12.1 Analytics for a smarter, safer world

Analytics are used to increase security and safety and optimize business operations and management. They can also be designed to actively protect people's privacy in surveillance.

Getting access to structured, labeled data highlighting the crucial details in a scene can enable automated actions and steer decisions in the right direction. It also reduces resources required to analyze data and make predictions based on trends and patterns.

Rule-based events or alerts that the user configures to trigger automated actions and alarms can enhance both operational efficiency and situational awareness. Getting an alarm when someone crosses a virtual line at a restricted area, or automatically opening a gate each time an authorized vehicle arrives can save on resources.

Analytics can also provide information about the objects in the scene and their attributes, such as the presence of hats or bags, and other characteristics such as color, shape, or speed. Event metadata and scene metadata are together referred to as *analytics metadata*, which is incredibly valuable for searching through vast amounts of video. It can also be used to detect patterns and trends to generate statistics or provide further actionable insights and even predict future events.

Use cases for analytics keep developing and future possibilities are virtually endless. This chapter presents some of the most important use cases today.

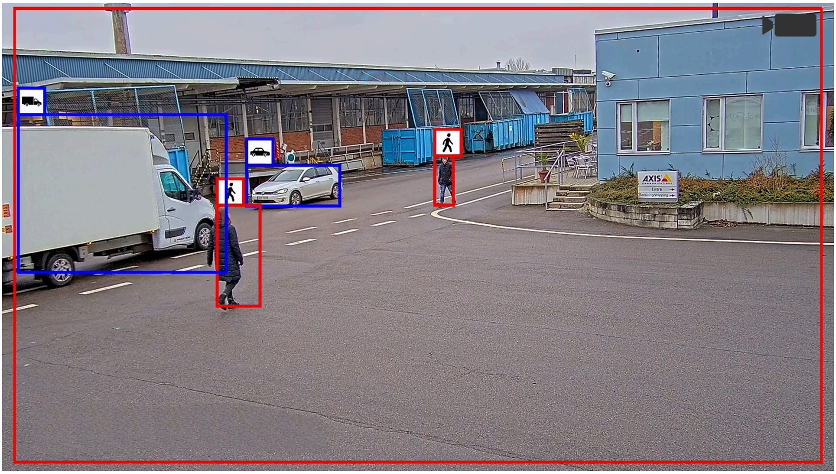
12.2 What are the benefits of analytics?

Analytics increase security, safety, and operational efficiency and can provide valuable business intelligence. They can help you:

- **Respond faster to critical incidents.** With real-time events and notifications and a clearer picture of the scene, you will be able to respond faster when time is of the essence. Responses can even be automated.
- **Make more informed decisions.** There are analytics for making data-driven decisions, optimizing operations, eliminating chokepoints, and improving profitability by using actionable insights.
- **Make better use of resources.** By automating tasks that machines can do just as well as, or even better than humans, operators will be able to focus on more advanced tasks.
- **Find what you are looking for.** Accelerate investigations by enabling efficient search in multiple video streams to find objects, their attributes, or incidents of interest in a scene.
- **Proactively prevent unwanted events.** Analytics can enable proactive action by providing early warnings about situations that might constitute a risk – such as people loitering or a stolen vehicle in the area.

12.2.1 Real-time monitoring

Using analytics means automating the process of watching hours and hours of video, extracting the useful information, and taking appropriate action. Objects such as humans and vehicles can be automatically detected and monitored to find significant events that you want to pinpoint or let the system automatically react to. Automatic actions can include notifying staff, starting a video recording, opening a gate or starting a pre-recorded announcement.



AXIS Object Analytics offers AI-based object detection and classification.

In a retail setting or similar environment, analytics can help make management of staff more efficient. For example, a long queue could trigger an announcement of, “More staff to the checkouts, please.” People and vehicle counting provide valuable information that can help you gain insights into visitor trends and traffic patterns. This data enables you to evaluate site performance, monitor traffic flow, optimize parking capacity, and ultimately optimize your business operations.

Analytics can also be used for license plate recognition, making it highly effective for access control, parking management, traffic enforcement, and more. These solutions help track vehicles involved in criminal activity, speeding, or theft, while also supporting everyday tasks such as automating toll collection, monitoring traffic flow, enabling seamless entry into parking facilities, and informing proactive traffic planning through data-driven insights.

AXIS License Plate Verifier offers real-time, AI-powered license plate recognition for a range of traffic applications including vehicle access, vehicle search, and parking solutions.

12.2.2 Efficient search

Using analytics to enhance search is one of the most common and valuable use cases, as it can save significant time and resources. Analytics accelerate various types of searches by streamlining queries for specific objects, attributes, and activities. In logistics centers, for example, analytics can quickly locate parcels, significantly reducing manual search time. In retail environments, they can help uncover customer behavior patterns, enabling businesses to optimize operations, enhance merchandising strategies, and improve the overall shopping experience. In forensic investigations, analytics assist in locating critical evidence such as vehicles or individuals connected to an incident, and can even help investigators track suspects' movements and activities. Powered by AI, these solutions extract detailed information, enabling fast, accurate, and efficient searches across a wide range of industries. Furthermore, analytics can integrate with existing systems and workflows, such as surveillance systems, databases, and investigative tools, to support search and analysis.

12.2.3 Spotting trends and patterns

Analytics can provide valuable and actionable insights and statistics to improve operations and help make more informed decisions, for example, when managing traffic flow or visitor movements. As analytics make use of metadata to describe the content in a scene, they can help you effectively collect, organize, and store content of interest to spot patterns and trends.

12.2.4 Privacy

With intelligent masking you can blur faces, entire bodies, and license plates in a scene for increased privacy. This means that the identities of individuals or vehicles are masked while their movements can still be observed. With AI-based masking, live video is analyzed for specific objects and you can mask either the objects or the background. This type of analytics is specifically designed to safeguard privacy, letting you monitor activities without collecting personal data.

12.3 System architecture – where is the video analyzed?

When designing a video analytics system, one critical consideration is where to process the analytics data. There are three primary options: on the camera, on a server, or in the cloud.

> **On the camera.** Analyzing video at the edge is beneficial for many reasons:

  - **Higher accuracy:** Running analytics on uncompressed video results in higher accuracy because video quality is not degraded.
  - **Fast response and action:** Edge-based solutions minimize latency by processing data near its source, avoiding delays caused by transmitting it to remote servers or cloud platforms. This enables real-time alerts, which together with automated triggers allow for fast response times and immediate action.
  - **Easy to scale up:** Running analytics at the edge makes scalability easier by reducing the processing load on centralized systems. This is particularly beneficial because processing all video data in the cloud can be very expensive. Additionally, it lowers server costs and maintenance needs.
  - **Reduced network load and demands on infrastructure:** By not transferring unnecessary data, you will experience lower network traffic, reduced bandwidth requirements, and decreased demand on hardware – ultimately leading to significant cost savings.
  - **Improved privacy:** Running analytics at the edge gives the option to only send anonymized data and/or alerts over the network, which could increase privacy.

> **On a server.** When you need a lot of processing power, analyzing video on dedicated servers is often required. Servers can also analyze multiple video streams simultaneously from many different sources and perform database searches in huge amounts of data.

> **In the cloud.** Sending video directly from cameras to the cloud for processing is another option. But processing all video data in the cloud can incur significant costs due to data storage, transfer, and processing fees, which may limit its suitability for certain applications. Cloud computing often requires a robust and reliable internet connection that is not always available in every situation. On the other hand, cloud computing lets you process multiple video streams at once. It is also easy to scale. Some companies need to keep all of the data on their premises due to regulations and are therefore unlikely to consider a cloud solution.

> **Hybrid solution.** A hybrid system that combines processing at the edge, in the cloud, and on on-prem servers, is often the best approach because it takes advantage of the strengths of each technology. In hybrid systems, object classification can occur in the cameras, while algorithms that require more power are performed on servers or in the cloud. Sharing the processing load between the edge and server makes systems much more scalable, because when you add a new camera with edge analytics capabilities you do not need to increase the server processing power.

12.4 Image usability – the foundation for great analytics performance

Analytics performance depends on many factors, most of which can be optimized once you are aware of their impact. These factors include, for example, camera hardware, image quality, scene dynamics, and illumination level, as well as camera configuration, position, and direction.

No matter how powerful they are, analytics rely on the technologies that support them. Without quality images and accurate classification (or labeling) of data you will not get acceptable results. Things like noise filtering, contrast enhancement, and motion blur affect the precision of analytics. Good performance in low light can be a challenge. Advanced image processing technologies such as Lightfinder, Forensic WDR, and OptimizedIR are important. Axis Scene Intelligence was developed specifically to boost scene understanding at the edge through superior image quality and AI-based analysis to extract crucial details.

It almost goes without saying that timely software upgrades – or *digital maintenance* – are important for well-functioning analytics. But something that often gets less attention is *physical maintenance*. A principal requirement for analytics is a clear view of the scene. Poor image quality, whether due to environmental conditions or equipment degradation, can compromise results. So, to get the most out of your investment in analytics, we recommend a proactive approach to camera maintenance, both digital and physical.

To help maintain optimal image quality, AXIS Image Health Analytics continuously monitors and analyzes camera images, detecting issues that may impact analytics performance. If a problem is detected, such as a blocked, blurred, underexposed, or redirected image, the system sends a notification, allowing for prompt corrective action.

12.5 Artificial intelligence

Artificial intelligence (AI) is a broad concept applied to machines that can solve complex tasks while demonstrating seemingly intelligent traits. Unlike traditional programming, which relies on explicit instructions and rules defined by humans, AI enables machines to process vast amounts of data and adapt to new situations autonomously. The advantage of AI over traditional programming is the ability to process much more data than humans can, resulting in a more accurate application. Machine learning and deep learning are subsets of AI.

Machine learning uses statistical learning algorithms to build systems that can learn and improve during training without being explicitly programmed, for example, to determine what is happening in images or video streams (computer vision). Conventional computer vision relies on manual feature extraction, where humans define the characteristics to be detected in images or video streams. The algorithm learns how to combine these features through exposure to large amounts of annotated training data collected and annotated by humans. The data is fed into the system until the program has learned enough to detect what is needed. When finished, the program will not learn anything new.

Deep learning is data-driven learning of features and how to combine them. Much like the human brain, the algorithm can learn very deep structures of chained feature combinations, which are simulated in artificial neural networks, the most common type of algorithm in deep learning. Deep learning algorithms can leverage a larger number of feature combinations, enabling them to tackle more intricate tasks and achieve greater accuracy.

Cameras with a deep learning processing unit (DLPU) offer more granular classification of detected objects. This can be very useful when time is critical, as the classification can take place directly on the camera. Deep learning-based analytics are ideal for busier scenes and more demanding requirements. They also offer better detection and classification capabilities for people in unusual positions (crouching, for example) as well as objects that are only partially visible. Given adequate training data, deep learning algorithms can accurately detect object attributes, including clothing color, hard hat presence, bag detection, and more.

12.6 AXIS Camera Application Platform

Most Axis devices support our open application platform, AXIS Camera Application Platform (ACAP). This powerful platform uses well-known toolchains, open-source industry-standard APIs, and high-level programming languages to enable development, deployment, and integration of applications on the edge, allowing for solutions tailored to specific customer needs. Applications can therefore run where they best optimize performance and minimize bandwidth. Maximizing processing efficiency and the total effectiveness of the system is important both for the end user, who gets a more powerful and streamlined system, and for the developers, who have more freedom to focus on the application instead of the platform. That means that the barriers are lowered for developers to enable innovation on Axis devices.

13.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 of local area networks, and in particular the Ethernet network 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, including how network video products can be accessed over the internet. We also cover virtual local area networks, Quality of Service, and an overview of the data transport protocols used in network video.

13.1 Local area networks and Ethernet

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

Today, Ethernet uses a star topology in which the individual nodes (devices) are connected to each other via active networking equipment such as switches. A LAN can contain several thousand networked devices.

A good rule of thumb is to always build a network with greater capacity than currently required. To future-proof it, you can design a network so that it only uses 30% of the total capacity when first put into use. As more and more applications run over networks, more and more network performance will be required. While network switches are easy to upgrade after a few years, cabling is normally much more difficult to replace.

13.1.1 Types of Ethernet networks

The following are the most common types of Ethernet networks in the video surveillance industry. They can be based on twisted pair or fiber optic cables.

Fast Ethernet. Can transfer data at a rate of 100 Mbit/s. 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 are equipped with a 10BASE-T/100BASE-TX 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. Supports a data rate of 1,000 Mbit/s (1 Gbit/s) and is now more commonly used than Fast Ethernet. 1 or 10 Gbit/s Ethernet may be necessary for the backbone network that connects many network cameras. 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 greater distances, fiber cables such as 1000BASE-SX (up to 550 m/1804 ft) and 1000BASE-LX (up to 550 m with multimode optical fibers and 5,000 m or 3 miles with single-mode fibers) can be used.

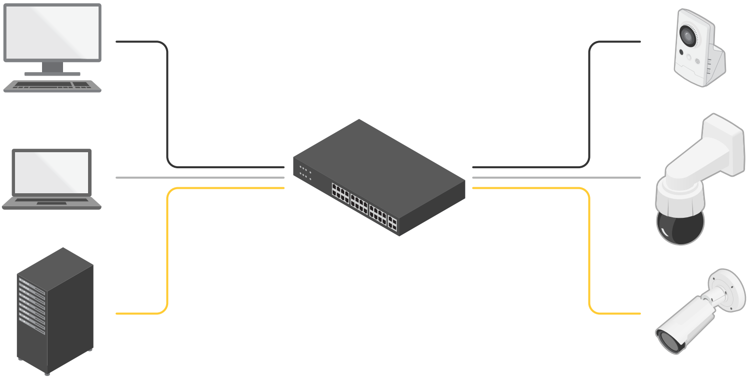
10 Gigabit Ethernet. Supports a data rate of 10 Gbit/s (10,000 Mbit/s). 10GBASE-LX4, 10GBASE-ER and 10GBASE-SR based on an optical fiber cable can be used to cover distances up to 10 km (6 miles). With a twisted pair solution, a very high quality cable (Cat-6a or Cat-7) is required. 10 Gbit/s Ethernet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

13.1.2 Connecting network devices and network switch

Networking multiple devices in a LAN requires equipment such as network switches. The main function of a switch is to forward data from one device to another on the same network, which it does efficiently by directing data from one device directly to the target device, without affecting other devices on the same network.

