EST™

BACKGROUNDER

access control

a life safety white paper

EST BRAND LIFE SAFETY & COMMUNICATIONS FROM EDWARDS

See what's possible now...

It seems like only a few years ago that in order to gain access to most workplaces, all you needed was a garden-variety Yale key. Easily duplicated at any hardware store, impossible to track, it offered little in the way of security, and virtually no protection against unauthorized use.

Today such a cavalier approach to building access control is unthinkable among even the smallest of companies. But in the past 15 years much has changed. Assets such as office computer equipment and the data stored on it have become increasingly portable. Factory floors are now rich with fragile and sophisticated production equipment highly vulnerable to innocent and not-so-innocent tinkering of the curious or ill intentioned. Today's just-in-time production strategies move raw materials and finished goods through rapid and complicated paths to market. All this has given rise to a heightened need on the part of all building owners to ensure that only authorized personnel have access – not only to their buildings – but also to specific areas within those buildings.

Multiple tenant capability allows leaseholders maintain their own database of cardholders while sharing control over common areas.

Equally important is the need to protect building occupants from harm. Access to hazardous areas obviously needs to be restricted. But in the wake of increased workplace violence, school shootings, and other real or perceived threats, building owners are much more cognizant of the fact that their people are also vulnerable to harm from other people.

Now put all this in the context of today's building occupancy patterns. Flexible work hours and multiple shifts make access problematic to predict. Meanwhile, public areas and private areas need to be taken into consideration. In the case of multiple tenant occupancies there is also the issue of common areas shared by the leaseholders, but not accessible to the general public. Add to this mix fire codes, which require unrestricted emergency exits, and the federally mandated Americans with Disabilities Act, which guarantees barrier-free access, and it's not difficult to see why the old Yale key just doesn't cut it anymore.

The good news is that you don't have to write a specification suitable for Fort Knox to address all these access control challenges. Fortunately, while need for access control has been developing over the years, so too has the technology. In fact, it is possible today to implement a highly sophisticated access control system that's virtually invisible to the people who move through the building. What's even better is the fact that there is technology emerging now that will make it nearly as invisible when you look at your bottom line.

The credential

The most visible elements of an access control system to the people who pass through a building are the credential and reader. A credential takes several forms. Usually it is a card validated and issued by the human resources or security department. The card can be carried in a wallet or clipped to a shirt pocket. Sometimes it bears the cardholder's photo. Other forms of credentials include special key fobs carried on a key ring, or devices fixed to vehicles, which allow them to gain access to parking lots and garages.

When the credential is presented to a reader, its serial number is recorded. The most common type of reader used for access control purposes today employs proximity technology. This accomplishes a successful read when the credential is held within a few inches of the reader. There is no need to remove the card from the wallet or purse. The credential requires no power source. This makes it possible for an authorized individual to pass through restricted areas of a building without hardly breaking stride. When the individual comes to a door for which authorization has not been granted, the door simply won't open.

While the magnetic door lock and now-familiar access card have replaced tumbler locks and keys in most commercial, industrial and institutional settings, standalone door control accomplishes little when it comes to managing the traffic that passes into or through a busy building. When we speak of an access control system, we are talking about some kind of centralized management system that validates credentials and tracks the movement of those credentials. In other words, a system answers the four Ws of access control: who went where and when.

Multiple functions operating on a single platform means lower installed costs, simpler maintenance, and reduced operating expenses.

To accomplish this, data has to be processed, managed, and communicated. These three elements form the basis of access control systems today. Each element is handled by a vital link in the chain: processing is handled by the card reader controller; management is handled by the access control database; and, communications is handled by the control platform.

When writing an access control specification, it is important to pay close attention to the overall integrity of the system. The best way to do this is to make sure that all critical components include built-in safeguards against fault conditions and unauthorized use. It is equally important that the system be easy to use and simple to set up and manage. And of course, the system must be cost-effective to install and maintain.

The card reader controller

The card reader controller is the system's doorperson. One is installed adjacent to each entrance to a protected area (which can include parking lots, garages, elevators, turnstiles, etc.). The controller monitors its attached card readers for activity. When a credential is presented to a reader, the reader passes a serial number to the controller where it is compared to a list of authorized numbers and valid schedules. If there is a match, the controller operates the lock, the door is opened, and the event is logged. If not, access is denied and the event is logged. When an individual leaves the area, the card access controller logs this event as well (by means of data received from an exit reader), thus, along with other controllers, a running tally of everyone who remains in the area can be maintained at all times.

When writing a specification for a card reader controller, reliability and security are the two primary concerns. The integrity of the entire access control system rests on the dependability of this component. A good spec will reflect that fact. Keep the following points in mind:

- **Protect the data.** Make sure any data that travels to the card reader controllers is encrypted. This prevents hackers from altering credentials or validating falsified credentials.

