AXIS COMMUNICATIONS

WHITE PAPER

TECHNOLOGY AND APPLICATIONS

Network Video – A New Installation

TABLE OF CONTENTS

1 Introduction - Network video system

This document will provide the necessary information to understand and design a truly digital, network based video installation, which we will refer to as a network video system. It will cover the user benefits derived from a digital solution, factors to consider when implementing such a system, and components that make up a top-functioning digital system.

A network video system utilizes standard LAN/MAN/WAN/Internet as the backbone for transporting information, rather than dedicated point-to-point cabling, which is used in analog video systems. Many businesses already use their computer networks for a vast array of functions. Network video technology utilizes and extends this same infrastructure for local and remote monitoring.

This white paper will provide a general introduction to the composition, operation and benefits of a truly digital video system. This system is one where the transmission of video, audio and data takes place without the presence of a dedicated physical infrastructure connecting the camera to the monitor. The growth of network video for surveillance and monitoring is driven not only by a general increase in the need for security, but also by its many performance and cost advantages, including flexibility in access to information, ease in distribution of images, capacity for integration, scalability, and more. In section 7, a list of Axis' white papers referred to in this white paper, can be found.

2 Benefits and installing a system

The end user gains a wide variety of benefits by implementing a digital video system. Below is a listing and explanation of a number of those key user benefits:

2.1 Flexibility in access of information

Ordinary analog CCTV installations operate on a point-to-point mode, requiring dedicated cabling from each camera. Viewing can only be done from designated monitors and operator keyboards connected to the system. With a networked security installation, video can normally be viewed from any point on the network locally, as well as remotely from around the world. Access to the video information is controlled through user names and passwords, rather than restricting physical access to a monitor and/or operator keyboard. As long as you can connect to the network, there's an excellent possibility to view and manage the information coming from the cameras. Improved access over an intranet (e.g. LAN) or the Internet provides more immediate access to images while substantially reducing travel costs to-and-from the monitored site locations. In addition, images can automatically be stored at off-site locations for convenience and/or for enhanced security.

2.2 Ease in distribution of visual information

One of the biggest problems with analog systems is the lack of an efficient means to distribute information. Information is usually available only as videotape or a printed picture. Both these modes require physical transportation, i.e. airmail, courier, etc., to get the information from one place to another. In the digital video environment, all information is treated as data files, containing either video sequences or images. A data file can easily be sent as e-mail to an unlimited number of recipients, or it can be posted on an internal web-server in seconds. This distribution of visual information can be accomplished without any degradation in image quality.

2.3 Utilize existing infrastructure

Unlike an analog system, which requires all that single-purpose or dedicated cabling to join devices point-to-point, the digital video system requires only limited cabling during installation. The digital system utilizes a normal IP-based network for transmitting and distributing video, thus eliminating the need for costly, time-consuming dedicated cable installation.

2.4 Integration and future-proof functionality

Network video technology has the capacity to provide a higher level of integration with other functions and services, making it a continually developing system. Use of open standard protocols and networks for communication enables easy system integration with equipment from a wide range of manufacturers. Changing over to digital technology means investing in a system that will last well into the future.

2.5 Scalability

A digital system is flexible and fully scalable in meeting a user's exact needs. Digital is designed to provide plug and play functionality for small installations or larger, more professional applications. Unlike most analog systems, a network video system can be expanded without the need for major rework or replacing various system components.

2.6 Total Cost of Ownership (TCO)

A network camera at this time is normally more expensive when compared to an "equal" analog video camera. But an analysis of the total system investment tends to be favourable to a digital video solution, when all factors are considered. Network video can leverage investments in the existing computer structure, network, and monitors. Installation costs are generally cheaper given that network cabling is cheaper than coax cabling. In addition, on-going maintenance costs are reduced by eliminating tapes and the need for VCR replacement and repair. Another factor that positively impacts TCO is found on the operational side. A digital system's powerful tools to search, locate, and distribute interesting video increases operator efficiency and efficacy. When all these operation and maintenance factors are added to the equation, the cost analysis is even more beneficial for the digital solution, especially if recording of video is required.