A network switch works by registering the MAC (media access control) address of each device that connects to it. Each and every networking device has a unique MAC address, made up of a series of figures and letters in hexadecimal notation, as set by the manufacturer. The address is often found on the product label. When a network switch receives data, it forwards it only to the port that is connected to the device with the appropriate destination MAC address.

Network switches typically indicate their performance in per port rates, and in backplane or internal rates (both in bitrates 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.



In a network switch, data transfer is managed very efficiently, as data traffic can be directed from one device to another without affecting any other port on the switch.

A network switch normally supports different data rates simultaneously. Previously, the most common rates were 10/100 Mbit/s, supporting the 10 Mbit/s and Fast Ethernet standards. Today however, network switches often have 10/100/1000 interfaces, 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 network switch also allows a connected device to function in full-duplex mode, that is, to send and receive data at the same time, resulting in increased performance.

Network switches may come with different features or functions. For example, some may include router functionality and many support Power over Ethernet. A switch that includes Quality of Service can control how much bandwidth is used by different applications.

13.1.3 Power over Ethernet

Power over Ethernet (PoE) is used to supply power to devices connected to an Ethernet LAN, over the same cable used for data communication. PoE is widely used to power IP phones, wireless access points, and network devices such as cameras.

The main benefit of PoE is the inherent cost savings. Hiring a certified electrician and installing a separate power line are not required when running PoE. This is advantageous, particularly in difficult-to-reach areas. The fact that power cabling is not required can potentially save hundreds of dollars per camera. PoE also makes it easier to move a camera to a new location, or to add new cameras to an existing video surveillance system.

Additionally, PoE can make a surveillance system more secure. A system with PoE can be powered from the server room, which is often backed up by a UPS (uninterruptible power supply). This means that the system can stay 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.

802.3af standard, PoE+, 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). This functionality is often built into the network device. Alternatively, it can be provided from a standalone splitter.

Backwards compatibility with non-PoE network devices is guaranteed. The standard includes a method for automatically identifying if a device supports PoE, and only when this is confirmed will power be supplied to the device. This also means that the Ethernet cable connected to a PoE switch will not supply any power if 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 it can overlay the current on the pairs used for data transmission. Switches with built-in PoE often supply power 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 there will be some power loss over a twisted pair cable, only 12.95 W is guaranteed as being available for the 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 300-500 W. On a 48-port switch, this would mean 6-10 W per port, if all ports are connected to devices that use PoE. Unless the PDs support power classification, a 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, then 300 W will be enough to supply power to all 48 ports.

Class	Type	Minimum power level at PSE	Maximum power level used by PD
0	Type 1, 802.3af	15.4 W	0.44 W - 12.95 W
1	Type 1, 802.3af	4.0 W	0.44 W - 3.84 W
2	Type 1, 802.3af	7.0 W	3.84 W - 6.49 W
3	Type 1, 802.3af	15.4 W	6.49 W - 12.95 W
4	Type 2, 802.3at	30 W	12.95 W - 25.5 W
6	Type 3, 802.3bt	60 W	51 W
8	Type 4, 802.3bt	90 W	71.3 W

Table 13.1a *Power classifications according to IEEE 802.3af, IEEE 802.3at, and IEEE 802.3bt.*

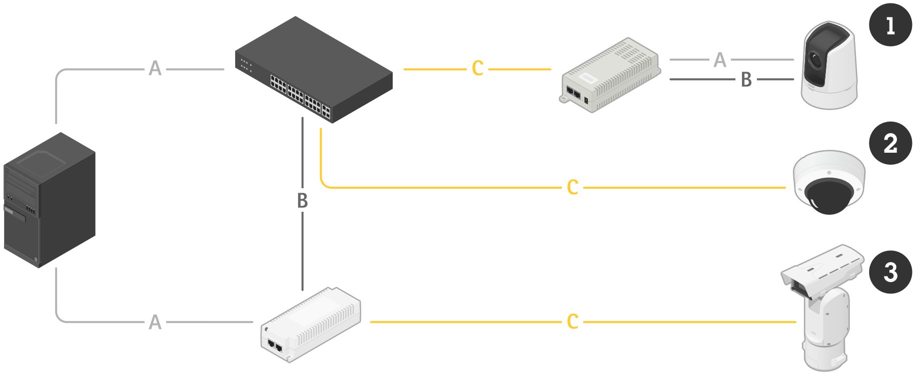
Most fixed network cameras can receive power via PoE using the IEEE 802.3af standard and are normally identified as Class 1 or 2 devices.

Other PoE standards are IEEE 802.3at, also known as PoE+, and IEEE 802.3bt. Using PoE+, the power limit is raised to at least 30 W via two pairs of wires from a PSE. For power requirements that are higher than the PoE+ standard, Axis uses the term, High PoE, which raises the power limit to at least 60 W via four pairs of wires, and 51 W is guaranteed for PoE.

PoE+ and High PoE midspans and splitters can be used for devices such as PTZ 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. For PoE+ and High PoE, Cat-5e or higher cable is recommended.

The midspan, which injects 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 (for example, the switch) and the device does not exceed 100 m (328 ft.). This means that the midspan and active splitter(s) must be placed within 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 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.



Using splitters and midspans, you can combine cameras without PoE support (1), PoE-enabled cameras (2), and cameras that need more power than PoE can provide (3) in the same system.
A. Power (from the UPS)
B. Ethernet (from the network switch)
C. Power over Ethernet

1. A camera without PoE support can be connected using a splitter.
2. A PoE-enabled camera receives both power and Ethernet connectivity through an Ethernet cable from the switch.
3. A camera that needs more power than a regular PoE switch can provide can be connected using a midspan, which feeds a higher power level to the camera. The midspan receives and forwards data from the switch, while the PoE power to the camera originates from the mains supply — through the UPS in this example.

13.2 Sending data over the internet

The basic elements of internet communication include:

Routers. To forward data packages from one LAN to another via the internet, network routers must be used. These devices route information from one network to another (hence the name) based on IP addresses. A router only forwards data packages destined for another network, and is most commonly used for connecting a local network to the internet. Routers are sometimes 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 in a combination of both. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks 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. When connecting to the internet, the term upstream describes the transfer rate (bandwidth) at 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 PC. In most scenarios, the download speed is the most important to consider. In a video application with a camera at a remote site, however, the upstream speed is more relevant, since video from the camera will be uploaded to the internet. Older internet technologies with asymmetrical bandwidth such as ADSL (asymmetric digital subscriber line) may not be suitable for network video applications since their upstream data rate may be too low.

Sending data from a device on one LAN to a device on another LAN requires a standard method of communication, since local area networks may use different technologies. This requirement led to the development of IP addressing and the many IP-based protocols for communicating over the internet.

13.2.1 IP addressing

Devices wishing to communicate via the internet must have unique and appropriate IP addresses, which 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 an IPv6 address is longer (128 bits compared with 32 bits for an IPv4 address). IPv4 addresses are the most commonly used today.

13.2.1.1 IPv4 addresses

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

Some IPv4 address blocks 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. These addresses can only be used on private networks and are not allowed to be forwarded through a router to the internet. A device wanting to communicate over the internet must have its own individual, public IP address, which will be allocated by an internet service provider. The address can be either a dynamic IP address – which can change during a session, or a static address – which normally comes at an additional monthly fee.

Ports

A port number defines a particular service or application so that the receiving server (a network camera, for example) 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.

Port numbers can range from 0 to 65535. Some 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

For a device to work in an IP network, an IP address must be assigned to it. Setting an IPv4 address for an Axis device can be done automatically using DHCP (Dynamic Host Configuration Protocol) which requires a DHCP server on the network. Another way to set the IP address is to use a management software tool, such as AXIS Device Manager. Alternatively, the address can be set manually. One way to do this is to use the device's web page to enter the static IP address, subnet mask, and the IP addresses of the default router, the DNS (Domain Name System) server, and the NTP (Network Time Protocol) server.

A DHCP server manages a pool of IP addresses, which it can assign dynamically to network devices. This function is often performed by a broadband router, which in turn is typically connected to the internet and gets its own, public IP address 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 device at a dynamic DNS server, which can always tie the domain name for the device 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*.

Using DHCP to set an IPv4 address works as follows. When a network device (such as a network camera) comes online, it sends a query requesting configuration from a DHCP server. The DHCP server replies with the configuration requested by the device. This normally includes the IP address, the subnet mask, and IP addresses for the router, DNS server, and NTP server. The device first verifies that the offered IP address is not already in use on the local network, assigns the address to itself, and can then update a dynamic DNS server with its current IP address so that users can access the device using a domain name.

AXIS Device Manager is software that can automatically find and set IP addresses and show the connection status. It can assign static and private IP addresses for all 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 Device Manager, is necessary to effectively manage the system.

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 translates the private IP address into a public IP address, for public exposure on the internet.

13.2.1.2 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 huge number of IP addresses it provides, 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, as well as any additional information. The prefix and host's suffix are then used, so DHCP for IP address allocation and manual setting of IP addresses is no longer required with IPv6. 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 device is as simple as checking a box to enable IPv6 in the device. The device then receives an IPv6 address according to the configuration in the network router.

13.2.2 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, is carried by TCP.

TCP provides a reliable, connection-based transmission channel. It ensures that data sent from one point is received at the other. TCP's reliability through retransmission may introduce significant delays, but in general TCP is used when reliable communication is preferred over reduced latency.

UDP is a connection-less protocol and does not guarantee delivery of the transmitted data, thus leaving the whole control mechanism and error-checking to the application itself. UDP does not re-transmit lost data and, therefore, does not introduce any further delay.

Protocol	Transport protocol	Port	Common usage	Network video usage
FTP (File Transfer Protocol)	TCP	21	Transfer of files	Transfer of images or video to an FTP server or an application
SMTP (Send Mail Transfer Protocol	TCP	25	Protocol for sending e-mail	Network video product sends images or alarm notifications using built-in email client.
HTTP (Hyper Text Transfer Protocol	TCP	80	Browsing the web, i.e. getting web pages from web servers	The video device functions as a web server, making video available for the user or application server.
HTTPS (Hypertext Transfer Protocol over Transport Layer Security)	TCP	443	Secure access to web pages using encryption technology	Secure transmission of video from network video products.

Protocol	Transport protocol	Port	Common usage	Network video usage
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	Transmission of video, and synchronization of video and audio. RTP provides sequential numbering and timestamping of data packets, enabling correct reassembly. Unicast or multicast.
RTSP (Real Time Streaming Protocol)	TCP	554	Set up and control of multimedia sessions over RTP	

Table 13.2a *Common TCP/IP protocols and ports used for network video.*

See also Axis documentation about commonly used ports at *https://help.axis.com/axis-os#commonly-used-network-ports*

13.2.3 SIP

Session Initiation Protocol (SIP) is a text-based protocol, similar to HTTP and SMTP, for communication over IP networks. It is used to start, change, and terminate media stream sessions, which can include voice and video elements. SIP is the standard protocol used in Voice over IP (VoIP) applications and unified communication platforms, for video conferencing, call control, and instant messaging. SIP constitutes a way to connect, integrate, and control Axis network products.

SIP calls can be set up in many ways, but there are three main types:

Peer-to-peer calls, also called local calls. These are calls between two devices (such as computers, network speakers, softphones, door stations, cameras, or IP desk phones) that belong to the same network. The call is made to the SIP address of the device.

SIP server calls, also called private branch exchange (PBX) calls. To make SIP server calls, the devices must be connected to a SIP server that handles the call exchanges. A SIP server, or a PBX, is a hub that works like a traditional switchboard. It can be hosted on an intranet or by a third-party service provider. The SIP-enabled devices register with the SIP server and can contact each other through their SIP addresses. A PBX can show call status, allow call transfers, handle voicemail, and redirect calls among other things.

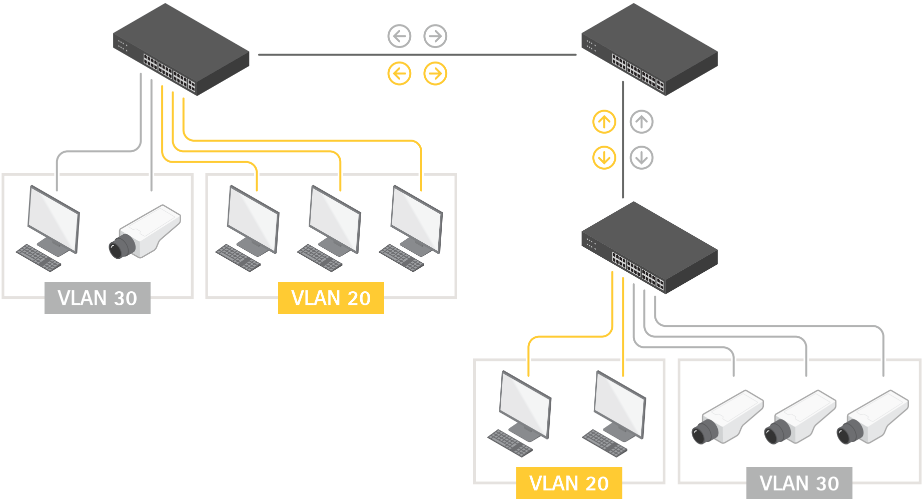
SIP addresses, also known as SIP uniform resource identifiers (URIs) or SIP numbers, are used to identify users within a network, just like phone numbers or email addresses. Like email addresses, SIP addresses are a type of URI that includes two user-specific parts, a user ID or extension, and a domain name or IP address. Together with a prefix and the @ symbol, they make up a unique address. In the case of a peer-to-peer call, the SIP address would include the IP address rather than the domain name.

SIP trunk calls. With a service provider that offers SIP trunking, the traditional telephone network can be used to make calls, and traditional phone numbers can be assigned to the SIP devices. In this way, calls can be made from a network speaker or a network door station to a cell phone or the other way around.

13.3 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. This can be achieved by dividing network users into logical groups. Only users in a specific group can exchange data or access 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 provide a flexible 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.

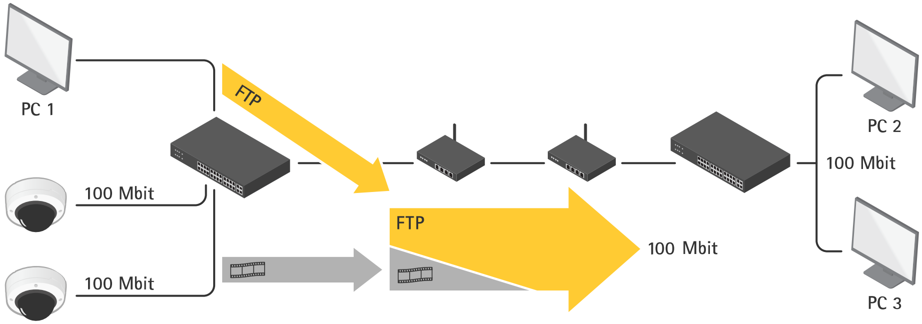


In this illustration, VLANs are set up over several switches. The two different LANs are segmented into VLAN 20 and VLAN 30. Only members of the same VLAN can exchange data, either within the same network or over different networks.

