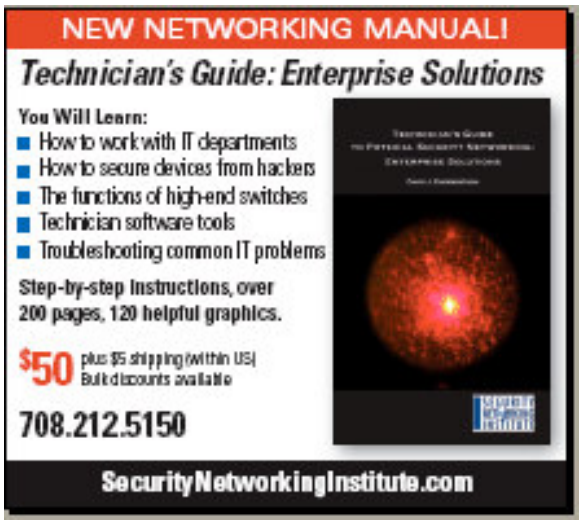


The new manual for alarm industry professionals:

Technician's Guide: Enterprise Solutions

By: Dave Engebretson, industry trainer and SDM technical writer

A complete guide to the connection, programming and troubleshooting of IP-enabled physical security devices (IP cameras, DVRs, access control) when connecting to enterprise networks. 260+ pages, 120+ illustrations.

This book is available for only $50 (shipping in USA included) at www.securitynetworkinginstitute.com.

Below is a sample chapter:

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

Why Networking - Why Now?

While the networking revolution in the physical security industry continues, a question is often raised - why should network-enabled devices replace the analog equipment that has been used successfully in the past? Analog equipment is relatively inexpensive, requires no new skills on the part of technicians, and provides the functionality needed for typical security system applications.

Our industry has seen many new technologies that were adapted or modified to create physical security system components; microwaves, ultrasonics, and RF devices are some examples. Each of these technologies included a (sometimes-steep) learning curve for both manufacturers and installation companies before the technologies could be considered reliable enough to use in security systems. Some technologies such as microwave-only motion detectors were found to be unusable because of fundamental technological issues - microwaves will easily penetrate walls and floors, so microwave-only motion detectors were very prone to creating false alarms. When microwave technology was combined with passive infrared into a single detector, the false alarms were greatly lessened. So it takes time for a technology to find its successful niche in our industry. As manufacturers develop more effective and lower cost components, and end-users start to envision the possibilities, networking will become the standard way that physical security is installed, controlled, and monitored.

A Seismic Shift

Networking is a major change and opportunity for our industry for one primary and simple reason. For the longest time manufacturers have produced equipment that communicated using vendor-specific formats and protocols. Can you connect a Honeywell keypad to a Bosch alarm control panel and make it work? No. But you can purchase virtually any off-the-shelf networking component such as a hub, switch, or IP camera for that matter, and those devices can be connected and will communicate with other devices from different manufacturers on the same network or over the Internet. The key issue is that network devices are built to communicate using standard protocols established by the IEEE, and every device can potentially communicate with each other, if programmed to do so.

Editorial Note: Unfortunately, our industry's manufacturers, at the time of the writing of this chapter, have failed to embrace standards for the reception and recording of IP video streams. Once again many of our major vendors in their wisdom think that they should use the old "proprietary protocol" philosophy in their IP video products. So while a network might have both Bosch and Pelco cameras connected to it, it's likely that both sets of cameras cannot be viewed simultaneously using the same software. This will change in time.

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

Existing Infrastructure

Fancy words for saying, "somebody else already put in the cable (and/or connectivity), we need to make this work." Because of the overwhelming popularity of Ethernet and Internet connections, just about every commercial business and a majority of residential clients have already installed wired and wireless networks and broadband Internet connections. So security dealers now have the opportunity to use existing Cat 5e, Wi-Fi, and fiber optic links to connect any manner of electronic security devices such as cameras, intercoms, access control components, or other network-enabled equipment. This is a key issue that can directly affect labor costs (therefore the price to the client) of installing a new or revised surveillance or security system. Look for the network cabling and connectivity when surveying a potential job and calculate what cost savings can be achieved by not running new cable.

Worldwide Connectivity

There are presently tens of thousands of IP-enabled security cameras that can be viewed over the Internet. This worldwide connectivity allows security dealers to provide benefits for their clients that could never be accomplished with traditional analog systems and equipment. Clients can view remote locations, saving themselves the time and money required to physically visit a remote site while increasing their peace of mind because they can see, in real time, what's going on at a location across town or thousands of miles away. Real estate investors can watch the progress of a building being constructed, parents can watch their children at a day care center, the water level of a dam can be monitored in real time and devices can be turned on and off remotely from across the country; the options are truly endless in terms of what can be viewed or controlled over WANs and the Internet.

As more end-users witness the power and opportunities available from network and Internet connections, they will want the same functionality and options from their security systems. Which brings us to....

