

## 7. Video Management

Network cameras are only ever as good as the selection and configuration of the video management systems that control them. Systems should enable users to monitor, analyse and store video output effectively. The chapter compares a 'PC Server platform' approach with an 'NVR platform' approach using a dedicated device such as a Network Video Recorder (NVR) for managing network video output. This chapter also covers options for building event management, motion detection and audio capability into systems.

Systems based on an network video platform are suitable for integration to other systems such as access control or building management, and the information from those systems can be used to trigger functions in the network video system, for example to store images related to events.

### 7.1. Hardware platforms

There are two different types of platforms for network video management: PC Server platforms and NVR platforms (Network Video Recorder). Both types are based on PCs but there are some noticeable differences.

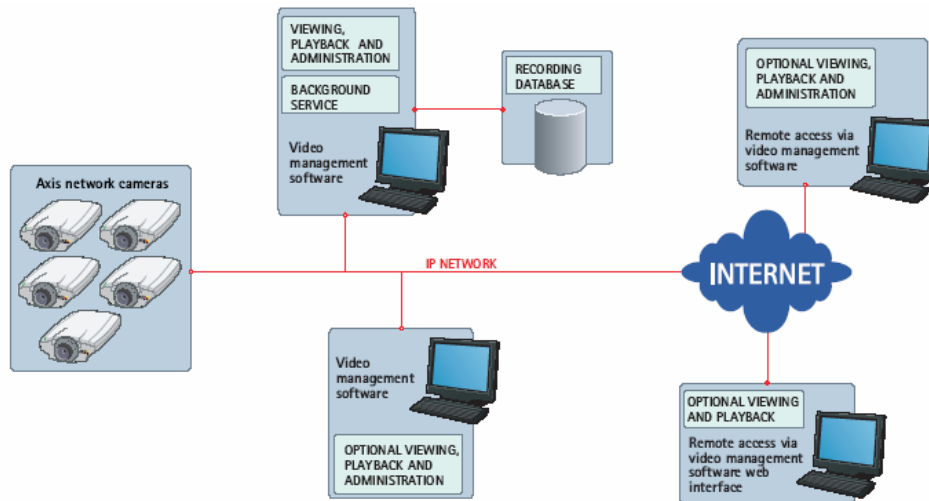
A PC Server platform solution on the other hand runs on 'off the shelf' hardware where hardware components have been selected to obtain the maximum performance. With a PC Server platform solution it is possible to leverage on standard components, such as increased or external storage, additional remote operator stations and to run additional software in parallel to the video application, such as firewalls and virus protection.

The most obvious difference between an NVR platform and a PC Server platform type solution is that an NVR comes as a hardware box with the video management functionality pre-installed. By definition, it is dedicated to its specific tasks of recording, analyzing and playing back of network video. NVRs do not allow for any other applications to reside on them. The NVR hardware itself is 'locked' to this application and the unit can very rarely be altered to accommodate anything outside its original specification.

Systems designed on a network platform are fully scalable. Cameras and licenses can be added one by one and the system hardware can be expanded to meet increased performance requirements. This platform is suitable for system scenarios where a large number of cameras are deployed or when the IT department has standard specifications on the server hardware and software allowed on the network.

#### 7.1.1. PC Server platforms

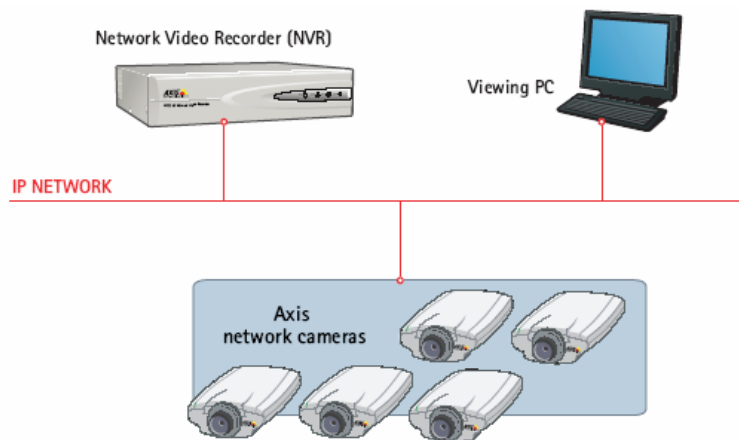
A PC Server platform solution, as mentioned above, runs on off-the-shelf hardware, where hardware components have been selected to achieve the maximum performance for the specific design of the system, such as detached storage or dual processor systems.