13.4 Quality of Service

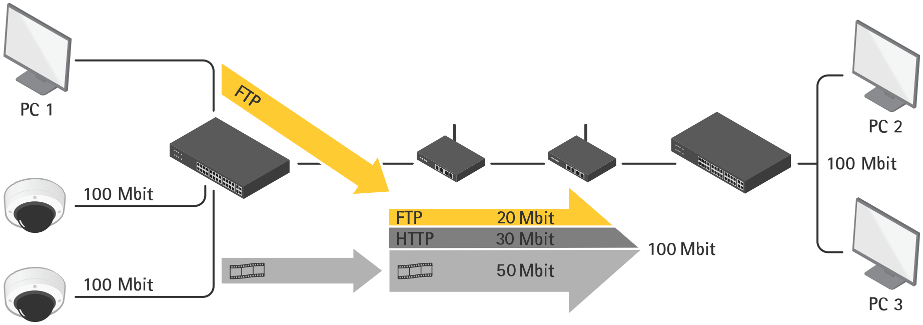
Since different applications—for example, telephone, email and surveillance video—can all use the same IP network, there is often a need to control how network resources are shared to fulfill the requirements of each service. One solution is to let network routers and switches operate differently for 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.

Quality of Service refers to a number of technologies, such as DSCP (Differentiated Services Code Point), 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. One main benefit of a QoS-aware network is the ability to prioritize traffic to allow critical flows to be served before flows with lesser priority. Another is greater reliability in the network, by controlling the amount of bandwidth an application may use and thus controlling bandwidth competition between applications. An example of where QoS can be used is with PTZ commands to guarantee fast camera responses to movement requests. A prerequisite for the use of QoS in a video network is that all switches, routers, and network video devices must support QoS.



Standard (non-QoS aware) network. In this example, FTP and video streaming have 100 Mbit/s to share and the video bandwidth cannot be guaranteed.

In this illustration, PC 2 is watching two video streams (from the two cameras), with each camera streaming at 25 Mbit/s. Suddenly, PC 3 starts a file transfer from PC 1. In this scenario, the File Transfer Protocol (FTP) will try to use the full 100 Mbit/s capacity between the two routers, while the video streams will try to maintain their total of 50 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.



QoS-aware network. Video streaming has a guaranteed bandwidth of up to 50 Mbit/s.

In this illustration, the first router has been configured to use up to 50 Mbit/s of the available 100 Mbit/s for streaming video. FTP traffic can use 20 Mbit/s, and HTTP and all other traffic can use a maximum of 30 Mbit/s. This means 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. Unused bandwidth can be used by any type of traffic.

14.System protection

Cyberthreats are commonly associated with hackers and malware, but negative impact can also be the result of unintentional misuse. When you deploy a system, it is recommended that you follow industry best practices. To be protected, a system needs to be both well configured and well maintained.

14.1 Network protection

A network needs protection from cyberthreats. All packages sent on the network may be collected by other computers on the same network. If the payload in the packages is sent in clear text, the data can be easily compromised, through what is called network sniffing. Another threat is network spoofing, which is when an attacking computer tries to impersonate a legitimate server, computer, or network device in order to get access to the network. Encrypted connections and CA-signed certificates provide protection.

For guidance on how to reduce the network's exposure to risks, see *Axis Network Switches Hardening Guide* at *https://help.axis.com/axis-network-switches-hardening-guide*.

For best practices about how to onboard and operate Axis devices in HPE Aruba Networking powered networks, see the integration guide *HPE Aruba Networking - Integration Guide* at *help.axis.com/axis-aruba-secure-network-integration*. The best-practice configuration uses modern security standards and protocols such as IEEE 802.1X, IEEE 802.1AR, and HTTPS.

14.1.1 IEEE 802.1X

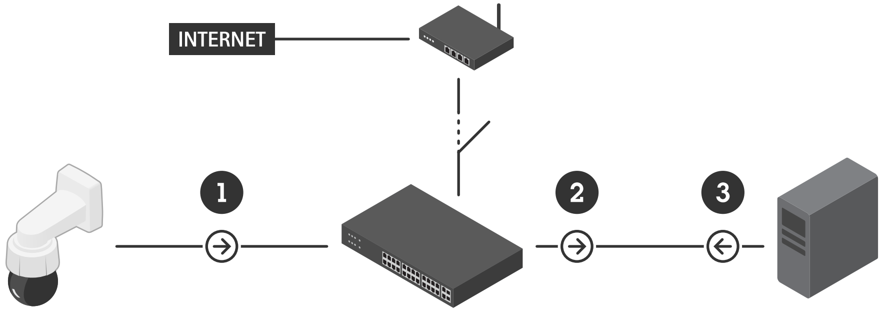
Many Axis products support IEEE 802.1X, which is a method used to protect a network against connections from unauthorized devices. IEEE 802.1X establishes a point-to-point connection, or it prevents access from the LAN port if authentication fails. IEEE 802.1X prevents so-called port hijacking; that is, when an unauthorized device gains access to a network by physically connecting to a network port/socket. IEEE 802.1X is useful in network video applications, since cameras are often located in public spaces where an accessible socket 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 like this:

1 A camera that is configured for IEEE 802.1X sends a request for network access to a switch.

2 The switch 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 to open its port and allow data from the network camera to pass through onto the network.



IEEE 802.1X enables port-based security.

14.1.2 HTTPS (HTTP over TLS)

HTTPS (Hypertext Transfer Protocol Secure) is a secure communication method that sends HTTP inside a Transport Layer Security (TLS) connection. This means that the HTTP connection and the data itself are encrypted.

Many Axis products have built-in support for HTTPS, making it possible for data to be communicated securely. To enable an Axis camera or video encoder to communicate over HTTPS, a digital certificate and an asymmetric key pair must be installed in the product. The key pair is generated by the Axis product. The certificate can either be generated and self-signed by the Axis product, or it can be issued by a certificate authority. In HTTPS, the certificate is used for authentication and encryption, which means that the certificate allows a client to verify the identity of the product, and it encrypts the communication using keys that are generated by public-key cryptography.

14.1.3 Trusted public key infrastructure (PKI)

A trusted public key infrastructure (PKI) consists of a private or public certification authority (CA), which is a service that issues (signs) certificates to be installed in networked devices. Certificates are used for end-to-end encryption of TLS-based connections between hosts in a network. A CA-signed certificate with a validated trust chain enables applications, such as a VMS or a web browser, to validate the identity of the Axis networked device. Commonly, a CA certificate (root-certificate) signs an intermediate CA certificate, which then in return signs client certificates for end devices. For this validation to succeed, the publicly known CA certificate (root and/or intermediate certificate) must be installed and used by the application to verify client certificates that are carried by Axis networked devices. AXIS Device Manager has a built-in CA service that can cost-efficiently issue and deploy server certificates to the devices.

14.1.4 NTS Network Time Protocol

NTS provides cryptographic security for the client-server mode of the Network Time Protocol (NTP), allowing users to obtain the time in an authenticated manner. Axis devices support NTS from AXIS OS 11.1 and onwards.

Time synchronization is traditionally done using NTP (Network Time Protocol). NTS assures that the device only gets time from sources that are trusted, with every synchronization authenticated and validated while keeping the time synchronization features of the NTP protocol.

14.1.5 Network isolation

Network isolation, or network segmentation, is a way to separate critical network resources from each other in order to reduce the risk of each of them having a negative impact on each other. This is an especially relevant tactic if different resources do not need to interact with each other – or should not. Network segmentation can be virtual (VLAN) and require an infrastructure of managed switches, or the networks can be separated with different cabling and network gear.

14.2 Cybersecurity standards

14.2.1 ETSI EN 303 645

ETSI EN 303 645 is a cybersecurity standard to which Axis devices running AXIS OS 11 or higher are certified. It establishes a security baseline for consumer products connected to the Internet and helps devices better comply with GDPR regulations.

14.2.2 FIPS (Federal Information Processing Standard) 140

FIPS 140 is recognized as a state-of-the-art security standard, which US and Canadian federal agencies and critical infrastructure must meet. FIPS 140-2 and FIPS 140-3 are information security standards for cryptographic computing modules, issued in the U.S. by NIST (National Institute of Standards and Technology). FIPS 140-3 superseded FIPS 140-2 in 2019 as its updated version.

Axis requires its incorporated hardware cryptographic computing modules to be certified at least according to Common Criteria EAL4 and/or FIPS 140-2/3 Level 2. The FIPS 140 standard provides four levels of security, levels 1-4. Each level adds more restrictive requirements and hence, level 1 has the lowest requirements and level 4 has the highest.

You can find information about the certification on the datasheet of an Axis device or in the Axis product selector.

14.2.3 Common Criteria (CC)

Common Criteria (CC) is an international standard (ISO/IEC 15408) for IT product security certification. Axis requires its incorporated hardware cryptographic computing modules to be certified at least according to Common Criteria EAL4 and/or FIPS 140-2/3 Level 2.

14.3 Device protection

A networked device and its resources must be duly protected. Protection may in this case refer to both physical protection, such as placing cameras out of reach, and protection of the camera's software. *AXIS OS Hardening Guide* provides more information about device protection.

14.3.1 Built-in cybersecurity platform

Axis devices are safeguarded by the hardware-based cybersecurity platform Axis Edge Vault. It relies on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

Axis Edge Vault minimizes exposure to cybersecurity risks and enables the device to be a trusted and reliable unit within the network.

> **Trusted device identity**. Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. It is securely and permanently stored in the secure keystore and can be leveraged for automated secure device onboarding and secure device identification.

- **Secure key storage**. The secure keystore provides hardware-based, tamper-protected storage of cryptographic information. It protects the Axis device ID as well as customer-loaded cryptographic information, and prevents unauthorized access and malicious extraction in the event of a security breach.
- **Video tampering detection**. *Signed video* makes it possible to trace the video back to the camera origin and verifies that the video has not been tampered with after it left the camera. Each camera uses its unique video signing key, which is stored in the secure keystore, to add a signature into the video stream. When the video is played, the file player shows whether the video is intact.
- **Supply chain protection**. The cybersecurity features, *secure boot* and *signed OS*, help establish a secure foundation for Axis Edge Vault by providing an unbroken chain of cryptographically validated software. *Secure boot* prevents physical supply chain tampering by ensuring that a device can boot only with Axis signed OS. *Signed OS* guarantees that the installed operating system (AXIS OS) is genuinely from Axis and ensures that any new operating system installed on the device is also signed by Axis. If the device detects that the integrity of the operating system is compromised or if it is not signed by Axis, the upgrade will be rejected.
- **MACsec.** Many Axis devices also support the IEEE 802.1AE MACsec security standard. MACsec is enabled by default and automatically encrypts data at the Ethernet Layer 2 level in the connections between Axis devices and MACsec-enabled Ethernet switches. Because it operates at this basic level, MACsec can encrypt and protect data that previously could not be encrypted, such as NTP, DHCP for general device operation, and RTP/RTSP for video streaming.

14.3.2 User account management

Device passwords tend to spread within an organization. For example, during device maintenance someone might request the password in order to adjust something. A couple of days or weeks later, someone else might have the same request. Within a short space of time, many new (or temporary) users know the password to all your devices, and you have lost control over who can access them. The strength of the password makes no difference in this scenario. Device management should involve using multiple accounts (role-based) and temporary accounts should be created for occasional maintenance and troubleshooting.

For account access, you should use the principle of least privileged accounts. This means that user access privileges are limited solely to the resources needed for a user's specific tasks. AXIS Device Manager helps you easily and efficiently manage multiple accounts and passwords, at the viewer, operator, or administrator level.

14.3.3 IP address filtering

Axis products provide IP address filtering, which allows or denies access to defined IP addresses. A typical setup is to configure networked devices to allow only the IP address of the server that hosts the video management software to access the product.

IP filtering acts like a local firewall in the networked device. Video clients will access live and recorded video from the VMS, never accessing a networked device directly. This means that the only computer or server that should be accessing networked devices during normal operations is the VMS server. The devices can be configured with an IP filter to only respond to listed allowed IP addresses, typically the VMS server and administration clients. If the device password is compromised, IP filtering helps mitigate risks from unpatched devices or brute-force attacks.

14.3.4 Keeping device software up to date

Running devices with an up-to-date AXIS OS version mitigates common risks. This is because the latest version generally includes security patches for all known vulnerabilities, including those newly discovered. As a consequence, attackers cannot exploit the vulnerabilities and possibly compromise the system, application, or devices. Axis device management software helps you manage upgrades of multiple devices and sites and automatically notifies you if there are newer versions.

As a CVE Numbering Authority (CNA), Axis follows industry best practices in managing and responding to security vulnerabilities discovered in our products. Vulnerabilities are scored using the widely used CVSS rating system, and patched within a specified period of time depending on the score.

To protect from the specific threat of supply chain tampering, the *signed OS* and *secure boot* features are widely available in Axis devices.

14.4 VMS protection

Many of the principles that apply for device protection and network protection apply for protection of the VMS as well. For example, you should follow the principle of least privilege when you define system accounts, and make sure you use the latest software release for the VMS, which has security patches for all newly discovered vulnerabilities. Furthermore, it is recommended that you deploy anti-virus software on all servers and computers that connect to the VMS server. Also, you should not run anything other than the VMS server software and trusted third-party integrations on the host hardware.

For more information, see AXIS Camera Station System Hardening Guide at *https://help.axis.com/axis-camera-station-system-hardening-guide*. It outlines cybersecurity policies and procedures to support secure deployment and maintenance of AXIS Camera Station systems.

14.5 Physical protection

While a networked device can never be 100% physically protected, there are various physical aspects to consider. For many types of devices, such as cameras and speakers, you can choose a design and color that blends into the environment, place the device out of reach, and always run the cable directly through the wall or ceiling behind the device. These principles provide substantial protection from both spontaneous vandalism and more planned attacks. For devices that need to be easily accessible, for example intercoms or door controllers, it is important to choose vandal-resistant models with tamper detection functionality. Important network equipment, such as routers and switches, and the host running the VMS server software should be placed in an environment with physically and logically restricted access.

