Access Control 101

An introductory training presentation to introduce basic concepts of access control

TEAM • PARTNERSHIP • SUCCESS

What is Access Control?

- In physical security, the term access control refers to the practice of restricting entrance to a property, a building, or a room to persons
- Historically this was keys and locks
- Electronic access control solves many of the issues a traditional key and lock cannot

VAX VICON ACCESS CONTROL

A Brief History Timeline of Access Control

- **Caveman** (*club*)

- **Brace** (*log*)

- **A key lock**

- **Electronic keypad**

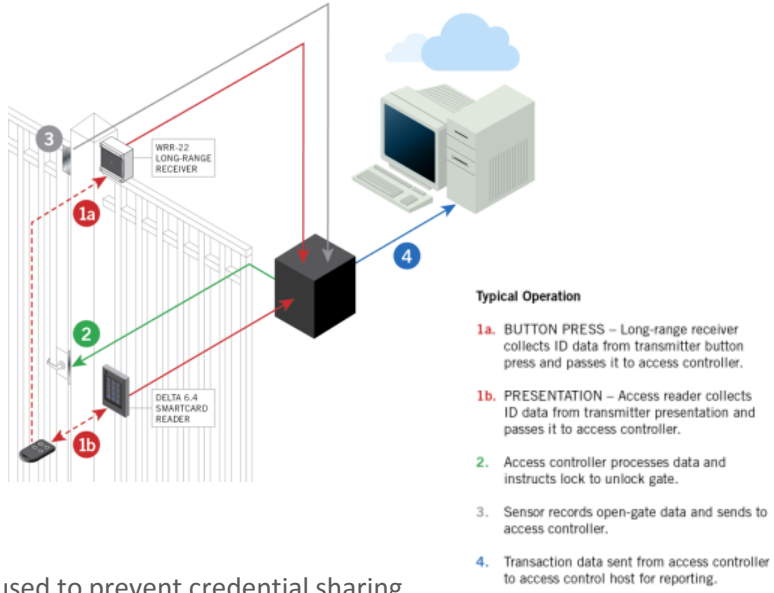
- **RFID cards and readers** (*125 kHz*)

- **Advanced RFID using encrypted authentication** (*13.56 MHz*)

- **Biometrics** (*fingerprint, hand, facial, iris recognition...*)

Access Control Operation

- **Credential ⟹ reader ⟹ control panel**
- **The control panel compares the credential number to an access control list**
  - Grants access or denies
  - Sends transaction to database
- **Access granted**
  - A credential match
  - Operates a relay that unlocks the door
- **Access denied**
  - A credential mismatch with a database list
  - Door will remain locked
- **Control panel will ignore door open signals to prevent alarms**
- **Reader can provide feedback such as a red or green LED for access denied or granted**



The description above describes a single transaction.

Features such as anti-passback, PIN, second credential or biometric input can be used to prevent credential sharing.

Access Control Credential Types

Some typical credentials in the access control world

- **Something you *know***
  - Example, a number or PIN
- **Something you *have***
  - Example, *access badge, card, key fob or any other key*
- **Advanced technology**
  - Biometrics; fingerprints, facial recognition, iris recognition, retinal scan, voice and hand geometry

Key Components of an Access Control System

The Controller, also referred to as a panel or head unit, is the brains of the system. Connected to the Controller are the peripherals that send data or state changes back to the Controller so that it can make a decision, based on its programming, as what to do next.

In a very simplified example, the most basic components connected to the main Controller would be as follows:

- Proximity Reader
- Door Contact
- Exit Button
- Electrified Strike or Maglock
- Power Source for the lock
- Power Source for the controller
- Communication Device to talk to the main computer

What is Proximity Reader?

A proximity reader is a device mounted at or near the door that requires controlled and monitored access

There are many "Wiegand" formats in existence, the most common being an industry standard referred to as "26-BIT Standard"

Types of Reader Examples

VAX-300R
Small and slim; ideal for narrow mounting areas or frames (3.125”H x 1.75”W)

VAX-500R
Standard wall mount electrical receptacle box (4.5”H x 3.0”W)

VAX-600KP
Standard wall mount electrical receptacle box (4.5”H x 3.0”W)

Types of Proximity Readers (cont'd)

Mullion or Single Gang Vandal Resistant Proximity Reader
Fully potted polycarbonate construction to resist tampering and corrosion
(5.25"H x 2"W) / (4.5"H x 3"W)

Mullion or Single Gang Vandal Resistant Proximity Reader
Solid stainless steel construction with reinforced and bullet-resistant insert
(5.25"H x 2"W) / (4.5"H x 3"W)

Types of Proximity Readers (cont'd)

There also exists the integration of other reader technologies that would be supported by Vicon VAX under certain conditions.

