INTELLIGENT IP-SURVEILLANCE:
MANAGING MORE WITH LESS

Technical White Paper
April 2008

aimetis

EXECUTIVE SUMMARY

Enterprises are now recognizing the importance of IP surveillance with integrated video analytics over more traditional DVR deployments as a means of reducing total cost of ownership, increasing productivity and limiting risk on IT investment. IP surveillance deployments consisting of Network Video Recorder (NVR) software installable on commercial-off-the-shelf (COTS) hardware offers the most scalable and longest life-cycle than any other deployment. This type of deployment is based on an open, standards-based architecture that enables companies to keep infrastructure expenses in control. As businesses become more network centric, IP Surveillance enables tighter integration of business processes and security systems, which increases overall value of the system.

As the popularity of video increases, this growing mass of raw video is putting increasing pressure on conventional video management and retrieval methods that are inefficient and costly. As a result, organizations are quickly embracing video analytics software, an emerging technology which intelligently analyzes video and promises to revolutionize the way in which video is archived, distributed and managed. Pure software NVR deployments can be easily upgraded to support this new business requirement.

Conversely, Digital Video Recorders (DVR) connected to CCTV cameras often consist of proprietary hardware. DVR deployments cannot be easily upgraded to supporting new standards and technologies such as video analytics without hardware reconfiguration or replacement. Software based NVR deployments support emerging and legacy cameras to co-exist on one platform such as USB, megapixel, network and analog cameras.
In sum, software based NVR platforms offer the greatest freedom to build a flexible, scalable and integrated deployment resulting in higher overall value and a longer life-cycle than DVR installations.

This document contains references to companies, products, and their trademarks. All trademarks remain the property of their respective trademark holders.

The information researched to create this white paper was obtained from sources considered to be reliable. Aimetis Corp shall have no responsibility for errors, omissions or inadequacies of this information.

All opinions expressed in this white paper are those of Aimetis, except where original author is credited. The opinions expressed in this white paper are subject to change without notice.

All costs were determined using the list/retail price available to the public at the time - no corporate or other discounts were applied.

MARKET TRENDS IN THE SECURITY INDUSTRY

Recent geopolitical events and advances in technology have caused an increased global focus on physical security in both private and public environments. As a result, the security industry is experiencing three key trends:

1) Convergence and integration of physical security technologies with other systems within the organization.
2) Transition from CCTV to IP surveillance.
3) Deployment of Video Content Analysis technology to manage exponential growth in raw video

Convergence and Integration

Organizations are under pressure to reduce risk on IT projects and deliver rapid return on investment. As a result, a new breed of network-centric organization is emerging whose business processes and security networks are linked. The divide between physical security solutions and other IT projects is shrinking as access control, video and intrusion detection are married with HR databases, point of sale and facility management. These new solutions are based on high-value, information based software that will support and enhance the organization's operations. This is specifically achieved through one unified platform sharing a single user interface, centralized data management, commercial off-the-shelf hardware and a cost-effective infrastructure. Finally, as security systems are treated like most other IT investments—responsibility, decision making and management is often multi-layered involving different departments.

Digital Video

Security systems are moving towards IP networks. Nowhere is this shift more prevalent than in the CCTV segment. With the advent of inexpensive and spacious hard drives, mega-pixel cameras and high bandwidth networks, video is quickly transitioning from standalone, analog video output to networked digital video, revolutionizing the way in which video is

The transition to networked digital video is also resulting in a shift from decentralized, local surveillance infrastructure to a more centralized monitoring station covering several remote locations via a private network or the Internet. Further, with high-resolution video now easily accessible on the network, new applications are emerging which increase the overall efficiency and accuracy of video surveillance not previously possible with CCTV.

Video Content Analysis

The growing mass of digital video is putting increasing pressure on conventional video monitoring processes that are labor intensive, inefficient and costly. Video Content Analysis (VCA) greatly improves the efficiency of surveillance and decreases labor cost, and as a result is one of the fastest growing segments in the security industry. VCA is based on a research field called "computer vision", which endows computers with the ability to understand video in human terms. Humans can understand the content of video; however, to a computer photographs or video are just an array of numbers representing each pixel's color value. VCA software analyzes these pixel values and can begin to make sense of the video the way a human does. As a result, VCA automatically filters extraneous data maximizing human attention where it is needed most. No longer is a person required to watch hours of continuous live or recorded video to analyze or identify interesting events. The efficiency gains of VCA software over conventional video surveillance are significant.