15. Wireless technologies

For video surveillance applications, wireless technology offers a flexible, cost-efficient and quick way of deploying cameras, particularly over large areas, such as in parking lots or a city center surveillance application. In older, protected buildings, wireless technology may be the only alternative if installing cables is prohibited.

Axis offers cameras with built-in wireless support, but cameras without such support can still be integrated into a wireless network through the use of a wireless bridge.

15.1 802.11 WLAN standards

The most common standard for wireless local area networks (WLAN) is IEEE 802.11. While there are other standards, as well as proprietary technologies, the benefit of 802.11 is that it operates in a license-free spectrum, which means there is no license fee associated with setting up and operating the network. The most relevant amendments of the standards for Axis products are:

> 802.11ac (also known as Wi-Fi 5) was approved in 2014. It builds on the 802.11n standard, although it operates exclusively in the 5 GHz band. Depending on operating conditions, data throughput can be 1.7–2.5 Gbit/s.

> 802.11n (also known as Wi-Fi 4), which most wireless products today support. Approved in 2009, it operates in the 2.4 GHz or 5 GHz band. Depending on which features in the standard are implemented, 802.11n enables a maximum data rate of 600 Mbit/s.

> 802.11g was approved in 2003 and operates in the 2.4 GHz range, providing data rates up to 54 Mbit/s.

> 802.11b, which was approved in 1999, operates in the 2.4 GHz range and provides data rates up to 11 Mbit/s.

Products referred to as 802.11b/g/n/ac are compatible with all four extensions.

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 the standard, due to signaling and protocol overheads.

15.2 WLAN security

When data is transferred over a wireless link, it is important to consider that the fixed boundary available in a wired LAN does not exist in the wireless alternative. In theory, anyone within range of a WLAN could attack the network and intercept data, so security becomes even more important in preventing unauthorized access to data and the network.

Some security guidelines:

- Enable the user/password login in the cameras.
- Enable encryption (HTTPS) in the wireless router/cameras. This should be done before the keys or credentials are set for the WLAN, to prevent anyone seeing the keys as they are sent to/configured in the camera.
- Use WPA2–PSK and a passphrase with at least 20 random characters in a mixed combination of lower and uppercase letters, special characters and numbers. WPA2-PSK can be used to secure small networks that cannot use an authentication server.
- WPA2-Enterprise with EAP-TLS provides the highest level of security and is recommended for enterprise environments that require robust authentication and encryption.

15.2.1 WPA2™ [1]

WPA2™ is based on the IEEE 802.11i standard. Note that the earlier WPA™ is no longer recommended for securing wireless networks.

WPA2-Personal, also known as WPA2-PSK (Pre-shared key), is designed for small networks and does not require an authentication server. With this technology, Axis wireless cameras use a PSK to authenticate with the access point. The key can be entered either as a 256-bit number, expressed as 64 hexadecimal digits (0-9, A-F), or a passphrase using 8-63 ASCII characters. Long passphrases must be used to circumvent weaknesses with this security method.

WPA2-Enterprise is designed for large networks and requires an authentication server with the use of IEEE 802.1X. See section for more on IEEE 802.1X.

[1] WPA and WPA2 are marks of the Wi-Fi Alliance.

15.3 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.

15.4 Wireless mesh network

A wireless mesh network is a common solution for city center video surveillance applications where hundreds of cameras may be involved, together with mesh routers and gateways. Such a network is characterized by several connection nodes that receive, send and relay data, providing individual and redundant connection paths between one another. Keeping the latency down is important in applications such as live video and particularly in cases where PTZ cameras are used.

15.5 4G and 5G networks

The Universal Mobile Telecommunications System (UMTS) is a mobile communications standard and it includes a range of technologies. 3G was the first technology generation to offer bitrates high enough for data transfer and its use is now widespread, although it is rapidly being replaced by later standards.

The 4G standard provides peak bitrates up to 100 (Mbit/s) for mobile applications (for example, in moving vehicles) and up to 1 Gbit/s for more-or-less stationary use. 4G in its various forms is also in widespread use.

The successor to 4G networks currently being rolled out in many countries is generally known as 5G. As well as providing higher throughput speeds, 5G also has greater capacity and can thus connect many more devices in the same geographical area. The data rates available now and those coming in the near future make 5G networks of great interest to video surveillance applications. Some devices such as body-worn cameras have built-in 4G or 5G technology for streaming live video over the mobile network.

15.6 Z-Wave®

Z-Wave was first introduced as a consumer-level control system for lighting. Today, it has evolved into a complete home automation network mesh protocol and system that allows up to 232 smart devices to connect to each other in a single network. Although Z-Wave is not used for video, various Z-Wave devices, such as IR sensors, door/window sensors, and wireless alert buttons can be useful when incorporated into a video surveillance system. A Z-Wave network also has a controller, or smart hub, which is normally the only device connected directly to the internet. It offers transmission rates up to 100 kbps for small data packets. Z-Wave operates on the low-frequency 908.42 MHz band in the US and the 868.42 MHz band in Europe. Operating at these lower frequencies means that Z-wave has a greater signal reach and can better penetrate internal walls.

15.7 Zigbee®

Like Z-Wave, Zigbee is also a low-power, low-data rate, close-proximity network protocol. However, a Zigbee network can support more than 65,000 devices, with unlimited hops between devices. Zigbee uses multiple protocols and open standards and is licence-free. It operates mainly at the higher frequency of 2.4 GHz.

16. Video management systems

One important aspect of a video surveillance system is managing video for live viewing, recording, playback, searching, and storage, in addition to managing the video products. This is all handled by a video management system (VMS).

Axis offers VMS for use on-premises, Windows-based systems, as well as edge-based hybrid-cloud solutions, all with remote access and live view monitoring of sites, playback and storage of video, export of video, and the use of analytics. The systems can also include access management and other capabilities such as audio for security. The systems can be accessed using a PC or laptop or through viewing apps on a handheld device. Furthermore, the Axis network of technology integration partners offers solutions for any system type, size, or complexity.

16.1 Types of video management systems

Video management systems involve a combination of hardware and software platforms that can be set up in different ways. Recording, for example, can be done locally at the camera location, it can be hosted, or it can all be done at a central location. PC-based solutions offer flexibility and maximum performance for the specific design of the system, with the ability to add functionality such as increased or external storage, firewalls, analytics, and other IP devices.

The system to use should be based on your requirements and how you want to manage the system. For a small system with modest video management requirements, a cloud-based system can be ideal. Larger systems – possibly with multiple sites – with extensive recordings that require greater storage capacity would benefit from running on a private network.

16.1.1 Cloud-based systems

Cloud-based video management means that most of the service and software is hosted and accessed through the internet. The only parts of the setup that need to be on-site are the devices.

16.1.1.1 AXIS Camera Station Edge

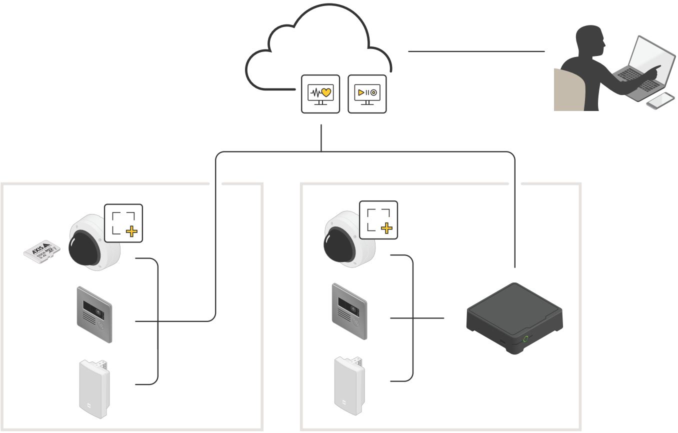
AXIS Camera Station Edge is a cloud-based Video Management System (VMS) that requires minimal maintenance and no server.

AXIS Camera Station Edge offers direct connections between cameras and the cloud, eliminating the need for local servers. You can access key functions such as live view, timeline search, and video export through a user-friendly interface. It is scalable and easy to add new sites or devices to existing installations.

AXIS Camera Station Edge is compatible with Axis cameras and devices. The system supports redundant cloud storage with AXIS Camera Station Cloud Storage, ensuring that recorded footage is always accessible. Real-time alert notifications can be customized using AI-based analytics, giving you instant awareness of suspicious activity. Device configuration and software updates are automated, reducing the need for manual intervention.

You can also customize permissions for managing access to system features, giving you control over who can perform certain actions (viewer, operator, administrator). Retention times for recorded footage can be easily managed, and devices can be remotely restarted if needed. Live sound detection let you respond to alarms and communicate with individuals on-site.

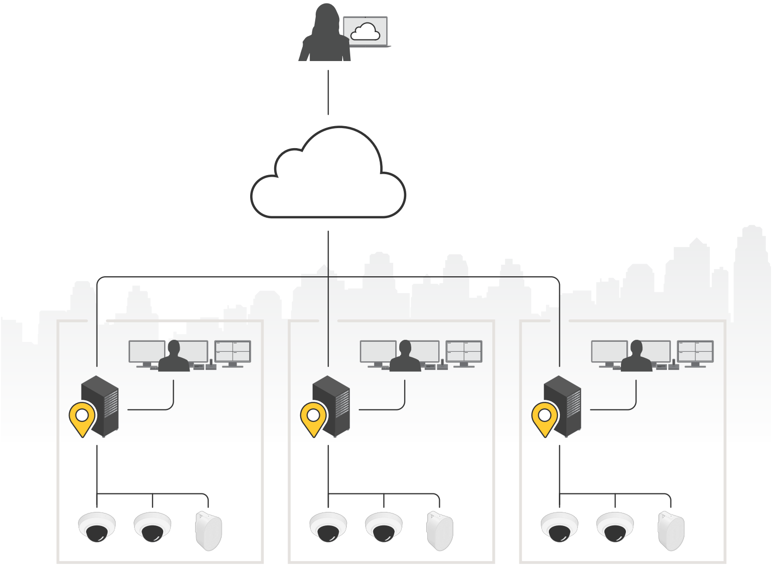
There are multiple ways to access and monitor the AXIS Camera Station Edge system. A dedicated mobile app gives access to system features on-the-go, while a desktop client application provides a comprehensive management interface. A web-based interface is also available, for monitoring system features from any location.



Left: AXIS Camera Station Edge with SD card storage. Right: AXIS Camera Station Edge with an Axis network video recorder.

16.1.2 Private networks

When you have greater demands on capacity or more stringent requirements on your video management system, then it is quite likely you will need to consider a setup on your own private network. The benefits of doing so can include: greater control over security measures, compliance with regulations that require you to store your data on your own premises, and savings on storage costs for large amounts of recorded video. A private network solution can be complemented by the addition of optional cloud capabilities.

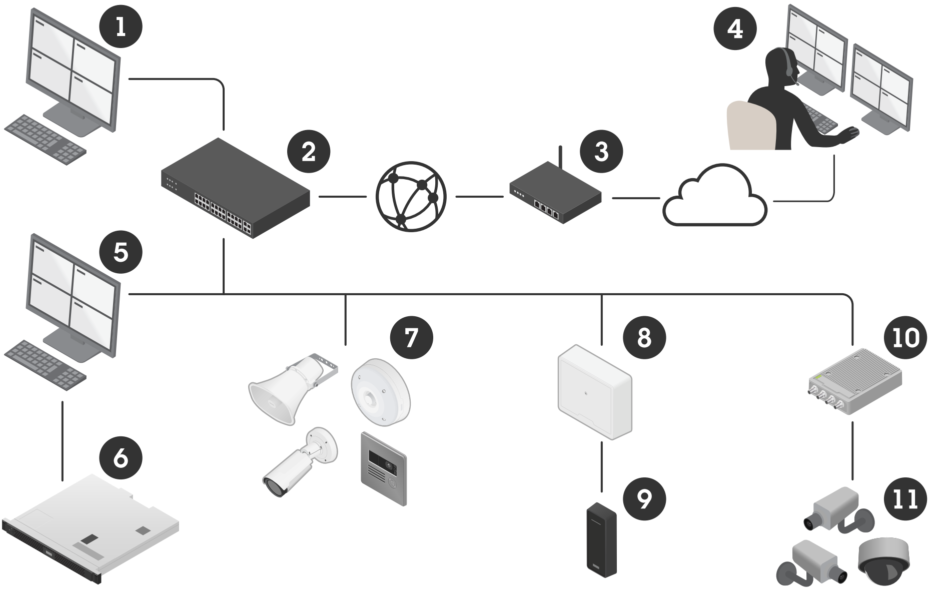


An example of a private network solution, complete with optional cloud access.

16.1.2.1 AXIS Camera Station Pro

AXIS Camera Station Pro offers advanced video management functionality and a complete monitoring and recording system including access control management. The software can be run on validated AXIS Camera Station network video recorders, third-party hardware, and virtual machines. It offers easy installation and efficient management of Axis cameras and other devices. The software has a rich feature set that helps users handle incidents and export evidence. This includes flexible live-view setup, a powerful action rule engine to set up automated triggers, smart search to quickly find video content, video redaction to protect third-party privacy, and incident reports to easily build a case.

Using a Windows client-server application, AXIS Camera Station Pro is a solution that requires the video management software to run continuously on an on-site server for management and recording functions. Recordings are made on the private network, either on the same computer where AXIS Camera Station Pro is installed, or on separate storage devices.



A surveillance system based on an open PC server platform with AXIS Camera Station Pro video management software.
1. AXIS Camera Station Pro Client software
2. Network switch
3. Router
4. Remote access through AXIS Camera Station Pro Client software
5. AXIS Camera Station Pro software
6. Recording server
7. Axis network video and audio products
8. Access control: door controller
9. Access control: reader
10. Video encoder

11. Analog cameras

There are several ways to connect to your AXIS Camera Station Pro System. For a fully-featured experience, a client application can be installed on any computer for viewing, playback, and administration, all of which can be done on-site or remotely via the internet. Multi-site functionality is supported, allowing users to access cameras connected to different AXIS Camera Station Pro servers. This makes it possible to manage video at many remote sites or in a large system, including advanced video operation, access control, alarm notification, system configuration, device management, and system health monitoring.

A mobile app client is also provided, making it possible to access multiple systems, receive notifications, manage video, and perform actions – such as opening a door from an intercom. Additionally, you can access the system using a web browser within your private network or via the cloud, to view live video from cameras, operate PTZ cameras, search, replay, and export recordings, manage users and devices, and monitor system status.

