Network Surveillance: More Than Meets The Eye

With new intelligence capabilities and robust, smart features bursting into the scenes, discover how network cameras have surpassed their analog predecessors to take over the surveillance world today.

We had a brief peek into our first network camera that was released back in 1996. However, surveillance technology then was too raw with inadequate specifications or any supporting hardware and software to enable the surveillance application advantages it was designated for, mainly, to enable the security monitoring on physical premises "remotely".

Fast forward to present-day. Forget video-encoding. Not only has today's network cameras made image quality challenges and remote accessibility hassles a thing of the past, network surveillance technologies now boasts high-definition cameras that can be viewed at 1920x1080 multi-pixel resolutions at 30 frames per second – uninterruptedly in real time. Application-specific intelligence such as night-monitoring, people-counting or license-plate recognition have also evolved into mainstream, with technologies you would have previously witnessed only in spy flicks now becoming commonplace realities.

LOVE AT SECOND SIGHT?

With these innovations in network cameras shifting frame capturing, image quality and intelligence capabilities away from conventional Digital Video Recorder (DVR) limitations, more businesses, in particular Small- and Medium-Businesses (SMBs), are taking a second look at this forgotten technology. Despite the recent global economic downturn putting a stranglehold on organisational budgets, the network surveillance market posted a healthy 10 per cent growth rate in 2008 and 2009, with ABI Research forecasting the total video surveillance market to be worth more than US$41 billion in 2014.[1]

Now here's why.

DIGITAL VERSUS ANALOG

Visibility
An analog camera, even at the possible highest resolution, produces blurry images due to inherent interlacing limitations. This is because the images produced by an analog video signal are made up

---

[1] *10% growth despite recession, SearchSecurityEditors, 2 Apr 2009*
http://security.networksasia.net/content/research-shows-video-surveillance-market-maintains-10-growth-despite-recession

of lines, and image accuracy is compromised when capturing moving objects between two interlaced fields. For network cameras that employ "progressive scan" technologies, interlacing is effectively eliminated with whole images captured at any single time, thus offering crystal clear images even for objects with a high degree of motion.

In addition, while analog cameras are stuck at NTSC/ PAL specifications, network cameras can meet high-resolution requirements with megapixel resolution and HDTV capabilities. A typical Charge-Coupled Device (CCD) sensor in an analog camera requires a total of three conversions during the recording of an image, and with every conversion, image quality is lost. In the network camera system, images are digitized once and they stay digital for the duration. As such, investigative efforts can be significantly reduced during replay with images of an exceptional level of detail, and functions like digital pan, tilt and zoom can also be enabled with higher resolution capabilities.

Costs and Efficiency

The IEEE 802.3af standard used in network cameras enables Power over Ethernet (PoE), which effectively eliminates the long-standing problem of getting power to analog cameras. PoE capabilities enhances significant savings from additional installation and cabling costs, and also prevent outages because PoE enabled network cameras can enjoy centralized backup power from the server room, so in the event of a power failure, they will continue to operate.

While analog video is typically transmitted via wireless, or expensive coax or proprietary fiber where distance will also affect image quality, standard IP-based network cameras produces digital images with an established, relatively low-cost IP-based networking standards. Moreover, IP-based video streams can be routed anywhere across interoperable, standardized infrastructure, running much faster at up to one Gigabit Ethernet speeds.

Although the price for a network camera is higher, when comparing the cost per channel, a surveillance network based on analog systems will turn out much higher. The network camera also offers superior flexibility and performance, and operates on industry-standard, open systems-based servers, as opposed to proprietary DVR. The significantly reduced management and equipment costs results in a lower Total Cost of Ownership (TCO), making network surveillance solution a much more attractive option than its analog counterparts.

Integrated Functions & Added Capabilities

In an analog Pan, Tilt Zoom (PTZ) camera, the serial communication that controls PTZ movement requires an additional cabling separate from the video signal. For a network camera, it enables PTZ control over the same network that transports the video. PTZ commands are sent over the IP network, resulting in significant cost savings and greater flexibility. A network camera can also integrate input and output signals such as alarms and controlling locks.

In an analog system, audio is not possible without running separate audio lines to the DVR. A network camera eliminates this issue by capturing audio at the camera, synchronizing it with the video or even integrating it into the same video stream. It is also easy to install and relatively affordable. In addition,

network cameras with integrated audio can be used to automatically trigger recordings or alerts to surprise perpetrators such as, "This is a restricted area, please keep out!" when preset values are exceeded.

Security

In our current innovative age where collaborative technologies are increasingly employed, the network surveillance system offers a huge level of architectural flexibility, but also a playground for attackers. Security must be implemented at the source, the network, the storage system and the client. If security on the camera is breached, this also means that the perpetrator can view everything going on your physical premises. He can also access records of people in and out of your facility, and decipher conversations exchanged, or even confidential information typed on cipher-lock keypads or keyboards. If the PoE switches are breached, he can shut down all video, or even replace the signal with an image from another video signal (like in the scene from *Ocean's Eleven*). In a network surveillance system, the camera can encrypt video being sent over the network to ensure against tampering. The system can also be set to authenticate connections using encrypted certificates to eliminate hacking. Encrypted "watermarks" can also be added to the video data stream with specific information such as time, location, or users to secure a trail of evidence. All these security capabilities will not be possible on an analog system.