The Universal Interface

What does virtually every businessperson have sitting on their desk, besides a telephone? A PC, of course. The personal computer or laptop is the universal interface for just about every aspect of an individual's business and personal life. Email, file sharing, downloading, Internet access, bill payment, research...you name it, and it’s done from a computer.

The physical security industry has long used separate interfaces for the various systems in a client's location: A keypad for the burglar alarm, a monitor and joystick for the CCTV system, a desktop box for the intercom, etc. With networked security devices, all of the interfacing and control can be performed from the exact same machine, the desktop or laptop that clients use for everything else.

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

And the control and connectivity isn't limited to a single machine. Most IP-enabled devices being produced for electronic security systems are "web servers," and can be accessed using common web browser software such as Internet Explorer. Authorized users armed with the correct IP address information can use any standard PC to communicate to a device, view the video, issue commands, or interrogate a device.

New Viewing and Control Options

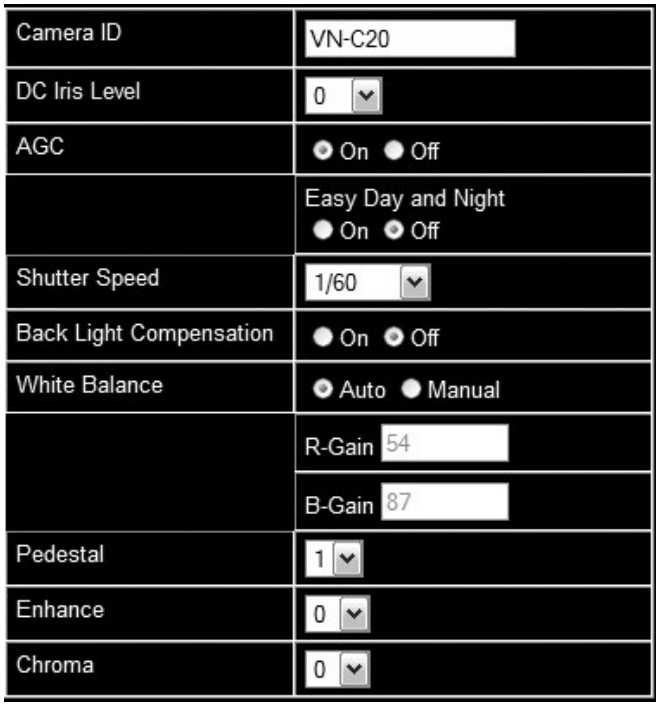
Along with new communications paths and user interfaces, networking provides many new options for what information can be provided for system users. Networked intercom systems can record all intercom communications as audio files that can be stored on the network and reviewed later. Network cameras can transmit video images via email, file transfer protocol (FTP) and live streaming video to multiple users simultaneously, whether they are viewing the camera's images from the local network or from the Internet. This is a key benefit of networking for security devices, the leveraging of common network properties such as email, instant messaging, and multicasting into direct benefits for clients and security companies.

Remote Servicing and Control

Networking devices can provide security installation companies with direct and detailed control of their client's security components, provided that the security dealer set up the ability to remotely service devices at the time of the initial installation. With this type of control in place, security dealers can monitor, change settings, and modify the outputs of network-enabled cameras, access control equipment, and other devices.

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

Here's the control screen from a JVC IP camera:



With IP cameras and encoders, video settings can be remotely manipulated.

Any and all of these settings can be remotely manipulated, providing security dealers and knowledgeable end users with the ability to remotely diagnose and manage devices on the network, either within the building or around the world.

What's Slowing the Process?

Even with all of the known advantages of networked security devices, the actual growth of IP-enabled physical security devices installed is relatively slow, when compared to the robust sales of traditional analog equipment. Why are dealers reluctant to hop on the IP bandwagon?
There are three reasons that dealers cite when asked why they aren't using these products:

1. *High Cost* - Simply put, IP-enabled devices are currently too expensive for a large section of the electronic security market. Consider the costs of IP cameras. Major manufacturers are selling good quality color analog CCTV cameras for about $200US wholesale to dealers. The same manufacturers are selling IP-enabled versions of the same type of camera for approximately $600US. These excessively high equipment costs are keeping average security dealers from making a wholesale change to IP devices...they and their customers cannot afford them.

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

Security dealers are not in the business of changing technologies for the sake of change alone. Dealers need to provide quality systems that afford a level of protection for their clients' assets, and timely service after the sale. But any security system starts with a successful sales proposal or bid, with most dealers bidding competitively with other dealers, so the cost of the overall system is of paramount importance.

2. *Knowledge* - Successfully implementing new technologies requires that salespeople, project managers, and especially technicians become familiar with the new products or techniques. Salespeople need to understand the advantages of the technology so they can explain to their clients why the new "stuff" is better, and close sales. Project managers need to understand the new technology in great detail so that cost-effective installations can be planned. And technicians need to know the ins and outs of a new device or service so that they can successfully install and service the equipment. All of this new knowledge must be gained by the people involved, which takes time and costs money.