AXIS Camera Station Pro provides the basis to create a solution using products from Axis complete portfolio, such as audio, access control, radar tracking, and analytics. Through the use of API and I/O modules, it also allows integration with other systems such as building management, industrial control, and other external systems.

16.1.3 Customized solutions from Axis partners

Axis works with more than 800 technology integration partners globally to ensure tightly integrated software solutions that support Axis video products. These partners provide a range of customized software solutions, and may offer optimized features and advanced functionalities, tailored features for a specific industry segment or country-focused solutions. There are also solutions that support more than 1000 cameras and multiple brands of video products. To find compatible applications, see *www.axis.com/partner*.

16.2 System features

Some of the most common features of a video management system are:

> **Recording**. Recording video and audio is a primary function of a video management system. This includes setting up recording rules and intelligent ways of searching through recordings and exporting them to other systems.

> **Viewing**. Most video management software lets multiple users view several different cameras at the same time and allows recordings to occur simultaneously. Additional features include multi-monitor viewing and mapping, the latter meaning that camera icons can be overlaid on

a map of the building or area, representing the true location of each camera. There is also a possibility to include external web pages, allowing integration with external systems. This can be used for the presentation of switch interfaces, people counting statistics, and even weather reports and more.

> **Searching**. Video management software should incorporate intelligent search functionality that allows users to quickly search through video material to find persons and vehicles of interest. AXIS Camera Station has a smart search function powered by motion object data from the camera. The data is further processed using machine learning and deep learning algorithms to quickly classify objects such as people, cars, trucks, and bicycles. This works with most Axis cameras and no extra hardware and software is needed. Performance can easily be enhanced by adding additional server capacity and by using Axis cameras with machine- or deep-learning capabilities.

> **Event management and analytics**. Video management software can receive, process, and associate event notifications from different sources, such as access control devices, point-of-sale (POS) terminals, analytics, and the video products themselves. Once an event notification is triggered, the VMS can register it, associate it with a video clip from a nearby camera, and alert an operator or investigator through a pop-up window on the monitor, or by sending a notification to a smartphone.

> **Administration and management**. This includes installation, device software upgrades, security, audit log, and parameter configurations of cameras and other components, such as cash registers, door controllers, and door stations. The larger the system, the more important it is to be able to efficiently manage the devices. System health monitoring provides an overview of the system including the recording hardware and generates notifications if a device or the system goes offline. Video management software should also have options to manage authorized users, passwords, user access levels, and differentiated access to specific devices. Some video management software can inherit a Windows user database, thus eliminating the need to set up and maintain a separate database of users.

16.3 Integrated systems

When video is integrated with other systems such as access control, point-of-sale, building management, patient information systems, or logistic systems, information from the other system 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.

16.3.1 Access control

Access control is one of the most used VMS integrations. AXIS Camera Station Secure Entry is part of the AXIS Camera Station Pro software and provides a unified solution combining both surveillance and access control functionality. Read more about access control in chapter .

16.3.2 Point of sale

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

This integration enables all cash register transactions to be linked to actual video of the transactions. It helps catch and prevent fraud and theft by 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 by activating event-based recordings when these events occur. The seconds prior to and following an event can also be captured using pre- and post-event recording buffers. Event-based recordings increase the quality of the recorded material, as well as reducing storage requirements and the amount of time needed to search for incidents.

16.3.3 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. This makes it possible for first responders and building managers to assess the situation at all emergency exits in real time and focus their efforts where they are needed the most.
- Analytics can be used to detect the reverse flow of people into a building due to an open or unsecured door from events such as evacuations.
- Automatic video alerts can be sent when someone enters a restricted area or room.
- Information from the video motion detection functionality of a camera 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.

16.3.4 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 substations in remote locations.

16.3.5 RFID

Tracking systems that involve RFID (radio-frequency identification) or similar methods are used in many applications to keep track of items. For example, tagged items in a store can be tracked together with video footage to prevent theft or provide evidence. Another example is luggage handling at airports whereby RFID can be used to track the luggage and direct it to the correct destination. When integrated with video surveillance, there is visual evidence when luggage is lost or damaged, and search routines can be optimized.

17. Cloud technologies

17.1 Moving to the cloud

Cloud technologies have revolutionized the way we approach network video surveillance. By leveraging cloud-based services and solutions, users can now access their video feeds remotely, at any time, and from anywhere. This increased flexibility enables more efficient monitoring and responses to security incidents.

There are many benefits of using cloud-based services and solutions. Cloud-based managed services can, for instance, perform automatic software updates, eliminating the need for manual maintenance and reducing the risk of system vulnerabilities. Scalability is another key benefit, allowing users to easily add or remove cameras and storage capacity as needed. Cloud storage provides a secure and scalable solution for storing large amounts of video data. By storing footage off-site, organizations can reduce the risk of data loss due to hardware failure or physical damage.

Additionally, cloud-based analytics enable advanced features such as object detection, people counting, and license plate recognition, boosting security and business efficiency. The most effective solution often involves a hybrid configuration that combines camera-based object classification with server-based or cloud-based algorithms for tasks that require more computational power.

Overall, integrating cloud technologies into network video surveillance systems offers enhanced flexibility, scalability, and security, making it an attractive option for businesses and organizations looking to modernize their surveillance infrastructure.

17.2 Cloud setups

Cloud video and device management often consists of a service that is hosted and accessed through the internet. Through subscriptions, you can pay for and use as much (or as little) of the service as you like. Any definition of a cloud-based system will be a combination of the system's functions combined with where those functions are located. Here are some common definitions:

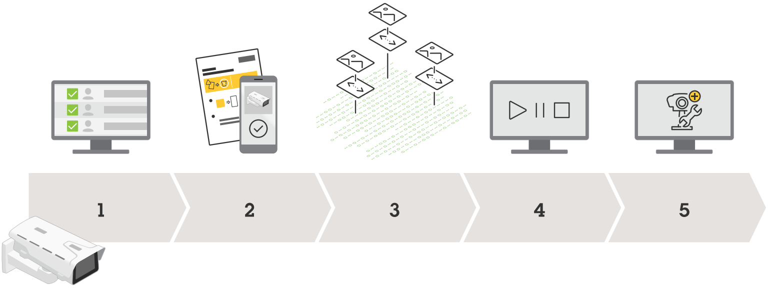
- **Direct cloud**: Also known as "cam-to-cloud" or "pure cloud", these solutions usually have three major functions in the cloud – viewing, management, and storage. Some may run analytics as cloud applications, although it is often more cost-efficient to have these at the edge.
- **Hybrid cloud**: This often describes a system where some functions are in the cloud and some are local. One example is an on-demand cloud, where most functions can be performed in the cloud, but in practice, some or all are performed at the edge to reduce latency.
- **Relay cloud**: A solution that only provides cloud viewing and possibly some basic management functionality. All other functions are either local or are available through other solutions.

The optimal solution will depend on needs, requirements, and system set-up. For organizations with several smaller sites, a cloud-only solution may make the most sense, while for an organization with one bigger site, an on-premises-only solution may be the right option. For most organizations, a combination of powerful connected edge devices, with cloud and private network is the ideal solution.

17.3 Axis Cloud Connect

Axis Cloud Connect is an open, hybrid cloud platform that together with Axis devices enables managed services such as system and device management, video and data delivery, and security and support. The services you get are based on technologies included in the platform.

Solutions using Axis devices and built with Axis Cloud Connect, such as AXIS Camera Station, AXIS Device Manager Edge, or AXIS Device Manager Extend, give you more flexible and efficient video operations, device lifecycle management, and access to data. They also provide new opportunities in security, safety, operational efficiency, and business intelligence.



Examples of services via Axis Cloud Connect: 1) User and access management, 2) Secure device onboarding, 3) Media to cloud, 4) Live operations, 5) Device management.

18.System design considerations

One of the main benefits of a network video system is flexibility and scalability: the freedom to mix and match the most appropriate components from different vendors and the power to optimize or expand the system to any size.

It is essential that you select the right camera, install and protect it properly, configure it to match the scene complexities, and to get it to stream live or record video at the right time, in the right format, and with the right quality. At the same time, the appropriate network and storage solutions depend greatly on the selected cameras, the camera settings (such as resolution, compression, and frame rate), and the number of cameras.

AXIS Site Designer helps you pick just the right cameras for any surveillance scenario, as well as add accessories and pick a recording solution. When you have completed your design project, AXIS Site Designer prints a comprehensive bill of materials that includes everything you need to complete your installation.

18.1 Selecting a camera

This section outlines what to keep in mind when selecting a camera.

18.1.1 Types of cameras

To determine which types of cameras are suitable and how many cameras are needed to cover an area, you must first understand the scene and its conditions. You also need to consider the purpose of your surveillance.

> **Indoor or outdoor**. If placing the camera outdoors, use an outdoor-ready camera or install it in an appropriate protective housing. Look for the IP rating (IP66 or better) or National Electrical Manufacturers Association (NEMA) rating (4X or better). The camera should also have auto-iris functionality.

> **Pan-tilt-zoom (PTZ) or fixed camera**. PTZ cameras with a large optical zoom factor can give high-detail images and survey a large area. Keep in mind that to make full use of the capabilities of a PTZ camera, an operator needs to control the movements, or an automatic tour must be set up. For surveillance recordings without live monitoring, fixed cameras are usually more cost-effective.

> **Light sensitivity and lighting requirements**. Light sensitivity is one of the most important factors of a camera. Day-and-night functionality means you get images in conditions that would otherwise be too dark. Some cameras come with built-in IR LED lights that provide power-efficient, discreet illumination that is invisible to the eye but enables sharp images in the dark.

> **Complete darkness and perimeter protection**. Thermal cameras can detect movement even in complete darkness and other difficult conditions. They can generally detect movement at greater distances than conventional cameras.

> **Tamper- or vandal-proof and other special housing requirements**. Proper protection against water, dust, temperature, and vandalism is essential.

> **Overt or highly discreet surveillance**. This will help in selecting cameras that openly act as a deterrent or are installed less obviously.

> **Area of coverage**. For a given location, you should determine the areas of interest, how much of these areas should be covered, and whether the areas are located close to each other or further apart. For example, if there are two relatively small areas of interest close to each other, you could potentially use a single high-resolution camera with a wide-angle lens instead of two cameras with lower resolutions.

> **Overview or high-detail images**. Determine the field of view or the kind of image to capture: an overview or high detail images for the identification of persons or objects, for example, face or license plate recognition, or point-of-sale (POS) monitoring.

> **Edge-based or server-based analytics**. Analytics enable efficient monitoring and searches, and they can provide valuable insights. Edge-based analytics have many benefits (if the camera has enough processing power), but power-hungry analytics may require a dedicated analytics server. Consider future-proofing your investment by purchasing cameras with support for analytics and with the performance needed for the type of analytics you might need later.

18.1.2 Image quality

Although image quality is one of the most important aspects of any camera, it can be difficult to select the right camera. The reality is that many aspects of image quality cannot be quantified or measured. The best way to determine image quality may be to install different cameras and compare the video. Keep in mind that even if a camera provides high-quality still images, the image quality might deteriorate when significant motion is introduced into the scene or in low light.

Many factors affect image quality. For example, white balance and a camera's ability to adapt to different lighting conditions from fluorescent, high-pressure sodium, to LED light, is important to ensure color fidelity. Low-light, backlight, dynamic light, and other extreme lighting conditions present challenges that the camera needs to be able to handle. Typically, a high-resolution camera is less light-sensitive than a lower-resolution camera. In other words, you may need to consider sacrificing resolution for better low-light performance, or else use a camera with a sensor and processing algorithms that are specifically designed to meet the challenges.

18.1.3 Resolution

When designing a surveillance system it is important to consider the system's purpose. You might check the technical specifications to find out which camera has the best resolution, but to optimize cost and effort you should focus on which camera and setup will best meet your operational requirements. For example, do you need to be able to identify individuals from the footage, or do you need to simply detect that a person is present?

We can distinguish between the need for **D**etection, **O**bservation, **R**ecognition, and **I**dentification. These requirements are sometimes known as DORI.

Operational requirement	Level of detail
Detection	Possible to determine whether an individual is present.
Observation	Possible to determine how many persons are present and to see characteristic details, such as distinctive clothing.
Recognition	Possible for a viewer to determine whether or not an individual is someone they have seen before.
Identification	Possible to identify an individual.

Table 18.1a *Common operational requirements in video surveillance.*

The specifications for these requirements (for visual cameras), come from the international standard IEC 62676-4 (Video Surveillance Systems for Use in Security Applications – Part 4: Application guidelines).

It should be noted that the specifications for these operational requirements are valid in situations where visual video images are interpreted by human operators. For analytics or other systems where image analysis is done by software, other definitions for the operational requirements would apply. Thermal imaging (using thermal cameras) also uses a different set of specifications for operational requirements.

The camera that you choose must be able to provide the adequate field of view, as well as an adequate pixel density on the objects that you prioritize, such as the faces of individuals.

The basis of the recommended pixel densities is the number of pixels needed to represent the width of a human face, with its distinctive identifying features, at the requested level of detail. To get a standardized pixel density requirement, the pixel density of the face can be recalculated to the corresponding number of pixels needed per meter or per foot, based on the assumption that an average human face has a width of 16 cm (6 5/16 in.). The table lists the resulting pixel densities for the different operational requirement categories.

Operational requirement		**Pixel density needed**	
Detection	4 px/face	25 px/m	8 px/ft
Observation	10 px/face	63 px/m	20 px/ft
Recognition	20 px/face	125 px/m	40 px/ft
Identification	40 px/face	250 px/m	80 px/ft

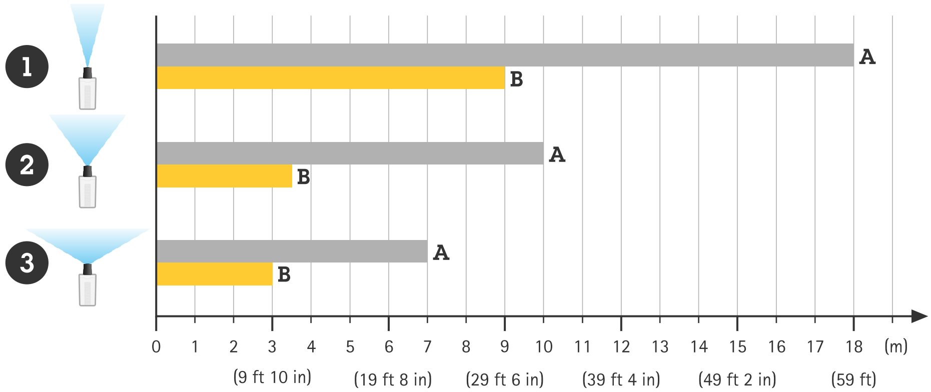
Table 18.1b *Pixel densities for different operational requirements.*

It is usually recommended, for example in IEC 62676-4, to have at least 40 pixels across the width of a human face to enable identification. Even higher pixel densities can be beneficial and provide a safety margin for difficult conditions, such as in sub-optimal lighting or where individuals are not directly facing the camera. If an installation does not comply with the pixel density guidelines, this does not necessarily mean that the operational requirements will not be met. In reality there are always other factors such as light direction, optics quality, and image compression that affect the result.