This would include the use of **BIOMETRIC** readers, which establish a personal identity verification using a physical or behavioral trait such as a fingerprint, full hand scan, retinal scan or facial recognition.

Another option is **MAGSTRIPE** readers typically using the ABA Track II method.

Lastly there is "**Contactless SmartCard,"** which reads and authenticates information stored on a chip embedded on the credential.

In order for any of the above technologies to connect to and function with the Vicon VAX system, the particular reader/device MUST have and support a Wiegand output that can be connected back to the controller.

Types of Proximity Readers (cont'd)

VAX-LRR2 and VAX-LRR4 Long Range RF Receivers with VAX-LRT4 and VAX-LRT2 Long Range RF Transmitters

These items are not actually "proximity" readers but rather use a higher frequency 433MHz wireless encrypted transmission between the receiver and the handheld remote. They have a transmission range of fixed at 100' (*VAX-LRT2*) or adjustable at 200' (*VAX-LRT4*).

However, the handheld remotes have built-in proximity, which means they will still also function at a conventional reader.

Most commonly used in parking garage and gate installations.

What is a Wiegand Output?

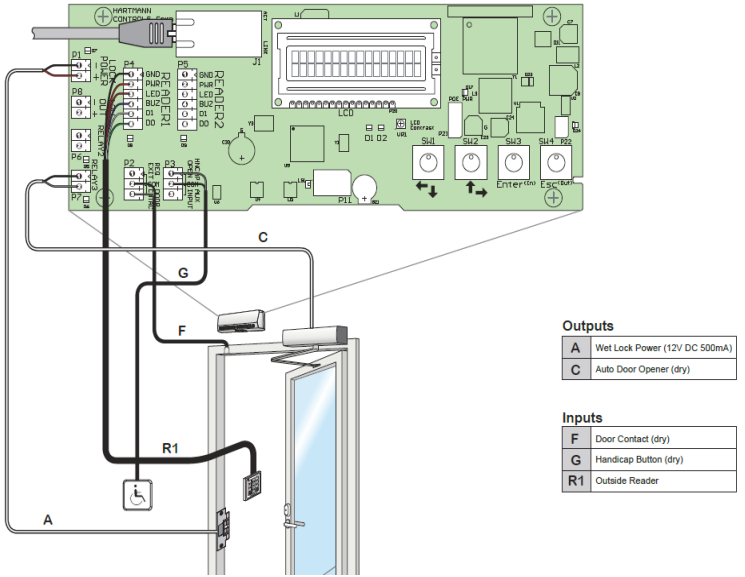
The **Wiegand** interface is a defacto wiring standard which arose from the popularity of **Wiegand** effect card readers in the 1980s. It is commonly used to connect a card swipe mechanism to the rest of an electronic entry system.

Vicon VAX supported formats:

- *26-bit Industry Standard*
- *26-Bit HID, 26-Bit Cansec*
- *32-Bit Kantech*
- *33-Bit DSX*
- *34-Bit HID*
- *35-Bit Xceed*
- *36-Bit Keyscan*
- *36-Bit Vertex*
- *37-Bit Xceed*
- *37-Bit Fairway*
- *37-Bit HID*
- *40-Bit Hartmann*
- *42-Bit VICON*

Single Door Typical

(with motion, single reader, door contact, auto door opener)



Outputs

A	Wet Lock Power (12V DC 500mA)
C	Auto Door Opener (dry)

Inputs

F	Door Contact (dry)
G	Handicap Button (dry)
R1	Outside Reader

Types of Credentials

Standard Clamshell Proximity Card
125kHz RFID credit card-sized media made of ABS plastic. Read range up to 8”.

Graphics Quality Printable Proximity Card
125kHz RFID credit card-sized media made of PVC plastic for dye sublimation printing. Available in 46MIL and 31MIL thickness. Read range up to 6.5”.

Multi-Technology Graphics Quality Printable Proximity Card
125kHz RFID credit card-sized media made of PVC plastic for dye sublimation printing and ABA Track II magstripe read. Available in 31MIL thickness. Read range up to 6.5”. (*Also available with embedded SmartChip 13.56MHz with 1K or 4K memory, CSN and Sector.*)

Proximity Key Tag
125kHz RFID media made of ABS plastic with brass eyelet for keychain loop. Read range up to 4.5”.

