How to Future-Proof Your Security Video System

Transitioning from Fixed-Life and Dead-End Video Technology to Scalable and Upgradeable Video Technology

January 2009 **(updated July 6, 2009)**

by Ray Bernard

White Paper

An Intransa *Technology Convergence Series* Paper

Table of Contents

Future Proofing

Future proofing is easy to grasp as a general concept. Wikipedia provides this definition:

> The phrase future proofing describes the elusive process of trying to anticipate future developments, so that action can be taken to minimize possible negative consequences, and to seize opportunities.

The challenge is to take that concept and determine what it means with regard to a security video system. To address that challenge this paper examines a number of technical and non-technical issues relating to video, and then provides several guidelines for future proofing both new system designs and upgrades to existing systems.

Trends

One way to get a glimpse of the future is to examine trends. Most discussions about future proofing focus on technology trends. However, it is important to incorporate four specific categories of trends that can have a significant impact on the design and planning for a security video system:

- Technology trends
- Business trends
- Risk trends
- Security practice trends

The most complex set of trends are the technology trends, because there are a number of interrelated trends whose effects compound when it comes to security systems in general and video systems in particular.

Digital vs. IP vs. Network Cameras

The preferred term for a digital security grade video camera is *network camera.* The term “digital camera” is currently used to refer to digital photo cameras, and has been used to refer to analog cameras that contain digital processing chips. Having to say “digital video camera” to maintain the distinction from other video cameras is about twice as many syllables as “network camera”. Also, technically speaking, webcams and cameras built into notebook computers are digital video cameras as well. The phrase *IP camera* doesn’t mean something to someone not familiar with the technology, but *network camera* at least instantly means “a camera that goes on a network”. Since that more plainly describes the function of the digital security video camera, this paper will use the term *network camera* unless specific emphasis on a digital aspect of the camera is intended.

Technology Trends

There are two concerns with regard to existing or planned video system technology: *obsolescence* of purchased technology and *compatibility* with future technology. It is actually not obsolescence in and of itself that is a concern, but *too-rapid an obsolescence*. The longer the life of the system or device, the higher its ROI, and the easier it is to justify its purchase. The reverse is true for a shorter life.

At one time security video system *obsolescence* and *compatibility* were not a concern, because the typical lifetime of a CCTV system was 10 to 15 years. It was expected that an entire system (cameras, video signal cables, recorders, display monitors and related equipment) would be purchased, installed and then later replaced when technology had advanced sufficiently to make replacement of the entire system worthwhile.

Computers, networks and other digital technology (including network cameras) have completely changed that situation. Today's pace of technology change would have been unthinkable 20 years ago, and the pace of technology change will only continue to accelerate.

It is both the *pace* of technology changes and the *nature* of the changes that present the primary challenge in future proofing a security video system. A look at the timeline of technologies related to security video can help. The timeline in **Table 1** below presents a number of interrelated trends.

Table 1. Time line of selected technology developments.

COLOR LEGEND			
Black	– Computer related trends	Violet	– Internet related trends
Blue	– CCTV & TV related trends	Brown	– Phone related trends
Green	– Network related rends	Orange	– Transistor related trends
Red	– Phone and Internet converge		

1942	• The first CCTV system installed by Siemens AG in Peenemünde, Germany for observing the launch of V2-rockets.
1954	• Silicon based transistors developed (as in "Silicon Valley")
1962	• 10,000 computers total exist in the world • Networking is by dial-up connection • The word "Internet" is not yet invented
1972	• The VCR – Video Cassette Recorder – is introduced
1976	• The VHS tape format is introduced
1978	• Intel introduces a chip with 29,000 transistors on it • Color CCTV cameras have been introduced
1980	• World's first gigabyte-capacity disk drive, the IBM 3380, was the size of a refrigerator, weighed 550 pounds (about 250 kg), and had a price tag of $40,000.
1983	• Ethernet networks speeds have reached 10 million bits per second • World's first hand-portable analog cell phone introduced (Motorola 8000x) weighing 1-3/4 lbs. and costing $3,995.
1984	• Motorola introduces a postage-stamp sized chip with 250,000 transistors in it • Toshiba invents flash memory. Smart phones, digital photo cameras, laptop computers and other devices all rely on flash memory.
1985	• Intel introduces a chip with 250,000 transistors in it
1986	• Standardization of SCSI disk interface (Small Computer System Interface)
1989	• Intel introduces a chip with over 1 million transistors in it
1991	• The World Wide Web concept was introduced • 2.5-inch 100 megabyte hard drive produced

COLOR LEGEND			
Black	– Computer related trends	Violet	– Internet related trends
Blue	– CCTV & TV related trends	Brown	– Phone related trends
Green	– Network related rends	Orange	– Transistor related trends
Red	– Phone and Internet converge		

1992	• The Internet has one million host computers • Computers are 100 million times faster than 1962 • Network bandwidth is 20 million times greater than 1962 • Digital telephone technology is one year old
1993	• The Web Browser will is introduced ushering an explosion of websites • Intel announces the Pentium chip with 3.1 million transistors • E-mail (introduced in the '60s) takes off with the introduction of the Web
1994	• First consumer digital photo camera introduced by Apple Computer, followed by Kodak (1995) and Canon (1996)
1995	• Ethernet network speeds reach 100 million bits per second • Intel announces the Pentium Pro chip with 5.5 million transistors
1996	• Axis Communications introduces the world's first network video camera (a color camera), also known as an IP camera or digital video camera, which contains a built-in webserver for access to live video
1997	• Business e-mail volume surpasses regular mail
1998	• Digital Video Recorders (DVR) introduced for security video • Color CCTV cameras are about 50% of camera sales
The Y2K projects of many companies included widespread upgrades and expansions to corporate networks, and the globalization of separated local area networks. Note the acceleration of network related technology development and adoption from this point on.	
1999	• Ethernet network speeds reach 1 billion bits per second • Consumer wireless networking arrives
2000	• Axis Communications introduces on-board motion detection in cameras
2001	• Axis adds camera on-board storage for pre-alarm video information • Companies – like Intransa and LeftHand – were announced to leverage the new Storage over IP network protocol introduced (iSCSI – short for "Internet SCSI")
2002	• Last year Bell South left the pay phone business due to cell phone competition • The FCC decides to shut down analog cell phone networks • Vonage launches its first service for Voice Over IP (VOIP) telephone via the Internet
2003	• Vonage completes phone call number 100 million • Serial ATA disk driver interface introduced • First iSCSI products come to market from Intransa and one other company
2004	• Cable services are adding 1,000 digital phone service customers per day (service is based upon VOIP technology) • Vantum introduces a camera with an on-board hard drive; several other manufacturers follow shortly afterwards