Intelligence

With the advent of intelligent video, this is becoming increasing relevant in our business world today where too much video is being recorded for monitor or search purposes. Effective video surveillance depends on accurately detecting and identifying objects, people or incidents, so that appropriate action can be taken. Innovations have made it possible for network cameras to have standard built-in motion detection, object recognition or alarm management. One major intelligent video application innovation would be the tampering alarm, which enables the camera to automatically send an alert when it is not fully functional, e.g. due to re-direction, spray-painting or other external damage. A network surveillance system that implements analytics at the edge will enable network efficiency and scalability and will be most successful if intelligence is deployed in the camera, network and storage system.[2]

Another major stride into the inroads of network surveillance technology has also been taken – to enable network cameras using thermal detection to capture usable images in complete darkness or under challenging conditions such as smoke or fog, or when subjects are hiding or obscured by a complex background.[3]

EMERGING DEVELOPMENTS IN NETWORK SURVEILLANCE

H.264 is an open, licensed standard that supports the most efficient video compression techniques available today. It is also the first, global video standard shared across all industries. Without compromising image quality, an H.264 encoder can reduce the size of a digital video file by more than

---

[2] *Video Surveillance, Pete Tenereillo, 28 July 2006*
  http://www.networkcomputing.com/other/video-surveillance.php?p=5
[3] *Video Surveillance – is thermal detection the next frontier? Axis Communications, 2 Mar 2010*
  http://security.networksasia.net/content/video-surveillance-thermal-detection-next-frontier

80 per cent as compared with the Motion JPEG format and as much as 50 per cent more than with the MPEG-4 Part 2 standard. For SMBs, this means that they no require much less network bandwidth and storage space for a video file, effectively reducing significant business overheads.

H.264 has already been introduced in new electronic gadgets such as mobile phones and digital video players, and has gained fast acceptance by end users. Industry leaders like Apple are already using it as the de-facto standard on the iTunes store for their video downloads. This has resulted in the birth of one of the most exciting surveillance apps usable on the iPhone.

As Stan Schatt, Vice President of ABI Research explained, "This is the app where you are essentially able to look at any camera anytime via your mobile device – that's the app SMBs go nuts over. Some functions can even be automated."

Along with this, software which aid in the evaluation of marketing efforts have been unveiled – for example, one that can gauge the effectiveness of marketing displays at the end of shopping aisles by detecting how long customers stare at the display and whether they buy the items there. There are even some others which can send alerts to managers if an item passes through the checkout aisle without being purchased – an event that would later be viewable on searchable IP video.[4]

HELLO DIGITAL, GOODBYE ANALOG

For SMBs and their limited resources, the idea of this technology being able to alleviate the need for constant monitoring or 24-hour security employees seems picture-perfect. Along with the advent of Managed Service Providers (MSPs) providing network surveillance services, what was traditionally seen as a luxury for the larger enterprises, the benefits of IP video surveillance are already catching on to accelerate the demise of the analog standards in today's video surveillance market.

However, this inherent "remote accessibility" capability celebrates only the icing. With more innovations in functions, features and supporting software bursting at the seams to add more superlatives to its existing cocktail of benefits in *performance, open systems interoperability, flexibility, future-proof, and network connectivity,* network surveillance is now carving into verticals to go beyond security, to enable SMBs to integrate surveillance with specific business processes and operations. The dawn of the new surveillance era has now opened the floodgates to a whole new world of dramatic technological possibilities, and infinite business opportunities along with it – that is really the cake.

Is anyone watching?

---

[4] *The IP video surveillance opportunity, part two: SMBs, Ed Gubbins, 4 May 2009*
    http://connectedplanetonline.com/business_services/news/ip-video-surveillance-part2-0502/index.html

KEY SUMMARY

Network surveillance is not a new technology, with the first network camera released in 1996.

The main selling point for network surveillance is the ability to enable the monitoring and management of security remotely.

Despite the recent global economic downturn, the network surveillance market posted a healthy 10 per cent growth rate in 2008 and 2009, with ABI Research forecasting the total video surveillance market to be worth more than US$41 billion in 2014.

The network camera has accelerated the demise of analog cameras due to inherent application advantages in *performance, open systems interoperability, flexibility, future-proof, and network connectivity.*

The business advantages offered by network surveillance system include: cost benefits, lower TCO, reduced service outages, enhanced security and intelligent functions and features.

INSIGHT

Network Surveillance Beyond Security Monitoring

With network surveillance now carving beyond verticals to go beyond security, you can now utilise this technology to satisfy alternative business functions. For example, "monitoring" can take on an auxilliary role as "an invisible watcher". You can monitor your employees for performance, attitude at work, attitude towards customers, or even morale, instead of performing the traditional function of enhancing security for physical inventory in your warehouse. As network surveillance innovation advances into unexplored business territory, you can also venture into novel ways to leverage on these unprecedented powerful capabilities to uncover exponential business benefits and advantages.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel : 408 526-4000
800 553-NETS (6387)
Fax : 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**