

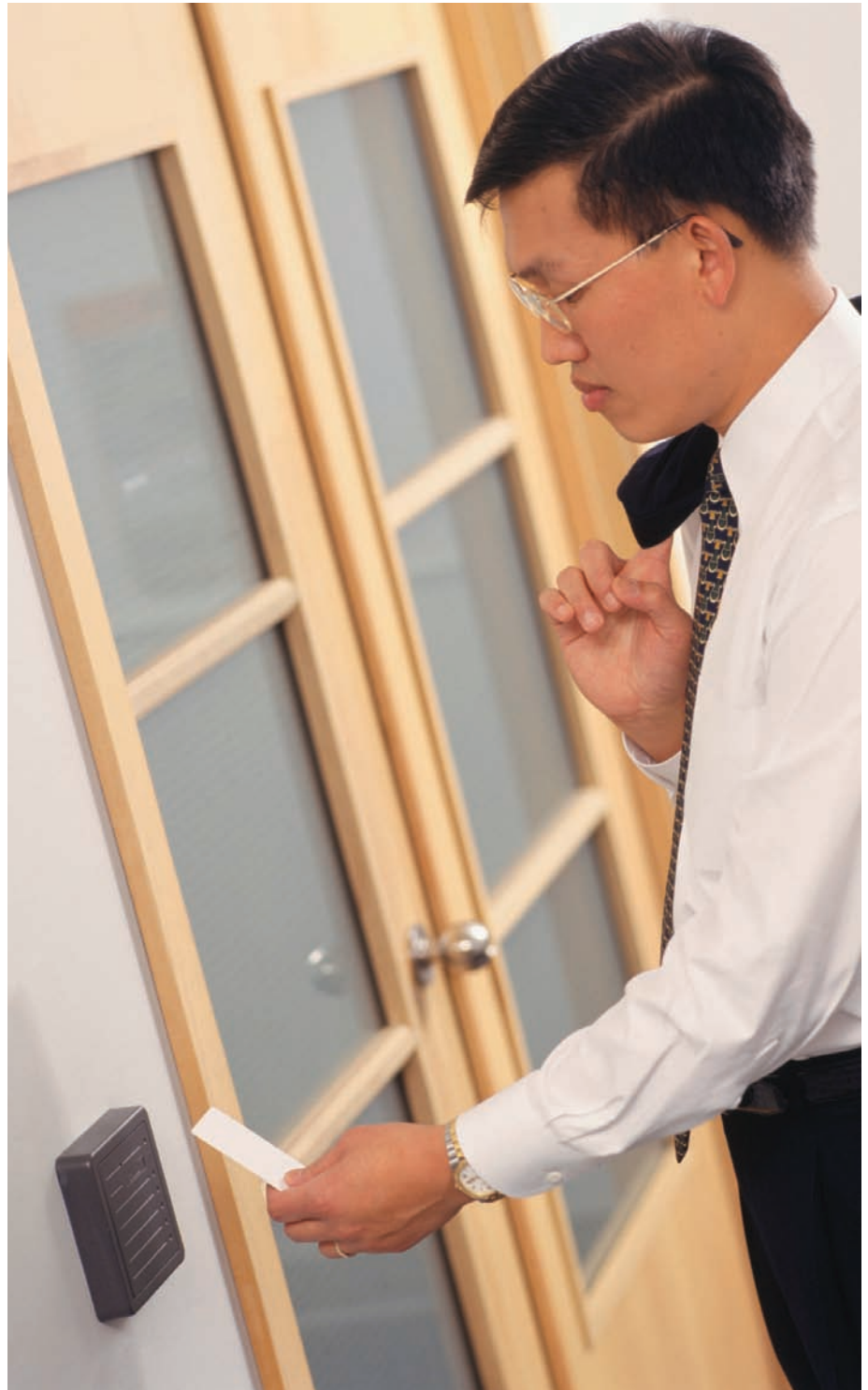
MANAGING TODAY'S EXISTING ACCESS CONTROL SYSTEMS

BY COLIN BEST AND GLEN KITTERINGHAM

The access control system is a vital part of a building's infrastructure and plays a valuable role in the building's protection. It expands and shrinks on a regular basis as tenants move in and out, new cards are created, cards are lost, access levels change, and companies move from floor to floor.

