

News	Technology	Markets	Products	Companies	My SWM	2007 Best
	CCTV Surveillance	Access Control	Biometric ID	Alarm & Detection	Security Parts & Devices	Integration & Convergence

Search All

for ... [Homeland Security Cap...](#) [Augusta Systems Techn...](#) [Night vision alternat...](#) [PennDOT announces nea...](#)

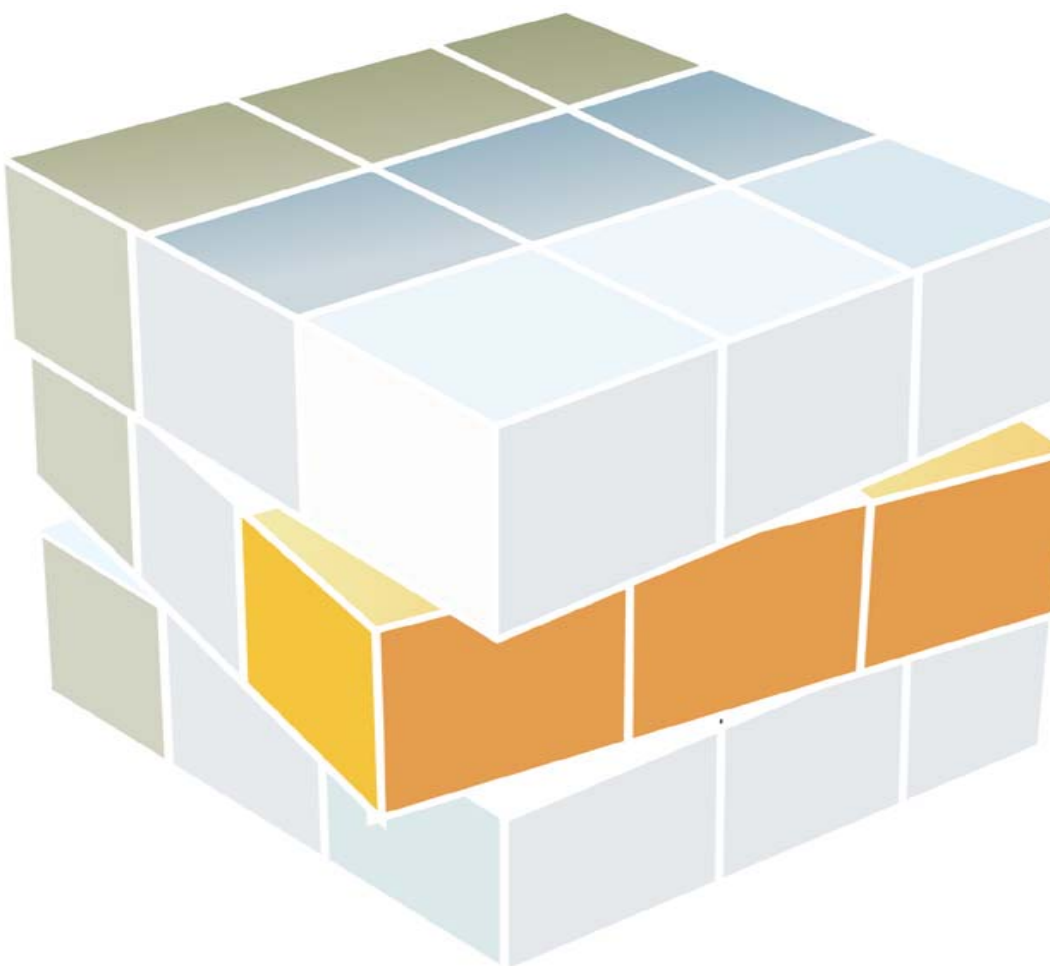
- [Home](#)
- [Table of Contents](#)
- [Cover Story](#)
- [Technology](#)
- [Focus](#)
- [Business](#)
- [People](#)

Cover Story

Security over IP: Converging All the Pieces

Security systems, hosted on a PC and linked over a network, have proven themselves by easing wiring and connection headaches. They provide a leap in capabilities

By Scott Stogel



As the SUV approaches the unattended gate, a camera tilts a bit lower to focus on the license

low light capabilities, peers behind the driver to view faces in the back seat. A loud clear, "If passengers they are in a monitored area. At a PC workstation 160 miles away, a security access. The integrated, unattended entrance is just one of many monitored by a single operator. All control will be transferred to another operator, in another time zone, in another country. These PC and linked over a network, have proven they facilitate far more than just easing wiring provide a leap in capabilities. Alarms, sensors, access controls, biometrics and enhanced connections that must converge together to be useful for both monitoring and decision-making runs to a single microprocessor control board has moved to a network with Internet Protocol security application software.

CONNECTING IT TOGETHER

Connecting multiple IP-based security devices does not guarantee the interoperability required. Most of today's IP hardware will work together only when the protocols match or a software interface. A complex set of rules must be followed to allow a camera from manufacturer A, an internet biometric device from manufacturer C, and an access control from manufacturer D to all interface.

Application Program Interfaces (APIs) are often used to integrate IP equipment to various software. These solutions allow IP devices performing diverse services to be controlled. It exceeds the expectations of the operator. The benefits are substantial, offering enhanced control and 'Play' flexibility for software and hardware connections.

USING THE PUBLIC HIGHWAY

The Internet is simply a large public network that allows almost continuous connectivity to security systems the trick is to move the data and route the traffic quickly, securely and reliably. In the past, network latency has been cited as a major concern in security system deployment. It is common to communicate between network points on opposite ends of the earth in less than a second. In a Local Area Network (LAN) environment the speed is a far faster. However, data theft and security are still a concern. Encrypted networks, such as VPNs, can provide moderate protection, and end-to-end encrypted links. Note that use of high-end encryption requires consideration of international laws in many countries (including the USA, Europe and Asia).