3 Building and installing a system

To design a successful, high-performance network video system, there are multiple factors that need to be considered before installing a digital system. These include items that can be controlled through system design, as well as external factors like networking performance, environment, and others, which the designer must consider and adequately compensate for.

3.1 Networking factors

Since digital video systems utilize computer networks as a transportation medium for content, network design can and will affect the overall performance of the video system, as well as the overall performance of the network. A large majority of new networks being installed these days are Ethernet-based, and are layed out in a star structure with a communication backbone between the different switches. Some of these networks may be a local network within a building, while others may be several different local networks, all routed together to a corporate network. The following sections will explain, from a network standpoint, the different network factors that may affect the performance of a digital video system.

3.1.1 Structure of the network

The actual structure of the network can be a limiting factor. Network structure or shape refers to how different nodes in the network are connected to each other and how they communicate. For our purposes, bus and star are the most relevant structures. In the bus network all devices are connected to a central cable, called the bus or backbone. In the star structure, all devices are connected to a central hub.

When comparing Ethernet (bus) and analog CCTV (star) network structures there are a number of major differences. Ethernet networks allow for considerably shorter total cable distances with several devices sharing the same cabling (the bus). While in the star structure, each device needs a separate cable to the central point. An Ethernet network allows the user to share cabling among several systems—security and non-security systems alike. The Ethernet bus structure has no central point in the system, making it significantly more fault tolerant than a star structure and the cabling is flexible and easier to expand. In nearly all enterprises, Ethernet cabling is already in place and well documented, and this existing cabling infrastructure can also be utilized for security and surveillance applications. An Ethernet network provides easy integration with intranets or the Internet, allowing controlled and supervised remote access to cameras and the wealth of data and information they provide, while also enabling the user to do all recording locally or from a remote location over, for example,. a secure Virtual Private Network (VPN). For our purposes, the Ethernet network represented by the bus structure is superior to the current CCTV star network structure.

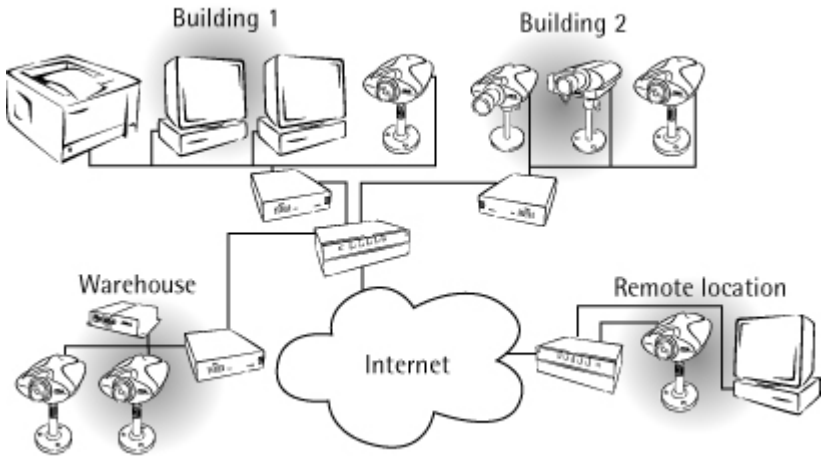


Figure 3: *An example of a network video system.*

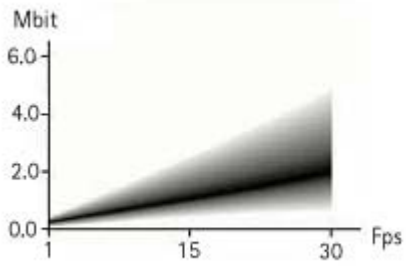
3.1.2 Network capacity

Depending on system configuration, video can consume large amounts of network bandwidth. Therefore, it is important to fully understand the performance of the current network—where bottlenecks are today and where new bottlenecks can occur if a digital video system is installed. This is normally done by the IT manager, or at least in co-operation with the IT department.