- **Guard against unwanted lockouts.** Specify that a standby battery and charging circuitry be an integral part of the card reader controller. This keeps locks operational in the event of a power failure at the door. There's nothing more irritating for building occupants than access denied because of a fault in wiring. It can lead to doors being propped ajar to let others into the area, defeating the purpose of the system – perhaps when it's needed most.

- **Trust nothing.** Don't rely on communication from the central data source for real-time access control decisions. Instead, specify a card reader controller that maintains all the relevant data, including work and holiday schedules, in its on-board memory. This type of controller uses communication with the data source for periodic updates only. It is invulnerable to temporary communication breaks and will continue to operate at 100 per cent effectiveness even if communications is lost.

- **Keep it simple.** Select a card reader controller that can handle all the hardware for a single door, including the exterior card reader, the lock mechanism, the automatic door opener, PIN keypad, and the interior request-to-exit reader or motion detector. Anything less can lead to cumbersome wiring, power supply problems and increased equipment costs.

- **Hedge your bets.** A good card reader controller will accept output from all industry standard card readers, including magnetic stripe, proximity, and even biometric. Specify Wiegand (26-bit) compatible readers in addition to any proprietary protocol your supplier may offer. This will ensure that replacements and compatible additions will be easy to find at a reasonable price.

- **Get a second opinion.** Make sure the card reader controller is listed to all the applicable Underwriters Laboratories standards including UL 294 (Access Control System Units), UL 864 (Control Units for Fire Protective Signaling Systems), and UL 1610 (Central Station Burglar Alarm Units). Comprehensive listings are a seal of approval that ensure regulatory compliance and provide the opportunities derived from emerging cost-cutting technology that shares system resources among access control, fire alarm, and security functions.

The access control database

The access control database manages data on the system. It resides on one or more networked computers, typically in the human resources or security department (where employee access is validated), a guard station (where credentials can be verified), and the reception desk (where visitor badges are issued). With password control, each user will access only authorized information and privileges.

The database is the card reader controller's overseer. It issues instructions as to which credentials are valid at what time and in what location. It receives information from the card reader controllers and collates it into understandable reports that detail precisely who went where and when.

The most visible side of the access control database is the user interface. Through this interface authorized users set schedules, define access levels, and validate and cancel credentials.

A good access control database interfaces with video badging software that creates photo badges and stores a picture of the person as part of their access control record. Advanced programs also have user-definable fields that store personal data about the individual. For employees this might include start dates, termination dates, benefits details and other information, thus making the program a single source for both employment information and access control.

Ensure the program has abundant customizable fields that users can set up for their own purposes.

When writing a specification for an access control database, flexibility and ease of use are two primary concerns. A program that is difficult to use will compromise the effectiveness of an access control system. A program that cannot be customized for a specific application will soon stagnate and disappoint. A good spec will reflect these facts. Keep the following points in mind:

- **Cover your assets.** Make sure the program is password protected with assignable operator privileges. This will allow it to be used in a number of different settings without compromising confidentiality or system integrity.

- **Follow a migration path.** Specify that the database be ODBC (open database connectivity) compliant. By using this industry standard, information in other databases such as Microsoft Access, SQL, and Oracle can be used to populate the records. This will smooth migration from and to other record-keeping programs.

- **Extend the playing field.** Ensure the program has abundant customizable fields that users can set up for their own purposes. This will extend the life and reach of the program and promote creative uses for it.

- **Simplify, simplify.** Choose a program that supports definable schedules and access levels. A schedule is a pre-defined list of times for which an individual assigned to it can gain access to an area. An access level is a pre-defined list of doors and keypads, allowable access times, and cardholder privileges. Everyone on the same shift or technicians who work in a particular lab can be assigned the same access level. This is a real time saver for database operators. Specify capacity for at least a couple of hundred access levels and the same number of schedules for the program. Also specify support for multiple access levels assigned to a single individual. Additional access levels are useful when an individual is on temporary assignment to a different department or location. Secondary access levels should be configurable to expire after a certain amount of time has passed.

The latest generation of control equipment merges building functions on a common platform.

- **Have happy holidays.** Holiday scheduling is a perennial problem for administrators because most fall on different dates every year. Make sure the program you specify has the ability for the user to create rules that shift holiday schedules to different days if they fall on a weekend. This will prevent unpleasant surprises when someone neglects to reconfigure the program in anticipation of an upcoming holiday.

- **Stay in the mainstream.** Make sure the access control database program you specify supports standard network protocols and that it doesn't require a dedicated computer. Specify standard operating system requirements, such as or Windows XP or 2000.

