Understanding Access Control

To understand access control, we must understand the language of the industry. Terms like alarm inputs, relays, timezones, anti-passback, shunt, and access levels are commonly used when discussing access control systems. It is not uncommon for someone to say we will shunt the alarm on the anti-passback door during timezone 2, and trip the relay during timezone 4. But what does this mean? Let’s examine the basic terminology used in today’s systems. We will start with timezones.

Timezones

Timezones are used to control when things will happen. A timezone usually consists of a start time, a stop time, and selected days of the week. Rather than re-keying the entire timezone each time we want to use it, systems will generally provide the ability to use a name or a number which will represent the entire timezone.

For example: Timezone number 5 may be programmed for the warehouse crew to work from 8 AM to 12 PM every Saturday.

When programming timezones a 24 hour clock is always used; use of a 24 hour clock allows the system to differentiate between 11 AM and 11 PM. When using a 24 hour clock midnight starts at 0:00, while lunch time is 12:00. Hours are to the left of the colon ( : ) while minutes are to the right. Afternoon, begins at 12:00 and continues to 13:00, 14:00, 15:00 etc. In some systems timezones cannot span midnight, but by linking two timezones together the system can handle events which begin one day and continue to the next.

The following chart helps to explain the time cycle:

<table>
<thead>
<tr>
<th>Time</th>
<th>Equates To</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00</td>
<td>Midnight</td>
</tr>
<tr>
<td>02:00</td>
<td>2 AM</td>
</tr>
<tr>
<td>06:00</td>
<td>6 AM</td>
</tr>
<tr>
<td>12:00</td>
<td>12 Noon</td>
</tr>
<tr>
<td>13:00</td>
<td>1 PM</td>
</tr>
<tr>
<td>14:00</td>
<td>2 PM</td>
</tr>
<tr>
<td>19:00</td>
<td>7 PM</td>
</tr>
<tr>
<td>23:59</td>
<td>One Minute before Midnight</td>
</tr>
</tbody>
</table>

At midnight the clock starts at 00:00 again.

When setting up timezones, the days are just as important as the time. Typical needs include access for staff 9:00 AM to 5:00 PM Monday through Friday. Supervisors, managers, and owners may have access 24 hours a day, 7 days a week, including all holidays.
Most systems will allow holiday programming, so if a holiday occurs during a weekday, the system will allow only people designated for holidays to gain entry.

If a particular cardholder has access for an area on a normal weekday, but that day has been designated as a holiday, the user would be denied access unless his timezone includes holidays. The operation of alarms and relays may also be programmed for different operation on holidays.

Timezones may get quite detailed. For example, a user may have different access needs on different days, as in the following example:

<table>
<thead>
<tr>
<th>Time</th>
<th>Days</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 - 17:00</td>
<td>Mon Wed Fri</td>
<td>Standard Hours</td>
</tr>
<tr>
<td>08:30 - 19:00</td>
<td>Tue Thur</td>
<td>Stays Late 2 Days a Week</td>
</tr>
<tr>
<td>08:00 - 12:00</td>
<td>Sat</td>
<td>Half a day on Saturday</td>
</tr>
</tbody>
</table>

Different timezones may be assigned to different people for the same areas. Likewise, a single user may be allowed through some doors always, and other doors during certain times only. Lunch rooms and break areas may only be open from 11:30 to 1:30, while the lobby area may be entered at any time. A single card can be programmed for both these areas.

Timezones can be used to control other things besides access times to various areas for employees. Relays can be turned on and off, alarm zones can be activated or deactivated, and doors can be unlocked, all automatically when a timezone is activated by the system clock.

Access Levels

Access levels determine where a user’s card will be valid. A single name is assigned to each access level, and represents the group of doors the cardholder will be programmed for. When we assign an access level for a card, we are assigning an entire group of doors to that card. This eliminates the tedious programming of each door for every user that would otherwise be required.

Access Levels are combines with timezones to determine both where and when a cardholder can gain access.

Anti-Passback

Tailgating is when one user enters with a valid card read, and several people enter without using their cards. Anti-passback can be implemented to help alleviate this problem, by tracking whether the card is inside the secure area or outside.

