# The Top 10 Myths about Network Video

*The IP-Surveillance solution shatters misperceptions surrounding networked video*

*By Fredrik Nilsson, General Manager, Axis Communications U.S. Inc.*

**TABLE OF CONTENTS**

# 1  What is IP-Surveillance?

IP is an abbreviation for *Internet Protocol,* the most common protocol for communication over computer networks and the Internet. An IP-Surveillance application creates digitized video streams that are transferred via a wired or wireless IP network, enabling monitoring and video recording as far away as the network reaches, as well as enabling integration with other types of systems such as access control.

According to industry analyst, J.P. Freeman and Co., Inc. there are more than 20 million analog cameras installed in the U.S. alone. Of this 20 million, 1.5 million analog cameras were sold in 2002. Despite these rather impressive numbers for analog cameras, it is network cameras that have emerged as the fastest growing product category, providing a clear indicator that IP-based systems are poised to take over. Network cameras are connected directly to an IP-based network and integrate to applications on the network, enabling users to have cameras at remote locations and view, store and analyse live video at another location, or multiple locations, over the network/Internet. Network cameras are forecast to comprise more than half of the security camera market by 2007 and the global network video market is expected to reach approximately $790 million by 2005.

Whether it's network cameras or analog cameras connected to video servers, or an installation that employs both camera types, IP-Surveillance is proving to be attractive in nearly all vertical markets. In numerous applications this revolutionary technology is replacing traditional systems to reduce costs and increase safety. While in other applications, it is being used for the first time to create and stimulate new, exciting markets.

Because of its scalability, among other advantages, IP-Surveillance is an established, attractive technology not only for enhancing or revitalizing existing surveillance and remote monitoring applications, but also for a vast number of new applications in vertical markets as well including,

- Education: security and remote monitoring of school playground areas, corridors, halls and classrooms, as well as security of the buildings themselves.
- Transportation: remote monitoring of railway stations and tracks, 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 making store management easier and more efficient
- Industry: monitoring manufacturing processes, logistic systems, warehouse and stock control systems

# 2   Why Misperceptions about IP-Surveillance Technology?

As with any new technology, there is an initial period of market education. The more complicated the technology and/or the more entrenched the current technology and business model—the longer the period of market education. During this learning phase it is only natural that there are gaps in knowledge and misunderstandings. It is from these conditions that misperceptions and myths can grow and foster.

IP-Surveillance technology is by no means highly complicated, but the "IP" portion of it does take security out its natural state and move into the IT realm, unknown territory for many. In this sense, new technology and entirely new conditions can compound fears and stir support for the status quo. The fact that IP-Surveillance competes directly with the Digital Video Recorder (DVR) raises a number of issues, not the least of which is that it challenges the current assumption that DVR technology and the analog camera represent the end-point, and therefore best, technology. Let's face it, there is an entire industry, from manufacturers to installer and integrators on down to end users and their organizations, who have a vested interest in seeing the DVR be the dominant technology. To add to these "myth-making" market conditions, consider that the security industry is one in which proprietary, single-brand solutions are common and expected. IP-Surveillance solutions combine "best of breed" products and services from a number of different vendors. This ends up being great for the end user, but it is rather different from current conditions and expectations.

Now that we understand the reasons for the misperceptions and half-truths that have grown up around IP-Surveillance, let's examine some of them more closely.

# 3  Ten Greatest Myths about IP-Surveillance

There are a number of myths, large and small, surrounding IP-Surveillance technology. We've taken the 10 most often-heard myths and organized them into two categories: general and technical. We'll take the general un-truths first and then launch into some of the technical misperceptions.

## 3.1   Myth #1: DVRs are the latest, greatest CCTV security technology

**Reality**: In addition to people perceiving digital video recorders to be latest and best technology, many people also believe that the DVR is an all-digital networked technology—it is not.
A DVR does have a lot of advantages compared to a VCR (video cassette recorder): no need to change tapes, consistent image quality, and quicker search capabilities. But you still have all those analog cables, which first of all can distort image quality, but are also very expensive to run throughout a facility. IP-Surveillance has all the advantages of a DVR and many more:

- Scalability. IP-Surveillance scales from one to thousands of cameras in increments of a single camera. There are no 16-channel jumps like in the DVR world. IP-Surveillance offers any frame rate for any camera at any time—no limitations.

- More cost efficient infrastructure. Most facilities are already wired with twisted pair infrastructure, so with IP-Surveillance no additional wiring (a major expense of a CCTV install) is required. Only one type of network (IP) connects and manages the enterprise for data, video, voice, and others— making management more effective and cost efficient.

- Remote accessibility. Any video stream, live or recorded, can be securely accessed and controlled from any location in the world over wired or wireless networks.

- Intelligence at camera level. Motion detection, event handling, sensor input, relay output, time and date, and other built-in capabilities allow the camera to make intelligent decisions on when to send alarms and to whom, when to send video, and even at what frame rate or resolution to send the video.