- **Timing is everything.** The program you specify should have the ability to control door functions such as unlock times, door open times, door ajar times. This will allow the user to fine-tune standard access control operations without having to pay a technician to configure each card reader controller to accommodate minor timing adjustments.

- **Keep tenants happy.** Advanced access control database programs support multiple tenant operations under which leaseholders maintain their own database of cardholders while sharing control over common areas like lobbies and elevators. Any system in a multi-tenant environment should have this capability.

- **Leave a paper trail.** Make sure the database program you specify has a wide range of predefined reports including cardholder, card transaction history, projected holiday, operator level, and resource usage. The program should also support user definable reports and the ability to filter data. Ensure that report data is exportable to other programs such as word processors and spreadsheets.

- **Spec all the tools.** Specify a program that includes a good assortment of functions as part of its standard package. These functions should include mustering, anti-passback, two-person rules, barrier-free access, and visitor operations. (See the sidebar on terminology for more on these functions.)

The control platform

The control platform handles communications for advanced access control systems. With the access control database at one end of the system and the card reader controllers at the other, it is the control platform that forms the vital link that makes everything work. This is where emerging technology is making its greatest strides. It is also where the most significant cost savings can be achieved.

Typically, an access control system is a separate entity that hosts its own network wiring, power supplies, master control panel, keypads, and so on. Several manufacturers have implemented communications protocols that allow the access control system to exchange information with the security system and the fire alarm system. Sounds like a lot of systems for one building, right? It is. But due to a regulatory logjam that requires the insulation of these systems to ensure that nothing will compromise any building's fire alarm operation, listing agencies will not permit any other functions to piggyback on the life safety network.

Edwards, the life safety innovator that pioneered breakthroughs such as intelligent smoke detectors and multiplex audio communications, has developed a method by which fire alarm, access control, and security all coexist on a common communications backbone. They have done this by successfully listing access control and security equipment to life safety standards. This not only elevates reliability and survivability of access control and security to the level required of fire alarm equipment, it also results in a synergy that creates a whole much greater than the sum of its parts.

This new generation of control equipment does not merely interact with separate building functions using artificial mechanisms that get them talking to one another. They merge these functions on a common platform. This renders the whole notion of gateways and communications protocols irrelevant. Why? Because data concerning all the functions flows across the same network. There is no reason to look for a common means of expression because they share the same nervous system.

Look at it this way: most people don't have a separate desktop computer for each task they want to accomplish. If you want a webcam, you plug it into the same PC that supports your scanner and printer and speakers. Your PC supports these different functions because the architecture allows it and because it's impractical and expensive to do it any other way.

Building systems are about to go the same way. But there are some significant differences. Fire alarm architecture has built-in redundancy that makes these systems extremely reliable and highly survivable. Fire alarm systems are required in all buildings in America today. So that redundancy and that infrastructure would have to be there whether or not your access control system takes advantage of it. The opportunity for an access control system to benefit from this inherent system reliability – at little cost – is an opportunity many in the field have chased after for years.

In addition to the reliability benefits of this new system synergy, there are performance advantages that streamline system management and cut costs significantly. Multiple functions operating on a single platform mean shared wiring, shared power supplies, and keypads that record access PIN numbers communicating over the same network as smoke detectors and motion detectors. It means lower installed costs, simpler maintenance, and reduced operating expenses.

Seamless interaction

Synergy permits access control functions to interact seamlessly with other functions by means of the common infrastructure. For example, to unlock exit doors during a fire, a simple program rule replaces additional conduit, wiring and interposing relays. To disarm pre-determined security partitions automatically when an authorized cardholder enters the building, another system rule easily provides a solution that would otherwise have required more hardware and related expense.

When writing a specification for an access control platform, look for opportunities to cut costs by sharing resources and taking advantage of an existing communications infrastructure. Thanks to this new and emerging technology, those opportunities are now endless, but the cost is insignificant.

Sharing system resources is simply a matter of using what's there already to achieve what used to take a mammoth effort to accomplish. We've come a long way from the Yale key, but by all accounts, this is just the beginning.

EDWARDS
A UTC Fire & Security Company

Detection & alarm since 1872

U.S.
T 888-378-2329
F 866-503-3996

Canada
Chubb-Edwards
T 519 376 2430
F 519 376 7258

Southeast Asia
T : +65 6391 9300
F : +65 6391 9306

India
T : +91 80 4344 2000
F : +91 80 4344 2050

Australia
T +61 3 9239 1200
F +61 3 9239 1299

Europe
T +32 2 725 11 20
F +32 2 721 86 13

Latin America
T 305 593 4301
F 305 593 4300

utcfireandsecurity.com