A network can consist of segments with different bandwidths. A single point connection to a hub or switcher may be a 10Mbps or 100Mbps connection, while the backbone communicating between the two switchers may be a 1Gbps or even 10Gbps connection. In this situation, the best solution is to create a plan to define available bandwidth (minimum available bandwidth and maximum usage) for the application. This will guarantee the level of performance that is needed to be able to operate a security system, and at the same time prevent consumption over capacity and the resultant decrease in performance of other systems operating on the same network.

It is difficult to define the exact bandwidth usage of a camera, as it will depend on several factors such as:

- Image size
- Compression
- Frame rate (images per second)
- Resolution (complexity) of the image



Regarding bandwidth management, it is important to understand that Axis network video products (based on M-JPEG compression) will utilize bandwidth based on their configuration. A high-resolution picture (4CIF) contains four times as much data as a normal resolution picture (CIF). A reduction of the frame rate to half (for example, 25 frames per second

down to 12.5), will reduce the amount of data by half as well. The figure pictured here provides further guidance on bandwidth management.

For more information about compression and digital video systems, please read Axis White Paper, "Video Compression" (Section 7, Reference: Axis White Papers).

3.1.3 Network design solutions

Now, we turn to different design elements that can also affect network performance and management. In the left-hand figure below, we see a solution that is vulnerable due to several points of potential congestion in data traffic. In this set-up, all cameras are sent from hub #1 to hub #2 over a single link. This link must have a high capacity so as not to risk potential bandwidth problems. Furthermore, if for any reason this link goes down, no video will be accessible until the problem is fixed.

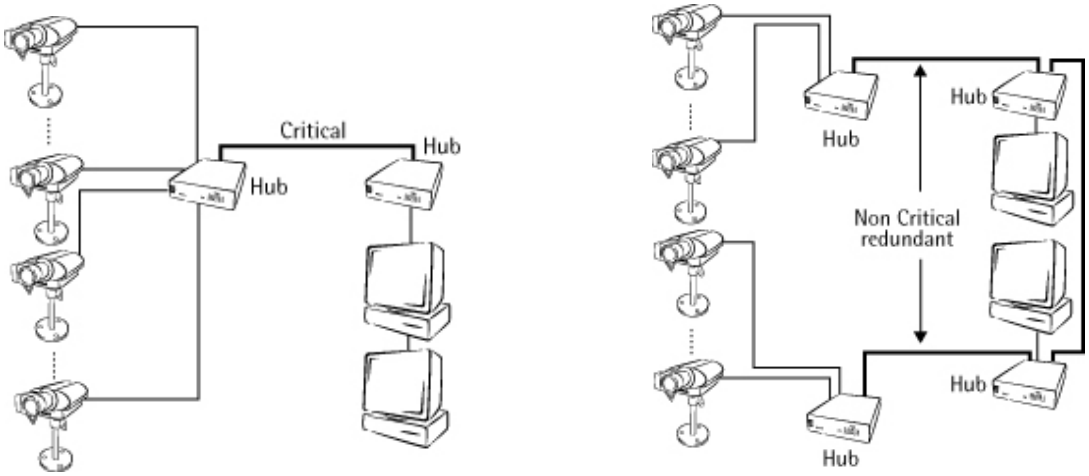


Figure 4: *Two different network lay out concepts.*

In our figure on the right, the vulnerabilities we saw on the left are properly managed and minimized by implementing two more hubs/switches and creating a second link between the cameras and the monitoring areas. There are two distinct advantages to this set-up: first, this can potentially improve bandwidth and eliminate the risk of congestion. Secondly, it creates a redundant system, so even if one of the links goes down, the user will have access to some or all of the cameras. By designing the system wisely and splitting the number of cameras between different sections or links, the user gains the benefits of higher reliability and improved performance.