When anti-passback is used, a card must first be used at a designated “in” reader, then at a designated “out” reader, before it can be used to “read in” again. In the event that the user did not read in at the in reader, and tried to read out of an area, an anti-passback
violation would occur. The violation may just log the event as an alarm condition, or may not allow the door to be released. Since users who fail to use their card and walk in with other employees may get stranded or locked in, they are more likely to be sure to use their card each time they enter or exit. Readers on each side of the door are required for implementation of anti-passback.

Relays

*A relay is an electronically controlled switch. Similar to a light switch on the wall being used to turn on or off a light, a relay can be used to turn on or off other devices.*

Relays are used to activate the electric door lock, or to activate a variety of other items such as:

- Bells, sirens, or strobes
- Call up a specific CCTV camera to a monitor
- Turn lights on and off
- Bypass alarm systems
- Activate alarms locally or remotely
- Display alarms on a graphic enunciator
- Trip a digital dialer
- And many other uses.

Relays are located on the access control panel. Each panel will have one or more relays. Typically, one relay is used to control the electric strike. The others can be used as needed.

When a relay is activated or deactivated, the device wired to it is turned on or off. Relays can be activated or deactivated for a short, user-programmable time period from 1 second to several minutes, or even several hours. The electric door locks used on access control systems are usually turned on for 3 to 5 seconds.

Relays can be activated or deactivated by a variety of events. An alarm input, a valid card read, an egress button being pushed, or a timezone can all activate a relay. The relay will then turn on or turn off the device wired to it.

Alarm Monitoring

Access control systems typically have multiple alarm inputs. Alarm inputs are used to monitor various devices which are wired back to the panel. When a card reader is installed on a door, an alarm contact is usually installed as well. The alarm contact is used to monitor whether the door was forced open, or left open after a valid access was granted. The alarms are reported to the system operator on a display or printout.
Some of the devices that are typically monitored by access control systems are indoor motion detectors, panic alarms, various doors (doors with and without card readers), loading dock doors, temperature, windows, glass break sensors, etc.

**Shunting of alarm devices which are being monitored, means to bypass or ignore the alarm for a specified period of time. Alarms can be shunted by an event or a timezone.**

When an access control door is monitored with an alarm contact, the alarm contact will be shunted on a valid card read. The shunt time is user programmable; typical shunt times are 30 to 45 seconds, but may be adjusted as needed in the panel’s programming.

If the access control door is monitored with an alarm contact, the alarm contact must be shunted (bypassed) every time an authorized person passes through the door. If the door is opened without the point first being shunted, an alarm will be activated.

If a valid card read shunts the alarm when going in, what about when going out?

Alarm contacts must be shunted on egress.

There are two ways to shunt an alarm when leaving. First, a card can be required to open the door from each side. This is a called read in and read out. The second method is to install a special alarm input called an egress button. Virtually every access panel has a special egress input. When activated this input will shunt the associated door alarm, and may also be used to activate the relay, which in turn unlocks the electric door lock.

Egress buttons may be activated and deactivated by timezones. This would set up valid times that the door could be exited from. If the egress button were pressed at any time other than the valid timezone, the door would remain locked or sound an alarm if opened. Car must be taken to provide effective door alarm shunting when people exit. Otherwise excessive false alarms will be reported.

The choices for egress devices are influenced by your choice of electric door locks. Some styles of electric locks keep the door locked from both sides, until a valid card read or egress request is received. Egress buttons work well with these types of locks; drop bolts and magnetic locks fall into this category.

Other locks will allow free egress by turning the door knob. Remember if the door knob is turned and the door is opened without the egress button being pressed first, a false door alarm will be received. The problem is that human nature being what it is, no-one will press the egress button when they can simply turn a knob to go out the door. Passive infrared motion detectors work well in these applications, since they will automatically trip the egress input as someone approaches the door.
**Alarm Supervision**

When alarms are supervised, they are constantly monitored for opens or shorts caused by faulty wiring or tampering. When a fault is detected, a trouble report is sent to the operator.

Systems are available with and without supervised alarm inputs.

**Access Control Panels**

The access control panels vary depending on your application and the particular manufacturer you are working with. Every panel or device made serves as an interface to the readers and door locks. Most of these panels are interconnected by wiring in a network.

**Electric Door Locks**

The electric door lock keeps the door locked and secure, and releases the door when a valid card is used, or a valid egress request is received. The electric lock is an electro-mechanical device. Since it has many mechanical parts, electric locks are subject to wear and failure. Since a lock failure can defeat the entire security of a facility, a quality lock should be installed on every door.