A system can cost a considerable amount of money to design, install and maintain. Tracking and documenting physical changes to the systems alone presents a challenge. But maintenance, and the reliability or integrity of alarms, is critical to the overall value of the system.

The systems designed decades ago were based upon the assumption that technology was expensive, but electrical work was cheap. In high-rise office installations, this meant that a field processor or control panel would be installed and used to feed door controls vertically to several floors. This complicates future moves, particularly where fire alarm systems need to interact with security systems to release doors during fire alarms. This is something that is a complex issue. First, access systems have been able to perform a complex array of instructions based on certain input or



combinations of input for decades. This, however, would never satisfy building codes that dictate that a door lock or unlock upon activation of a fire alarm. Multi-stage fire alarm systems dictate that certain lock types in certain locations must release. As a general rule, we have adopted the belief that any EML (electro-magnetic lock) must release upon second stage alarm. In a high-rise environment, this will dictate that the fire alarm system provides a set of dry contacts for each floor to interact with the card access power supplying the EMLs. In a complex vertical riser network, often (we have seen) doors are relocated to other floors, while still tied to a fire release on another floor. With perhaps 100 door relocations in the space of a year, after failing annual testing and verification, the cost to investigate and correct fire release deficiencies for that many doors may amount to hundreds of thousands dollars.

With doors several floors from their control panels, detailed record keeping is critical to reduce confusion. Recently, the cost structure has shifted – now electrical wiring and labor costs are higher than the rapidly falling technology costs. The expense of installing a ‘flat line’ design in a high rise is reasonable compared to running vertical pipe to maximize the use of hardware. All interconnections of power and fire alarms are local to each floor, making troubleshooting and planning easy.

Another issue is the management of alarms. In most large access control systems, alarms have become so much of a nuisance that they are almost meaningless. When alarms are consistently ignored because so many of them are false, the value of the system is greatly diminished. Often, the remote operator will wait for a point to become normal prior to acknowledgement. This means that an alarm that has returned to it’s regular state, for example: a door alarm that has changed state to ‘closed’. Alarms generally have four states of supervision, Normal, In alarm, Trouble (short), and Trouble (open). An alarm is rarely responded to unless the door remains open. They are treated this way purely due to volume. In an enterprise sized system where there are 10 to

20 thousand alarms generated in a 24 hour period, there is no feasible way to respond to this amount of alarms without the addition of an unreasonable amount of manpower. Some installations will have higher priority alarms that demand a certain response and to insure that the alarm is NOT missed and ignored like the others, it is usually programmed with a specific sound file to let the operator know not to ignore it like the thousands of other alarms that are disregarded. Lost in the clutter of thousands of alarms are the legitimate ‘forced door’ and ‘door held open’ alarms. Therefore, security levels are reduced because all alarms are deemed to be a ‘nuisance’. When staff stops responding to alarms, complacency quickly sets in. To correct this situation, it is important to generate reports on the troublesome alarms in order to investigate the cause. Once it has been determined why the point is generating too many alarms, a maintenance program can be developed to correct these deficiencies. In one installation, the authors reduced overall false alarms by 55% by repairing damaged points, correctly installing them or simply adjusting them. The most significant drop in alarms was due to the maintenance of PIR (passive infrared) detectors. While there are still many false alarms, the project to reduce them to a more manageable level is still in progress. This has been done over a three year period; it is not a project that is easy or quick. Thus the authors offer a word of warning: implementing such a program can require significant dollars and time.

In many cases, the problem alarms are fixed by simple programming changes in the access control system to reduce the impact of glass door ‘bounce’, or changing shunt times (programmed time differences often between regular business hours and after hours). Some may be simple changes to the door such as the location of an exit sign in front of the Passive Infrared request to exit motion detector. Sometimes the problem becomes more complex—there have been situations where the wiring for two or more door contacts has been reversed because architectural changes meant an electrical contractor (with lit-

tle knowledge of the function of access control systems) incorrectly wired existing doors to new locations.