It should also be noted that if an external display is used to monitor the scene, the ability to detect, observe, recognize, or identify individuals depends greatly on the display’s resolution.

Axis cameras provide a pixel counter feature to make it easy to check the pixel density in the image. This is a visual aid shaped as a frame, with the frame’s width and height (measured in pixels) clearly shown.

The pixel density for an object under surveillance depends on the camera sensor's resolution, on how far the object is from the camera, and on which type of lens is being used. The choice of optics is particularly important and this is a science on its own, which is why it is advisable to work with vendors who supply cameras that have been tested end-to-end with the included lens. The illustration shows a general example of how the maximum distance for recognition and identification may change with different lens types (that is, different fields of view).



Examples of how the maximum distances for recognition (A) and identification (B) change with the lens type: tele (1), normal (2), wide angle (3).

Axis offers several online tools for designing a surveillance site, taking both pixel density and many other factors into account. AXIS Site Designer can help calculate image resolution and field of view based on the camera model and position. Using the tool, it is possible to specify the required pixel density and adjust the camera's mounting height and field of view, to determine whether or not the camera can satisfy the use case requirements.

18.1.4 Compression

Cameras that offer support for more than one type of video compression standard give users greater flexibility in optimizing viewing and recording needs.

Design of the network and storage system is highly dependent on the selected compression standard. The following are some basic recommendations:

> **AV1**. This new standard is the recommended option if your system supports it. AV1 is optimized for video transmission over the internet and provides high-resolution and cost-efficient streaming and storage.

> **H.264**. The dominant video compression standard in video surveillance today. Compared to AV1, H.264 video requires roughly twice as much storage.

> **H.265**. H.265 encoding does not yet entirely meet the requirements of surveillance type video. Most surveillance equipment supports H.265, but there are limitations in decoder support and browser support. Many users have to continue using H.264 to view video on their preferred clients, but this should not be a problem since Zipstream with H.264 is very bitrate-efficient.

> **Axis Zipstream**. Filters out areas of low interest and compresses them more aggressively, while recording the details of interest and motion at a higher quality. This switching between a maximum GOP value and a lower value drastically reduces the bitrate and the requirements for storage and bandwidth.

18.1.5 Networking functionality

In the same way that high-quality images are essential, networking functionality is also important. Besides Ethernet connectivity, a network camera should also support the following capabilities:

> **Power over Ethernet (PoE)** means that the camera can receive power over the same cable as the data, thus eliminating the need for power cable runs. Outdoor PTZ cameras may require more power, which can be provided by a midspan.

> **Dynamic Host Configuration Protocol (DHCP)** is used to manage IP addresses. A DHCP-enabled switch or router automatically gives each connected device an IP address. However, the predictability of static IP addresses and the ability to match IP addresses to the cameras' ID numbers may be preferable.

> **HTTPS** encryption for secure communication.

> **SNMP** helps IT administrators monitor conditions on the network and determine if connected devices need attention.

> **IP address filtering** allows only defined IP addresses to have access to the camera.

> **Cybersecurity functions** are essential to protect the camera and the network it is connected to. Built-in cybersecurity features counter different types of cyber-attacks, effectively combat vulnerabilities, and prevent unauthorized access to your system. For example, *secure boot* ensures that any unauthenticated, altered code is blocked and rejected during the boot process before it can attack or infect the system. With *signed OS*, you can verify the integrity of the device software before installing new devices or upgrading existing ones.

> **Wireless technology** is a good option if running a cable to a network camera is impractical, difficult, or expensive. Wireless access can also be provided for a standard network camera by equipping it with a wireless bridge or wireless dongle.

18.1.6 Other functionalities

Network cameras have many other functionalities apart from providing a video stream. When selecting a camera, it is also important to evaluate these capabilities. Some examples of additional functionalities are:

> **Audio for communication and detection**. Users can detect and classify different types of sounds and communicate instructions, orders, or requests to visitors or intruders. When microphones detect sounds above a certain level, they can trigger alarms or trigger cameras to start recording. Consider whether one-way or two-way audio is required.

> **Built-in analytics**. Built-in intelligence makes the system more scalable and helps reduce bandwidth and storage requirements, because the camera can decide when to send and process video.

> **Input/output (I/O) connectors**. Connecting external input devices to a camera (such as a door contact, infrared motion detector, radar detector, glass-break sensor, or shock sensor) enables the camera to react to an external event by, for example, sending and recording video. Outputs enable the camera or a remote operator to control external devices, for example, alarm devices, door locks, or lights.

> **Audio/visual alerters**. An audio/visual alerter can be used to deter intruders or improve operational efficiency with strobe lighting and siren alarms. This fully networked device is especially valuable when connected to a camera with perimeter protection or license plate recognition (LPR) analytics.

> **Edge-to-edge connectivity**. Edge-to-edge is a technology that makes IP devices communicate directly with each other. It offers smart pairing functionality between, for example, Axis cameras and Axis audio or radar products.

> **Radar**. A motion detector based on radar is a valuable complement to a video surveillance system. In addition to triggering an alarm when it detects an intruder, it can also trigger recording for visual verification. If radar is combined with a PTZ camera, the radar can control the camera automatically. There are also cameras combined with a fully integrated radar. These can detect objects over wide areas regardless of visibility and then visualize the speed and distance of moving objects directly in the application view.

> **Alarm management functions**. Advanced cameras can perform alarm management tasks such as processing and linking input, output, and other events. Pre- and post-alarm buffers in a camera can record video before and after an alarm occurs.

> **Other physical security devices**. When evaluating a video surveillance system, also look at other systems, such as access control, intercom, audio, and intrusion detection, to determine if there is a way to construct an integrated system that covers all physical security needs.

> **Multi-application support and ease of integration**. Make sure you select cameras that have open application programming interfaces (APIs) that can integrate with several video management software applications. All Axis cameras are compliant with ONVIF, which provides interoperability between network video products regardless of manufacturer.

18.2 Installing a network camera

How a network camera is installed is just as important as the process of selecting it. The following are some recommendations on how to best achieve high-quality video surveillance based on camera positioning.

18.2.1 Surveillance objective

To best position a camera, you need to know what kind of image you need. For example, to track people or objects moving to and from many positions in several directions you will need an overview image, as this gives you the best chance of spotting such events. After selecting a suitable overview camera, you can install it in a position that achieves the purpose.

AXIS Site Designer can help you find the best position for a camera and it provides plug-ins for various diagram and 3D software. These tools can help with placement of cameras, calculating viewing angles and coverage, and finding blind spots and items that block the view.

18.2.2 Handling challenging light

Scenes with very little light, direct sunlight into the camera, or other types of backlight can be problematic for conventional cameras. Axis cameras are equipped with various solutions for providing good images despite poor conditions. Examples are Lightfinder, IR LEDs, and Forensic WDR. If the scene and location allows, you can add external lighting. Some cameras have sun shields that help reduce the impact of direct sunlight and make camera placement easier.

Even though automatic settings in Axis cameras usually provide the best images, it is also possible to adjust settings manually, for example, brightness, sharpness, white balance, and WDR.

As an alternative to visual cameras you can also use thermal cameras to overcome challenging lighting conditions.

18.2.3 Lens selection

When selecting lenses, the required field of view must be defined. The field of view is determined by the focal length of the lens and the size of the image sensor. A lens' 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 of the lens, the narrower the field of view (FoV) will be.

The FoV 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 the human eye can see. 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.

AXIS Site Designer and the product selector tool can assist in the camera and lens selection process. See the Axis tool portal, *www.axis.com/tools*.

18.3 Physical protection of the camera

Surveillance cameras are often placed in very demanding environments. In outdoor installations they need to be protected against all kinds of weather conditions. In industrial settings, cameras may require protection from hazards such as dust, acids, or corrosive substances. In vehicles such as buses and trains, cameras must withstand high humidity, dust, and vibrations. Some cameras may also require protection against vandalism and tampering.

The sections below cover such topics as protection ratings, external housings, positioning of fixed cameras in enclosures, domes, vandal and tampering protection, and types of mounting.

18.3.1 Protection and ratings

The main environmental threats to a video product – particularly when installed outdoors – are cold, heat, water, dust, and snow. Today, many indoor and outdoor Axis devices are designed to meet environmental challenges out-of-the-box, and do not require separate housings. This results in a more compact device and simpler installation. For example, Axis cameras that are designed to operate in temperatures up to 75 °C (167 °F) are very compact, even with a built-in active cooling system.

A camera design can also ensure reliability and maintenance of a camera's lifetime, especially under extreme operating conditions. For instance, some Axis fixed and PTZ cameras incorporate Arctic Temperature Control, which allows the cameras to start up in temperatures as low as -40 °C(-40 °F) without causing extra wear and tear on the mechanical parts. Some Axis dome cameras without Arctic Temperature Control can also start up at -40 °C/-40 °F and can send video immediately.

The level of protection provided by enclosures, whether built-in or as separate housings, is often indicated by classifications set by such standards as IP, NEMA, and IK ratings. IP stands for Ingress Protection and is applicable worldwide. NEMA stands for National Electrical Manufacturers Association and is applicable in the United States. IK ratings pertain to external mechanical impacts and are applicable internationally.

The most common environmental ratings for Axis indoor devices are IP42, IP51 and IP52, which provide resistance against dust and humidity/water. Axis outdoor devices usually have IP66 and NEMA 4X ratings. IP66 ensures protection against dust, rain, and powerful jets of water. NEMA 4X ensures protection not only against dust, rain, and hose-directed water, but also snow, corrosion, and damage from the external build-up of ice. Some Axis cameras that are designed for extreme environments also meet the U.S. military's MIL-STD-810G standard for high temperature, temperature shock, radiation, salt fog, and sand. For vandal-resistant products, IK08 and IK10 are the most common ratings for resistance to impact.

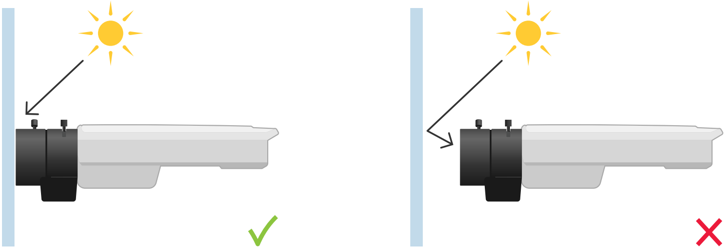
In situations where cameras may be exposed to acids, such as in the food industry, housings made of stainless steel are required. Special enclosures may also be required for aesthetic considerations. Some specialized housings can be pressurized, submersible, or bulletproof. When a camera is to be installed in a potentially explosive environment, other standards come into play. For example, IECEx – a global certification, and ATEX – a European certification.

18.3.2 External housings

When the environmental demands of the surroundings are beyond the operating conditions of a network video product, external enclosures must be used. Housings come in different sizes and qualities and have different features. Housings can have heaters and fans (blowers) to accommodate changing temperatures. Some have peripherals such as antennas for wireless applications, although an external antenna is only required if the housing is made of metal.

In outdoor installations, special enclosures may also be required for video encoders and accessories such as I/O audio modules and video decoders. Critical system equipment such as power supplies, midspans, and switches may also require protection from weather and vandalism.

18.3.2.1 Positioning a fixed camera in a housing



When installing a camera behind a glass, correct positioning of the camera is important to avoid reflections.

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 reflections from appearing in the image. Special coatings can also be applied to any glass used in front of the lens to reduce reflections. Axis outdoor fixed cameras come in protective, outdoor-ready housings, which saves installation time and prevents errors.

18.3.3 Transparent domes

The “window” or transparent dome of an enclosure is usually made of acrylic (PMMA) or polycarbonate plastic. As windows act like optical lenses, they should be of high quality to minimize their effect on image quality. Any inherent imperfections in the material will compromise clarity.

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

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

A variety of domes are available, including clear and smoked versions. While smoked versions enable a more discreet installation, they also act much like sunglasses do – they reduce the amount of light available to the camera. They will, therefore, influence the camera's light sensitivity.

Clear, smoked, and partially smoked domes for PTZ and dome cameras.

18.3.4 Vandal and tampering protection

In some surveillance applications, cameras run the risk of vandalism. Impact resistance can be indicated by the IK rating on a camera or housing. IK ratings specify the degree of protection that electrical equipment enclosures provide against external mechanical impacts. For example, an IK10 rating means the product can withstand 20 joules of impact, which is equivalent to a drop of a 5 kg object from a height of 40 cm. The goals of vandal protection, regardless of actual technical implementation, include the following:

- **Making it difficult**. Tampering with a video surveillance camera should be difficult. Perhaps even more importantly, their design and placement should make them look difficult to tamper with.
- **Creating uncertainty**. If vandals decide to attack a camera, they should remain uncertain as to whether they succeeded in destroying the camera or interrupting the recording.
- **Prolonging and delaying**. Even if it is not possible to protect a camera from a determined attack, it is worthwhile to make it very time-consuming for a vandal to redirect or destroy the camera. Every second gained increases the chance of discovery or that the vandal gives up.
- **Detecting and sending alarms**. A camera with built-in analytics can detect that someone is tampering with it and can notify operators.

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. A housing or a traditional fixed camera that protrudes from a wall or ceiling is more vulnerable to attacks (e.g., hitting it) than more discreetly designed housings or casings for a dome or PTZ camera. The smooth, rounded covering of a dome camera or a ceiling-mounted PTZ dome makes it more difficult, for example, to block the camera's view by hanging 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.

Mounts. A camera that uses a recessed mount, where only the window part of the camera or housing is visible, is less vulnerable to attacks than a camera that is mounted so that it is completely accessible from the exterior. When making plans for mounting cameras and protecting the system from vandals, always include the cable runs. Running the cable directly through the wall or ceiling behind the camera provides the best level of protection. A metal conduit is also a good alternative when trying to protect cables against attack.