As the PC Server platform system is based on standard hardware components it is possible to still use the end user's preferred choice of hardware as well as their existing suppliers of IT equipment and maintenance services.

### 7.1.2. NVR platforms

An NVR has some similarities to a Digital Video Recorder (DVR) in relation to recording and playback. A DVR is in fact a hybrid system that can accommodate analog cameras and store the video on a hard disk in digital format. An NVR is a true digital system that receives digital images/video streams over the network and records them on a hard disk in a digital format. Some DVRs have a rudimentary interface to the network that offers remote viewing capabilities. An NVR does not have a dedicated monitor and keyboard. All viewing and management of the NVR takes place remotely over the network via a PC.



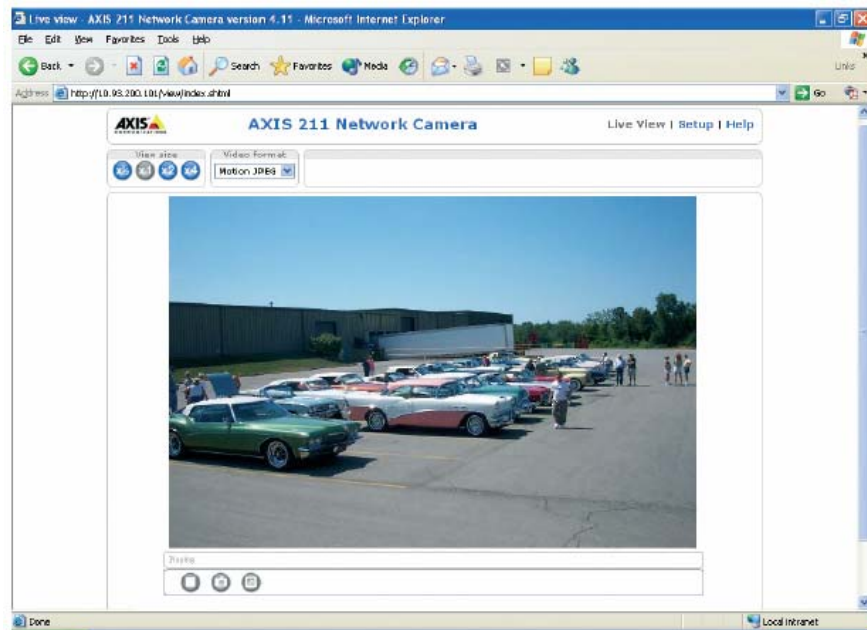
An NVR is designed to offer optimal performance for up to a set number of cameras, which makes it less scalable than a PC Server platform system. This makes the unit suitable for smaller system configurations where the number of cameras stays within the limits of the NVR design capacity. An advantage is that an NVR is less complex to install in comparison to a PC Server platform.

## 7.2. Monitoring and recording

Video management of a network video system includes video monitoring, which can be conducted from a web browser or specific video management software, and video recording, which can be conducted from video management software installed on a PC or using a Network Video Recorder.

### 7.2.1. Monitoring using the web interface

In a network video system, video can be viewed from any point on the network provided there is access to a web browser. Each camera has a built-in web server with an IP address, so to view the images on a PC, one simply opens a web browser and types in the camera's IP address in the Address/Location field:



Once the computer has established the connection, the network camera's 'start page' is automatically displayed in the web browser. This start page will display live video feeds from the camera along with hyperlinks for changing the camera set-up, such as image resolution, network and e-mail settings – unless the system is set up with security/password limitations.

### 7.2.2. Monitoring using video management software

Even though video can be viewed directly from a standard web browser, video management software can be installed if more flexible viewing options, as well as the ability to store and manage video, are required. A wide variety of software solutions exist on the market, which range from independent solutions for a single PC, to advanced client/server-based software providing support for multiple simultaneous users. Common functionality includes video monitoring, event management functions and alerts to alarm events via siren or e-mail for instance.