- Lower system cost. For many installations, the IP-Surveillance system has proven to be a lower cost alternative. Open and standard network, server and storage equipment enables market competition between choices versus the single vendor locked-in approach of a DVR. And that's just hardware—add lower installation and maintenance costs and all the performance benefits, and it's clear IP-Surveillance saves substantial sums.

Contrary to some popular opinion, the DVR is not an end-point solution, but rather one milestone in the continuing development of CCTV technology. As the marketplace assesses DVRs more carefully, it is emerging that the DVR represents outdated, solution-in-a-box thinking. IP-Surveillance technology has quickly proven to be superior to DVR technology. There is an enormous difference between the two technologies and the marketplace is only just beginning to understand this critical point.

## 3.2   Myth #2: IP technology is unproven. If it's better, why aren't security solution providers selling more?

**Reality:** This myth raises some very relevant questions that have more to do with security market structure and buying practices than with the performance and reliability of the IP-Surveillance solution.

IP-Surveillance is a relatively new technology and many existing, powerful players have a competing solution, the DVR. It's only natural that these players want to protect their investment in DVR-oriented solutions. Related to this, a new technology and a new mind-set require building up the knowledge and infrastructure among the integrators, consultants, and industry influencers in order to overcome normal, status-

quo thinking and procedures. How many of us remember when we told typewriters provided all the technology required, who needs these new-fangled word processors? Too long ago? What about cassette players or that VCR you haven't exchanged for a DVD just yet? Entrenched technology and entrenched interests require time to overcome.

The fact is, the number of IP-Surveillance installs out there is growing quickly, and the number of integrators and distributors is growing daily. It won't be long before the market recognizes IP-Surveillance's superiority, and then we'll see a rapid increase in the installed base and infrastructure to support it.

If this argument is not compelling, we really don't need any further proof than the recent entry of a giant like IBM into the networked security market, as well as interest from players like Cisco and Proxim to drive and educate the market.

## 3.3   Myth #3: IP-Surveillance cannot meet the demands of enterprise level applications.

**Reality:** The larger the installation, and the higher level of performance desired, the more competitive—and impressive—the IP-Surveillance concept proves to be.

In fact, of the many advantages of IP-Surveillance outlined above, scalability is the one that high end users often point to as the most impressive. Axis regularly sees requests for 200 and 300 plus camera installations—our largest to date is 1,300 cameras—some of which have been in high security installations such as international airports and prisons. This myth is an easy one to correct: IP-Surveillance has proven that there is no problem to meeting enterprise-level demands. In fact, we see major government and airport surveillance deals that are now specifying IP as the preferred architecture, which was not the case just 12 months ago.

## 3.4   Myth #4: Networked video image quality is not as good as analog.

**Reality:** Good quality network cameras have the same high quality image sensors (CCDs) and optics as analog security cameras. Furthermore, by employing video servers an analog speciality camera or existing already installed analog cameras can be incorporated into an IP-Surveillance system. In comparing network and analog cameras, we must emphasize "good" quality network cameras, built for professional use. These high quality professional network cameras should not be confused with lower-end network or PC webcam cameras used for "web attraction." Indeed these cameras cannot deliver the same capabilities as a full-function network camera.

Soon, network cameras and IP-Surveillance technology will deliver superior image quality by means of mega-pixel resolution. Analog cameras are limited by the 0.4 Mpixel resolution of NTSC/PAL standards.

## 3.5   Myth #5: Network cameras cost more than analog cameras, making IP-Surveillance too expensive.

**Reality:** It's true a network camera is more expensive than a comparable analog camera because it includes considerably more functionality, such as digitalization, image compression and intelligence. If we analyze the total cost of the hardware (cameras, cables, and recording), an IP-Surveillance system will usually compare quite favorably to a DVR based system. If we then add the installation cost component, the advantages with the IP-Surveillance system become obvious since the IP-based infrastructure is considerably less expensive than analog coax cabling. In addition, systems using PTZ controls require extra cabling, something not needed with IP. Power over Ethernet is another cost-saving feature that saves on power lines and connects to uninterrupted power supplies at the IT center.

In a high-end installation Axis completed in 2002, 300 network cameras were deployed in a mission-critical high security area, with a high frame rate recording requirement. The total cost for installing the complete IP video surveillance system was $800,000, or $2,700 per channel. If a similar functioning, DVR-based system had been deployed; the cost was estimated at $1.8 million, or $6,000 per channel—more than twice the cost of the IP-Surveillance system.

## 3.6   Myth #6: If I already have analog cameras installed, IP-Surveillance isn't an option because I need a DVR.

**Reality:** Perhaps DVR providers want us to believe this, but video server technology is riding to the rescue and smashing this myth. Leading IP-Surveillance vendors have video servers readily available at a reasonable investment level. A video server converts the analog video signal into a digitized video stream over the network, basically converting any analog camera into a network camera. Most IP-Surveillance installs today have a combination of analog cameras, networked via video servers, and sections that are comprised completely of network cameras. An installation with fully functioning and already paid-for analog cameras is not a barrier to utilizing superior IP-Surveillance technology.