THE BUSINESS CASE FOR INTELLIGENT IP-SURVEILLANCE

A carefully selected video solution can help organizations meet today's challenges—enabling them to increase productivity, limit risk on IT investments, and reduce their total cost of ownership (TCO). Two key criteria are important to consider before investing in a surveillance solution—its design architecture and application support—both of which will impact ease of use, cost, and long-term value. Advances in IT have created two strategic choices when deploying video:

Digital Video Recorders (DVRs) containing analog to digital capture cards connected to analog (CCTV) cameras

IP-Surveillance which includes Network Video Recorders (NVRs) utilizing normal PC hardware to record digital video from network devices such as network cameras or video servers. A video server digitizes analog video signals and sends digital images directly over an IP network, such as a LAN, intranet or Internet.

In the following sections we'll compare the potential business benefits of a pure IP-Surveillance solution versus DVRs and illustrate the strategic advantages of investing in IP surveillance.

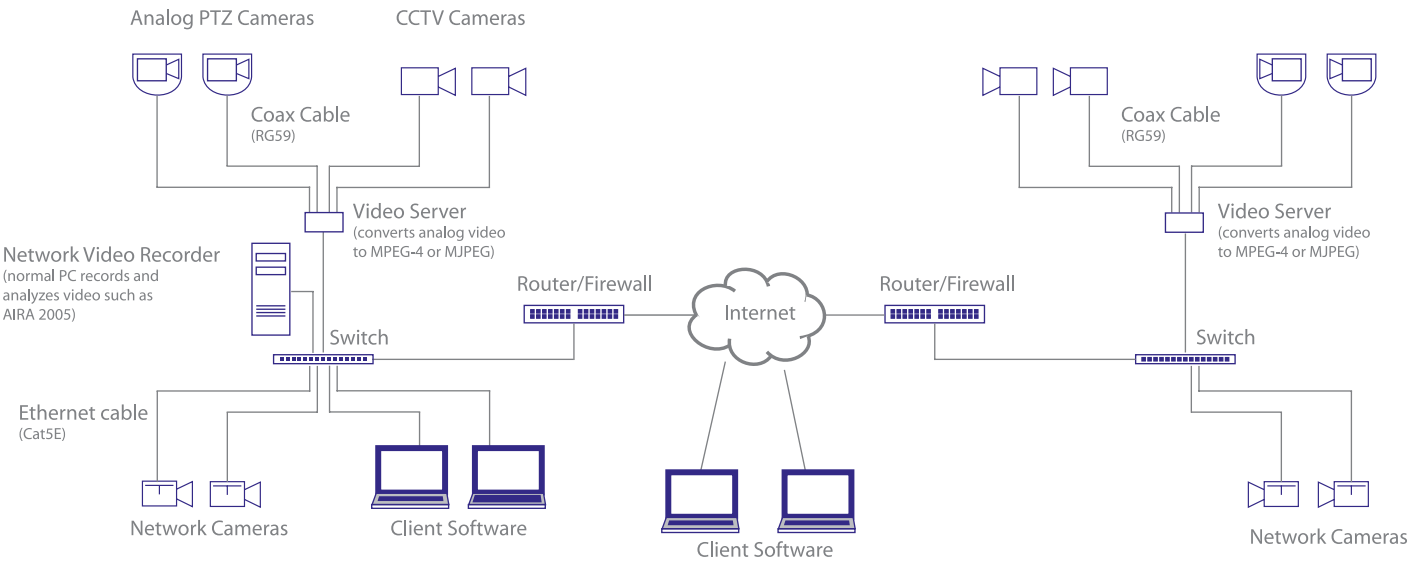
Reducing TCO through greater flexibility

When doing a cost analysis, there is more to consider than the initial purchase price. A proper total cost of ownership (TCO) includes capital costs, technical support, administration, upgrades and expansion costs. As we will explain in the following sections, IP surveillance works best across all of these areas to drive down the TCO as compared to DVR products.

Interoperability Benefits

An effective video solution is based on an open, standards-based architecture that enables companies to keep infrastructure expenses in control. NVRs consisting of Windows based software installed on industry-standard x86-based PCs or servers offer significant advantages over DVRs which are almost always closed and proprietary.

Figure 1 - Sample multi-site IP-Surveillance typology



The ability to reuse hardware already existing in an organization's inventory or centralize data management through enterprise level databases is not normally possible in DVR deployments.