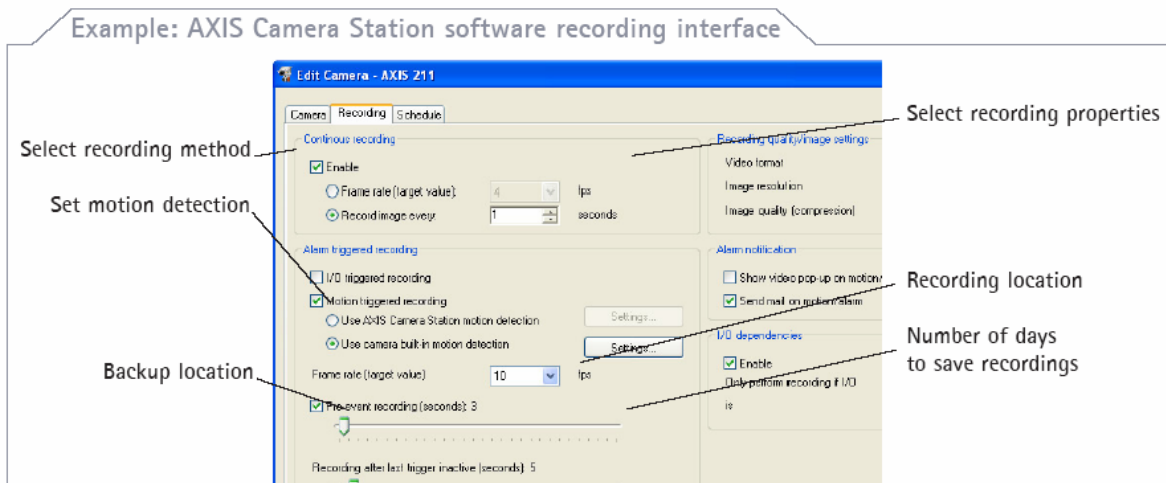


### 7.2.3. Recording network video

There are several ways to record network video:

For simple recordings, the network camera's built-in functionality can be used to record images or video, based on scheduled or triggered events. These images are then uploaded to an FTP server or to the hard drive of a computer.

For advanced recording and event management, video management software serves as the core of professional video surveillance systems. The software is installed on a PC and can be an independent solution or a client/server-based application for multiple simultaneous users. From the software interface, operators can, for example, record video continuously, on schedule, on alarm and/or on motion detection or search for recorded events.



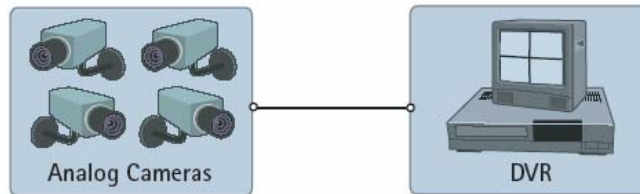
## 7.3. System features

### 7.3.1. Video motion detection (VMD)

Video Motion detection (VMD) is a way of defining activity in a scene by analyzing image data and differences in series of images.

### **VMD in DVR systems**

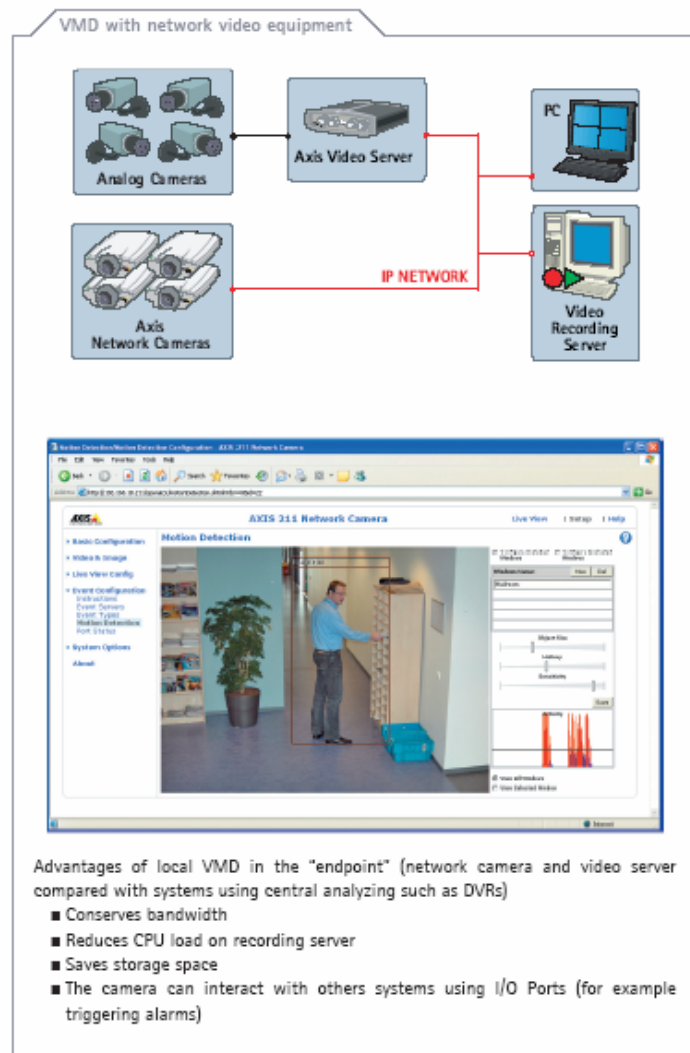
Cameras are connected to the DVR, which performs the VMD on each video stream. This allows the DVR to decrease the amount of recorded video, to prioritize recordings and to use motion in a specific area of the image as a search term when searching for events. The downside of this method is that performing VMD is a CPU intensive process and performing VMD on many channels puts a heavy strain on the DVR system.