Electric locks are available in a variety of configurations to fit virtually any door made. Let's discuss various doors that may need to be secured. There are many.

One type which is common is a wood or metal door, with either a wood or steel door frame. Some doors on schools, industrial buildings, and warehouses are outfitted with a crash bar for exit. These doors have a bar, which is about waist high and runs across the door. When depressed the bar releases the door. Other doors encountered may be clear herculite, and may or may not have a frame. Banks and retail stores, and some industrial buildings may have aluminum door frames, and aluminum framed glass doors.

Determining the proper locks for the door can be an intimidating experience. Electric locks used on access control systems include electric strikes, magnetic locks, drop bolts, and electrified locksets. With careful consideration, the proper lock can be easily specified.

Doors can be hinged on either the right or left side. Some locks may be used on either right hand or left hand doors, while others must be ordered properly handed for the door. To determine if a door is a right handed door or a left handed door, stand on the push side of the door. If the hinges are on your right, it is a right handed door. If the hinges are on the left it is a left handed door.

An electric lock which is installed at knob height on the door frame is called an electric strike. When this type of electric lock is installed, the existing lockset strike plate on the
door frame is removed and the new electric strike is installed in its place. Electric strikes are installed by cutting into the door frame at the same height as the door knob. The strike chosen must be compatible with the lockset (door knob) on the door. When evaluating a lockset look to see if it is a mortise, cylindrical, or rim type, and what the latch projection is.

The latch is the part that sticks off the edge of the door, and is retracted when the knob is turned. Typical latch projections are $\frac{1}{2}''$, $\frac{5}{8}''$, or $\frac{3}{4}''$. The strike should be deep enough to allow the latch to be fully extended, without hitting the back of the strike.

**Cylindrical and Mortise Locks**

Cylindrical locks are common today. They can be identified by looking at the edge of the door. Cylindrical locksets are installed in a door by boring a hole of about 1” diameter in the frame for the latch. A cover plate keeps the latch in alignment and provides a finished look.

Mortise locks can be identified by looking at the edge of the door as well. A mortise lock is installed into a mortise. A mortise is a large rectangular pocket, which is chiseled into the door itself, and is usually 3” to 4” high.

Rim strikes are installed for doors which have crash bars on them.

Door hardware comes in standard sizes. When installing a strike the existing catch on the frame will be removed and the electric strike will be installed. The existing catch is usually a standard ANSI size. Some cutting of the door frame is always required for installing electric strikes. The cutting can be minimized by choosing a strike that will fit the standard ANSI cutout for the door frame. By using a strike that matches the existing cutout on the frame, only a small cutout on the face of the door frame needs to be made. The strike can then be fitted into the existing ANSI cutout, and fastened to the existing screw holes.

Wood door frames are inherently weak. When choosing a strike for a wood frame door, look for a unit that will require a minimum cutout, and that will space the screws which fasten the strike to the frame as far away from the cutout as possible. Minimizing the size of the cutout in the frame provides the strongest installation possible.

**Magnetic Locks**

Magnetic locks are surface mounted and are quite easy to install. A magnetic lock, which is sometimes referred to as a Mag Lock, is a two piece lock consisting of an electro-magnet, and an armature plate. The electro-magnet is installed on the door frame; the armature is mounted to the door itself. The lock creates a magnetic holding force of up to 1,500 pounds which hold the door shut by holding the armature to the magnet until the electric power is removed. Magnetic locks have no moving parts and are therefore very reliable.
Electric Lock Considerations

When choosing a lock for an access control system, you would almost always want to use a continuous duty model. Electric locks are available in intermittent or continuous duty models. Intermittent duty models are designed to be powered for less than 1 minute, while continuous duty models can be powered for longer than 1 minute. Virtually every access control system provides the operator with the ability to continuously unlock a door. An intermittent duty lock will burn out if energized beyond a few minutes, and therefore would not normally be used.

Locks are available in fail safe and fail secure versions. Simply stated fail safe versions are normally powered and released or unlocked when power is removed. Fail lock versions are normally locked when they are not powered, and unlock when power is applied. To look at them from another viewpoint:

*Fail lock strikes, which are also known as fail secure, remain locked in a power failure condition. Fail safe strikes release the door in a power failure condition.*

Fire Egress

Safety and security of the personnel in the facility are of paramount consideration when implementing an access control system. Every local code requires safe uninhibited exit from a building in the event of fire or other emergency. However, in order to provide an effective access control system, it is sometimes necessary to secure these egress points with access control card readers. When this is necessary either mechanical egress must be provided, or a fail safe strike or lock is installed on the door.

