

**Infinova<sup>®</sup>**



White Paper

## Should You Jump to IP?

A commonsense guide for chief security officers (CSOs), directors and managers on how to reduce costs and extend the life of existing surveillance equipment when migrating from analog to IP surveillance.

### **Should you jump to IP?**

The simple answer is YES, but in a cost-managed way that extends the life of existing equipment. You and your colleagues know you'll migrate to IP but the challenge is in how to do it. Of course, the jump – how quickly, how far – all depends on your specifics. For most sites, this migration will take place gradually; and, during the process, analog and IP solutions will coexist, in some cases for many years to come.

Let's tag along with CSO Terry Jones and Helena Smith his second-in-command, who work for a mid-sized enterprise, as they start to answer the question: Should I jump to IP?

### **Systematic Approach**

The duo, in the profession for a number of years, realizes that, before facing any decision that will make such an important and potentially costly change, they need to do their homework. At a brain-storming meeting, they see the need to spend time exploring the “basics” in the front-end. On the meeting room wall, three steps are posted.

- Determine what surveillance needs to do.
- Prioritize the risks and vulnerabilities of your site.
- And then select a migration strategy and technology to fit those real-life needs.

This white paper presents a guide on how to manage that migration to IP at your own pace, reduce costs and extend the life of existing surveillance equipment.

### **Author**

Mark S. Wilson  
Vice President, Marketing  
Infinova

Dazzling technology, industry buzz, information technology challenges, infrastructure needs, legacy investments, conflicting advantages and disadvantages. There are a lot of decisions to be made along the path to IP security video, including the path itself.

But at the heart of any migration plan – no matter how conservative or aggressive – the bottom line decision is a business one.

No doubt, IP security video is, sooner or later, inevitable and a good thing, too. There're better images from IP cameras and the introduction of megapixel and high definition cameras, with their advantages, demand an IP approach. In addition, there's lower installation cost for Cat 5 and 6 Ethernet cabling compared to coaxial or fiber as well as the potential of Power over Ethernet. The days of video tape storage are long gone and good riddance; storage has moved to digital. Video analytics, whether as simple as motion detection or as complex as alerting to certain types of human behavior, depend on IP video to blossom. In the command center, it's a software world where integration is the password and joysticks are being eased out thanks to ease-of-use computer mice, dropdown menus and even touch screens.

### **Attraction of Digital Video**

Global studies of purchasing trends prove the increased growth of digital video, even in a soft economy.

Digital video surveillance systems exhibit significant growth, driven by heightened public and private security concerns in addition to a technology shift, according to research firm Frost & Sullivan. The security industry is experiencing convergence as information technology slowly and gradually transitions to video services, although a complete convergence of physical and logical security – for most operations – still is many years away.

For Terry and Helena, and most security executives, migration at this time often will mean coexistence, where analog and IP exist side by side. Security systems integrators, with their own keen eyes fine-focused on IP, agree. "In the integrators' world, migration to a new technology is a gradual process. While IP-based solutions are likely to witness high growth rates over the next few years, the large installed base of analog solutions are an indication that analog will remain in existence for the foreseeable future. Both solutions are expected to coexist for many years to come, while finding applications that they are best suited for," points out Dilip Sarangan, the industry analyst, physical security, at Frost & Sullivan.

### **Driving the Advances**

In doing their homework, Terry and Helena listed seven overall drivers of digital video surveillance.

- The need for better monitored and retrieved images.
- Less expensive installation compared to traditional security video.

- IP platforms as the enterprise’s primary infrastructure.
- Video analytics.
- Homeland security.
- Integration into a complete solution (access, intrusion, ID).
- Multi-tasking into business applications beyond security and life safety.

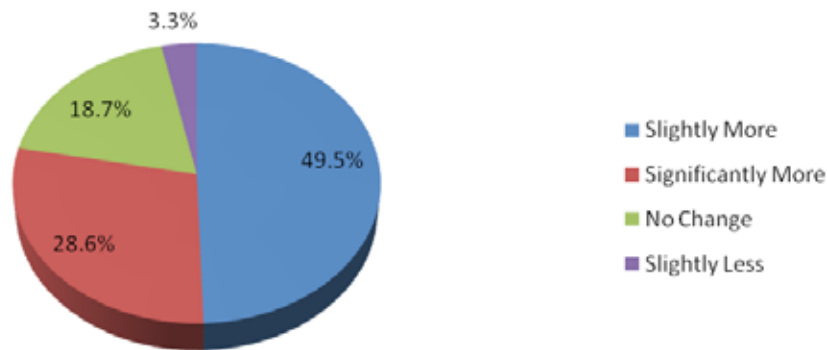
It is estimated that 80 percent of the installed base of cameras in the United States today is analog. In addition, today’s tough economic climate suggests a need to pinch those pennies, which stepped migration and coexistence can help accomplish.