Most organizations have IP infrastructures which can be leveraged by IP devices such as cameras or video servers, making them less expensive to deploy and maintain than CCTV. Furthermore, as IP cameras mature and increase in capability with rich features such as PoE (power over Ethernet) or increased image size, the advantage IP cameras have over CCTV is widening.

Although mega-pixel cameras are quickly becoming popular, backward compatibility is still required. Using a NVR platform, organizations can enjoy migrating to mega-pixel cameras while still supporting their traditional resolutions. DVRs do not offer this flexibility and would require replacement by a NVR if increased frame rates, image size and video standards are required to co-exist on one unified platform. A further limitation with DVRs is the video resolution which can be archived. DVRs can archive a maximum of 575/2 TV lines vertical resolution per image. NVR solutions with mega-pixel cameras using progressive scan technology can currently archive more than three times the maximum vertical resolution of a DVR.

Scalability

Since NVR deployments involve Windows based recording software installed on a commercial-off-the-shelf (COTS) platform, organizations can quickly and easily scale their infrastructure to support changing requirements such as mega-pixel cameras, increased storage requirements or increased number of cameras. When hardware changes are required due to failure or increased demand the ability to source COTS hardware, regardless of vendor, strongly reduces cost and down time.

Conversely, DVRs require manufacturer approved components and accessories which are usually expensive and not quickly available. As a result, a NVR platform offers the greatest freedom to build a flexible, scalable and easily managed deployment resulting in a much longer life-cycle.

The ability to deliver multi-site connectivity is much more easily deployed and managed through a NVR solution connected to IP cameras (via LAN or WAN) or an analog camera connected to a video server. Once an IP device has connectivity to the network, the deployment is essentially finished. The modular and scalable design of the NVR and IP device approach is a significant advantageover a CCTV and DVR deployment (see Figure 1).

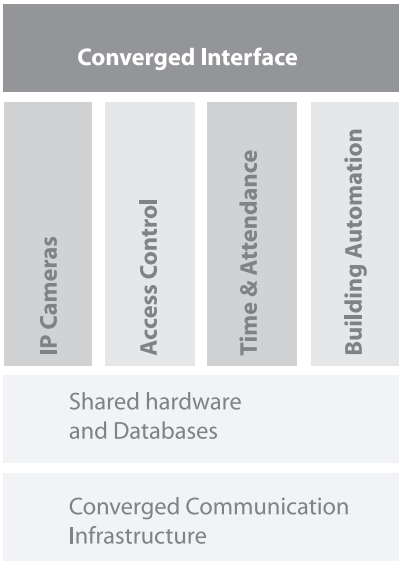
Application Support

Organizations continue to become more network centric as business processes and security networks are integrated. Proprietary DVR solutions simply cannot not keep pace with changing business needs, and as a result, present and future value will not be fully realized. As the "solutions" oriented focus prevails over asking for product specifications, implementation and application flexibility is a key differentiator between a DVR and NVR solution, with the latter drastically outperforming the former. In the following sections we will review the potential business benefits and key technical requirements in deploying an integrated video solution. However, one new technology deserves special attention due to its fundamental impact on video surveillance. Video Content Analysis (VCA) is revolutionizing the way video is processed, analyzed and stored.

Integration and customization

Open and standards based architecture is critical for easy network integration with third-party applications. A system that includes open application programming interfaces (APIs) is critical for easy integration with third party applications or integration with other systems. This will enable independent software developers

> ***"One of our key initiatives at infraserv Höchst was to reduce the number of hardware vendors in our server room. Aimetis Symphony™ software impressed us with its sophisticated video analytics while enabling us to use commercial-off-theshelf hardware. Not only are we more efficient at video surveillance, but our hardware maintenance and acquisition costs have decreased substantially."***
>
> *Volker Bachmann*
> *infraserv GmbH & Co. Höchst KG*
> *Unternehmenssicherheit / Gefahrenabwehr*



the ability to integrate, customize or extend many different systems such as access control, intrusion, video and building automation, which affects the overall effectiveness of the entire system. As a result, software is driving overall value as opposed to proprietary hardware.

Appropriately, devices that use proprietary hardware such as DVRs which limit the ability for customization or integration should be avoided. For example, access control systems can interact with Time and Attendance systems by sharing information to track and maintain attendance records while controlling access to the premises. Intrusion detection and video surveillance systems can integrate and share arming and disarming schedules. The possibilities are endless, and with the ability for seamless integration with additional applications, organizations can quickly begin enjoying the productivity and cost benefits of a fully converged and integrated system only possible through IP-Surveillance.