Mechanical egress systems allow the door to be released by a crash bar, or by turning the knob to open the door, which will allow the user to exit the building uninhibited during an emergency.

If securing the door will inhibit emergency egress and mechanical egress is not available on the door, then the strike, Mag Lock, or dropbolt is additionally tied into the building fire system which will break power to the lock whenever a fire condition is detected.

*Local codes and authorities should be consulted to ensure all systems installed will be in compliance.*

Certain doors on a facility may be fire rated doors. Fire rated doors are designed to stop the spread of fire throughout a building. Building codes require fire rated doors to remain locked, and to withstand certain duration of fires without burning through. Fail lock strikes are required on fire rated doors; the lock must be designated as a fire rated unit, which will withstand a sustained duration fire condition. Fire rated doors can be identified by a tag on the hinge edge of the door.
**Reporting Logging Printing and Interfacing with the Users**

Access control systems range from simple to complex in how they provide the ability for the customer to program them and receive activity logs from them.

Some simple systems use a hand held programmer which can be taken to each individual reader on the system. Some of these systems will allow the user to retrieve or log the cardholder’s entry to each door to a printer.

Other systems can be wired together in the facility, on a data communications buss. These systems will allow the operator to program any panel without leaving their office, by using a proprietary programmer that is compatible with the field panels. These systems also report valid access activity back on the communications buss to a central logging printer.

More sophisticated systems use a network of field panels wired on a communications network back to a central computer. Central computers provide excellent user interfaces for access control systems and offer the following improvements and advantages.

- Permanent storage of alarm and access events into a history log.
- Searching and reporting of information in the history log, such as each time an individual entered a particular door last week or last month, is much easier and more accurate than trying to review printouts.
- Permanent storage of the system database. If a system component fails, the data can be sent from the computer to the new panel when a replacement is installed, rather than having an operator re-key the data manually.
- Operator instructions, floor plans, maps and graphics can be displayed on alarm, or when a card is used. Using this feature makes it very easy to train new personnel to respond to events, and makes the security system more effective.

Advanced computer based systems can have several computers or workstations, wired together in a network. These systems will allow various system operators to perform different functions at each workstation. One operator may be handling alarms, while another would be programming additional cardholders, while a third might be running a report.

Many systems available today offer a software interface to allow events received by the access control system to be sent out to a CCTV system to call a particular camera to system monitor, when an alarm or card read is received. The software interface uses data communications, as opposed to hard wiring alarms and relays between the two systems.

**Systems Architecture**

Access control systems use centralized processing, distributed processing, or hybrid arrangement. The system architecture should be taken into consideration when designing an access control system, since it can have a significant effect upon operation during a catastrophic system failure.
Centralized Processing

In computer dependent processing systems, all events are gathered by the field panels, and are then sent to the computer for processing. For example if a card is presented at a reader, the reader sends the card number to the central computer or processor. The computer checks the card number against its programming and determines if that card is allowed through that door at that time. If the card is valid the computer sends a command back to the panel to release the door.

In these systems if the computer goes down, or if communications between the panel and computer is lost, the system can no longer function, to verify proper access, and to process alarms.

In computer dependent systems, the field panel checks the facility code of the card prior to sending it to the computer. When the panel can not communicate with the computer, the system will go onto a “degraded mode.” When in degraded mode, the panel will verify the facility code of the card, and will let anyone in who has a valid facility code. This means that entry is granted regardless of whether that person is allowed at that door, and whether it is a valid time for the entry or not, provided the cardholder’s facility code matches the system facility code.

Some centralized processing systems will prevent any access during degraded mode, while others will allow only a small pre-selected group of cards to gain entry during degraded mode; and some systems will provide little or no control letting virtually any cardholder go anywhere.

Distributed Processing

In distributed processing systems the database is loaded to the field panel. All decisions are made at the field panel and are passed to the computer or logging printer for storage. In these systems if communications is lost, access control continues uninhibited. Furthermore, the events can sometimes be stored in the panels, and can be sent up to the computer once communications is restored.

Due to their architecture, systems which employ distributed processing generally offer better reliability, and faster response than systems that rely on central computers for all decision making.