**Long-term Goals, Too**

But that doesn’t remove the long-term assignment: Think strategically and plan ahead to meet growing requirements when the economy loosens the security budget or when risks overcome the cost of the new investment. In many cases, with encoders and digital recording in place and working just fine with analog cameras, it will be an exceedingly hard sell to rip it all out. And there is no need to.

One jump that’s become easier today is the security leap to sharing the enterprise’s network infrastructure. Not too long ago, Terry’s information technology (IT) colleagues lived in their own “silo,” avoiding hanging so-called outside and bandwidth-hungry applications on their net. For the most part, that attitude has diminished. Security now works more closely, ideally in partnership, with in-house IT. At times, an integrator or architect/engineering firm, coming from the security or IT side, helps bridge the gap. For instance, IT managers now are involved in almost six in every ten major decisions to purchase IP-based physical security products, according to IMS Research.

**Security System Integrators’ Dealings with IT Managers Compared with One Year Ago**



Source: IMS Research

With all the stars coming together, it's the time, at least, to fashion some level of migration path. However, there is no one-plan-fits-all solution. The commonality is coexistence in an ever-evolving plan that best serves the core business. Laid on top of that cost-managed plan, architectural/engineering design and subsequent technology selection process are critical to any successful deployment. Charting a way that legacy and new technology can live side-by-side means that video security is not simply a technical challenge, but an operational and business challenge as well.

Among key business factors that Terry and Helena consider are:

- An understanding of budget constraints and the enterprise culture.
- Recognition of the true functional requirements of the system – what you want the system to do.
- Finding ways to accomplish the most with existing infrastructure.
- Leveraging existing assets in ways that don't seem possible at first.
- Delivering needed improvements for operational functionality.

#### **Budget and Culture**

Budgets and the budget process vary among organizations. A budget is nothing more than a written estimate of how a department or business unit such as security or loss prevention will perform financially. There are various types of budgeting strategies such as top down, bottom up and zero-based.

Corporate culture is the total sum of the values, customs, traditions and meanings that make a company unique. Corporate culture is often called "the character of an organization" since it embodies the vision of the company's leaders. The values of a corporate culture influence the ethical standards within a corporation, as well as managerial behavior.

For Terry, his enterprise uses bottom up budgeting within a culture that stresses its feeling of family. So his strategy will be adjusting his new budget a bit while stressing the commitment for a safe and secure family of employees, contractors, customers and visitors.

#### **Technology's Turn**

The tech elements of coexistence may be easier to achieve, what with tech price tags loosening up. But a big jump can be complex and harrowing. Issues can range from site locations, if an existing system is proprietary, means of communications, quality of images, storage and retrieval as well as the economics of transition technology such as DVRs and encoders. Along the path, security may have to manage two systems while contending with the capital appetite (or lack) of the enterprise.

Five major system areas need to be considered.

- Cameras.
- Transmission and cabling, including power supplies.
- Storage and retrieval.
- Command and control.
- Integration.

### **Cameras**

A key consideration is whether or not the existing cameras or new ones will provide the image quality needed to achieve the functional requirements of the system – what the system should do. Different applications have different requirements; some users require the ability to see and track license plates outdoors in changing lighting conditions, while others simply need to see that a corridor is clear. The need should define the technology – not the other way around. That concept makes it obvious that in many migration plans, specific locations of greater vulnerability or image detail requirements are ideal places for IP-based cameras, including megapixels and high definition ones.

Part of a co-existence plan, analog-to-digital encoders at the camera end can transform images from an analog camera to digital transmission and storage.