Video Content Analysis

Business drivers for intelligent video are clear, and enterprise organizations are rapidly embracing this technology. Without intelligent software, the onus is completely on the human operator to find interesting events in real-time. While a human brain performing at optimum efficiency can analyze and react to a critical situation with reasonable speed, experience shows the limitations of the human brain due to its limited memory, intrinsic biases and distractibility. Large amounts of data can prove fatal obstacles to quick, intelligent responding. Video Content Analysis (VCA) improves the overall effectiveness of video monitoring by analyzing and filtering video and notifying personnel as required making video surveillance more scalable, proactive and cost effective. As a result, VCA is becoming a standard requirement in any CCTV or IP surveillance scenario, quickly displacing the use of external sensor inputs such as Passive Infrared. By leveraging VCA, users can build rules which filter, index and organize video automatically much the same way anti-spam filters operate to keep unwanted email from your inbox. Before deploying an "intelligent" security system, organizations face an array of choices. There are many flavors of VCA and not all are created equally. Motion Detection, Motion Tracking and Object Persistence are different types of VCA which analyze the pixel values of video to understand scene activity without human intervention. It is important to understand the differences as not all methods will be appropriate for all environments. Furthermore, substitute technologies exist to help improve video monitoring (such as installing an extra PIR sensor). The capabilities and limitations are briefly described in Table 1.

Table 1: Comparison of different methods of motion detection.

Technology	How it works	Capabilities	Costs and other factors
Motion Detection (software only)	These are the simplest systems and are the least useful of the three software approaches discussed here. MD systems look for a bunch of pixels that are different than the current background model in the same region of the scene. If a DVR vendor simply "piggybacks" the video compression technology in order to get intelligence, their system will be MD based and of limited value.	These systems cause significant false alarms, especially in outdoor environments. Only viable in indoor applications. Unable to classify the moving objects or automatically control PTZ cameras.	Less computationally expensive than other software based detection methods. No additional device required.
Motion Tracking (software only)	These are the most interesting and intelligent type of VCA. MT systems reduce the high number of false alarms seen in MD systems by making use of future frames. The assumption is that if there was a change in frame1 in one area, there should also be a change close to the same area in frame2, and frame3. The more frames where a change can be tracked, the more evidence the system has that this is really a moving object. Assumptions are made about the maximum speed of an object, and often perspective information is also used.	Most sophisticated and reliable method of motion tracking in indoor or outdoor environments. Not adversely affected by weather conditions or changing lighting conditions. Auto PTZ tracking is possible in outdoor environments. Can often classify objects and alarm based on object type and other characteristics.	No additional hardware device required Object classification and tracking performance degrades in busy environments (such as airports), but will work well in environments that are not as busy.
Object Persistence (software only)	These systems are usually advertised as being able to pick up left luggage at airports. They work by looking for persistent changes to the background (someone just dropped a bag) and the area has been in this new state for a specified length of time (ie. the bag has been there for three minutes). Eventually, the object would be incorporated into the background model.	In addition to detecting if objects were removed or left in an area, these systems can be used for traffic analysis to detect accidents or vehicles that pull off on the side of the road since the event will cause a persistent change to the background. Will normally work better in busy environments for certain types of applications.	Not normally capable of tracking and classifying objects Not appropriate for general video surveillance applications (such as perimeter protection or auto PTZ camera control)
PIR sensors (extra sensor input)	Passive infrared (PIR) sensors respond to movement of infrared sources, such as human bodies in motion. They are designed to be maximally sensitive to objects that emit heat energy near or around human body temperature. The detection pattern of PIR sensors is fan shaped -- formed by the cones of vision seen by each segment of the faceted lens.	Most PIR sensors are sensitive to hand movement up to a distance of about 10 feet, arm and upper torso movement up to 20 feet, and full body movement up to about 40 feet. The sensitivity range of PIR sensors can vary depending on product quality and electronic circuiting design. Works reliably in indoor environments for motion detection. Cannot automatically classify moving object or detect left items or removed items.	Limited capabilities in outdoor and dynamic environments due to inability to alarm based on object type, speed or direction object is traveling. Performance of device adversely affected by background temperature of environment (human can be undetected if outdoor temperature is very hot)

As summarized in Table 1, software based VCA provides the most comprehensive ability to filter and organize video with the fewest false alarms when properly implemented (specifically Motion Tracking). Installation is also easier as an external sensor (PIR) would not be required alongside cameras. If you purchased NVR software in the past, it is likely that a software upgrade will enable you to reap the benefits of VCA. If you purchased a hardened DVR product, your migration to video analytics will be more costly, involving expensive hardware upgrades or add-on devices. However, even with hardware upgrades to a DVR solution, users will not experience the same productivity and cost benefits enjoyed

by integrated NVRs. If DVRs are deployed where VCA is required, it is in fact more cost effective to replace the DVR with an intelligent NVR platform than performing continuous hardware upgrades and intelligence integration.