Camera placement. A camera that is mounted high up on a wall or in the ceiling is less likely to attract a spur-of-the-moment attack. The downside may be the field of view, which to some extent can be compensated for by selecting a different lens.

Tampering switches. Adding tampering switches to camera housings and boxes enhances protection. When these accessories are triggered, an alarm or notifications can be sent to selected clients.

Analytics. Intelligent algorithms can also detect if a camera is redirected, obscured, or tampered with and can send alarms to operators in central control rooms or to staff in the field. There are algorithms for detecting: a changed view (tampering), abnormal sounds (audio), if the camera is subjected to violence (shock), if the housing is opened or tampered with (casing open), and if cables are cut (supervised I/Os). Specifically, AXIS Image Health Analytics notifies you if the image is blocked, blurred, underexposed, or redirected.

18.3.5 Types of mounts

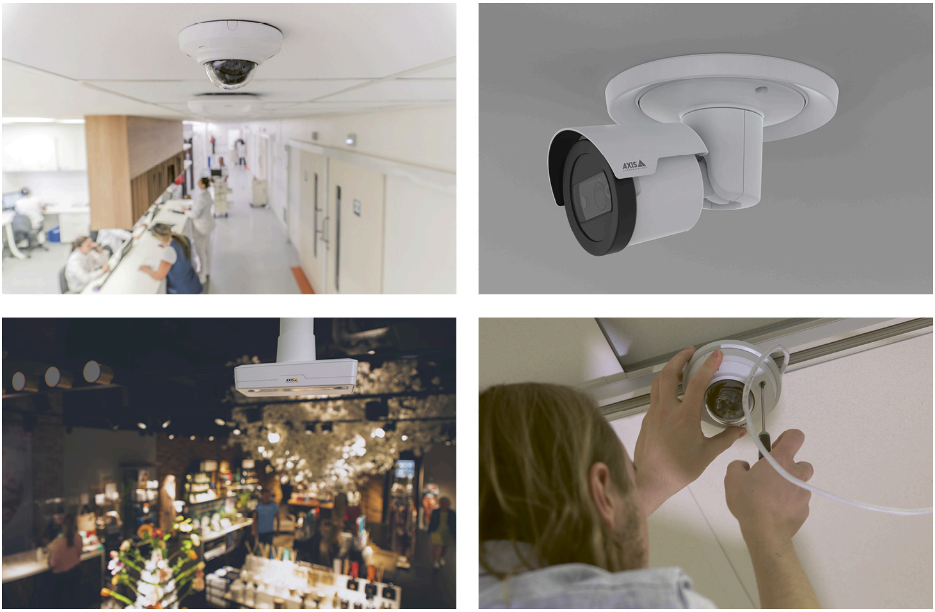
Because the need for surveillance is not limited to a specific type of space, there needs to be a wide range of mounting options available. Axis provides an accessories selector online tool that can help users identify the right housing and mounting accessories needed. See the Axis tool portal, *www.axis.com/tools*

To minimize vibrations, you should always make sure that the camera mount is stable. Because PTZ cameras can move around within their housing, this action can cause image interference if the camera mount is not properly secured. In outdoor situations, sturdy mounting equipment is necessary to avoid vibrations caused by strong winds. If the mount is not strong or stable enough, the camera could fall and endanger people or property.

Ceiling mounts. Cameras can be mounted on ceilings by using a:

> Surface mount: Mounted directly on the surface of a ceiling and therefore completely visible.

- Recessed mount: Mounted inside the ceiling with only parts of a camera and housing (usually the dome) visible. This mount is also known as a flush mount or drop-ceiling mount.
- Pendant kit mount: Enabling the camera to be hung from a ceiling.
- Lighting track mount: Enabling the camera to be attached to an existing lighting track without any additional drilling.



Examples of surface mount and recessed mount (top); pendant kit mount and lighting track mount (bottom).

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 the wall. Advanced mounts have an internal cable gland to protect the cable. To install an enclosure on the corner of a building, a normal wall mount, together with an additional corner adapter, can be used.

Pole mounts. Pole mounts often hold PTZ cameras in large outdoor areas such as parking lots, roads, and city squares. This type of mount is usually designed to absorb and minimize the effects of wind and ground vibrations, to limit their impact on the camera. When calculating the sway, consider the height and diameter of the pole, as well as the material. Concrete poles sway less than metal and wooden poles. Factor in the weight and dimensions of the equipment the pole needs to bear. This is especially important for PTZ cameras and cameras with high optical zoom – if the pole is under-dimensioned, there will be a greater risk of motion blur in the images. More advanced PTZ cameras have built-in electronic image stabilization to mitigate the effects of wind and vibrations. However, heavy cameras can cause serious injuries if they fall. As with wall mounts, the cable can usually be run inside the pole, and cable exits and outlets must be sealed properly.

Examples of a wall mount and a pole mount.

Parapet mounts. Parapet mounts are used to mount cameras on rooftops or to raise the camera for a better angle of view. One benefit of parapet mounts is that the camera is cheaper and easier to service than if hung from a wall mount. Because the arm can swing inwards, maintenance staff can access the camera from the rooftop rather than having to use a lift or other type of work platform.

Highly discreet mounts. Highly discreet mounts are typically used to mount tiny modular cameras in spaces where discretion is key. These mounts can be completely discreet, barely visible (pinhole mount), partly visible (flush mount), or fully visible (surface mount).

Examples of a parapet mount and a highly discreet mount (a modular camera hidden in a height strip).

18.4 Bandwidth and storage considerations

Network bandwidth and storage requirements are important considerations when designing a video surveillance system. With AXIS Site Designer, you can effectively estimate the needs for your system. Bandwidth and storage requirements depend on the following factors:

- Number of cameras
- Continuous or event-triggered recording
- Edge recording in the camera/video encoder, server-based recording, or a combination
- Number of hours per day the camera will be recording
- Frames per second
- Image resolution
- Video compression type: H.264, H.265, AV1, and whether Zipstream is used
- Scene complexity: image complexity, lighting conditions, and amount of motion
- The length of time data must be stored.

18.4.1 Bits or bytes?

There is often confusion as to what is meant by various terms such as bits, bytes, Mbit/s, Gigabytes, etc. Which is for capacity? Which is about speed?

Data sizes

The smallest unit of digital information is one binary digit, more commonly known as a bit (b), which can have one of two possible values, often represented as 1 or 0 but sometimes as on/off, true/false, yes/no, +/-.

As bits are such small increments of data, we use multiples to talk about larger values:

- 1 thousand bits = 1 kilobit (kbit)
- 1 million bits = 1 megabit (Mbit)

Bits can also be represented in groups, by using the byte. 1 byte (B) = 8 bits (b), these eight bits being the minimum required to represent a single character of text.

The same prefixes for bits are also used for bytes:

- 1 million bytes = 1 megabyte (MB)
- 1 billion bytes = 1 gigabyte (GB)

Good to know is that computers are binary systems and not decimal – that is, they work with base two instead of base ten. This means that the exact totals in the two systems will differ, even if the various prefixes (kilo, mega, giga, etc.,) are often used for both decimal and binary values.

For example, to multiply 1 byte by 1,000:

- In base ten (decimal), this would be 10^3 = 1,000
- In base two (binary), the nearest equivalent is 2^{10} = 1,024

Although slightly different, both these values are generally given as "1 kilobyte". This is because most people find it much easier to count in decimal than in binary. Hard drives are routinely specified in decimal values, where, for example, 1 GB is defined as exactly one billion bytes.

However, as the computer using the drive is a binary system, a disk specified at 10 GB will be seen by the computer as having only 9.31 GB, as in a binary system 10 GB = 10,737,418,240 bytes.

As there are 8 bits in every 1 byte, it also follows that:

- 1 Mb = 0.125 MB
- 8 Mb = 1 MB

See the following table for further comparisons of data sizes.

Unit	**Size (binary)**	**Size (decimal)**
Kilobyte (KB)	1,024 Bytes	1,000 bytes
Megabyte (MB)	1,024 Kilobytes	1,000,000 bytes
Gigabyte (GB)	1,024 Megabytes	1,000,000,000 bytes
Terabyte (TB)	1,024 Gigabytes	1,000,000,000,000 bytes
Petabyte (PB)	1,024 Terabytes	1,000,000,000,000,000 bytes
Exabyte (EB)	1,024 Petabytes	1,000,000,000,000,000,000 bytes

Table 18.4a *Comparisons of data sizes.*

Data transfer rates

Network or internet connections are specified in megabits per second (Mbit/s). Although this is technically a measure of capacity (number of bits moved per second), values in Mbit/s are generally viewed as speeds, that is, a high-capacity connection is often perceived as being "fast".

For network video, remember that data is sent over a network "bit by bit" and not in bytes. This means that Mbit/s can be useful to describe a connection over which you might view a live video stream, that is, when not downloading and saving the video. A "fast" connection will give a smoother viewing experience (by reducing latency) and will better allow the viewing of high-resolution video. If, instead, you simply wish to download and save the video, then the connection speed is of less importance. A "slower" connection might take slightly longer than a "fast" connection to download the video, but does that really matter?

Also relevant here is that bits transferred over a network do not always arrive in the correct order, nor do they necessarily originate from the same source. This is not a problem, as the application receiving the bits assembles them in the correct order, but it highlights why network speeds are usually specified in Mbit/s rather than bytes.

Although Mbit/s is the most common way to specify data speeds, MB/s can also be used, for example, when saving a video to disk. To download/transfer a 100 MB video file over a 100 Mbit/s connection would take 8 seconds, as the write speed converted to MB/s is 12.5 MB/s
(that is, 100 megabytes = 800 megabits).

18.4.2 Bandwidth requirements

In a small surveillance system with fewer than 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 approximately 2–8 Mbit/s of the available network bandwidth.

> With more than 12–15 cameras, consider using a switch with a gigabit backbone. If a gigabit 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-triggered recordings.

18.4.3 Storage requirements

One of the factors affecting storage requirements is the type of video compression used. H.264 is the dominant video compression standard in video surveillance today, even though the AV1 and H.265 formats are much more efficient.

New systems are getting support for AV1, which reduces storage requirements by 50% compared to H.264. H.264 will be supported in parallel with AV1 for many years to come.

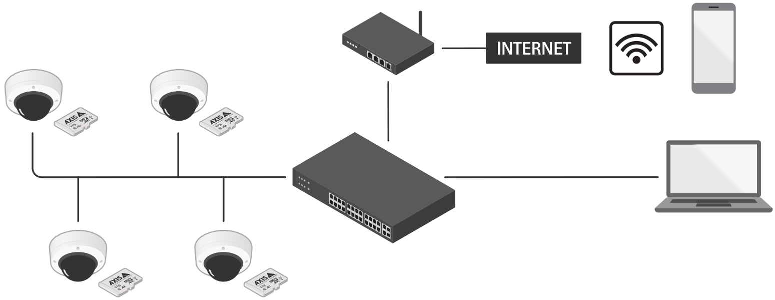
H.265 does not yet entirely fulfill the requirements of surveillance type video.

Enabling Zipstream is recommended, since it can greatly reduce the system storage size without compromising the forensic value of the video.

The best way to estimate storage need without doing any on-site measurements is to use AXIS Site Designer. This tool helps you to choose the right cameras and accessories for your surveillance scenario and purpose, and automatically estimates storage and bandwidth needs. It is important to configure each camera in the tool with scene type, resolution, frame rate, quality selection, and recording settings.

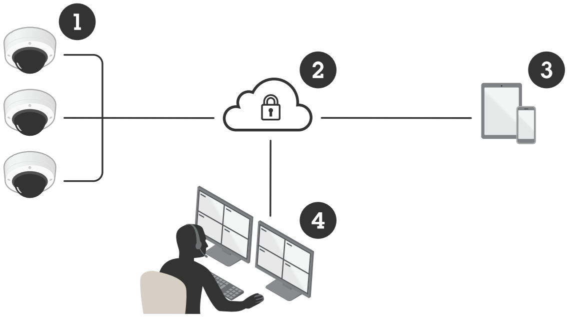
18.4.4 System configurations

Edge solution. A camera can have an SD card to store video and metadata. Axis has high-endurance SD cards developed specifically for surveillance. Edge or cloud storage means there is no need for a network video recorder or file server. Even analytics that process video and/or metadata can be run directly in the camera. Systems can benefit from a combination of edge, cloud, and on-prem components in a hybrid setup. Cloud-based components can offer remote viewing, cloud storage, remote system monitoring, and remote management.



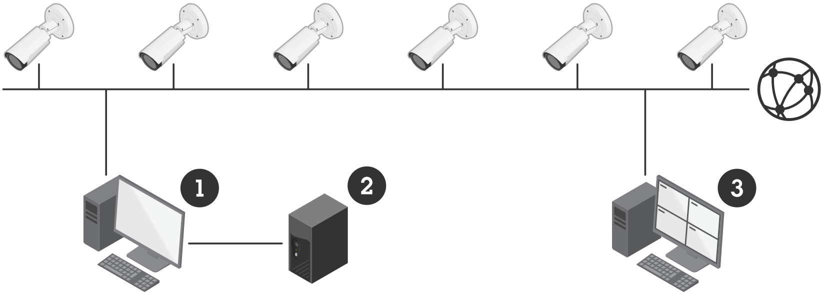
A solution utilizing edge storage and a VMS for video management.

Cloud solution. In a cloud video setup, most of the system components are handled by a service provider, which in turn provides users with access to live and recorded video over the internet. Axis Cloud Connect is an open hybrid cloud platform that together with Axis devices enables managed services.



In a cloud solution, video (1) is stored and managed in the cloud (2). Live and recorded video can be accessed by authorized users through mobile devices (3) or any browser (4).

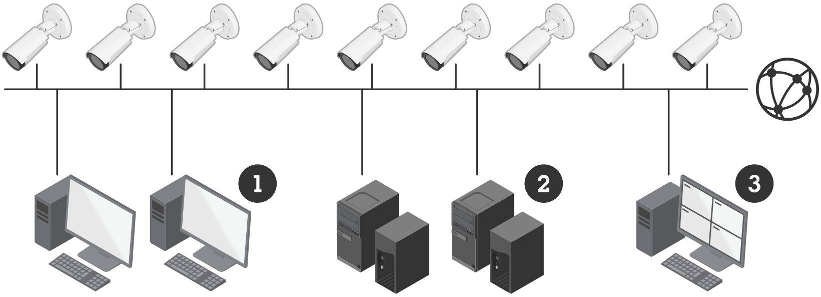
On-prem solution. In a typical on-prem installation, a server is used to handle storage, management, and maintenance of the system, while viewing and operation of video and event notifications are managed from a client. The storage is usually RAID-configured to increase performance and reliability. Analytics can be edge-based but also server-based.