The standardization of installed hardware is also key to better managing an access system. This is the reason there needs to be a proper maintenance program combined with a detailed design criteria. Access control systems in multi-tenant high-rise complexes are certainly not static. An access system is not installed and expected to be the exact same in 20 years. In many complexes, a tenant will hire an electrical consultant that will use a general specification for security dictating power, manufacturer, etc. that will directly conflict with an established standard.

The standardization of installed hardware is also key to better managing an access system.

Rather than make corrections to comply with the established standard, a general contractor will use contingency to “make” the mistake work with the established standard. This kind of error happens in many properties that have no established control. A consistent installation will look very inconsistent in 5 years time. Trying to establish a standard following these errors can create more confusion, where you try to apply building standards to changes to an already existing mistake (ie: specifying 24 VDC strikes where the tenant was already permitted to use 12VAC strikes and only has power installed for this type of strike). Standardizing the type of locking devices means a smaller stock of replacement parts, reducing down/insecure times in the event of hardware failure. There will sometimes be situations where the design of a door might require a unique device. In this event, see if the manufacturer of your chosen standard has a suitable locking alternative. Often, manufacturer’s electric strikes will use interchangeable components despite the body style.



Standardizing hardware to be used can be a challenge. While this seems odd that there is lack of standardization it is due to the constant moving target of managing and maintaining an enterprise system with hundreds of moves, deletions and additions per year. It goes a long way if this equipment can be specified and detailed in the building's design criteria manual. This manual is very helpful to building staff and tenants as they do alterations to the building. While many tenants and some property managers balk at the concept of being told what hardware to install, having a standard will be valuable for ongoing operations of the building.

Database management of a large system can be an easy task, provided the operator has been given a clear roadmap of standards for data entry. Too many people entering data without a documented standard will eventually lead to a combination of entry styles that will make it difficult to decipher the location of doors, time-zones and even cardholder identity. In a multi-tower high-rise, a standard might be an acronym referring to the tower, then the floor, then the door – for instance

“ST-05-NLSD” would be South Tower, Fifth Floor, North Lobby Single Door. Keeping an all ‘caps’ standard for data entry will make it easier to manage. A standard format also comes in handy when training new staff.

It is also important to keep up-to-date records and drawings that reflect the constant changes associated with a large system. Tracking of changes by an administrator as they occur, then comparing them to the as-built documentation prepared by electrical engineers at the end of each year will ensure consistency. What was “as-built” this time last year will often require 200-300 change markups in a large system.

Also, a large card access installation has to be protected from failure due to accident, error, criminal intent, etc. Applying good physical security to the infrastructure and main file servers is crucial to the protection of the systems. Take note of the location of your valuable data and IT related assets. Always ask yourself ‘what if?’ when choosing a location. Look at the areas vulnerable to break and enter, flood, fire, etc. A best case scenario is for security systems to have dedicated riser rooms which are

rooms for security equipment and risers (vertical piping for network cabling) and fiber optics which have limited access. Dedicated risers and limited access means that there is far less chance of accidental equipment damage when people are installing other equipment, reduces the chance that people will start tampering with panels and cabling or that those people up to no good deliberately try to damage or destroy the access control system network.

Assure there are limited privileges for the operators working on the system. If they don't need access to something, don't give it to them. Implement a suitable training program that will give them the proper instruction on the operation of the system prior to giving them access.

Assure that the information is protected by routine backups with a library large enough to retrieve information from at least two weeks prior. Keep an off-site monthly backup in the event that a failure has also affected the backup library. Large modern systems should also have servers with various levels of redundancy. RAID (Redundant Array) hard disk controllers and multiple redundant hard drives are relatively inexpensive and can save hours or even days of recovery time. Manufacturer training for those responsible for the system has its advantages for in-house support. Integrator staff (system dealer) will almost always have manufacturer-trained technicians, however your system is only one of many that they work on and have to continue to be familiar with.

Discussed here are several strategies to assist in maintaining the life of your building's access control system. The investment you make will extend the life of the system, increase the level of protection and make people's lives easier when the system is in proper running order.

Colin Best is the Manager of Security Systems and Glen Kitteringham is the Director, Security & Life Safety. Both are with Brookfield Properties, responsible for the Western Canadian portfolio encompassing several million square feet of commercial high-rise properties. www.brookfieldproperties.com