

## **Specifying Today's Buildings for Access Control and Security** by Jim Russell, vice president—sales, Matrix Systems

Specifying access control (AC) systems today is decidedly different from 10 years ago, or at least it should be.

AC today encompasses many more engineering considerations, such as IT and building automation system (BAS) integration, not to mention new trends in technology, including biometrics, wireless and increased user-friendliness. Most importantly, consulting engineers must provide their commercial clients with AC products that are not only cost-effective and promise a long lifecycle, but are also flexible enough to integrate future technology innovations.

End-user queries should surface the expected growth of the facility/company to provide scalability for five to 10 years, not just 12 to 18 months. Will the facility remain a single location with a limited number of doors, or could it grow to dozens of doors, supplemental locations on a campus, or even multiple distribution centers around the globe? The specified hardware and software must be able to accommodate both scenarios in scalability and cost.

In addition to scalability, AC software should be able to adapt and integrate future technological innovations as they become available. If a hospital implemented software five years ago, and it now doesn't integrate easily with newer equipment protocols, then the facility can't take advantage of current cutting-edge technology, such as wireless, biometrics and other current trends. Scalability points directly to open architecture systems. A consulting engineer who fails to specify a system with open architecture is essentially boxing-in the customer and limiting future integration of equipment that could improve security.

### **Cutting Costs Through High Technology**

Fortunately, today's security solutions can incorporate such innovations. The consulting engineering community today recognizes the value of wireless card readers and wireless stand-alone locking devices. Wireless has demonstrated its value as a retrofit solution when existing buildings need to incorporate new access doors or areas into the total AC system. Instead of hiring electrical contractors run 120V or low voltage wiring through existing walls, which can cost \$2,000 to \$3,000 per area, maintenance departments can simply wall-mount a wireless interface device near a door or a group of doors. The wireless device communicates to a Wiegand output device that, in turn, sends a hard-wired signal to the AC software workstation. With a potential cost of less than \$1,000, a wireless door set-up is an affordable and efficient solution.

The Cleveland Clinic, one of America's top hospitals, saved nearly 25 percent on installation by implementing wireless to establish new doors at its facilities. With a 40-acre main campus and more than two dozen regional hospitals and family health centers from Canada to Florida, the hospital needed a scalable, cost-effective solution to accommodate the growing roster of buildings in its AC system. The cost savings

using wireless has enabled them to complete more building projects while maintaining the same high level of security.

In addition to wireless, new innovations such as biometrics and Power over Ethernet (PoE) are cost-cutting trends. An AC retrofit at Flowers Hospital in Toledo, Ohio, included an anti-microbial biometrics device for the surgery room entrance. Previously, doctors had to fumble with ID cards. Now the “card-less” reader provides access with the touch of a hand and/or PIN input, providing much more convenient entry. The only drawback of the new technology is that biometric readers can cost two to three times more than conventional card readers.

Power over Ethernet (PoE) is another alternative to conventionally powered door hardware. This uses existing Cat5 Ethernet wiring to deliver both data and power to the outlying devices. Of course, PoE requires availability of LAN or WAN connectivity via existing Cat5 throughout the building or campus.

### **Integration with BAS and IT?**

Combining an AC system with an HVAC building automation system (BAS) is a practice some engineers use, however, it is better to keep the two systems separate. BAS systems are excellent at controlling the HVAC, lighting and energy systems of a building, but adding an AC package to the BAS typically doesn't provide the sophistication, scalability or integration capabilities necessary for total building security. In addition, an AC system must be able to provide uninterrupted security during power failures without relying on a BAS.

While separating the BAS from security is in the best interest of the building owner, using the AC system to monitor mission critical functions such as chillers or IT equipment air conditioning can provide a building with another layer of observation redundancy. Therefore, it's important for AC systems to have input and output functions as well as compatibility with BAS protocols.

Convergence with IT systems is also a trend, but there are necessary precautions the specifying engineer should coordinate with the facility's IT director. For example, does the IT network have multiple paths for redundancy so that if the network goes down, the AC downtime is minimized? In addition, there are performance considerations. AC systems will not slow an IT network, but video can have an impact. Therefore, when video is an important part of facility security, it should run on a separate network, but remain integrated with AC for seamless functionality.

### **Planning for Installation/Maintenance Savings**

Significant construction savings can be passed on to the client by specifying systems that install faster and more easily. For example, the AC provider can provide ready-to-install AC electrical boxes that are pre-engineered for a specific building. Instead of picking components and building electrical box systems from scratch, it is more cost-effective, accountable and reliable to specify AC systems that are prewired with the proper power supplies, network hookups, RF converters, terminals, etc.

Another way to reduce installation and maintenance costs is by designing the AC system to share a closet with networking, telecom and other terminals.

The best systems typically result from the consulting engineer asking the right application questions:

- Is the building strictly AC or will the end-user want to monitor people entering and exiting the building?
- Will the AC go beyond the building into perimeter areas, such as fences, outdoor gates, parking lots and/or non-campus outparcel buildings or satellite locations?
- If there's surveillance, will someone be viewing it live or recording it for later? Where will the video footage be viewed?
- Depending on the size of the campus, will there be a need for several servers and/or workstations and a way monitor them?
- Will an onsite security employee automatically receive alarm notification or is there a need to send an alarm remotely to an off-campus authority's cell phone or e-mail?

The breadth of the system and whether it will have a dedicated employee for monitoring depends on the size of the organization. A company with 10 or 15 employees, for example, isn't large enough to warrant an AC monitoring employee. Instead, a manager or executive assistant will probably assume double-duty as the security administrator. Larger operations with more employees and at least 25 doors should consider a dedicated security employee. This consulting engineering decision is important because the end-user must plan for various levels of start-up education as well as well as ongoing AC training during software upgrades, new equipment integrations and other modifications. While equipment functionality and installation is important in choosing a manufacturer, AC choices should include vendors that offer training, upgrading and continuing education on the system as well as 24/7 customer support.

Usability is important, too. Is the workstation software just text, or does it include cutting-edge graphics that help lead the user to solutions and provide better visibility of the entire security system?

Part of the system's ongoing maintenance will include battery management, whether for wireless card readers or a system battery back-up uninterrupted power supply (UPS). Batteries for AC systems are almost always shrink-wrapped battery sets designed exclusively for the particular component they power. A preventative maintenance schedule for battery replacement and/or check-ups should be established based on the expected use of the card readers (frequency of door use) and other battery-operated components. Most AC software will send alarms as battery power dwindles. Battery disposal should be coordinated with the maintenance department's general battery recycling.

### **Retrofits and Compatibility**

Retrofitting an AC system is where all the boasts of compatibility and integration are revealed as fact or fiction. When retrofitting, it is in the end-user's best interest to use as much of the existing equipment as possible. However, not all AC systems have open architecture. Subsystems and cabling are likely candidates to be retained in a retrofit, but proper testing for integrity is critical. Likewise, the AC system will inevitably need retrofitting or additions of new technology in the future.



Matrix Systems, Inc.  
1041 Byers Road  
Miamisburg, Ohio 45342



800.562.8749  
fax: 937.438.0900  
[www.matrixsys.com](http://www.matrixsys.com)

The AC specifying engineer today has many choices compared to 10 years ago. The best advice is to rely on a vendor that will help an engineer take a project from concept and blueprints through customization and support for design, installation and customer service.