3.1.4 Network security

The network provider or administrator, usually the IT department, will have a set of security policies in place for network usage. These policies include items like log-on credentials, back-up procedures, and virus filtering & scanning. Many of these policies can affect system performance. For example, are external connections to non-corporate machines allowed? Such connections will be needed if the organization plans to use external alarm monitoring services. This would raise a host of questions: Will this alarm-monitoring centre have the capability to connect to the local site to do a guard tour, either locally or by remote alarm company?

Will video be stored, and in what manner? Should these stored images be included in general back-up procedures? Is the current back-up system able to handle the additional data? These are just a few examples of questions and policies that would need to be explored to assess how network security procedures can impact system performance.

3.2 External application factors

In addition to the various network-oriented factors covered above, there are several external factors that relate directly to the application of the network video system. These factors are basically the same for a digital video system as they are for an analog video system, but they bear review.

3.2.1 Environment

Are cameras to be used outdoors or in an unclean environment? If so, cameras need to be installed in a suitable housing that protects them from water, dust, humidity, unsuitable temperatures, and other unwanted environmental factors. The housing may also be equipped with heating and/or cooling to provide proper operating temperature.

We must also consider the visual field for the camera. Will the camera have a clear, direct view of the target area at all times? Or could the view be blocked (intentionally or not) by, for example, growing trees, a parked truck or a door left open? Another factor affecting camera location, especially when outdoors, is the direction to the target in relation to any strong light, particularly sunlight. If a camera for example is facing directly towards a rising sun, the picture in many cases will be completely useless. Installing the camera in a different location to view the same scene will improve picture quality dramatically.

3.2.2 Lighting

One of the most important factors to consider when installing a CCTV system is lighting. Is there enough light to provide a high quality picture? Generally, the more light, the better the picture. If light level is too low, images will be blurry and the colors dull. Light level is measured in Lux. Strong sunlight is approximately 100,000 Lux, full daylight is 10,000 Lux, and candlelight is 1 Lux. Usually, at least 200 Lux is required to capture good quality images. If lighting is not sufficient, installing additional lighting may be required. Ensuring adequate lighting can be controlled by external devices like light sensors, detectors sensing movement in the area, etc.

We should also consider if the installation is in a static light environment (i.e. indoors) or in a dynamic environment (typically outdoors), where light levels will vary considerably. To compensate for a dynamic environment's changes in brightness and contrast, the camera should be equipped with a lens that will automatically adjust the iris based on the amount of surrounding light. Bright areas should be avoided because images might become over-exposed and objects will appear too dark. The contrast of colors between object and background influences the exposure. A small dark object should be displayed towards a dark background to achieve correct colors.

3.3 Operating factors

In addition to network and application considerations, there are several factors regarding the operation of our new digital video system that also need to be considered.

3.3.1 Viewing of video

There are two types of systems when it comes to viewing live video. First, there are installations with dedicated security officers constantly watching the video and actively monitoring for incidents and/or objects in the picture. Examples of this type of installation include prisons, city centre surveillance, and airports. The second type of system is one in which the video is viewed only occasionally. These systems are those used, for example, to let someone through an entry door.

A fundamental issue with viewing video is that someone needs to be there to monitor it and take proper action based on what is observed. The real advantage of a network video system is that viewing can be done from anywhere on the network, and from several different locations simultaneously. To provide security and better management of the system, access to video can be restricted by password protection of the cameras. A network video system provides conditions to ensure video can be monitored more easily and more efficiently—creating better results.

3.3.2 Storage of video

In most security situations it is beneficial, or even essential, that video is recorded and stored for later review. Storing video allows the user to review an incident over and over again, isolate pictures or sequences of interesting video, and then distribute them in any manner that is needed for the application. While storage of video provides numerous advantages for security management, we do need to be mindful of limitations to recording and later viewing, based on potential legislation governing recording of images overall and restrictions on recording based on location.

3.3.3 Access to information

In the analog world, security for stored video is accomplished simply by limiting access to recorded videotapes, which are normally kept in a locked cabinet or storage area. With network video, all information is stored as data and if no limitations are put in place, this data can be viewed by anyone with access to the network. Since we're talking about systems that manage the security of an operation, there usually is strong incentive in limiting access to this information. Limiting access can be divided into two categories or reasons for restriction: operational and management issues and legislative issues.