COLOR LEGEND			
Black	– Computer related trends	Violet	– Internet related trends
Blue	– CCTV & TV related trends	Brown	– Phone related trends
Green	– Network related rends	Orange	– Transistor related trends
Red	– Phone and Internet converge		

2005	• The one-billionth Internet user goes online • Over 10% of Japanese and South Korean subscribers have switched to digital telephone service • First 500 GB hard drive shipping (Hitachi GST)
2006	• Ethernet network speeds reach 10 billion bits per second • First 750 GB hard drive (Seagate) • Axis Communications introduces a Pan-Tilt-Zoom (PTZ) network camera with no moving parts • Axis, Verint and IOImage introduce on-board analytics in their cameras
2007	• The iPhone launches • Hitachi GST introduces 1 terabyte hard drive • AT&T announces it is exiting the pay phone business in 2008
2009	• Axis and Cisco introduce HD (High Definition) security network cameras • Full-power U.S. TV station broadcasts become digital on June 12, 2009

Digital Makes the Difference

Nearly all of the significant improvements in security systems and devices are related to transistor technology (also known as “solid state” technology) and the chip-based devices and computers it has made possible. The ubiquitous hand-held radio is a good example of two attributes of solid state technology: portability and affordability.

What has made possible the rapid pace of technology development has been the use of solid state electronics in digital devices and systems. One significant impact of digital technology with regard to video is the *ease of maintaining quality* in recording and communications.

Generally speaking, information is expressed, stored and transmitted by either analog or digital means.

Analog Systems

In analog systems the strength of the electric signals is a direct representation of the sound or image that it conveys. Quality is maintained by keeping the signal free of changes or interference. In an analog communications system, care must be taken to preserve the quality of the signal all along the data path, and for any recordings.

This is evident with video signals recorded onto VHS tapes using VCRs. As the magnetic properties of a tape grow weaker over time and with use, the ability of a tape to preserve the quality of the video image lessens. Once a VHS tape had been re-recorded about 10 times, it is no longer capable of faithfully storing a video image. Stories are plentiful (and periodically seen on the news) of retail stores who thought they had captured an incident on tape, only to discover that because of tape reuse the stored images were useless. Except for very expensive systems, taped analog data plays back

at a lower level of quality than the original recorded signal. This is why a copy of a copy of a copy of an analog video tape provides a noticeably degraded image.

Repeated playing back of an analog tape also wears it out, as many a parent has noticed when watching a child's favorite movie after a couple of dozen playbacks. Both the sound and picture are noticeably degraded.

In digital systems, the original signal strength is converted into numbers. The numbers can be stored in many forms, and when converted back into the original format (such as video or audio) provide an accurate representation of the original sound or image at the same level of quality in which it was captured. This is an over-simplification but accurately portrays the primary difference between analog and digital systems.

Digital Systems

In a digital system (audio or video) a copy of a copy of a copy is always the same series of numbers. Therefore the sound or image quality remains high no matter how many times it is copied. Thus, for example, a theater movie with a digitally recorded sound track will have a higher sound quality at the movie theater, regardless of how many times it has been copied or played. The cost to maintain high quality in digital systems is lower than the cost to maintain high quality in analog systems.

High video and audio signal levels in analog systems (electrical voltage on wires or magnetism in tapes) can be recorded in digital systems using very low power levels, because the strength of a signal is captured as a number. Thus a very low level of power can be used to record the high levels in digital systems, regardless of the strength of the original signal.

Furthermore, in digital communications such as networks, data redundancy techniques can compensate for temporary interference or momentary loss of signal. The same is true for recorded data. Data redundancy techniques are used so that physical damage to the medium on which the data is recorded will not result in loss of the data. That is how RAID (Redundant Array of Independent Disks) data storage works. Data is stored on more than one hard drive, so that if a drive fails, no data is lost.

Digital Communications Benefit from Being "Data"

In analog camera systems, unless special communications technology is used, each camera requires its own coaxial cable to be run back to the point of recording and display. Because digital video signals are encoded as network data messages, each network camera's data can be tagged with a unique ID. This allows the data from multiple cameras to be sent over a single network cable without the video images getting scrambled together. This aspect of digital video data alone can provide significant savings.

Digital Systems Benefit from Computing Advances

Another benefit of digital systems is that they can continue to take advantage of increases in computing power.

For example, digital data can be compressed by identifying number patterns in the data and representing the number patterns using a smaller set of numbers. The data is uncompressed by reversing the process (recreating the original number patterns). This

is how the commercial program WinZip® works, and is the way that some types of video compression work. Obviously it takes time to study the data, identify the number patterns, and perform the substitution. As computers have become faster, more advanced methods of compression have been implemented that would have simply taken too much time on an earlier generation of computers. There are both lossless and lossy compression schemes. Lossy schemes average numbers or use other techniques that throw away some of the original information. Lossless schemes do not lose any information.

Today's PCs can process data 60,000 times faster than a PC of 1983. Today's Ethernet networks can send data 1,000 faster than the original Ethernet business networks of 1983. Computer processing that would have taken an hour in 1983 can be performed in under a 10^{th} of a second today. A file that would have taken an hour to transmit between computers in the same room in 1983 would take under four seconds to transmit using today's latest network technology.

