

Holding Down The Fort

By Edmonds H. Chandler, Jr., CPP

Seldom has there been a more difficult marriage than the one between electronic technology and physical barrier portals. While access control systems are faster than ever before and filled with control and data base management features, regular hinged swinging doors are still the barrier portal of choice. Fire and light-safety codes, not to mention moral responsibilities, mandate that exits require no special knowledge to use.

Does it make sense to use high-tech methodology such as retinal scanning with a door that, when opened from the inside, allows any number of people to enter? Where is the appropriate balance between electronic technology and physical barriers? To answer such questions we must examine both human nature and physical barrier portals.

Human behavior affects security. Our culture has a set of mores that dictates that you hold a door open for the next person if she or he is close behind. We cannot reasonably expect to change a population's mores. Therefore, tailgating will always be a problem at access-controlled swing doors. Security professionals and designers must consider the implications of such behavior and plan appropriately.

If a person is ready to go through a door and is called by someone who has not yet reached the door, he or she is likely to allow the door to close without going through. If the access control system has an antipassback mechanism and is checking for passage through the door, it will log the person through to the inside, when in fact he or she is still outside. Such an error is a logical failure mode. Such failures occur when users don't quite follow a system's rules, but don't do anything wrong, either. Access control systems should be designed to automatically correct all logical failure modes.

Barriers can be of two types: physical or psychological. Physical barriers include fences, parking lot barrier arms, and doors. Psychological barriers are more subtle and include property lines, lighting, signs, parking lot stripes, and visible closed-circuit television (CCTV) cameras. Barriers may be located outside, inside, or on the perimeter of a building.

Portals are gates or doors used as controlled openings in a physical barrier. They allow only people who have a legitimate need to transact business to enter a secure area. Portals are divided into authorization, validation, and authentication classifications.

Authorization is official approval or permission to enter a secure area. Typically, authorized individuals are included on a list of names or are issued identification such as an access control card or a visitor's badge. Keys to a building or area are perhaps the most common implied authorization.

The most common authorization portal is a card-in/free exit swing door with controlled access. This barrier consists of a standard swinging door with an electric lock, a door alarm connected to a monitoring computer, and an automatic sensor as an exit device.

The type of access control technology used is not critical. A portal can use any number of card readers, such as proximity, Wiegand, magnetic stripe, or barium ferrite. A card reader can be combined with a personal identification number (PIN) keypad.

The card reader or card reader/PIN pad combination, when used, releases the electric door lock, allowing the door to open, and at the same time shunts the door alarm contact for a present period. If the door is held open longer or is forced open without a valid card reading, an alarm is sent to the access control computer.

If the door is a free exit type, a sensor automatically picks up the motion of an approaching person and shunts the door alarm contact. An alarm is not sent to the computer every time someone exits from a secure area.

If the exit has a card reader or card reader/PIN pad combination, the card reader shunts the door alarm contact and releases the electric lock, allowing the door to open. Variations of this setup include electric locksets or electromagnetic locks instead of electric strikes, and microwave request-to-exit devices in lieu of infrared. The basic operation of all of the variations is similar.

Once a door is open, any number of people can walk through. So the throughput, or average number of people moving through a portal, cannot be determined for a card-in/free exit or card-in/card-out swing door. If you expect people to use access cards to enter your building, then the peak loading should be fewer than four people per minute so that the door can be closed and locked between transactions.

Obviously, that rate is impractical. Therefore, the design of card-access swing doors should not assume one card-per-person transactions. Also note that the increase in the degree of security between using a card reader alone and using a card reader with a PIN pad is minimal. A swing door with a PIN pad does not limit tailgating the way a revolving door or mantrap does.

A swing door is a non-validating portal, and adding a PIN pad decreases the throughput, which increases personnel time costs. The best you can hope for with non-validating portals is some kind of an audit trail from card-in/card-out doors combined with a very strong management policy against tailgating.