Because video recording in many instances is viewed as a potential infringement on personal privacy, there is strong motivation to limit access to this recorded data or information. Governments or corporations have a strong interest in limiting and controlling video access not only to avoid future problems or questions, but also to gain approval from individuals and organizations (e.g. trade unions, parent groups, etc.) for video recording. Limitations such as these ensure that only security staff has the ability to view and work with the video.

Another aspect for restricting access is on the operational side, and this is to reduce the risk of someone trying to delete or manipulate recorded material. The less access people have to the information, and the fewer people who have access, the better control organizations have in maintaining the integrity of recorded data. In many countries and/or municipalities, specific limitations on access are legally required if the recorded data is to be used as evidence or in any official investigative procedures.

In general, it is only those people who have a real need for the information that should have any access to it at all. To manage such access more effectively, many organizations log access by user, date, and time.

3.3.4 Integration

As video resides on a network, and that network is commonly used for other applications such as access control, intrusion, building management, etc., the foundation for powerful integration combinations and synergies is already present. In the past, integration was normally accomplished either on the relay/input level, or between two PCs using serial RS232 communication. With a network video system, other applications and systems can have direct access to selected cameras or to stored video, without the need for additional hardware or wiring. Using an Open Windows-API (Application Programming Interface), network video technology's capacity to provide a higher level of integration with other functions and services makes it a continually developing, efficient, and future-proof system.

3.3.5 Existing legislation

As mentioned before, another factor that may impact system performance is relevant legislation. A number of countries have stringent regulations protecting individual privacy rights. These laws and regulations can in some cases restrict viewing and/or storage of video. System owner/operators need to be aware of these rules and regulations. In some cases, video storage particularly can be affected. Whereas the actual recording may not be prohibited, the duration video may be kept can be restricted to as little as 24 hours. In other cases, video storage may be allowed for up to 31 days; nevertheless, length of storage is still restricted and will affect the manner in which these systems can be used. Appropriate governmental bodies within each country can provide further information regarding recording and/or storage restrictions.

4 Network video system components

4.1 Cameras

The camera is the core component in all video installations. This device picks up the light and converts it to a recognizable set of pictures, which can then be sent over the network. All cameras generate "still" images that are sent to the viewer at a certain frame rate. The human eye requires approximately 17 images (or frames) per second to perceive the video as "live." The camera itself consists of a chip, which converts the light into electronic signals, and various sub-electronic circuits like the digital signal processor (DSP) and others that are not important for our discussion here. (For more information, please see Section 7, Axis White papers, "The Network Camera")

As we've briefly mentioned above, analog cameras have been the standard for many years. Increasingly, we see more network cameras being installed. Network cameras provide all the functionality of analog cameras and more, as we'll review below.

4.1.1 Fixed network camera

A fixed network camera provides a static picture from the area in front of the camera. In addition to the camera unit, a lens is needed for the camera to operate correctly. The lens adjusts the amount of light entering the camera, similar to a normal photo camera. The lens also focuses the image onto the image sensor (CCD). Before reaching the image sensor, the images pass through the optical filter, which removes any infrared light so that the "correct" colors will be displayed. The image sensor converts the image, which is composed of light information, into electrical signals. These electrical, digital signals are now in a format that can be compressed and transferred over a network.

Network cameras provide the end user with many benefits including, greater functionality over analog cameras at a lower TCO; network cameras plug directly into the existing network so the coaxial cabling required for analog cameras isn't needed and installation costs are minimal; when computers are already in place, no additional equipment is needed to view network camera output; and output can be viewed in its simplest form in a Web browser over a computer monitor and in more complex security solutions with the aid of dedicated software.

4.1.2 Network Pan Tilt Zoom (PTZ) Camera

A networked PTZ camera basically combines into one product a fixed network camera, a zoom lens, a device that allows a remote user to move the camera around to change its field of vision, and a network interface. The camera can be moved either manually or automatically. In some cases one might use external lenses and so-called pan tilt units.