It is the increases in computing power and network speed that help make new technologies like network telephones possible, and make it feasible to send high resolution video data over a network. This makes it possible to favor lossless schemes over lossy schemes where the detailed information in the video picture is important.

Today's digital video camera is basically a "computer with a lens". Digital video camera technology continues to evolve as computing and networking capabilities evolve.

It is important to realize that in the past, compromises were made with regard to video quality to make systems affordable. Today, the rapid pace of technology development, accompanied by the periodic reduction in the cost of technology, makes it more important than ever not to compromise the quality of video information. Strategies to avoid such compromise will be presented later in this paper.

Computing and Network Trends Impact on Video Decisions

Intel's mandate from Andy Grove, when he was CEO and Chairman, was to "double machine performance at every price point every year". Thousands of companies in the IT domain are working to accomplish such advances, or to take advantage of them with new technologies.

With the IT industry, three computer and network trends have been identified:

- **Moore's Law:** "Processing powers doubles about every 2 years while prices are halved."
- **Gilder's Law:** "Network bandwidth doubles every six months."
- **Less's Law:** "The cost of storage is falling by half every 12 months, while capacity doubles."

This is good news for security video technology, whose continued advancement depends upon all three trends. However, this raises an important question. When technology capabilities continue to increase at an accelerating rate, does that mean that security practitioners face shorter and shorter "rip and replace" cycles? The answer is "No", thanks to two things that work together to extend the working life of systems and equipment: *standards* and *software/firmware upgrades*. The ability of a product, such as

a video camera, to have its firmware code upgraded means that as standards continue to develop the product can be kept current with regard to network and video technology developments.

Not all products will be designed to be upgradeable, and some products will have more limited upgrade capabilities than others. This is a point of research when considering and comparing products. The general trend will be for increasing upgrade capabilities, as the physical security industry adopts IT industry successful practices.

Standards

The explosion in digital technology development is made possible by standards. For example, the iPod and iPhone are products that both leverage existing standards. The result is that customers didn't have to throw their MP3 music collections away when these devices hit the market.

Unfortunately, many companies in the physical security industry built their business models on "customer lock-in" based upon proprietary technologies. It is difficult for such companies to embrace standards fully, and some companies are still struggling with this issue today. This has caused IT companies, like Cisco Systems, to view this as a business opportunity and to enter the physical security market.

At the same time the Security Industry Association (SIA) has accelerated its standards-building efforts. Thus the trend within the industry is for increased development of standards that enable interoperability among products and systems.

Video-Related Standards

Here are some of the standards that security video system deployments can benefit from:

- Power over Ethernet (PoE)
- Simple Network Management Protocol (SNMP)
- Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP)
- Motion JPEG, MPEG-4, and H.264 / MPEG-4 Part 10 (video compression standards)
- For cameras with audio: G.711 PCM 64kbit/s, 726 ADPCM 32 or 24 kbit/s
- Image resolutions: QCIF, CIF, 2CIF, 4CIF, VGA, SVGA, and higher (see Figure 1 below)
- Networking protocols: 802.3af, TCP, IPv4/v6, HTTP, HTTPS, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, ICMP DHCP, UPnP, Bonjour, ARP, DNS, DynDNS, SOCKS
- SSL/TLS (Secure Sockets Layer and Transport Layer Security – security over the Internet)
- Network Quality of Service (QOS)
- VLAN (Virtual LAN) – a means of segregating security video traffic to reduce its burden on the network

- iSCSI (pronounced “eye-skuzzy” – a protocol for high-performance network-based data storage)

A complete discussion of standards is outside the scope of this paper. However, there are some important points worth mentioning about standards. Standards can be implemented in part or in full. This is not as clear-cut as it may seem, because video standards such as H.264 are intended to cover a wide range of implementations, and so are not likely to ever be implemented in full for a single system or device. *This means that it is important to understand how a vendor has implemented standards support in a product.*

Interlaced vs. Progressive Scanning

As the importance of security video increases, and as the uses for video expand within organizations, the quality of the video images becomes increasingly important—especially for recorded video. One very important aspect relating to video quality has to do with the type of image scanning performed by the camera. There are two types of scanning: interlaced and progressive.

Here is a very good explanation provided by Hal Landen on VideoUniversity.com[1].

Interlaced Scanning

In the U.S., the video picture is composed of 525 horizontal lines. These lines are created by a beam of electrons that write the lines one at a time on a picture tube. When the beam has sprayed 525 of the lines, the viewer sees one still frame of a video picture. The illusion of motion is then created by repeating this process 30 times each second. Each of the 30 frames is a still image, but each shows a progressively different stage of the motion.

It's really like watching a slide show in fast motion. You're seeing 30 stills every second, but they blur together in your mind's eye to produce the illusion of motion. This little trick is called "persistence of vision." Without it, neither motion pictures nor video would exist.

The scanning electron beam starts at the top left of the picture tube and writes one horizontal line. Then when it reaches the right hand side of the picture or raster area, the beam drops down and writes the next line from left to right. In the early television systems, this process of writing 525 lines for each frame created noticeable flickering. To minimize the flicker, engineers developed a system of "interlaced scanning."

The interlace system divides each frame into two separate fields each with half of the picture information for a total of 525 lines of picture information. The first field contains all odd- numbered lines #1, #3, and so on. The second field contains the even numbered fields #2, #4, etc.

After field one is scanned for all the odd-numbered lines, a vertical synchronization pulse returns the camera’s electron beam to the top center of the picture tube and then scans all of the even numbered lines. Each of the 30

[1] http://www.videouniversity.com/engineer.htm

frames of a video picture includes these two interlaced fields so the actual scanning rate is 60 fields per second.

Progressive Scanning

Progressive scanning is the scanning of each TV line in sequence, instead of scanning every other line. In the past year discussions and misunderstandings about interlaced vs. progressive scanning have increased due to the introduction of HDTV and 1080i (interlaced) and 1080p (progressive) video. The issues around 1080i and 1080p for home entertainment systems are not the same issues as for security video systems.