### **VMD in network video systems**

VMD as an integrated function of network cameras or video servers offers substantial advantages over the scenario mentioned above – the most significant being that the VMD is processed in the network camera or video server itself. This alleviates the workload for any recording devices in the system and makes “event-driven surveillance” possible. In that case, no video (or only video with low frame rate) is sent to the operator or recording system unless activity is detected in the scene.

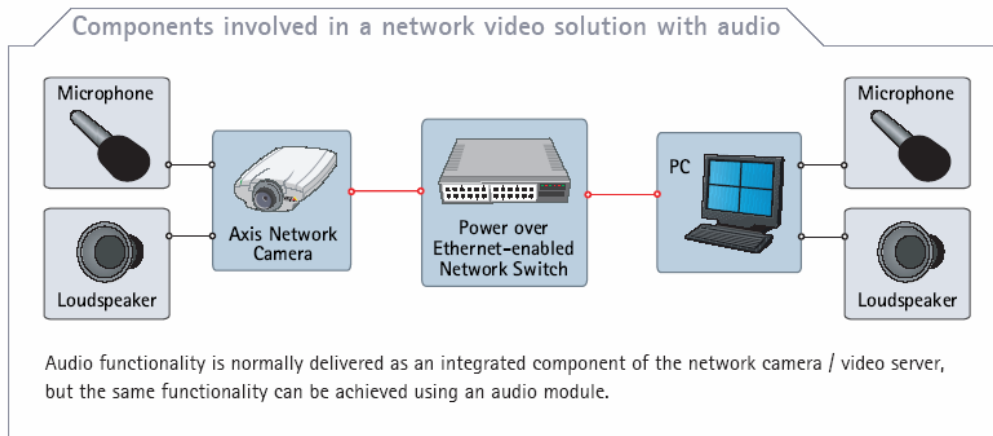
VMD data with information about the activity can also be included in the video stream to simplify activity searches in recorded material. VMD can also reside in the video management software, thus providing VMD functionality to network cameras that do not originally embed this feature.



### 7.3.2. Audio

Audio can easily be integrated into network video as the network can carry any type of data, which reduces the need for extra cabling - as opposed to analog systems where an audio cable must be installed from endpoint to endpoint. A network camera captures audio at the camera, integrating it into the video stream, and then sending it back for monitoring and/or recording over the network.

This makes it possible to use audio from VMD remote locations. For instance, monitoring personnel at a company's headquarters can interact with "surveillance scenes" at remote branch offices. They can inform possible perpetrators that they are under surveillance and listen in on situations using the audio as an additional confirmation method. Audio can also be used in network cameras or video servers as an independent detection method, which triggers video recordings and alarms when audio levels above a certain threshold are detected.



### Audio transmission

Audio can be compressed and transmitted as an integrated part of the video stream, if MPEG-1/ MPEG-2/MPEG-4 or any of the H.x video conferencing standards are used. It can also be transmitted in parallel if using a still image standard, such as JPEG. However if synchronized audio and video is prioritized, MPEG is the preferred choice. Nonetheless, there are many situations where synchronized audio is less important or even undesirable (for example if audio is to be monitored but not recorded).