### **Transmission**

Coaxial, shielded twisted pair and unshielded twisted pair cable, fiber optics and – to a lesser degree -- a variety of wireless approaches carry most security video. In an IP environment, transmission is usually over fiber, Cat 5 and Cat 6, and wireless. One strategy to handle both analog and digital networks is to transmit all the signals over a single fiber optic cable that is secure and immune to electrical or environmental interference. Installation is dramatically simplified by eliminating the need for multiple fibers, transmitters and receivers. The difference and business advantage of the various transmission schemes are in cost of installation and cost of maintenance. Not to be forgotten are power supplies. Following a co-existence plan, power supplies that are multi-tap, addressable and programmable have advantages.

### **Storage and Retrieval**

Even with their feet firmly in the analog world, Terry and Helena already have digital and network video recorders for storage and retrieval. There was no choice when moving from those Flintstone-era VCRs. At the camera edge, and catching on, are SD or secure digital storage cards, too.

DVRs, NVRs and off-shelf dedicated servers have an important role to play. But storage solutions do have their own challenges, thanks to myriad features and benefits that can range from common specs to helpful elements such as intelligent PTZ control with preset positions and e-mail or SMS message notification upon motion detection or event alerting. Some DVRs are difficult to scale.

### **Command and Control**

There is a lot to consider with command and control. Traditional matrix switching and joystick GUIs are workhorses but – in a fast-approaching software world – a solid next step for Terry’s operation and others is consideration of IP networkable video matrix switchers.

### **Integration**

True security systems integration is a goal of most security operations. Beyond relays and interfaces, seamless integration of security video with electronic access control, intrusion, perimeter and identification systems is a beneficial endpoint of any operation and one made simpler through IP.

Specific to the jump to IP, John Honovich of the Web site [www.IPVideoMarket.info](http://www.IPVideoMarket.info) and technology guru suggests Terry and Helena and others face some key areas when determining:

- If IP cameras can eliminate long distance analog cabling.
- If higher resolution cameras can help at special locations or in special applications as a stepped approach.
- The increased bandwidth impact on the enterprise’s network. This is a tricky assignment and IT can help.
- If newer types of compression, decompression or codec such as H.264 can reduce bandwidth traffic load but at a cost of more storage and command center processing, for instance.
- If and when the budget can afford increased transmission and storage for megapixel cameras.

Still, no matter the speed of the change-over, a solid plan is one in which both analog and digital, or IP, cameras can coexist.

The two reasons that this overall solution is so desirable are common to most end-users such as Terry and Helena: They need to protect stranded assets for as long as practical while moving to a new platform and components. Depending on a specific physical and logical environment, there exist various architectural approaches and technical solutions. Such coexistence increases security’s overall situational and domain awareness, improves its operational effectiveness and efficiencies, and one that is easy to manage and grow.

The degree of migration also depends on comfort with the technology.

So users looking to transition their video systems should consider the broad picture of how networked video can benefit their businesses, no matter the number and size of the steps. Cost-justification analysis and comparisons of return-on-investment, among various tools, are helpful.

**A Toolbox for Analysis**

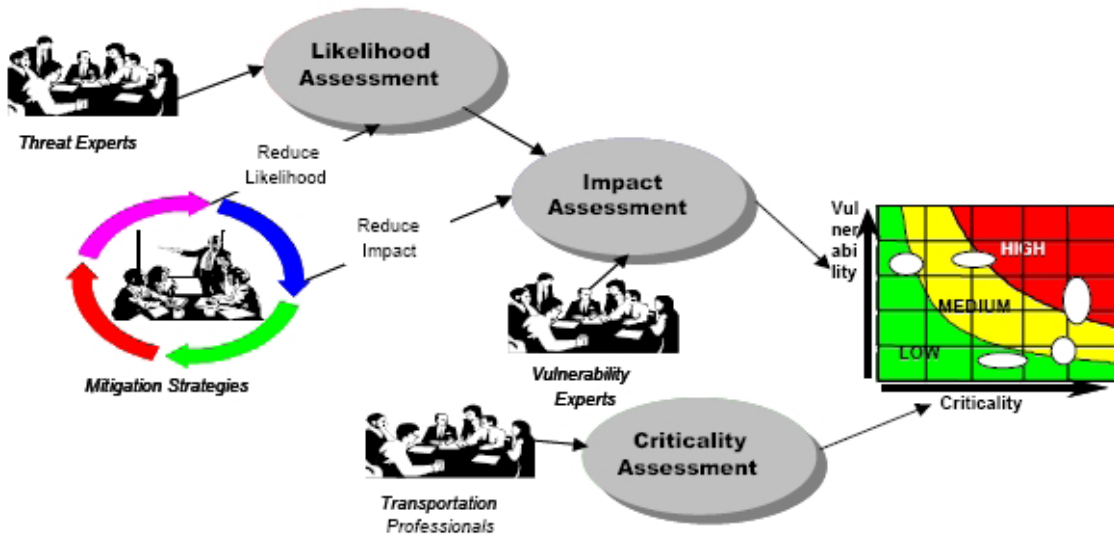
Site survey, down to individual camera locations – A site survey is a vehicle for finding out what is right and what is wrong with an enterprise’s perimeter security and internal access and identification controls.