An on-prem solution with a server (1), optional RAID storage (2), and a workstation client.

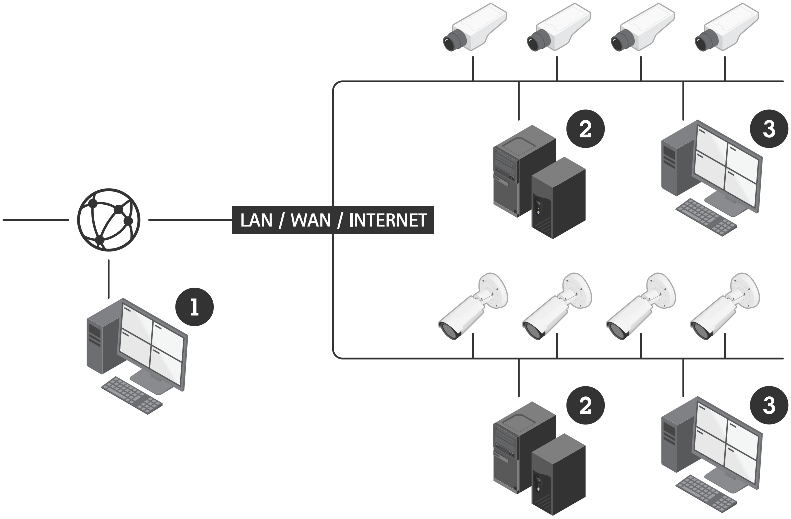
Large centralized system. A large installation requires high performance and reliability to manage the large amounts of data and bandwidth. This requires multiple servers with dedicated tasks. A main server controls the system and decides what kind of video is stored on which storage server.

As there are dedicated storage servers, it is also possible to perform load balancing. The setup makes it possible to scale up the system by adding more storage servers when needed and to perform maintenance without bringing down the entire system.



A large centralized system with main servers (1), storage servers (2), and a surveillance workstation (3).

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



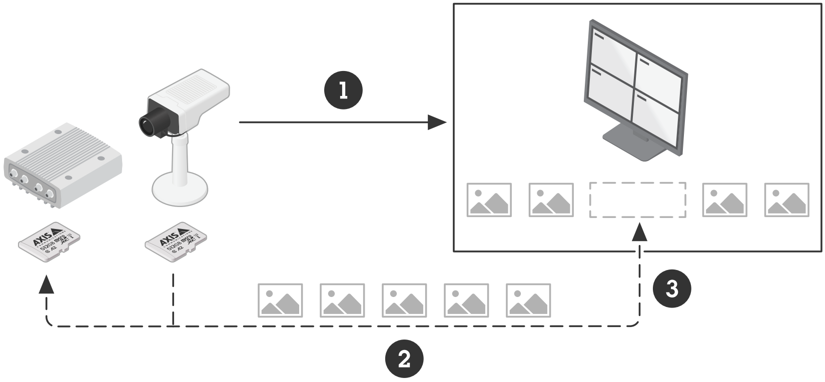
A large distributed system with surveillance workstations (1, 3) and storage servers with RAID (2).

18.4.5 Edge storage

Edge storage, sometimes referred to as local storage or onboard recording, allows cameras and video encoders to create, control, and manage recordings locally on an SD (Secure Digital) memory card, network-attached storage (NAS), or on a file server. Edge storage can be used as the main storage in a hybrid cloud solution.

Edge storage facilitates the design of flexible and reliable recording solutions. Advantages include increased system reliability, high-quality video in low bandwidth installations, recording for remote and mobile surveillance, and integration with video management software. Using SD cards as the sole type of recording medium makes for a very cost-efficient solution.

Edge storage can work as a complement to central storage. It can record video locally when the central system is not available, or it can record continuously in parallel. When used with video management software such as AXIS Camera Station, failover recordings can be stored. This means that missing video clips from network disruptions or central system maintenance can be retrieved later from the camera and merged with the central storage, ensuring that video recordings are uninterrupted.



Edge storage for redundancy (failover recording).

1 *During normal operation, the camera transmits video to the VMS for storage.*

2 *In case of network failure, video clips are temporarily stored on the SD card in the camera.*

3 *When the network is up again, the VMS retrieves the missing video clips and merges them with the recording.*

Additionally, edge storage can improve video forensics for systems with low network bandwidth where video cannot be streamed at the highest quality. By employing low bandwidth monitoring with high-quality local recordings, users can optimize bandwidth limitations and still retrieve high-quality video from incidents for detailed investigation.

Edge storage can also be used to manage recordings in remote locations and other installations where there is intermittent or no network availability. On trains and other track-bound vehicles, edge storage can be used to first record video onboard and then transfer video to the central system when the vehicle stops at a depot.

Axis offers surveillance-grade cards, that is, SD cards specially developed for optimal performance in video surveillance. These are industrial grade cards and thus resilient to the impact of extreme temperatures and environments. They also have improved endurance, to match the typical writing behavior of a surveillance camera. This means that they can be written and overwritten many more times than an ordinary SD card. Thus, the same card can be used for longer without wearing out.

With surveillance cards, video is recorded in a way that makes optimal use of each memory block. This not only saves memory but also keeps down the number of write/erase cycles, effectively increasing the lifespan of the card.

Edge storage with SD cards or NAS. The following pros and cons of using SD cards or NAS for edge storage need to be considered:

- SD cards are easier to deploy and configure than NAS.
- SD cards can be tampered with if physically accessible. NAS can be placed in a secure location.
- SD cards are resilient to single-point-of-failure. If the NAS or its connection is disrupted, multiple cameras will be affected.
- NAS can have RAID configuration.
- SD cards may be costly to replace if the camera is mounted in hard-to-reach places, such as on a pole or wall more than 4.5 m (15 ft.) off the ground.

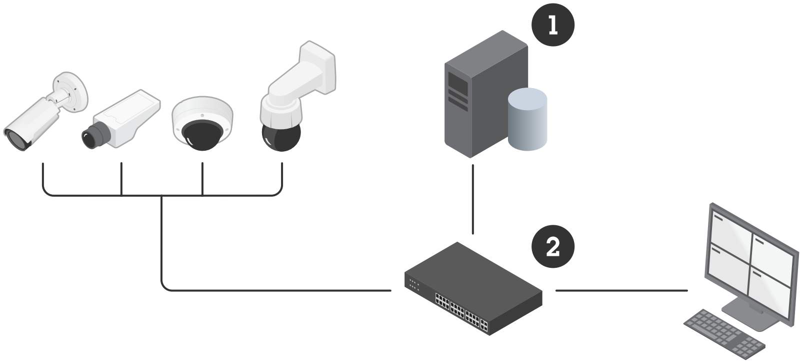
18.4.6 Server-based storage

Server-based storage involves a server connected locally to the network video devices for video management and recording. The server runs video management software that records video either to the local hard disk (direct-attached storage) or to NAS. Depending on the server's central processing unit (CPU), network card, and internal RAM (Random Access Memory), it will be able to handle a certain number of cameras, frames per second, and image sizes. Most servers can hold several hard disks.

18.4.7 NAS and SAN

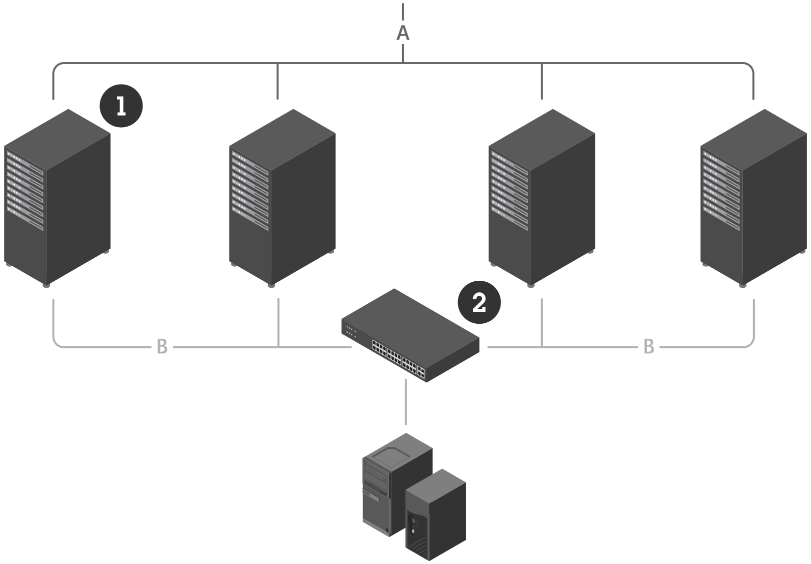
When the amount of stored data and management requirements exceed the limitations of direct-attached storage, network-attached storage or storage area network (SAN) allows for increased storage space, flexibility and recoverability.

NAS provides a single storage device that is directly attached to a LAN and offers shared storage to clients on the network. A NAS device is simple to install and easy to administer, providing a low-cost storage solution.



Network-attached storage (1) is connected to a network video system through the network switch (2), a broadband router, or a corporate firewall.

A SAN is a high-speed, special-purpose network for storage devices. It is connected to one or more servers via a fiber channel. Users can access any of the storage devices in the SAN through the servers, and 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 transfer at up to 16 Gbit/s and to allow large amounts of data to be stored with a high level of redundancy.



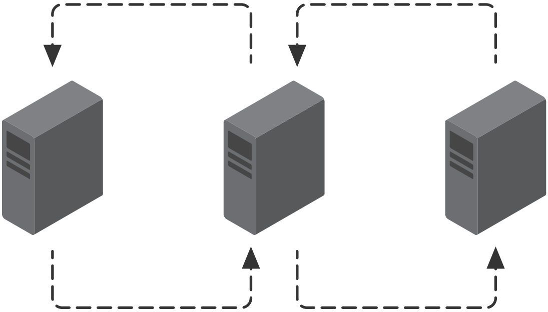
A SAN architecture where storage devices are tied together and share the storage capacity. Users can access any of the storage devices through the servers (1) and a fiber channel switch (2).
A. TCP/IP LAN
B. Fiber channel

18.4.8 Redundancy storage

Redundancy in a storage system allows video or 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 several options for providing this added storage layer in an IP surveillance system, including a redundant array of independent disks (RAID), data replication, server clustering, multiple video recipients, cloud redundancy storage, and SD cards.

RAID. RAID is a method of arranging standard, off-the-shelf hard drives such that the operating system sees them as a single 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.

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



Data replication.

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.

SD card. Edge storage using SD cards can work as a complement to central storage. It can record video locally when the central system is not available, or it can record continuously in parallel. When used together with a VMS, failover recordings can be handled. This means that missing video clips from network disruptions or central system maintenance can be retrieved later from the camera and merged with the central storage, ensuring that video recordings are uninterrupted.

Cloud storage. Cloud storage is data is stored on remote systems, where it is managed and available to users over a network. Cloud storage can be offered commercially by a third party provider, in which case users usually pay a subscription. Private cloud storage is managed (and usually owned) by the user organization, for example, when there are elevated security requirements. Hybrid solutions are useful when an organization needs to separate different types of stored data, or when they need to extend their storage.

19. Tools and resources

Axis offers a variety of tools and information resources to help design IP surveillance systems. We have tools that help you find and compare products, plan and design sites, install and manage systems, and add downloads and plugins. Many tools are accessible from *www.axis.com/tools*. This chapter lists some of our most used tools.

19.1 Find and compare products

Product selector. This tool helps you select the right cameras, speakers, intercoms, and other network devices for your project based on the features and functionalities you need.

Accessory selector. This tool helps you pick the right mount, housing, bracket, and power accessory for the cameras in your project.

Lens calculator. Use the lens calculator to view available lenses for a specific camera and easily establish the optimal camera placement and required focal length for a particular scene size and resolution.

Camera selector for AXIS People Counter. This tool helps you find camera models that are pre-calibrated to achieve the best accuracy for people-counting analytics.

19.2 Plan and design sites

AXIS Site Designer. Use AXIS Site Designer to streamline surveillance system design through installation workflows. Whether you need to create a system with thousands of Axis devices or just a few, AXIS Site Designer lets you design, approve, and install surveillance systems that fit your exact operational requirements and needs. Intuitive product selectors make it easy to identify the ideal cameras and devices for each situation and choose the mounts and accessories to match them and their placement. System storage and bandwidth can also be effectively estimated.

AXIS Site Designer can be used to design surveillance systems featuring Axis end-to-end products as well as products from selected third-party VMS partners for larger systems.

AXIS Plugin for Autodesk® Revit®. Select and place interactive Axis products directly in your Autodesk Revit building plan and incorporate surveillance into your design. The plugin includes an embedded product selector and lets you verify coverage and adjust settings to match the scene.

19.3 Install and manage systems

AXIS Device Manager. Enables efficient managing of installation, security, and maintenance of major devices. Key functions include assigning IP addresses, managing device lists, managing users and passwords, upgrading device software, renewing and managing certificates, and deploying cybersecurity controls to protect your network devices and align them with security infrastructure.

AXIS Device Manager Edge. Provides a site-by-site overview, allowing you to remotely monitor device connectivity status and perform simple management tasks. It offers an instant status overview of all devices in the system, enabling automatic upgrades and secure remote access. This allows for easy application and maintenance of safeguards throughout a device's lifecycle.

AXIS Device Manager Extend. Ideal for multi-site operations, AXIS Device Manager Extend offers a unified, user-friendly interface that helps you proactively manage your Axis devices and sites from anywhere.

20. Axis Communications Academy

20.1 Building expertise for smarter business

At Axis Communications, we understand that your business success depends on continually building your strengths and staying on top of the latest solutions and technologies to offer your customers the very best.

We have designed Axis Communications Academy to work with every facet of your business, providing training on everything your customers expect you to be an expert in, as well as the things they don't even know they need yet.

Keeping up on the latest about Axis solutions, technology, industry trends, and sector-specific issues lets you provide your customers with expert competence. From sales and business and system design to installation and configuration.

Choose from a range of learning formats – in-person or online – to suit your learning style, preferences, and needs.

- Educational videos
- Educational articles
- Interactive apps
- eLearning
- Virtual instructor-led training
- Classroom instructor-led training
- Blended learning (mix of formats)
- Webinars

Axis Certification Program

Gain a competitive advantage by validating your network video knowledge with global industry-recognized credentials.

For more information, visit Axis Communications Academy at *www.axis.com/academy*

T10121303/EN/M12.10/2506

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.aboutaxis_text

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.