

## Security: Today's Technology Expands Your Options

**S**ecurity-system technology is moving ahead rapidly, evolving to become more sophisticated and streamlined. Digital options allow managers to store and retrieve security data more quickly and less expensively. Software advances make it easier for access control, monitoring and other equipment to communicate with other building systems.

Such new solutions can raise important questions. Perhaps there should be a boundary between the security and information technology departments. But that line is fuzzier these days than it once was and seems to be fading over time.

As a result, thoroughly planning your security system is now more critical to your installation's success. These systems once were added to a building after construction had already begun but today they must be included in any new building's up-front planning.

### *Choices expand, costs fall*

Advances in commercial building security parallel those taking place in our homes. As computing and communications technologies have become less expensive, they've also become more common throughout our daily lives.

In the home, DVD players and digital video recorders (DVRs) have replaced VCRs. Wireless home networking systems allow us to access office e-mail from a laptop in the bedroom. Infrared cameras allow us to monitor a sleeping infant visually, a service the old-school, audio-only baby monitors could never have provided.

Facility security managers have even more sophisticated options (and more of them). As technology has come down in price (while providing more capabilities), the range of new tools at a facility's disposal has increased.

Significantly, options that might be seen as "ordinary" today would probably have been excluded (for budgetary reasons) just a few years ago. Some examples:

- Security cameras that operate using Internet-based commands instead of hardwired control systems are affordable.



## What is *Power over Ethernet*, and Why Do You Want It?

One new technology that could help drive adoption of networked security equipment ever further is Power over Ethernet, or PoE. This approach uses standard Ethernet data cable to distribute low-voltage power to remote devices.

That's right—data and electrical power over a single cable. This means installers only need to run data cable to a wireless access point (WAP) and a separate power outlet isn't required.

***Why you'll like PoE:*** You'll save on both labor and equipment costs.

First introduced in 2003, PoE is the result of a standard from the Institute of Electrical and Electronics Engineers (IEEE 802.3af-2003). It provides for up to 15.4 watts of electrical power to be carried over Ethernet cable.

There's more to come. While sufficient for WAPs and some stationary cameras, that power limit wasn't high enough to meet the needs for cameras that can pan, tilt and zoom. IEEE has since been working to upgrade this standard.

***Hoped-for result:*** A new standard (IEEE 802.3at, also called "PoE-plus") is expected to be ratified in late 2009. This guideline will expand PoE cable capacity to 25.5 watts, enough for pan/tilt/zoom cameras and more wireless-network equipment (such as WiMAX transmitters).

***How does PoE work?*** It's similar to old-fashioned land-line telephones (aka "plain old telephone service"). The wire connecting a landline phone to the wall carries low-voltage electricity to power the phone's operations and illuminate the keys on those old "Princess" models.

With PoE, power is supplied to Ethernet cable in one of two ways. Newer server equipment and switches now come with powered PoE ports, ready for instant connection. With older equipment, an "injector" unit (installed between the switch or router and the end device) adds electricity to the cable.

When using PoE-plus, facility owners will gain greater flexibility in placement of remote devices. However, effective use of this equipment still will require comprehensive planning backed by professional experience.

■ DVRs store enormous libraries of data in a fraction of the space once needed to house VHS tapes (which tended to degrade over time).

■ High-tech biometric readers—the retina- and fingerprint-recognition systems that once were seen only in James Bond movies—are more common elements in today's security plans.

## ***Expanded software-enabled options***

Software advances are adding to the functionality of up-to-date security hardware. Security managers use the software to process the vast quantity of data generated by new systems. *This element is critical.* Your facility's cameras could well feed new DVR storage systems 24 hours a day! Identifying a key perpetrator in one or two frames of video might well be an impossible task without computer assistance.

Today's facial-recognition software can scan the digital video, much as Internet search engines scan the web. In moments, it returns to human reviewers all instances of a single individual for later review.

But there are additional, expanded options. Some manufacturers *build this capacity into the cameras.* Sophisticated algorithms recognize suspicious behavior as it is happening and send alerts to appropriate security staff.

Further, these options are accomplished efficiently. These special cameras operate at low resolution most of the time (storing video on internal DVRs). When suspicious behavior is detected, however, it triggers higher-resolution recording.

What's more, some models allow audio transmission. Built-in speakers enable remote operators to warn off intruders or otherwise respond to incidents as they are occurring.