Now that we've successfully demolished several often-heard general myths surrounding IP-Surveillance, let's examine some of the more technically oriented misunderstandings about networked video systems.

## 3.7 Myth #7: Transferring all that video data over my network will overload it, making this an unworkable technology.

**Reality:** If you will only have a few cameras, then an existing Fast Ethernet (100 Mbit) office network will normally meet any transmission demands. For comparison, a typical single network camera video feed is 0.2 to 2.0 Mbit/second depending on compression, size and frame rate. For any larger deployment of network cameras and video servers, we recommend a separate network for the video. Think of it like rail transportation— once the existing track becomes too congested, you simply build another set of tracks. For enterprise size, your local network core would probably be running at Gigabit Ethernet. With today's network switches and routers, separating networks is easy. In addition, other specific steps can be taken to ensure that IP-Surveillance technology can be integrated into an organization's operations and will not tax the network.

Additionally, because of the local intelligence inside a network camera, the camera can actually decide which frame rate to send over the network based on events, motion, time of day, etc. So in many cases the camera will only send video over the network if the video is worth recording, which might only be 10% of the time. 90% of the time nothing is being transferred over the network.

## 3.8 Myth #8: Transmitting video for security purposes over an IP network is not secure.

**Reality:** Although primarily used as a domain for public information, the Internet can also be used to transfer all types of sensitive information—provided the correct security measures, such as firewalls, VPNs and password protection are implemented. With banks and financial institutions regularly using the Internet as a medium for global money transactions, it has emerged as a proven medium for other secure applications like surveillance and security monitoring. In stark contrast to this new digital technology, analog surveillance systems have no encryption or authentication of information whatsoever, making it extremely easy for anyone to tap into the cables and illicitly view "secure" video transmissions, or even feed their own false video information into the network (like in the movie Ocean's 11). This is impossible to do with secure IP networks.

## 3.9 Myth #9: IP-Surveillance is less reliable than alternative technologies; for instance, the network go down.

**Reality:** When the basis for the IP networking architecture was developed in the 1960s and 70s, the ability to provide redundancy was the top requirement. In the same way today, transmission links, application servers, storage and switches can all have parallel layers of services and alternative routes of communications. Storage can be consolidated to secure off-site locations, and servers can use redundant power supplies,

hot-swap RAID disks, error-correcting memory and dual network cards. This is all up to the network designer, and although a small network will not deploy all of the possible safety measures, choosing high-quality IT components in the network is in any case likely to be a more reliable solution than CCTV with VCRs or black box DVRs. And don't forget, by using standard server and network equipment, replacing faulty hardware takes much less time and is less costly than with proprietary DVR solutions.

## 3.10 Myth #10: IP-Surveillance is still five years away.

**Reality:** This is the biggest myth of all! Consider that the first network cameras were introduced in 1996. Axis Communications has already installed more than 200,000 channels of this "future" solution to date, and the interest in and orders for IP-Surveillance technology continue to mount. Whether it's cost, performance, reliability, or any other measure, IP-Surveillance has proven it is a solution for today and one that will grow and improve to ensure it is a solution for the future as well.

In this paper, we have effectively disproved a number of existing myths and we've established that IP-Surveillance is highly scalable, while effectively and efficiently utilizing a company's network capacity, and it provides significant cost and performance advantages over the DVR model that many think is the premier solution today. We've also seen that IP-Surveillance is flexible, based on high-functioning and affordable network cameras, and is highly reliable.

# 4  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**
Axis Communications AB
Emdalavägen 14
SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

**Subsidiaries**

| | |
|---|---|
| U.S. - BOSTON<br>Phone: +1 978 614 2000 | ITALY - TORINO<br>Phone: +39 011 841 321 |
| U.S. - SAN DIEGO<br>Phone: +1 858 458 0471 | SINGAPORE<br>Phone: +65 683 627 77 |
| U.K. - LONDON<br>Phone: +44 870 162 0047 | AUSTRALIA - MELBOURNE<br>Phone: +61 392 255 244 |
| SPAIN - MADRID<br>Phone: +34 918 034 643 | CHINA - SHANGHAI<br>Phone: +86 216 431 1690 |
| GERMANY - MUNICH<br>Phone: +49 811 555 080 | TAIWAN - TAIPEI<br>Phone: +88 622 546 9668 |
| FRANCE - PARIS<br>Phone: +33 149 691 550 | JAPAN - TOKYO<br>Phone: +81 355 318 041 |
| NETHERLANDS - ROTTERDAM<br>Phone: +31 104 443 434 | KOREA - SEOUL<br>Phone: +82 278 096 36 |