Home Entertainment Systems

The number 1080 refers to the number of display lines in the HDTV screen. That's twice as many lines as in a standard TV screen. Movies and most television shows are recorded at 24 video frames per second. HDTV movies are 24 fps. Nearly all television set screens are refreshed (redrawn) 60 times per second. (This is due to the fact that U.S. power system is an alternating current system that cycles [alternates] 60 times per second. Thus it is called 60-cycle AC.)

There is a mismatch between the 24 frames per second display of HDTV and the 60 frames per second refresh rate of televisions. Thus most HDTV sets have a scheme of copying each frame 2 or 3 times to generate 60 frames out of 24 frames. This is part of the processing of HDTV video and has nothing to do whether the video signal is interlaced (1080i) or progressive (1080p).

Some DVD players output a 1080i signal and some a 1080p signal. However, most HDTVs turned 1080i into 1080p by processing the signal before it is displayed. This occurs along with the processing to turn each set of 24 frames into 60 frames. Thus "interlaced vs. progressive" is really not much of an issue with regard to HDTVs and home entertainment systems.

Security Video Systems

With security video the difference between interlaced and progressive signals is much more important, because the quality of individual images can be critical for investigative or evidentiary purposes.

Security video cameras capture the video image at 60 or 30 frames per second, and provide a video signal that is 60, 30, 15 or 7.5 frames per second (for example) according to how the camera settings are set. Analog cameras provide an interlaced scan signal, while many network cameras provide a progressive scan signal. The difference is shown in **Table 2** and **Table 3** using images provided by Axis Communications. Some of the images in **Table 2** and **Table 3** are the result of "line doubling", a technique used by some DVRs to increase the size of the recorded image from analog cameras.

(In the images in **Table 2** and **Table 3**, the cameras have been using the same lens. The car has been driven at 15 mph using cruise control.)

Video image resolution is described in pixels (picture elements), which are the individual dots of information that make up an image. Image resolution determines how much

detail a digital image can hold. The greater the resolution, the greater the level of detail is in the video image. Video image resolution is specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g. 320x240. In the U.S. the CIF (Common Intermediate Format) resolution is 352x240 pixels, and 2CIF is 704 by 240. Line doubling is the technique of duplicating each line of a 704 by 240 image to obtain an image that is 704 x 480. See **Figure 1**.

Table 2. Progressive vs. Interlaced Images

Progressive Scan	Interlaced Scan	2CIF with Line Doubling
Used in: Some Network Cameras	Used in: Analog CCTV Cameras	Used in: DVRs
		

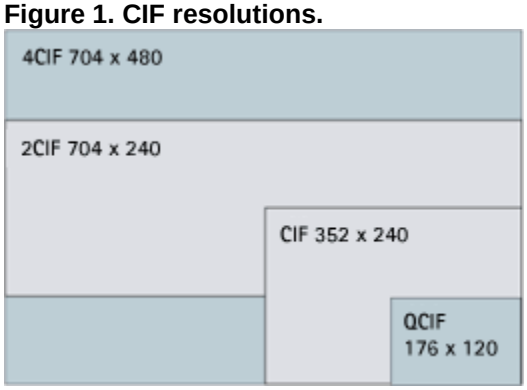
Table 3. Details of Progressive and Interlaced Scan Images

Progressive Scan Details	Interlaced Scan Details	2CIF Details
		
		
		

Many DVRs cannot record images at the same quality produced by the camera. It is common to find analog cameras providing a 704 x 480 image that is recorded at 352 x 240 in the DVR, which is one-quarter of the detail available in the original image.

Today's network cameras are not bound by the limitations that analog cameras were subject to. That means cameras and recording resolution levels can be set according to the organization's needs, not technological limitations.

Figure 1. CIF resolutions.



(image provided by Axis Communications)

When considering the upgrade of an existing system, it is important to determine where any compromises exist. Some security practitioners have replaced cameras when in fact it was the recording system that was limiting the resolution, not the cameras.

IT Involvement

One very big difference between past, current and future security technology is the increasing level of IT department involvement. It is typical for security system projects to include collaboration with the following IT functions:

- **IT Software** (product evaluation, product configuration and support)
- **IT Computer Operations** (manage server and workstation boxes)
- **Storage Management** (for external storage for video and other security data)
- **Network Transport** (IP address management, video traffic management on backbone, Quality of Service QOS)
- **IT Procurement** (purchasing)
- **Network Design** (physical and logical, including IT department standards)
- **Computer and Network Security** (including IT department standards)
- **Business Process Analysis** for business processes of interest to security, such as the employee on-boarding and off-boarding processes of Human Resources

IT-Style Systems

Just as VCRs were replaced by DVRs, NVRs (network video recorders) are replacing DVRs. However, there is a significant difference, as most NVR systems are software applications running on typical IT servers. This type of design provides an affordable approach to system expansion that is very different from the approach to expanding

analog video systems. For analog video systems, each additional camera meant a new coax cable run, and if the camera port capacity on the DVR was filled, adding a new DVR. Systems scaled up mechanically by adding new equipment.

With the server-based NVR approach, expansion means connecting a new camera to an existing network, and perhaps adding an additional camera port card to the server computer.

DVRs usually have a limit of 10 simultaneous connections (i.e. ten people can access video at one time), and in practice actual performance limits the connections to fewer than 10. With a server-based NVR, the number of network connections is usually limited only by the bandwidth of the network, which can be expanded as the situation warrants.

Storage capacity in DVRs is fixed, while NVR systems can use IT-style external data storage systems of the type used in IT data centers. Storage can be expanded independently of the NVR. This is important because as the cost of computers and hard drives continues to fall, while their performance and capacities continue to increase, each system expansion will cost less than the previous one. This requires some different thinking than previous system expansion planning.

Additionally NVRs capabilities can be kept on a par with the capabilities of high-resolution cameras through software upgrades.