FUTURE APPLICATIONS AND DIRECTIONS

Just as the limitations of the current generation of security system architectures are becoming painfully apparent, new methods of organizing technology resources are appearing. IT is quickly shifting to "service-oriented" architectures (SOA) that will enable companies to introduce new business practices and processes more rapidly and at a lower cost. The current deployment of Web services technology is a promising early initiative in this direction. In particular, Extensible Mark up Language (XML) provides a major advance by creating ubiquitous standards for presenting data and for defining the interfaces that platform independent and loosely coupled connections require. The business value is clear—SOA promises to deliver the capacity for unprecedented agility. As we have already learned, integration and interoperability reduces TCO and increases the life cycle of your technology investment and SOA aims to drive integration costs down even further.

Today, the emerging standards and protocols of SOA in the security industry remain largely conceptual.

However, CIOs, enterprise architects, and other IT staff responsible for delivering solutions to the business need to make strategic decisions today to maximize business value in the future. They can begin with a focused effort to invest in technology which will support maximum flexibility down the road, no matter which standards and technologies emerge. As we have already seen, NVR platforms will inherently be more flexible and benefit faster from new industry standards and technologies as compared to its DVR counterparts. Nowhere is this case better demonstrated than through VCA, where those who invested in NVR solutions are experiencing intelligent video than those who invested in proprietary DVR products.

COMMON MISCONCEPTIONS RELATED TO INTELLIGENT IP SURVEILLANCE

As with any disruptive technology, IP surveillance lives with its fair share of misconceptions. However, with "intelligent video" or VCA the confusion and misconceptions are even more prevalent. Below we will address misconceptions that seem to feed residual concerns about the technology.

Embedded DVRs are more stable and secure than IP-Surveillance:

DVRs will typically run a Linux distribution while pure IP-Surveillance solutions involve software installed on Windows based PCs which records video (also called Network Video Recorders). Many people claim Windows to be inherently insecure and unstable while Linux is not. As many IT professionals seek the most "stable and secure" platform they may consider a DVR thinking Windows based systems incapable of meeting this requirement. In reality, however, Microsoft Windows XP or Vista can be deployed far more securely than was the case with past versions, and the notion that Linux distributions such as Red Hat are more secure is has not been necessarily true for some years now. While older versions of Windows were inherently more dangerous since they did not isolate users from the system, Windows has long since evolved from a single-user design to a multiuser model, meaning users and applications do not have access to the entire system. When any operating system such as Windows or Linux has been compromised by intruders or infected by virus a major cause is often improperly configured security settings. A properly configured Windows XP or Vista system will be no less secure than Linux systems and Windows Vista includes Microsoft's continuous and significant OS security improvements. Both Windows and Linux distributions can be deployed in a stable and secure fashion, therefore the Linux vs Windows debate is inconsequential. IT professionals should focus buying decisions on the merits of the DVR or NVR application itself—not the platform it runs on.

Bandwidth and impact on LAN:

While most networks are 100Mbps with a usable bandwidth around 50Mbps, this only allows for approximately 10 cameras at the highest resolution and maximum frame rate (30 fps). However, using managed switches or event driven frame rates can help overcome the bandwidth limitations. Furthermore, as networking technology becomes more affordable and Gigabyte networks become increasingly popular, the bandwidth issues will quickly become trivial.

VCA has been around for a long time:

VCA is new technology and not to be confused with "motion detection". For instance, the difficulty in finding "automatic PTZ tracking" functionality for outdoor environments is due to the inherent limitations of motion detection which simply relies on pixel changes in determining if there was motion. In outdoor environments, pixels values are constantly changing—due to weather conditions or lighting changes—making traditional motion detection completely inadequate. VCA is based on computer vision which is more computationally intensive but more reliable, in that it uses multiple metrics in determining whether motion occurred in a region or not. Be careful of DVR manufacturers who claim to have "intelligent" products when in reality they are not.