### Audio compression

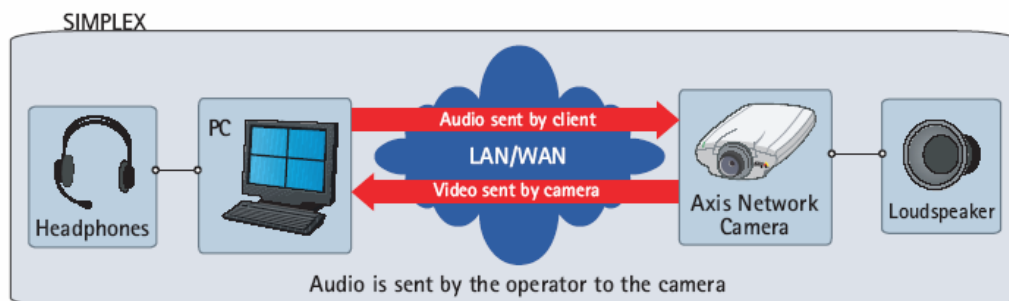
Digital audio compression allows for efficient transmission and storage of audio data. As with video, there are many audio compression techniques, which offer different levels of compressed audio quality. In general, higher compression levels introduce more latency. Audio in digital form offers many advantages, for example high noise immunity, stability, and reproducibility. It also allows for efficient implementation of many audio post-processing functions, such as noise filtering and equalization.

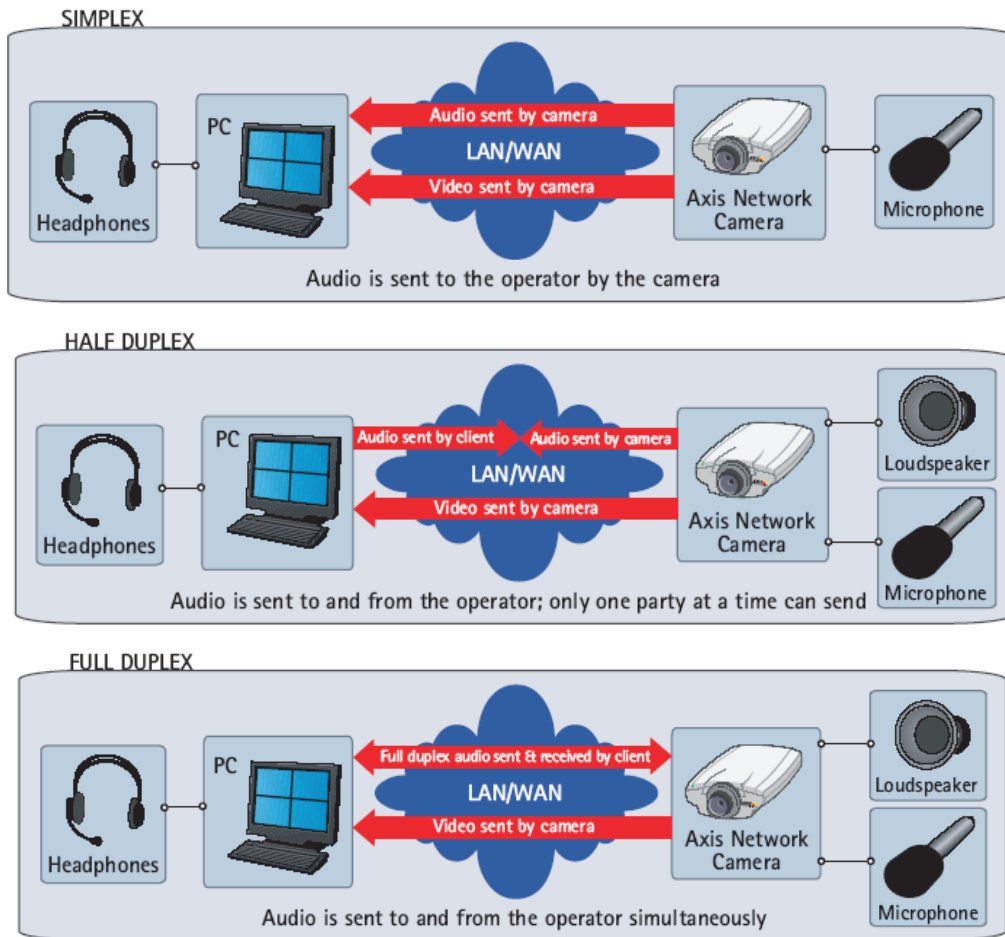
Popular audio compression formats include:

