



## Security Technology and Design

By **Lionel Silverman, P.E.**

October 12th, 2005

### Upgrading and Updating Access Control Systems

Every access system eventually needs a little technology pick-me-up. Here are some tips on how to handle your next improvement.

Upgrading a working access control system, while on the surface a somewhat mediocre task, has many hidden traps that can spoil your day. It is to a very slight degree like open heart surgery. Once you start the operation, there is no going back, so you'd better have a good game plan.

The first step is to have a clear understanding of what is installed and working. If you have been there for some time, this task should not be too challenging. If you are new, you had better get writing, because there is a lot of work to do.

1. Make a detailed inventory of what is installed at your facility.
2. Speak to the IT staff and make sure you understand what their policies are in respect to upgrades and updates. These things change.
3. Advise IT of what you are contemplating. They can be your strongest ally in getting things done in a timely manner.
4. Speak to your security vendor to see which of your as-builts are up to date and which aren't.
5. Note the other systems that are connected to the access control system (video, intercom, etc.).
6. Find out from your security vendor what updates are current, who has used them (references) and how much they cost.

These steps will help you determine whether you need an upgrade or an update, and how extensive your changes should be.

If you plan simply to bring the current access control system up to date, it may be as simple as installing a new Service Pack on Windows. Updates are usually benign changes—low cost and low risk—and they are very often covered by the vendor's or system integrator's maintenance agreement.

Upgrading, on the other hand, takes an existing access control system to the next level. This could include replacement of the PC, field controller, readers or cards. An upgrade could be initiated by a variety of factors, such as PC failure, access control equipment reaching the end of its life, the absence of available spares, new security requirements or a merger with another company. The cost and risk of an upgrade depends on the extent of the work involved.

Once you've analyzed your situation and come to understand your needs, you can begin to plan your system improvements.

## **Keeping Software Current**

Jay Vaitkus, product and market manager for Stanley Security Solutions, said that one of the most important aspects of an access control PC is that in most cases it runs on a Windows™ operating system. That means if it's connected to a LAN, the security system PC can receive all the viruses and other attacks to which Windows-based systems are subject. Viruses are the biggest concern, and the system needs to be fully tested for them. The following should be considered the minimum protection:

- Virus protection should run all the time and be checked daily. McAfee, Norton and Trend Micro are all good brands.
- Check regularly to see if any DLL files have been corrupted, since these files are used by the access control software and damage to them could impede system performance.
- Windows updates should be installed weekly, or more frequently if required, to keep the operating system current.
- Full software operating system upgrades should be implemented twice a year to keep the system in peak running order, but check with your security vendor first to see if the latest operating system update is supported by the factory.

## **Avoiding Obsolescence**

Some security companies, like Brivo Systems, offer their customers the opportunity to avoid dealing with software or computer upgrades. Brivo operates an ASP-based remote hosted system, where the entire computer aspect of the system is remote. They can connect to the field panels via dial-up, DSL, T1, or cellular wireless connection. Data can be accessed through a secure Web account using a standard browser. The big selling point for this service, according to Christie Walters, director of business development for Brivo Systems, "is the elimination of technology obsolescence, as Brivo users are not dependant on updates or upgrades."

Using a service like this is one way to deal with upgrade and update requirements. Those who wish to keep their systems in-house have a number of options as well.

## **Migrating Upward Within Your Product Line**

Many of the larger U.S. access control manufacturers are addressing upgrade needs by creating upward migration paths in their product lines. Paul Piccolomini, vice president and general manager of Software House, said providing upgrade options is a requirement for a manufacturer that wants to keep its customers happy.

"Upgrades should not be treated like in the video world," he said, "where the migration from VCR to DVR left many end users behind because no credible migration path was provided for the existing video recording equipment.

"Leaving the end user the prospect of throwing out old equipment merely because it cannot migrate to the next level is a totally wrong approach. The objective of an upgrade must be to take the people forward and protect the existing investment," said Piccolomini. Upgrades can take various directions depending on the requirements of the site and the nature of the equipment. Very often a low-cost "quick fix" to an upgrade requirement proves in the longer term to be a very expensive solution, especially when, for example, the upgrade is to an operating

system that will soon become obsolete. The existing security vendor may not advise you of this because they want to hold you captive until their next version is available—very bad decision. Always check with your local IT professionals as to what the next generation of operating systems is going to look like.

### **Hardware Upgrades**

One approach to hardware upgrades is to use a multi-technology card reader capable of reading several different types of cards. Peter Boriskin, chief technology manager for Software House, said, "(The) multi-technology card reader (MTCR) is one piece of technology that helps customers who are trying to bet on which technology will go forward in the future, as these card readers read many different formats and can thus minimize the potential exposure of the end user."

The traditional card reader exchange project is long and torturous. First one has to make up an entire set of new badges and issue them to all the company personnel. Then all the readers have to be changed out, and then the old badges have to be collected.

"The MTCR," said Boriskin, "allows for the readers to be replaced in a planned, progressive manner without disrupting the entire company ... Where the customer has no cohesive plan for which format they wish to use in the future, having the MTCR is the way to go."

If MTCRs will not work in your environment, then a significant amount of careful planning is required to select the next best solution, which could be a single card reader technology and the re-badging of a limited card population.

### **Watch for Peripheral Upgrades**

Upgrades do present an expense, and it is important that you get true value for your money. Jay Vaitkus advises customers undergoing access upgrades to explore other upgrades as well to ensure that they are getting best value.

- **Integration with CCTV**

- Can provide video on alarm
- Can allow video of access breaches to be sent directly to law enforcement

- **IP-based systems and devices**

- Fault-tolerant/disaster-tolerant solutions allow for systems to remain operational in all circumstances
- Remote managed systems allow for ease of audit capability

- **Visitor Management**

- Increases access security by badging registered non-employees

In many areas, especially with older systems, there appears to be very little documentation as to when scheduled updates and upgrades are needed, and this leads to a degree of uncertainty. Stay in close contact with both the systems integrator and the manufacturer, who should be able to advise you on this matter. At the same time, consider their advice carefully, keeping in mind your own needs

and your budget. Manufacturers and integrators may view upgrades differently, since they have vested interests in the process.

A well planned and properly executed upgrade should bring you lots of kudos, especially when management realizes you are protecting their investment and making use of all the new features and functionality that the upgraded system has to offer. Happy upgrading!

Lionel Silverman, PE, is vice president of business development for Facility Robotics Inc., a nationwide systems integrator specializing in building automation and security systems for larger multi-location and prestigious clients. He is a member of IEEE and ASIS.