   Many security installation companies are committed to the networking future, and are in the process of training their personnel to understand IP today. This process will continue, and those dealers will have a competitive advantage when the balance tilts toward IP-enabled security equipment.

3. *Reluctance to Change* - Long-term professionals in successful electronic security installation businesses, having seen other technologies come and go, are waiting on the sidelines until they are forced to pick up the IP football and run with it. Only when they start to lose sales to competitors who are wielding the networked security tool will many established alarm companies embrace networking technology.

Each of these issues is a real concern and an impediment to the growth of IP networking in the physical security industry. However, as we'll see in the next section forces are at work that will drive IP to great market penetration in relatively short order.

The Future

Lower Cost Devices

Just as with every other technology, IP-security device manufacturers will develop new versions of products that are less expensive until a "magic number" price is reached that explodes sales. Consider the color television set market in the USA. In the late 1950s color TV sets cost over $1000US, which was a lot of money in those days. Most people purchased black & white televisions, which cost in the range of $200US. In 1965, the prices of color TVs dropped to $500US, and within three years over twenty million color television sets were sold. And now about the only place you can find a black & white TV is in your attic, gathering dust. The color technology provided a better viewing experience, and the manufacturers found a way to make their customers buy them.

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

In the old days, burglar alarm systems consisted of magnetic door contacts and window foil; motion detectors were both very expensive and false alarm prone. With the advent of inexpensive high quality motion detectors, the foiling of windows has become a lost art. It is less time consuming for a security technician to install a motion detector than to properly foil a number of windows in a room, so future problems with foil have been eliminated.

We can expect the costs of IP security devices to drop dramatically until the balance of price versus the number of units sold reaches a profitable level.

Standardization of Video Protocols

Yeah, I'm a dreamer...But someday a number of mainstream vendors will get together for the good of the business and standardize the video compression protocols that are used in their IP-enabled surveillance cameras and encoders. This sort of protocol convergence is already happening in companies such as Milestone, who will adapt their video control/recording software to a wide variety of manufacturer's IP video devices. The Security Industry Association (SIA) is leading the way on this initiative and should be applauded for their efforts.

It only makes sense for our industry to follow the successful examples of standardization in networking protocols, which have propelled the IT business for the past twenty years.

Use of Common Networking Devices and Technologies

What's a DVR? At a basic level it's a software set, one hard drive (or more), inputs for analog CCTV cameras, a power supply, and a box to hold it all. As networking of physical security devices grows, manufacturers and installation companies will increasingly take advantage of existing network devices for functions such as video storage and management and viewing/control of IP video streams, access control systems, intercoms, and the like. So in the DVR example, the software can be installed on a networked PC (which can double as the viewing station), the video storage can be gathered onto network attached storage devices, and we've eliminated the analog inputs and power supply along with their associated costs. This is the wave of the future; utilizing common (and relatively inexpensive) enterprise network devices to perform necessary physical security functions. This trend will lower costs and increase functionality as the networking of physical security systems continues.

Mega Pixel IP Cameras - HD TV for Security Cameras

Do you have an HD television in your home? Anyone who's stood at an appliance store and has compared the images on a standard TV and a high-definition version can immediately see the dramatic quality difference that HD brings to the viewing experience. As the prices drop and the concept takes root, discriminating security system end users will start to demand the same high quality of images from their security cameras that they receive on the HD television set in their home. The widespread

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.

acceptance of HD for entertainment viewing will drive our industry towards mega pixel cameras, which are only available as networked devices. History will repeat itself. I remember conversations with security dealers in the early 1990s where the opinion expressed was that there was no need for "color" CCTV cameras; black & white was just fine. Now color is dominant in CCTV and black & white devices are rarely used.

Just as the personal computer and home broadband connections have opened vast markets for computers, software, and Internet-based businesses, the evolution of broadcast television toward HD will drive the desire of clients to view the excellent security images that are only available from mega pixel cameras.

High End User Acceptance

The IP revolution is well underway for high-end installations, such as casinos, banks, chain stores, and universities. These users clearly understand the benefits of networked physical security; otherwise they wouldn't spend the money on what is currently higher-priced technology compared to the analog equivalent.

IP-enabled security devices and systems will migrate from the high-end to medium-sized and lower cost systems over time, as more end users see and can value the benefits of networked systems. Consider card access systems. When this technology came to market, it was expensive and only utilized by high-end clients who could accurately value the cost vs. benefit equation of these nascent systems. Medium-range clients saw the benefits of "card access" and wanted it for their locations; our industry responded with smaller and lower cost systems to fit that mid-market need. The progressive growth of IP security systems will follow along this familiar path.

Sample Chapter from "Technician's Guide: Enterprise Solutions" by Dave Engebretson. All rights reserved. All materials are copyright 2008 David J. Engebretson. No reproduction without permission.