A PIN pad is of benefit primarily when cards are lost. If an unauthorized person finds an access card and tries to use it at the portal without the PIN, he or she will not be granted access. However, most lost or stolen cards are quickly reported and programmed out of the database.

Most lost access cards also cannot be matched with their facilities because they don't have the building's address on them. Typically, a return PO box is printed on the back with a notice "Postage guaranteed. Drop in any mail box." Both instances cut down on the need for a PIN pad.

Also beware of double fire doors that are supposed to be access controlled. Chances are they will not close and latch properly. You simply cannot guarantee proper functioning—even just a few months after installation—without installing a \$3,000 door operator. Your best bet is to set up the double doors as equipment doors and alarm them. Then put a single door next to them for access and egress.

Validation involves comparing a form of identification, such as a driver's license, credit card, access control card, or visitor's badge, to an up-to-date list or database to determine whether it is, in fact, valid. A validating portal requires each user to have an access card.

Validation portals, in ascending degree of security, include the following:

- Low turnstiles monitored by a security officer
- Optical lanes monitored by a security officer
- Full-height barred turnstiles with a manual method for resolving normal failure modes
- Motorized revolving doors that account for failure modes
- Mantraps with card readers and/or PIN pads

Turnstiles are aesthetically oppressive. They are noisy, uncomfortable, and an obstacle to emergency egress. They are also costly to maintain. Briefcases and coats get caught in the bars. Corporations and building designers are reluctant to install these devices in their lobbies.

Lanes are really optical turnstiles. They serve the same purpose while allowing for a much more aesthetic lobby. When properly designed, they blend into any environment and are quiet. Since proximity access technologies read through most nonmetal surfaces, they can be used with marble, glass, and formica surfaces.

Both turnstiles and optical lanes must be monitored by a security officer to ensure that each passage is associated with a valid card read. When an access card is accepted by the system, the lane signals a person to proceed with a series of green lights. The person walks forward, tripping an optical beam.

Once the user is through the beam, the system resets to accept the next card, flashes an amber light for the next person, and turns the card reader back on. These systems process 30 people per minute per lane. Each entrance is validated, since each person must present an access card, but antipassback is required for valid operation.

An antipassback mechanism allows the access control system to differentiate between "in" and "out" card readers and keeps track of each user's status. This tracking forces people to use the cards properly and, after they have entered, prevents them from passing back a card to someone who has not yet entered.

Antipassback is a good tool for obtaining a reasonably valid audit trail. However, when antipassback is applied to a non-validating barrier, people tailgate. The result is always management headaches and user frustration. When users tailgate to enter, for example, they cannot use their cards again until their cards are reset to reflect their proper location. They are inside the barrier, not outside as the card thinks.

Full height barred turnstiles provide a secure, reliable barrier. They are considered even less aesthetically appropriate than low turnstiles, however. One of the two types of barred turnstiles uses a solenoid locking mechanism like the low turnstiles. The potential logical failure modes are numerous for these portals, requiring a security officer to reset cards that are logged to the opposite side of the barrier. Revolving doors normally use a CCTV camera and intercom link to handle any problems that might arise. A second type of full-height barred turnstile is motorized and operates like a motorized revolving door.

The glass storefront type of revolving door does not require a security officer and also controls tailgating. A revolving door is also a physical barrier. It is typically set up as a four-leaf, six-foot-diameter door, and each quadrant is a 90-degree pie wedge with a three-foot radius.

It is socially uncomfortable for two people to be in one compartment at the same time. If two people do enter the same wedge, they end up walking on each other's feet. Americans require more personal space than one compartment allows for two people. Therefore, most people simply don't walk in two at a time. Once again, social mores are a factor, but this time in security's favor.

No electronic method exists to detect tailgating reliably. Some methods partially succeed in detecting two people in a wedge, but at times they can successfully enter as one. A door of this type has a very aesthetically pleasing look and, as previously indicated, can operate without an officer present.