VCA and behaviour analysis:

Video Management and Video Content Analysis have been around now for some time, but confusion continues to exist as to the exact capability of the technology. While the technology is advanced and drastically outperforms PIR sensors and "motion detection" technology, its own limitations are still misunderstood. Humans are adept to understanding the world around them based on visual information and prior learning. While the current state of artificial intelligence has made significant strides and adds tremendous value to video, it has a long way to go before it will approach the visual understanding of a human. Before investing in VCA technology consider what the vendor is claiming while understanding the current state of research in computer vision—the branch of artificial intelligence that endows computers with heightened visual functioning. Asking for sample video of the system in action and asking for customer references is recommended in order to limit the risk of purchasing inferior VCA technology. Some key things to remember include:

Beware of systems that claim to classify a myriad of different objects

When an object gets tracked around a scene there is usually a box around that object. The question naturally arises – what is inside the box? Is it a person or a vehicle (this scenario is possible to detect)? If it is a person, then who is it (not possible in a free environment)? In most surveillance scenarios the object that is being tracked may be a distance from the camera such that you only have a small number of pixels from which to classify the object. In these situations very little can be concluded by what is inside the tracking box. A little bit can be concluded by the speed, size and aspect ratio of the tracking box. We are lucky that vehicles are usually more horizontal than vertical and humans are usually more vertical than horizontal, so we have systems that can reliably discriminate between those classes.

Beware of systems that claim to recognize behavior

Many vendors speak about "behaviour analysis" but this statement alone carries with it great ambiguity. Ask the vendor to be clear on how he defines behaviour of the object. When an object gets tracked around a scene there is usually a box around that object. There are two types of behaviour analysis:

1) Behaviour that depends on what is happening inside the tracked box
   I. Person smoking
   ii. Person pick-pocketing another person
   iii. Vehicle letting down the sunroof
2) Behaviour that is determined by the movements of the tracked box
   I. A person stopping
   ii. A vehicle starting (maybe it is being stolen)

Class 1 is very difficult to discriminate even in controlled environments. Class 2 is possible in uncontrolled environments.

When vendors claim to have detected events such as "erratic movement" or "suspicious activity" ask to see sample video in an uncontrolled environment. Today these systems work unreliably.

> *"It is a well-known phenomenon that we do not notice anything happening in our surroundings while being absorbed in the inspection of something; focusing our attention on a certain object may happen to such an extent that we cannot perceive other objects placed in the peripheral parts of our visual field, although the light rays they emit arrive completely at the visual sphere of the cerebral cortex."*
>
> *Rezso Balint 1907 (translated in Husain and Stein 1988, page 91)*

Human monitoring is more reliable than software based Video Content Analysis

Experience has shown the limitations of the human brain—due to its flawed memory, intrinsic biases and distractibility—which limits the quality and productivity of conventional human-based video monitoring.

Human monitoring normally results in high false conclusions due to our short attention spans and distractibility. In a properly configured VCA system, proper detection of events can be close to 95% accuracy whereas humans may be closer to 50% or less. A Harvard University study concluded that humans may be so fixated on certain objects that we are surprisingly unaware of the rest of the details of our environment.

DEPLOYMENT SCENARIOS

Many video surveillance deployment strategies are available. However, in order to maximize productivity and long-term value the recommended deployment strategy for your digital video is an advanced IP-Surveillance solution. If you have already deployed CCTV, then migration to true IP surveillance is closer than you think. These options are explained below:

Scenario 1: IP cameras with NVR

The simplest, most cost effective and flexible deployment involves IP cameras (such as an Axis 211) connected to a network where video is archived using a PC running NVR software such as Aimetis Symphony™ software (see Figure 1 - cost analysis of various deployment scenarios). Remote locations can be connected via the internet without the need for a NVR in each remote location (see Figure 1 on page 3). Migration to video analytics is straightforward involving a mere software upgrade. Conversely, DVRs require expensive hardware upgrades or replacement as upgrades and integration is not easily possible with hardened solutions.

Scenario 2: CCTV cameras with video servers and NVR

You can still reap the benefits of IP-Surveillance even in cases where CCTV has been deployed. Analog cameras can be connected to a video server which enables analog video to be digitized, transmitted and viewed over an IP network. Using NVR software and video servers such as the Axis 241Q, IP cameras and analog CCTV can co-exist on one unified platform.