- G.711 PCM providing high quality audio at 64kbit/s bit rate
- G.726 ADPCM providing audio at 32 or 24kbit/s bit rate
- MP3 (which stands for ISO-MPEG Audio Layer-3), a popular format geared towards music, with bit rates around 100 kbit/s
- Standard MPEG-4 audio using AAC LC compression (Advanced Audio Coding Low Complexity profile), 16 kHz sampling with a bit rate of 40 kbit/s.

### Audio modes

When using Axis network cameras, there are several audio modes to choose from:

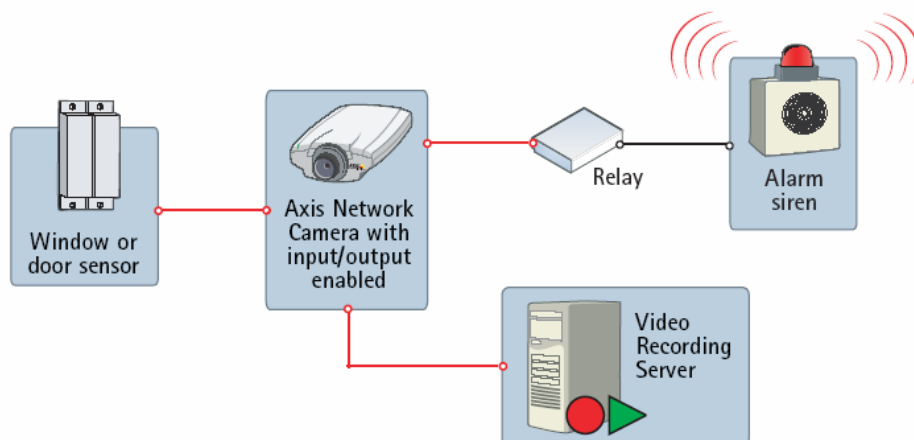




### 7.3.3. Digital inputs and outputs (I/O)

A unique feature of network video products, is their integrated digital inputs and outputs that are manageable over the network. The output can be used to trigger mechanisms either from a remote PC or automatically, using the camera's built-in logic, while inputs can be configured to respond to external sensors such as PIRs or push button initiating video transfers.

The I/Os can be used in conjunction with alarm sensors for instance, to eliminate unnecessary transfers of video, unless the sensor attached to the camera triggers.



*I/O usage example - A camera attached to a window switch and to an alarm system/siren*

## Digital inputs

The range of devices that can be connected to a network camera's input port is almost infinite. The basic rule is that any device that can toggle between an open and closed circuit can be connected to a network camera or a video server.

### Examples of alarm devices and their usage

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

## Digital outputs

The output port's main function is to allow the camera to trigger external devices, either automatically or by remote control from a human operator or a software application.

### Example of devices that can be connected to the output port

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

## 7.4. Integrated systems

In a network video system, all devices are connected to an IP network – enabling the use of a cost-efficient infrastructure to transport video for recording or monitoring. It also enables integration with other systems for increased functionality and easier operation. Examples of systems which can be integrated include:

- Access control: Using a video surveillance system with integrated access control systems, means for example that video can be captured at all doors when someone enters or exits a facility. Additionally all pictures in the badging system can be accessible to the operator of the video surveillance system, for quick identification of employees or visitors.
- Building management systems (BMS): Video can be integrated into building management systems, like heating, ventilation, and air conditioning systems (HVAC). The I/O ports of the

network cameras can be used to provide input to the system, or the cameras used to detect motion in meeting rooms for instance, and control heating or lights to save energy.

■ Industrial control systems: A visual verification is often required in complex industrial automation systems. Instead of the operator having to leave the control panel to visually check a part of the process, he or she can view network video using the same interface. Also in some sensitive clean room processes, or in facilities with dangerous chemicals, video surveillance is the only way to have visual access to the process. The same goes for electrical grid systems with a substation in a very remote location.