4.1.3 Software

Even though video can be viewed directly from a normal web browser without the need for dedicated software, it is strongly recommended to use a software application in combination with the cameras. This software can provide the user with more flexible viewing options as well as the ability to store and manage the video. The software can be a stand-alone solution for a single PC or a more advanced client/server-based application providing support for multiple simultaneous users. In some cases, the end user might select software to implement support for multiple systems like video and access control. Selecting a suitable software package to match the application and system goals is one of the keys to designing a useful and successful system.

4.2 Other components

In addition to the core components described above, there are accessories to the network video system that, in most cases, are useful for other applications and systems on the network as well. These items include printers, Network storage, CD/DVD-RW units, mail servers and others, all of which can add substantial value to the installation.

5 A network video system in action

After evaluating the existing network structure, installation environment, and components of a network video system, let's review what type of functionality is available from the system. This depends greatly on what type of business the installation is to secure. The needs in a retail environment will be fundamentally different from the monitoring of a parking lot, and both differ considerably from the needs in a casino environment.

Network video technology is proving to be attractive in a vast array of wide-ranging applications. This revolutionary technology is replacing traditional style systems to reduce costs, while in other markets it is being used for the first time to create and stimulate new and exciting markets. To date, the technology has been successfully deployed in the following markets: **Education,** for security and remote monitoring of school playground areas, corridors, halls and classrooms; **Transportation,** remote monitoring of railway stations, highways and airports; **Banking,** traditional security applications in high street banks, branch offices and anywhere ATMs are located; **Government,** within security surveillance applications, often integrated into existing and new access control systems; **Retail,** for security and remote monitoring purposes to make store management easier and more efficient; and **Industry**, for monitoring automobile manufacturing processes, parcels, and mail handling, warehouse and stock control systems.

6 Conclusions

In this white paper, the reader has been given a general introduction to the composition of a fully digital, network-based system for CCTV recording. This paper also covered the key elements and benefits of digital video recording.

A true and complete digital system is able to transmit video, audio and data without the need for a dedicated physical infrastructure connecting the camera to the monitor. Network video solutions provide impressive end-user benefits, and are quickly taking over the high-end range of the security and surveillance market. Soon, this technology will penetrate low and mid-range market segments as awareness grows, costs come down, and users implement more sophisticated cost-benefit analyses. The future for digital, network video systems has only just begun and is bright indeed.

7 Reference: Axis White papers

The Network Camera, 2002
Network Basics, 2003

To order these white papers, please send an email to info@axis.com

8 About Axis

Axis increases the value of network solutions. The company is an innovative market leader in network video and print servers. Axis' products and solutions are focused on applications such as security surveillance, remote monitoring and document management. The products are based on in-house developed chip technology, which is also sold to third parties.

Axis was founded in 1984 and is listed on the Stockholmsbörsen (XSSE:AXIS). Axis operates globally with offices in 14 countries and in cooperation with distributors, system integrators and OEM partners in 70 countries. Markets outside Sweden account for more than 95 % of sales.

Information about Axis can be found at: www.axis.com

Contact Axis
info@axis.com

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

Subsidiaries

BOSTON: Phone: +1 978 614 20 00	SHANGHAI: Phone: +86 21 6431 1690
LONDON: Phone: +44 870 162 0047	SINGAPORE: Phone: +65 6 836 2777
MIAMI: Phone: +1 305-860-8556	MELBOURNE: Phone: +613 9225 5244
MADRID: Phone: +34 91 803 46 43	TORINO Phone: +39 011 841 321
MUNICH: Phone: +49 811 555 08 0	TAIPEI: Phone: +886 2 2546 9668
PARIS: Phone: +33 1 49 69 15 50	TOKYO: Phone: +81 3 5531 8041
ROTTERDAM: Phone: +31 10 444 34 34	SEOUL: Phone: +82 2 780 9636