Product-Related Risks

There are three product-related risks that have developed as the physical security industry moves to network-based products. One is that IT companies are introducing physical security products, especially cameras, without having an understanding of the field requirements for such devices, and without understanding the application requirements related to their devices. Their strategy is price-based, to enter the market as a low-price leader. At a trade show not long ago, a sales person from one such company said, “Basically IP cameras are the same. Lens, sensor, processor, and network connection.” When asked about the support for SNMP, the reply was, “Yes”. But there was nothing in the literature about that. No IT group worth its salt would allow such a device on the corporate network.

Another risk is the use of “generic” IT products in security applications, where the security applications have different requirements than the IT applications do. For example, one IT storage company’s product was found to be subject to file fragmentation. When used in security applications, the performance of the product would grow worse over time. The overhead of using a disk defragmenter application detracts from system performance, and is not an option. In contrast, the Security Grade Video Storage system from Intransa is designed for security video applications, in which there is constant high-volume recording which must remain at peak performance levels, and then occasional spikes of video playback for review.

A third risk comes from incumbent security industry companies, who convert or upgrade their products to make them network-enabled, but still deploy a proprietary customer-lock-in strategy. One example is having cameras that work only with the company’s own video management system software. Such companies have a history of becoming

complacent with regard to product design, due to the customer lock-in factor, and the customer's system doesn't stay on a par with the technological advances in the industry.

IP Video System Scale Has Multiple Dimensions

Previously, the main concern for video system scaling was the question, "Can this system support the number of cameras that I will eventually require." With analog systems, scaling up meant the addition of equipment and coaxial cable to connect to the single point of monitoring and recording. Analog camera systems with DVRs and management software applications would generally have a limit of about 10 simultaneous users viewing video recorded on the same DVR. Other limits existed for viewing across a corporate network, some based upon network limitations, and some based upon video system limitations. There weren't many options with regard to increased scale of video use. Many systems were by default already scaled down in terms of video resolution due to expected bandwidth limitations. For most systems, increased quality of recorded video meant reduced retention period for video storage.

As described earlier in the section titled, "Computing and Network Trends Impact on Video Decisions", network and storage capacities continue to expand while their costs continue to shrink. At the same time video quality continues to improve. Depending upon the architecture of the video system and security requirements, at one time or another a system and its components will have to scale up in one or more of the following ways:

- Number of Cameras
- Quality of Live and Recorded Video Image (resolution and frame rate)
- Storage Capacity (# days of video at required quality)
- Number of persons who can simultaneously access live and recorded video
- Number of video analytics algorithms that can be run in-camera and on servers
- Number of systems to which the video system will be interfaced

As various aspects of the system scale up, the performance of different parts of the system must increase. For example, increasing the frame rate of existing cameras from 7 frames per second (fps) to 15 fps doubles the amount of video data being transmitted over cables or the network and recorded. *Data throughput* is the term for the amount of data that can go in and out of a system.

DVRs are fixed in terms of their data throughput—the total number of frames per second that they can handle overall—which must be divided among the cameras that are connected. IT-style storage usually, but not always, allows scaling up of the *data throughput capacity* of the storage system. It is important to find out how the data throughput of the storage system can scale up, and what its upper limitations are.

Lifecycle Planning

Instead of planning periodic wholesale "rip and replace" upgrades, the appropriate and much more cost effective approach is to follow the IT practice of system and product lifecycle planning. This is a long term perspective in which technology trends are considered in planning. As video systems grow, the server computer can be replaced by a less costly computer that is twice as fast, and other elements of the system can be

addressed individually depending upon their role in the system. As storage hard drives near their end of life, instead of waiting for them to fail, they are replaced with higher-capacity but less expensive drives. This reduces the security risks attendant with product failures, which typically seem to happen at the most inopportune times.

Video Monitors vs. Video Applications

The more things a video surveillance system can do, the higher the ROI. That's one of the very big differences between traditional analog video monitoring systems and today's digital video systems. Networked video allows sharing video information with other business functions. For example, the real estate group can be provided with secure video access to allow them to watch activities at a construction site via a networked video system, saving many time-consuming trips. Additionally, behavior when management is not on site is often not the same as when visiting management personnel are present. With old-style analog systems, the cost of dedicated display monitors and hard-wired video feeds made that kind of video sharing cost-prohibitive.

A retail application is the LaneHawk system by Evolution Robotics (www.evolution.com) that uses patented technology (visual pattern recognition) for object recognition, and automatically detects and identifies specific items on the bottom of the cart from a predefined list of items for the store. A smart camera is flush-mounted in the checkout lane, continuously watching for items. When an item is detected and recognized, its product code information is sent directly through an Ethernet network connection to the Point of Sale system. The cashier verifies the quantity of items that were found under the basket, and continues to close the transaction. Evolution Robotics estimates that losing as little as little at $10 per lane per day in a typical store represents $50,000 of annual lost revenue. This type of application is something that cannot be performed by human monitoring alone. It requires high resolution digital video cameras and computing power.

General Expectations

The general expectations surrounding video systems are increasing for the general public, based upon what is seen in movies and on TV. That includes management personnel. People in general are more open to advanced technology, and devices like the iPhone make a statement that the cost of advanced technology is not excessive. This contributes to the establishment of a climate favorable to new technology deployment.

Technology Decisions

As the examples above illustrate, decisions about video technology should not be based solely upon the technology elements and their security implications, but should also take into account business trends, security practice trends, and risk trends for the organization.

Business Trends

The affordability and networkability of digital video technology has generated a number of business trends including the use of video for non-security purposes like these:

- Manufacturing quality control monitoring
- Employee training and follow-up (applies to many business sectors)

- Marketing assessments of traffic patterns in stores
- Warehouse management and supervision
- Lean Manufacturing support (by reducing legwork and providing close supervision of the results of Lean initiatives)
- Train yard management
- Train station customer service (via two-way audio on cameras)

Implementing these kinds of applications doesn't happen overnight. It often takes a change to business processes to realize the full benefits. That means thorough up-front planning with the non-security stakeholders, and a realistic time frame for preparation and deployment.