Scenario 3: Option 1 & 2 with integrated VCA

By leveraging the flexibility of a NVR platform, Video Content Analysis can be utilized on a per camera basis only when needed. One unified NVR platform can be used for video playback and archiving, such as Aimetis Symphony™ software. VCA can be integrated on the fly by performing a mere software upgrade giving IT professionals maximum flexibility and scalability. Using an advanced NVR such as Aimetis Symphony™ software with IP cameras and video servers allows users to migrate to intelligent IP surveillance over time, without replacing your CCTV investment. In this scenario you configure your network as in Scenarios 1 and 2, and perform software upgrades for VCA on a per camera basis as required.

Cost analysis of various deployment scenarios

Below is a summary of the total cost for the entire life time of the solutions (assuming 32 cameras). Table 3 represents the 5-year Pro Forma cost sheet for an IP-Surveillance solution using Aimetis Symphony™ software as the NVR and IP cameras. Table 4 represents the DVR/CCTV solution for the same categories. It is diffiult to provide exact savings because there are many variables involved, ranging from level of features and management required as well as expertise of existing staff. However, it is possible to calcuate an approximate value based on commonly desired features and some assumptions about some fixed variables.

5-Year Pro Forma Cost Sheet - NVR Solution					
Cost Category	Year 1	Year 2	Year 3	Year 4	Year 5
NVR	4,200	0	0	1,240	0
Cameras	10,000	0	900	1,000	1,400
Installation Labor	10,000	0	200	700	800
Installation Materials	4,500	0	0	0	0
Upgrades	0	0	0	2000	0
Maintenance	0	500	300	0	1500
Total Cost / Year	**$28,700**	**500**	**1,400**	**4,940**	**3,700**
Total Cost of Ownership					**$39,240**

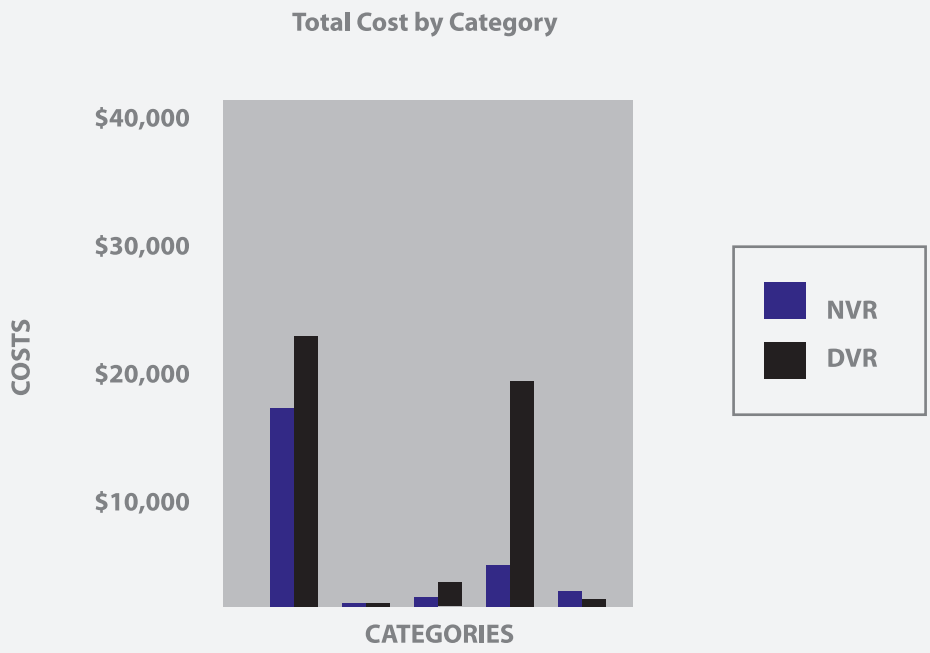
Table 3

5-Year Pro Forma Cost Sheet - DVR Solution					
Cost Category	Year 1	Year 2	Year 3	Year 4	Year 5
DVR	6,500	0	2,000	5,500	0
Cameras	9,600	0	700	1,000	500
Installation Labor	12,000	0	500	5,500	500
Installation Materials	6,500	0	0	2,000	0
Upgrades	0	0	0	6,000	0
Maintenance	0	500	400	0	500
Total Cost / Year	**$34,600**	**500**	**3,600**	**20,000**	**1,000**
Total Cost of Ownership					**$59,700**

Table 4

The figures clearly demonstrate that the DVR solution costs $20,460 more than the NVR solution. In terms of value, the NVR solution includes a digital network with megapixel cameras, while the analog deployment consists of an analog network which will require massive upgrading in the future. Note that the calculations do not take into account the "soft" costs, such as productivity enhancements of a converged NVR solution not normally available with DVR deployments. Taking productivity enhancements of a NVR solution into account would create a larger cost difference in favour of the NVR deployment which is not reflected in the numbers above.