### *Providing a more complete picture*

Security systems, consisting of various components, can be tied together to track the progress of a single individual throughout a facility—be it a store, an office building or a complete university campus. Another capability: Since the video recording is digital, it can be matched to other events tied to that particular individual.

**What this means:** Logged information on building access can be matched directly to the video, providing time-stamped visual evidence (if needed). Pertinent video segments can be saved, e-mailed and included in any digital reports—as easily as any other electronic attachment.

How might this level of cross-system communication work? Consider a college campus. On many campuses, student ID cards also serve as access cards and debit cards for use at school cafeterias and bookstores. Networked systems could track a student through an entire day, both visually—through security video—and through transactions made with his or her ID.

But this technology's application can go beyond security to enhance customer service. Example: Hotel operators have used digital cameras to track guest-registration patterns. Analyzing the video has helped them identify and predict registration behaviors, which has aided staffing plans and boosted operational efficiency.



### *Planning & people*

Communication is a critical component in using these new technologies effectively – *human* communication, not just that between connected electronic systems. Once security operations begin to become heavily dependent on digital information, security designers need to incorporate information technology personnel into their plans.

Without cooperation between these groups, new installations could end up duplicating—or, worse, competing with—existing facility wiring and data storage.

**What this means:** New plans must begin with a clear understanding of infrastructure

requirements and an analysis of the data network's current status—and future demands. Transmitting all that high-definition video from today's advanced security cameras could eat a lot of network bandwidth, even with cameras that provide some onboard data storage.

Additionally, your IT personnel likely will want to spend some time studying current data-security protocols to ensure the system is safe from external intruders.

Security personnel are more likely to be up-to-date on current equipment offerings, so members of that team should be a part of the effort to gather business requirements for new or upgraded designs. Their knowledge could provide insights into new solutions for meeting current or future needs. They also will have

recommendations on policies and procedures once new systems are in place.

Finally, a licensed electrical contractor should be a part of all conversations once a system layout begins to develop. Low-voltage technology is expanding rapidly—in some cases, Ethernet cable may be able to carry all the power security equipment needs (see sidebar). But power cable can interfere with data-cable transmission if it's not installed correctly.

Many NECA member contracting companies offer the expertise needed to ensure successful operation of your system (find a contractor at [www.necacconnection.com](http://www.necacconnection.com)).

Plans for future upgrades and expansion also should be considered at the planning phase. As sophisticated as today's equipment may be, the parade of new advances is far from over.

IP addressability enables a certain degree of plug-and-play functionality, making new system additions easier. But this is only possible if the network has the added bandwidth and power capacity to make it happen. Again, your electrical contractor—one that specializes in security systems—can help ensure that your facility's security systems meet today's needs as well as those of the future.

## ***How You Gain From Systems That Can Work Together***

Advanced implementations of digital, IP-based systems are networking security and access control with other building systems. In these situations, office locations and personal preferences can be stored by building management software. *Note:* IP = Internet Protocol.

***What's the utility of this?*** A worker coming to a building will routinely swipe an access card through a reader to enter. That action can trigger (to that user's specified settings) the office lights, appropriate ventilation units and even electronic blinds in that person's space.

Beyond the obvious coolness factor, this level of integration also promises great energy savings, especially during off-hour use. Instead of lighting an entire floor on weekends, building controls can ensure that the only fixtures operating are those used by those workers who have chosen to come to work. And when those workers swipe their access cards again and leave the building, those systems will shut down.

Some users are tying security into enterprise business systems. One example is using biometric access control to punch hourly workers into timekeeping systems. This approach prevents workers from fraudulently entering absent friends into automated payroll applications.

Further, connecting access card functionality with human resources applications helps maintain security when workers leave the company's employment.



### **About the Electrical Design Library**

**This document and other free reports are available at**  
[www.electricaldesignlibrary.com](http://www.electricaldesignlibrary.com)

©Copyright 2009 by the National Electrical Contractors Association (NECA). All rights reserved. Published by the National Electrical Contractors Association for the educational use of our present and future customers. To find a qualified, professional electrical contractor, use our online service at [www.necacconnection.com](http://www.necacconnection.com). NECA is located at 3 Bethesda Metro Center, Suite 1100, Bethesda, MD 20814. Phone: 301-657-3110. Fax: 301-215-4500. Web: [www.necanet.org](http://www.necanet.org). E-mail: [edlinfo@necanet.org](mailto:edlinfo@necanet.org).

Index No. 3025130