An advantage of finding non-security applications is that it can open up new sources of funding from the business units that will benefit.

Risk Trends

Security Risks

Internal and external security risk trends should be taken into account. For example, one high-tech company launched a campaign to acquire as many high-tech startups as it could with related products. Many of the startups had positioned themselves as "enemies" to the company, and had made their success out of being a viable small-company alternative to the big company. The acquisitions strategy included the plan to let go about half of the employees of the acquired companies after acquisition. The plan was to "fast track" the integration of the newly acquired companied. Insufficient consideration had been given to the increasing risk from insider threat to existing intellectual property in both physical and electronic form prior to and after the migration. Most of the acquired companies had poor physical security of critical information areas, and of their networks equipment rooms. Although security risk had skyrocketed during this acquisition campaign, little thought had been given to the increased risks in the facilities of the acquired companies. Because the acquisitions were all high-tech companies with completely networked facilities, network cameras could have easily been placed strategically, along with reader-controlled access to critical areas, using IP-based systems.

An increase in parking lot prowlers may call for higher-resolution cameras, so that identifying characteristics and license plates can be more clearly captured.

Technology Risks

A significant and nearly universal risk trend is the collection of increased risks associated with placing physical security systems on corporate networks. There are two categories of risks: risks to the corporate networks and the data on them, and risks to the security systems themselves from implementations that don't meet IT's security standards.

Because the physical security industry had little or no knowledge of the risks and challenges inherent in large-scale networked information systems, traditional security systems were "converted" to IP-enabled systems without accounting for the security risks and networked device management challenges.

The security industry's failure to address the network security risks has put both the security systems and the corporate information systems at risk when security systems are connected to the corporate network. Additionally, failing to address the *networked device management challenges* creates problems for the IT department personnel who manage the corporate network.

One of the first groups to recognize and begin addressing these convergence risks is the Alliance for Enterprise Security Risk Management. AESRM (www.aesrm.org) is a coalition formed in February 2005 by three leading international security organizations: ASIS International (ASIS), Information Systems Security Association (ISSA) and ISACA. AESRM was created to address the integration of traditional and information security functions and to encourage board-level and senior executive-level attention to critical security-related issues and the need for a comprehensive approach to protect the enterprise.

Fortunately, dozens of companies have begun addressing the risks involved, and many of their lessons learned have been captured in a 32-page report by AESRM titled, *Convergent Security Risks in Physical Security Systems and IT Infrastructures*, downloadable from the AESRM website www.aesrm.org). The report identifies seven major security concerns based upon real-life examples of risks from organizations deploying electronic physical security systems on their corporate networks.

The report states, "Increasingly, as a means of reducing costs, increasing efficiencies or making better use of technology investments, organizations are integrating physical security devices for access control, monitoring and process control into the IT infrastructure. This collision of two different technology worlds, each coming from a separate management approach and protection philosophy, does not always come together easily. The differences in design, functionality, implementation, maintenance and management can present conflicts, possibly resulting in a security breach involving the IT systems, the security systems or both."

For example, in analog camera systems cutting a camera's coax cable will cut off the signal from that one camera. With networked video, cutting a network cable can cut off the signal from many cameras. Additionally, the failure of a network component that takes out a portion of the network may also cut off camera recording or access to video from certain locations in the organization. This is why for critical systems IT uses redundant networking approaches. For networked security systems, IT's approaches must be learned and applied.

Beyond addressing the risks involved, there is also tremendous business value in physical security collaborating with IT to ensure that all the benefits from physical security technology are available to the organization. An added bonus is that the knowledge gained can be used to enhance the physical security of the corporate network infrastructure. It's a win-win situation for physical security and IT when organization-specific strategies are put in place to manage physical security/IT convergence.

Security Practice Trends

Security practice trends in your business sector, relating to the use of video, may be more applicable now that the price of very high quality video is coming into affordable

price ranges. Megapixel cameras can strategically replace older cameras where high resolution images are important.

At one airport in a major entertainment center, several video initiatives placed a high number of cameras throughout the retail areas, and at the security checkpoints. With high quality video in use, the airport achieved a “100% prosecution rate” of criminal offenders because the video evidence was too strong to refute. Every suspect caught red-handed immediately opted for a plea bargain, after viewing his or her own actions clearly on video. When last reported on, their 100% plea bargain rate was still intact after four years.

An emerging practice is the upgrading of existing DVRs using network-based storage, to eliminate hard drive failure and increase video retention capability. This usually requires the addition of two high-speed (1 Gigabit) network cards to each DVR along with an iSCSI driver from Microsoft. One New Jersey manufacturing plant affordably doubled their video retention period by adding an iSCSI Video SAN (Storage Area Network) from Intransa. At the same time this eliminated the risk of hard drive failure. The Intransa storage uses hard drive and component redundancy to allow the storage system to keep on receiving and playing back video, even if a power supply, hard drive or other component fails.

Moving to an IP video system on a large scale is not a short-term initiative. For security practitioners with regional, national or global technology responsibilities strategic partnering with selected vendors and with a security systems integrator well-experienced in digital video deployments can provide strong allies who will dedicate themselves to understanding security objectives, the current security picture, and help develop and then execute on long term technology plans.

Many practitioners are sharing their successes, including the ROI in formation from their projects. They are also sharing how they collaborated with their IT departments, which is another growing security trend. Information on such projects can be found in security publications and is often captured for presentation in security association workshops.

Guidelines and Recommendations for Future Proofing

The following guidelines and recommendations take into account the trends described above. Many of these recommendations are preparatory steps, with little cost or effort involved. One good approach is to find a step that you feel comfortable with, and take it. Then find the next step, and so on.

Future proofing your systems means not just future-proofing in terms of future compatibility with technology, but also compatibility with your company’s current and future IT initiatives and future security needs.