Vulnerability matrix – With traditional security threats and increasingly sophisticated attacks on the rise, the ability to quickly mitigate vulnerabilities is imperative. If left undetected, vulnerabilities pose a serious security threat to enterprises, people, assets, brand, reputation and systems. Vulnerability assessment is a process of identifying the effectiveness of an enterprise's security posture against greater and lower vulnerabilities.

Probability criticality assessment and ranking – Another way of assessing vulnerability is more often expressed by the numbers. Critical asset factors are the criteria used to identify and prioritize critical assets. Collectively, these factors are an indication of the conditions, concerns, consequences, and capabilities that might cause an enterprise or its security operation to label an asset “critical.” Each factor is assigned a value based on the importance of the factor in establishing an asset as “critical.”

But take care. Often these exercises do not take into account how the availability of video on the enterprise network and systems integration can create tangible benefits for business operations beyond security.

Here is an example of the process of assessing vulnerability and criticality for transport security published in the paper, Highway Vulnerability and Criticality Assessment, Jan Husdal, [www.huscal.com](http://www.huscal.com).





**After Homework, Initial Conclusions**

So Terry and Helena have done their initial tech. homework and security threat analysis. Boiling everything down, they see three jumps they can take – do nothing, do something or do everything. And there are consequences in all three.

Doing nothing to prepare for that inevitable IP future is froth with dangers. Maintaining legacy systems gets more expensive and time-consuming as the tech clock ticks. There are the disappointments of poor images and difficult image retrieval when using video for investigations or for sharing with internal business units or external law enforcement.

Trying to do it all at once has its own hazards. There are the obstacles in justifying a very significant investment while discarding what is usefully in place. Overreaching IP-based security could overwhelm the enterprise’s network either perceived or in real-time.

For our CSO, Terry, the best bet – and one his team chose – was to do something, with emphasis on coexistence of existing analog with introduction, where it makes security and business sense, of IP video surveillance.

Whatever the plan, however, it does not have to be a go-it-alone proposition for the security department. There are security systems integrators, consultants and architecture and engineering firms that boast a track-record of help and advice.

**Case Study: University of South Florida’s IP Jump**



Infinova has worked with Nate Rice, USF’s engineer for video surveillance, and his team, performing site surveys to analyze where new IP cameras can provide the greatest coverage and the best return on investment. “There are several reasons why it is important that we begin to migrate to an IP solution,” Rice reports. “First of all, we must reduce costs. We have over 200 buildings on campus. Any one of them may request surveillance coverage and, when they do, our team visits them, analyzes their needs and designs a system.

“In too many cases, we end up with a need for only one camera and there is no way to connect it to another head-in running fiber. So, all too often, that means we need to include a dedicated DVR. Even when we use a 10-port DVR, the cost of that one-camera solution is ridiculous. With an IP camera, we can simply plug it into the network and allocate storage for that camera. “In addition,” Rice adds, “we have many departments who have created their own ‘big box retailer’ surveillance system with ‘no-name’ DIY residential type cameras and DVRs. Then, they want us to service and manage it. In almost every case, we decline. With our new system, we want a single solution for all video surveillance used throughout the campus. We will be using the VMS and IP cameras we select to set our standard. Equally as

important, we also want to take advantage of the higher resolution that an IP surveillance solution provides. We want to have the availability of megapixel images when needed and that is very difficult to provide in a DVR environment.” USF also gained an ability to integrate systems through its IP migration.