A revolving door's throughput is one person every three seconds, maximum. Numerous factors lower the throughput, however, resulting in a realistic average of one person every five seconds. A revolving door's advantages over lanes are that it provides a physical barrier and does not require a security officer. Such a door has a payback of six months to two years, depending on the required hours of operation.

You should watch out and compensate for two failure modes in motorized revolving doors. First, someone may present a valid access card to either the "in" or "out" reader, but fail to enter the building due to some distraction. If an antipassback feature is operating, the access control system shows a person with a valid card on the inside of the barrier when in fact he or she is still outside.

A revolving door that accounts for failure modes allows the user another chance to enter. Custom software for an access control computer contains an algorithm allowing the computer to sense that a user did not go in.

Second, two people may approach a door simultaneously from opposite sides and present their cards to the readers. The “in” reader reads a valid card, but the “out” reader doesn’t. However, the door has already started revolving to accommodate the incoming party. The door stops in mid-cycle, backs both people out, and allows the valid cardholder another opportunity to enter.

The barrier with the highest degree of validation is a mantrap with a card reader or PIN pad. The following design is just one of many ways to set up a mantrap.

As the name implies, a mantrap is a small room with doors at both ends, one leading to a secure area and one to a non-secure area. Users normally enter a mantrap after using a card reader, which eliminates unwanted traffic. That card reader may also turn on a light above one of two other card readers inside the mantrap, indicating which reader controls the second door leading to the secured space.

To exit a secure space, users push a button that unlocks the door into the mantrap and turns on the appropriate light above the outgoing card reader inside. Users then present a valid access card to exit the mantrap. Again, a CCTV camera and intercom link handle any problems and determine that only one person is in the mantrap at a time. Even though a mantrap improves the chances of valid access control and audit trail, the throughput is less than half that of a revolving door—one person every ten seconds.

Authentication is determining that a person presenting an access card or PIN is in fact the person he or she claims to be. Authentication uses a physical characteristic such as fingerprints, hand geometry, or retinal pattern to verify identity. An authentication portal verifies a user’s identity and his or her right to be in a secure area.

Authentication, the highest degree of barrier portal security, is achieved with a mantrap and a biometric device such as a hand geometry reader or retinal scanner linked with one inside card reader. Authentication is recommended for a controlled environment only, such as a mantrap, because only a controlled environment ensures that the people entering are the same ones that went through the authentication process.

A CCTV camera and intercom link are used for counting people and making exceptions. As usual, the higher degree of security costs more—in this case in personal time. Some mantraps are set up to weigh the entire unit, including walls, floor, ceiling, and doors. As long as only one person is in the mantrap and authentication includes an acceptable weight limit, the entire process is automatic. Control room personnel are involved only in exceptional cases.

The authentication mantrap has an average throughput of only three people per minute. A cost comparison of barrier portals should consider long-term operation costs—mainly personnel time—as well as short-term initial installation costs to achieve a proper perspective.

Mantraps are not good emergency egress points. The best idea is to put an alarmed door parallel to the mantrap in the barrier.

With all barrier portals, time costs have substantial economic ramifications. Slowing people down on their way to and from work is psychologically difficult. Therefore, conducting loading studies of each minute of each peak period is important. Then design the system's capacity to handle the volume without queuing. Use density and work schedule data to estimate loading when the building is in the design phase.

A barrier's portals should be consistent in what they achieve. A swing door using an authentication control on one end of a space coupled with a higher-security validation portal on the other end makes little sense. Sites should be designed using a concentric circle approach to security. Portals should be consistent within each circle.

With the barrier portal designs available, any site can be secure, aesthetically pleasing, and free from queuing—ideal for getting business done efficiently.

About the Author... Edmonds H. Chandler, Jr., CPP, is chairman of Security By Design of Concord, CA, which provides security, fire, and data control center consulting and engineering services to commercial, industrial, and government clients. Ed Chandler is also a member of ASIS.