Future proofing will also involve compliance with corporate IT standards and best practices, and compatibility with the company’s future needs for video security applications outside of the Security department.

Apply these guidelines and recommendations as appropriate at the facility level and at corporate headquarters.

IT Collaboration

1. **Initiate an ongoing collaboration with IT, instead of approaching IT on a project-by-project basis.** The following references will be helpful.
   - "Ten Rules for Putting Your Physical Security Systems onto the Network"
     for physical/corporate security departments
     http://www.intransa.com/solutions/techdoc.php?src=22

   - "Twelve Ways to Address the Risks from Putting Physical Security Systems On Your Network"
     for IT departments
     http://www.intransa.com/solutions/techdoc.php?src=21

   Both papers can be downloaded from either link.

2. **Get up to speed on network issues relating to security video.** An outstanding recorded webinar on this subject was developed by Cisco:

   Traffic Engineering for IP Video Surveillance
   By Robert Sayle, Cisco Systems, Inc.
   March 28, 2007
   http://www.isc365.com/webinar/Traffic_Engineering.aspx

   Share this webinar with your IT network design folks.

3. **If your company has an IT Voice over IP (VOIP) initiative, learn about it and its timetable for upgrading the corporate network.** Most VOIP equipment contains video support and Quality of Service support that is appropriate for security video.

4. **Identify the corporate IT standards that apply to security systems placed on the network.** There will probably be standards for the following items: servers; *Power over Ethernet (POE)* enabled network equipment; LAN and Virtual LAN configurations, and computer and network security such as anti-virus.

5. **Learn how IT calculates Total Cost of Ownership (TCO)** for its systems and takes into account system and component lifecycle planning.

Upgrading

6. **Prior to upgrading, perform a camera audit of your current cameras.**

   Data Capture Phase
   Update or create the following information for each of your cameras:
   - Camera Number (arbitrary number assigned to facilitate camera management)
   - Camera Make

- Camera Model
- Resolution (such as 648 x 480)
- Frame Rate (such as 15 fps)
- Owner (meaning the manager responsible for assets in the area)
- Critical Assets Covered
- Camera Current or New Security Objective (intended purpose or use)
- Camera Current or New Other Objective (other intended purpose or use)
- Quality Sufficient for Security Investigations (yes or no)
- Quality Sufficient for Other Investigations (yes or no – and what kind)
- Quality Sufficient for Forensics Use of Video (yes or no)
- On-Board Motion Detection Capable (yes or no)
- On-Board Motion Detection Enabled (yes or no)
- On-Board Analytics Capable (yes or no)
- On-Board Analytics Enabled (yes or no)
- Camera Location
- Camera View Description
- Camera View Acceptable to Security? (yes or no)
- Camera View Acceptable for other Purposes (such as training, supervision, quality control, etc.) (yes or no – bring owners into command post to observe camera views)
- Light reading on floor or ground in center of camera view (for PTZ: home position, best case and worst case lighting)
- Does light reading meet minimum standard recommended in the lighting tables of the U.S. Army Field Manual 19-30 (recommended by ASIS and NFPA)? (yes or no)
- PTZ or Still?
- (For PTZ) Has Presets Functionality (yes or no)
- (For PTZ) Presets Used Manually (yes or no)
- (For PTZ) Presets Used in Automation (yes or no)
- Display Call-Up Integrated for Alarm Events (yes or no)
- Display Call-Up Integrated with Access System Events (yes or no)
- Date camera reviewed (sometimes the audit can take a week or more if there are a lot of cameras and only an hour or two to perform the evaluation)

Add whatever other information you want to track for each camera.

Download the *U.S. Army Field Manual 19-30 – Physical Security* from:
http://www.enlisted.info/field-manuals/fm-19-30-physical-security.shtml

Data Evaluation Phase
Review the data and fill in the following information

- Change resolution to (new resolution or “no change”)
- Change Frame Rate to (new frame rate or “no change”)
- Owner (meaning the manager responsible for assets in the area)
- Enable On-Board Motion Detection (yes or no – will require new camera if not motion capable)
- Enable On-Board Analytics (yes or no – will require new camera if not motion capable)
- New Camera Location
- New Camera View Description
- New Lighting Recommendation
- Reason for New Camera View
- Change to PTZ or Still
- (For PTZ) Enable Presets Functionality (yes or no)
- (For PTZ) Enable Presets Use Manually (yes or no)
- (For PTZ) Enable Presets Use in Automation (yes or no)
- Enable Display Call-Up Integrated for Alarm Events (yes or no)
- Enable Display Call-Up Integrated with Access System Events (yes or no)
- Date camera evaluated
- Additional Comments from Security
- Additional Comments from Area Owner
- Additional Comments from Other Stakeholders

While it is possible to manage such information in a spreadsheet, it is generally much better to use a database application such as *Office*® *Access*® or *Visual FoxPro*® from Microsoft®, *Lotus*® *Approach*® from IBM®, or whatever your company typically uses to manage data of this size and scope. One of the low-cost online database services is another option.

Don’t skip this step just because you plan a wholesale replacement. Having this information on hand will be of tremendous value for the upcoming design effort.

For guidance regarding evaluation of camera image quality, use the following tools from Axis Communications:

Video IQ (Image Quality) Tool

http://www.axis.com/edu/

Camera Reach Tool

http://www.axis.com/edu/cam_reach/

7. **If your security video system—including cameras—is very old and not sufficient for security's current needs,** consider the creation of a new security video network backbone and the replacement of old analog cameras with a 100% IP-based solution.

8. **If you have analog cameras that do fulfill their security requirements in terms of image quality,** consider developing a hybrid system that supports both analog cameras (there are IP encoders for them) and network cameras. There are one or two NVR software applications that can integrate with several main-brand DVRs (such as Cameleon from 360 Surveillance in Vancouver). As NVR capabilities are always improving, it's worth checking out the current offerings with regard to this capability.