### **Infinova’s Partnering Advantages**

Some manufacturers can help, too. With this first in a series of generic white papers from Infinova, the firm shows its commitment to helping end-users during a period of transition.

Complementing that important cost-managed migration to IP, Infinova – at the beginning of 2010 – has a new V1770 High Definition (HD) PTZ Dome camera, one of a new family of megapixel and IP products. Based on Texas Instruments’ Da Vinci technology, the approach emphasizes how Infinova can enable organizations to cross the bridge to IP at their own pace, as budgets and requirements dictate, while extending the life of their existing surveillance assets.

The new products include fixed, mini-dome and high-speed megapixel dome PTZ cameras and provide both analog and digital output at up to 3-megapixel resolution. The cameras offer megapixel resolution at 20 frames per second (fps) and all products feature SD (secure digital) storage cards. PTZ cameras also provide high quality video and 360 degree continuous rotation at both high and low pan speeds.

In another example, Infinova’s V2216 Network Video Management Software enables IP and analog surveillance cameras and equipment to coexist and manages them as a single, seamless solution. The technology brings together traditional analog surveillance solutions, cameras, DVRs, video walls, matrix switchers and system keyboards, with IP cameras and other digital equipment on a full featured NVR video management solution with a graphic user interface for operators.

The flagship camera of the new family is the Infinova V1770 HD 360° continuous rotation megapixel IP PTZ dome camera with 1.3 megapixel resolution, which hits today’s megapixel sweet spot.

On the Web site, [www.infinova.com](http://www.infinova.com), there is a useful A&E Specifications section.

Watch for the second in this White Paper series. Join Terry and Helena as they face and overcome the challenges of camera selection in a cost-managed way. The blueprint remains co-existence of analog and digital IP video as decision makers succeed at handling the devilish details of camera choices.

# **Infinova**<sup>®</sup>

By helping channel partners provide their customers with complete, affordable, best-in-class, large and small video surveillance solutions, Infinova helps integrators generate more business more profitably. Leveraging a manufacturing process certified to ISO 9001:2000 standards and over 250 engineers with a list of video industry firsts, Infinova channel partners provide their end-users with industry-acknowledged product reliability and technical leadership.

So that Infinova channel partners can create complete solutions, Infinova provides IP surveillance cameras and components, CCTV analog cameras, DVRs and components, camera accessories, monitors, power supplies and fiber optics communications devices. Infinova also has the technical ability and manufacturing flexibility to let integrators propose customized solutions. In addition, Infinova will partner with other manufacturers making other surveillance equipment and software to help its channel partners create turnkey solutions. Contrary to most other companies, Infinova will back-up their partners' products as well as its own to assure both the integrator and its customers that one call – to Infinova only – takes care of everything.

Infinova works diligently to assure its channel partners can provide cost-conscious solutions. With Infinova's hybrid systems, channel partners can propose systems that protect a customer's investment in its already-installed analog surveillance system but that also put them on a dynamic migration pathway to IP systems.

Infinova is lauded for its exceptional maintenance programs. A major highlight is the company's 24-hour advanced replacement policy in which a substitute product is shipped immediately upon notice of a problem.

With such customer focus, Infinova is often referred to as "the integrators' manufacturer."

# **Infinova®**



United States  
Infinova  
51 Stouts Lane  
Monmouth Junction, NJ, 08852  
United States  
1-732-355-9100  
1-888-685-2002 toll free  
1-732-355-9101 fax  
Email: [sales@infinova.com](mailto:sales@infinova.com)

Latin America  
1 305 436 8931 Mexico  
1 305 436 8931 Venezuela  
1 305 436 8931 Brazil  
Email: [Sales-LAR@infinova.com](mailto:Sales-LAR@infinova.com)

Europe  
+40 2 6841 5582  
Email: [Sales-EUR@infinova.com](mailto:Sales-EUR@infinova.com)

Middle East  
+965 247 5678  
Email: [Sales-ME@infinova.com](mailto:Sales-ME@infinova.com)

India  
+852 2795 6540  
Email: [Sales-IND@infinova.com](mailto:Sales-IND@infinova.com)

Hong Kong  
+852 2795 6540  
Email: [Sales-HK@infinova.com](mailto:Sales-HK@infinova.com)