When the categories are placed next to each other, the differences are easier to see. The graph below illustrates that the NVR solution costs less in every category over the life cycle. Figure 1 (5-Year Pro Forma Cost by Category) represents the differences by category for each solution.



CONCLUSION

The challenges in today's fast changing marketplace are putting increased pressure on IT executives who are asked to deliver rapid return on investment, reduce total cost of ownership, and limit risk on IT projects. As discussed in this White Paper, IP-Surveillance, through their use of IP cameras and Network Video Recorders (NVRs) have significant advantages over DVR deployment due to its simplified deployments, ease of integration, greater application support and longer life-cycle. Some of the key advantages IP-Surveillance holds over DVRs are summarized below:

Lower acquisition costs

NVR solutions are installed on commercial-off-the-shelf (COTS) hardware meaning time is not wasted evaluating and acquiring products from new or multiple vendors. IT executives can safely standardize and reduce the number of hardware vendors which in turn reduces maintenance and downtime.

Greater interoperability

IP-Surveillance benefits from a converged infrastructure, enabling existing IT investments to be leveraged such as cabling or database servers. DVR installations which normally include proprietary hardware and analog cameras cannot leverage existing investments and as a result are more costly to deploy.

Increased application support

Open, standards-based architectures and application programming interfaces (APIs) enable NVRs to be easily integrated with other applications allowing organizations to enjoy productivity and cost benefits of an integrated system not normally possible with DVR deployments.

Increased flexibility

NVR software such as Aimetis Symphony™ software enables analog, network and megapixel cameras to co-exist on one unified platform.

Hardware can be easily upgraded or tailored on a per solution basis. DVRs include static product specifications which cannot be easily upgraded or customized as changing business requirements emerge.

Superior multi-site capability

IP-Surveillance easily allows centralized management and storage without PC hardware required in remote locations. CCTV and DVR deployments normally require at least one DVR per location, which increases maintenance costs.

Longer life-cycle

IP-Surveillance deployments enjoy a longer lifecycle as NVR software and COTS hardware do not become obsolete as quickly as proprietary DVR products. IP-Surveillance solutions can be easily upgraded where DVR products normally require replacement. Further, as new enhancements emerge such as Video Content Analysis, software products running on COTS hardware are easily upgraded to support new applications or standards while hardened DVR products require replacement.

Video Content Analysis more accessible in NVR deployments

VCA improves the overall effectiveness of video monitoring by analyzing and filtering video and notifying personnel as required. As a result, video is more scalable, proactive and cost effective. DVR products are normally less technologically advanced and will not support VCA. More importantly, as VCA greatly improves in quality and capability, DVR deployments will continue to lag behind generation to generation.

These business benefits can ultimately increase productivity and reduce IT risk in an agile business environment making IP-Surveillance the obvious choice.

RECOMMENDED SOLUTION PROVIDER: AIMETIS

Why Aimetis?

Aimetis award winning software is an affordable, comprehensive, fully integrated network video recorder.

Aimetis Symphony™ software has evolved from Aimetis's first product which was the first integrated NVR with true VCA. This deep integration enables capabilities that are not possible with disjointed systems. The user does not have to continually juggle multiple applications. On the client side and IT professionals save on installation, maintenance and integration costs because one package from a single vendor integrates all IP and analog devices with VCA. Aimetis Symphony software offers many capabilities not found in other NVRs or DVRs alike, such as automated PTZ camera control in outdoor environments. Aimetis Symphony software integrates deeply with video servers and network cameras from all types of manufacturers and fully supports MPEG-4 or MJPEG video. Aimetis Symphony software simultaneously enables digital video recording, intelligent video analysis and remote access to live and recorded images from any networked computer. Symphony can automatically track and classify objects such as cars and people and push content to security personnel as required. Symphony is based on proprietary tracking algorithms that work in adverse weather conditions, lighting changes and shadows to isolate potential threats and limit nuisance alarms. Symphony sees instantly, filters extraneous data and delivers clear information in the blink of an eye. For more information on Aimetis Symphony software, please visit http://www.aimetis.com