   It is also worth repeating that many DVRs do not record at the full resolution the camera is capable of. Many DVR manufacturers have software upgrades that bring the DVR capabilities up to match those of most analog cameras.

   Megapixel cameras are another story because they usually exceed the capacity of existing DVRs, but that is a moot point since they are network cameras, and their signals will be going straight into the NVR application for recording.

Business Trends

9. **Research business trends in your business sector.**
   - Determine if any of them apply to your company.
   - Determine if any of them can benefit from the application of video.

Risk Trends

10. **Purchase current and recent-year CAP Index reports** (Crimes Against Persons and Property) on www.CAPIndex.com, to identify any environmental crime risk trends.

11. **Perform or update existing site security assessments.** ASIS provides a free *General Security Risk Assessment Guideline* at: http://www.asisonline.org/guidelines/inprogress_published.htm

12. **Find out what changes management has in store for the business for the next 3 to 5 years.** Determine what security implications the changes may have.

Security Trends

13. **Command and Control.** Determine the benefits to your local, regional, national and global security operations monitoring for a command and control application, such as *Surveillint* by Proximex (www.Proximex.com) that provides situation management capabilities including rules-based workflow and distribution of video to field personnel, and which can automatically build case files with video clips of

the alarm areas, and so on.

For broad look at security operations center design, see this online article on SecurityInfoWatch.com:

Security Operations Center Design
Examining the key design elements in a successful SOC implementation
(Originally published in the January 2008 issue of *Security Technology & Design* magazine)
http://www.securityinfowatch.com/print/Security-Technology-and-Design/Features/Security-Operations-Center-Design/13943SIW2

This article contains a list over a dozen standards and design references for a security operations center.

14. **Operations Review.** Implementing advanced technology without changing operations procedures will deny many of the benefits of the technology. Make sure to examine the potential improvements in operations that can result from deploying advanced security technology.

15. **Total Cost of Ownership.** The TCO from many new technologies is lower than for older technologies, especially when the appropriate operations changes are made. Compare the TCO from the previous system with the TCO from the new system, taking into account the full lifecycle of the system and its components.

16. **Reference Sites.** Find companies who have implemented the kind of video system that you would like to have, and arrange a tour of their security operations.

About Ray Bernard

Ray Bernard, a security industry analyst, journalist and author is also President of Ray Bernard Consulting Services (www.go-rbcs.com), a security management and technology consulting firm. Bernard has provided pivotal direction and advice to the security industry (manufacturers and service providers) and to the security profession (security management) for over 20 years. Bernard was named as one of security's *Top 10 Movers and Shakers of 2006* by *Security Technology & Design* magazine.

Bernard is also founder and publisher of *The Security Minute* electronic newsletter (www.TheSecurityMinute.com), the first newsletter for security practitioners and management security stakeholders—the people involved in making or approving security decisions, policies, plans and expenditures.

Bernard writes a monthly column called 'Convergence Q&A" for *Security Technology & Design* magazine, as well as six feature articles per year around key convergence issues. Bernard is also a contributing editor to *The Encyclopedia of Security Management*, 2nd Edition, for its security convergence subject entries.

Bernard is Board Certified as a *Physical Security Professional* (PSP) by ASIS International; Board Certified in Homeland Security (Level III) by the American College of Forensic Examiners International (ACFEI); active council member of the ASIS IT Security Council and the ASIS Physical Security Council; Bernard is also a supporting member of the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the IEEE Computer Society.

About Intransa

Intransa, Inc. is the leading innovator of simple, green Video Data Management and Retention (VDMR) platforms for future-proof, affordable solutions to physical security requirements and delivering advanced video surveillance-specific appliances.

The Intransa VideoAppliance™ family comes ready-to-run, eliminating the complexity, cost and ongoing support challenge of integrating commodity hardware with video management systems. Each appliance comes preloaded with the choice of leading video management system, including those from Exacq Technologies, Genetec, JDS Digital Security Systems, Milestone Systems and On-Net Surveillance Systems, Inc. (OnSSI).

Intransa solutions are ideal for new IP solutions in support of cameras, open NVRs, VMS and PSIM systems, or to upgrade and extend the life of existing CCTV DVRs, improving video retention capacity and quality while eliminating the risk of lost recordings. All of our scalable and modular solutions cut electrical, heating and cooling consumption, shrink the amount of rack space and equipment needed, and reduce the purchase and operational cost of physical security systems.

Launched as a spin-off from Fortune 500 member and networking pioneer 3Com, our advanced, patented technology is certified with more than 150 physical security, imaging and technology products by the StorAlliance Technology Labs. Alliance products include

DVRs, NVRs, video management systems, IP and megapixel surveillance cameras, physical security information managers, infrastructure, video analytics, utilities, authentication, access control, imaging, and biometrics.

Intransa supports industry standards and green technology, and are members of the Security Industry Association, the American Correctional Association, the National Retail Federation, the Green Grid consortium for advancing energy efficiency in computing ecosystems, and the Storage Networking Industry Association and its Green Storage Initiative. Intransa employees are also supporters and members of the American Society of Industrial Security (ASIS) International and the ASIS Physical Security Council.

Since 2003, Intransa solutions have benefited customers worldwide in an ever growing mix of hotels and casinos, correctional facilities, police departments and law enforcement agencies, financial institutions and insurance providers, airports, hospitals and medical centers, managed service providers, telecommunications vendors, retailers and shopping centers, auto dealers, transit authorities, ports and shipping hubs, pharmaceutical makers, Native American organizations, colleges, universities and school districts, digital entertainment providers, energy, utilities and resources companies, and a wide variety of government users.

For more information about Intransa, to locate an authorized dealer or integrator offering Intransa solutions, or to join the StorAlliance, please visit us at www.intransa.com or www.videoappliance.com.

Intransa, Inc. Corporate Headquarters, 2870 Zanker Road, Suite 200, San Jose, CA 95134-2114
t: 408.678.8600 • 1.866.446.8726 • f: 408.678.8800 • www.intransa.com