As speed and privacy issues are solved in modern IP systems, a larger challenge takes the form of network reliability.

NETWORK RELIABILITY

- What if the network dies?
- How quickly can a backup system be online?
- What if our main command center is no longer operational?
- What if we need multiple teams working together in a hurry?

System deployment using networking backbones can be a simple CAT5 cable between two buildings, cities and countries with vast, dynamic independent network paths. It can be difficult to diagnose, and nearly impossible to access for repair. The good news is because of clever system design can be used to take advantage of the great features inherent in network backbones to address potential downtime issues.

Any network device can be assigned to a single specific connection destination. For example, a PC in just one operations center. However, good planning must accommodate alternate reconnection schemes. Ideally, endpoints should be smart and able to connect directly to a fixed, dedicated distribution head-end. Reliance on a single hardwired nerve center is far less desirable. Intercoms and sensors working without dependencies. In a best-case scenario, communicate with Fail-Forwarding, IP addresses on each IP device. This would enable every endpoint device to have an 'alternate host' IP addresses to be used to establish control in the event of a primary contact point might include a simple standby workstation or a series of redundant disaster recovery host consoles is another means of safe and reliable backup protection. Careful software selection to address this issue. Buyers should require transfer capability and software flexibility that suit their needs.

not only provides redundancy capability, but also eases planning and deployment of the supervise entire systems.

THE HUMAN FACTOR

Given the fact that IP provides connectivity anywhere in the world, there is no longer a common location. One or more monitoring centers may be used and have command and control or city-to-city. This permits guards and security staff to be located anywhere in the world located off-site. In a small system, this simply permits night desk transfer. In a larger system command centers can adopt IP addressing changes to transfer control to various centers and and complexity of deploying such systems is a perfect fit for IP.

SAVE IT FOR A RAINY DAY

In the analog domain, data backup and reliable recovery is a project within a project, requiring to be used in multiple locations. This is further complicated because companies are situated at secure sites. Once again, IP offers a seamless modern solution. A true IP backbone supports archiving that is free, limited only by data storage costs. Events, camera DVR storage, audio may be saved, transferred and archived in real time, and in multiple locations, with little or no systems storage may also be encryption for secure record keeping.

BANDWIDTH

An important consideration in all IP topologies is data rate capability or bandwidth. The common refers to 10M.bits/sec or 100M/bits/sec. Security systems should incorporate an end-to-end cameras are involved. To further reduce camera-based traffic limitations, video and image compression. The Table shows the need for video compression and other security system components, with utilization. When designing IP systems the key calculation is combined peak security system not exceed 80% of most limited speed crossroad in the system. For example a 1 GB/sec network though an older 10mb 8- port system switch, or travels over a VPN/DSL connection.

WHAT TO LOOK FOR IN AN IP-BASED SYSTEM

When shopping for a system there is more to consider than simply looking for an RJ45 network. Each device needs to connect independently, and integrate to a common control host search consider before you specify or buy.

- Video Scalability: Flexible fps per camera with high compression
- High quality digital audio, with a 2 way capacity for paging, intercom and monitoring
- Flexible powering options including network Power Over Ethernet (PoE) capabilities
- When required, integrated real time Encryption using secure 3DES or AES standards
- Software and application support for convergence to single and/or multiple security workstations
- API programmer interface
- Peripheral support for relays, sensors, and future add-ins
- Support for non-legacy and non IP-based devices via connectors or terminal access point
- Bandwidth usage specifications that meet required total system network capabilities
- Diagnostic capabilities via common protocols such as USB RS-232, I2C® or SPI®

Here is a quick review of some 3-letter abbreviations you'll need to understand before you shop

- TCP/IP: Common protocol used in network connections and transmissions
- AES/3DES: Secure data encryption algorithm used to protect network
- API/SDK: A software component used by programmers for seamless integration of multiple solution
- PoE: Power Over Ethernet standards transmit up to 14 watts of electrical power, within the network

AUDIO OVER IP

Audio distribution and paging has proven to be a perfect match for IP-based security systems. The banking, parking, education and military markets have all adopted digital audio 2-notification and emergency services. Special enhancements, enabled by IP control, provide monitoring, paging and voice logging operated over multiple enterprise workstations, tie sophisticated biometrics. IP audio systems also provide a great path to upgrade outdated technologies coming to market.

IP audio upgrade modules, such as Digital Acoustics ii3-Intercoms, are used to migrate aging audio stations and dynamically connect them to centralize security and mass notification systems around the country. In the coming years, IP intercoms, video and biometric systems and paging technology in security systems undergoing modernization and in virtually all new project specifications.

Scott Stogel is Co-founder and Vice President Engineering of Digital Acoustics (www.digitalacoustics.com)

For more information, please send your e-mails to swm@infoth.com
©2007 www.SecurityWorldMag.com. All rights reserved

[pre](#)[Millennium, A Singular Sensation in Single-door Technology](#)[next](#)[The Ingredients of a Successful Sale](#)

[Home](#) | [New Product Showcase](#) | [Gold Suppliers](#) | [Trade Shows](#) | [email Newsletter](#) | [About SWM](#) | [Help](#) | [Site Map](#) | [Partnership](#)

Copyright Notice © 2004-2007 www.SecurityWorldMag.com Corporation and its licensors. All rights reserved.