Types of Credentials (cont'd)

VAX-LRT2 and VAX-LRT4 Long Range RF Transmitter with Built-in Proximity

Available in 2-button and 4-button models for integration with the 433MHz VAX-LR22/44 Long Range Receivers (*primarily for parking/garage applications*). Transmit range up to 200 feet.

Each button can be configured to manage a specific access point.

Also has built-in 125kHz RFID proximity so that it can be used for dual purpose and presented to a standard proximity reader and function same as a card or fob for access. Read range up to 2" RFID.

What is a Door Contact?

- A door contact is a non-powered (*dry contact*) magnetically influenced device that is commonly used to monitor the state of a door or access point.

- The advantage of using door contacts to monitor the state of a door is that if a door is opened without the use of a credential, the controller will generate a "**Forced Open**" message.

- If a door is legitimately opened with a credential and access granted, the door contact state going to an "open" state will identify to the system that the door was physically opened and likely a person walked through "**Access Granted – Door Opened**".
  You can also assign a maximum time to allow a door to be opened from a valid access; exceeding this time parameter would generate a "**Held Open**" message.

- Its natural state when a door is closed is referred to as "**Normally Closed**" and when a door is opened, the magnet no longer holds the door contact switch closed and its state changes to "**Normally Open**".

Types of Door Contacts

A door contact is available in a variety of styles, shapes and sizes as well as how they function.

Below are the most common types available:

Door/Door Frame
Concealed Magnetic Door Contact

Door Frame
Hidden Magnetic Door
Contact/Switch

Door/Door Frame Surface
Mount Magnetic Door Contact

Door Frame Surface
Wireless Magnetic Door
Contact/Switch

What is an Exit Button?

- An Exit Button is a device that is used to allow a person to pass through a door from the non-secure (*non-reader*) side if access control and credential monitoring is not required both directions through a door.

- This device can be a wall mounted button that is physically pressed and then sends a command to the panel to unlock the strike to allow for egress (*action of going out*). It can also be a push bar attached to the door.

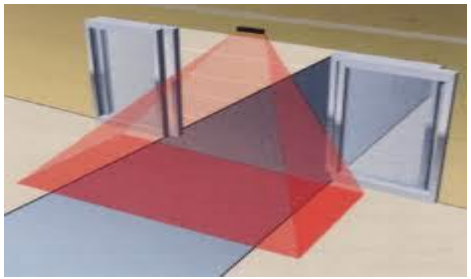
- Typically the natural state of an Exit Button is "**Normally Open**" and when pressed or activated goes into a temporary "**Normally Closed**" state, which the controller recognizes and performs the action of unlocking the strike and allowing egress. This can be inverted if necessary. Similar to a door contact, the exit button or device is a non-powered (*dry contact*) input signal.

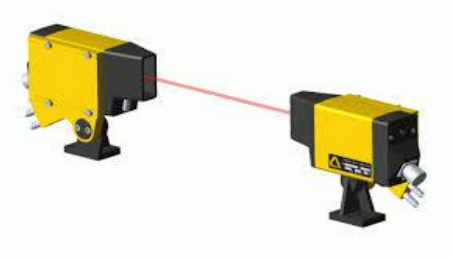
- VAX controller has a built-in request-to-exit (REX) button.

Types of Exit Buttons

An exit button (*or egress triggering device*) is available in a variety of styles, shapes and sizes as well as how they function.

Below are the most common types available:





What is an Electrified Locking Device?

An electrified locking device is a mechanical device that uses power to either unlock a door or keep a door locked.

There are 2 basic categories:

- **Door Strike**, which is a device that is either mounted into the door frame or into the actual door itself, and uses a powered solenoid to unlock the door or hold a door locked. It is typically an integrated assembly that also incorporates the door handle mechanism and may also have a keyed option.
- **Maglock** (*also referred to as Electromagnetic*), which is a device generally mounted at the top of a door frame (*opposite to the door hinges*), which when powered, magnetically holds a steel plate which is attached to the door to keep the door securely closed.

Door Strikes are available in many configurations of styles, mounting and operation

- Simple put, door strikes generally will be powered from an external power supply (*the Vicon VAX controller, however, does have a powered output for door strikes*). Most strikes are powered by 12VDC, however some are 24VDC and some even have the configurability within the same lockset to choose its voltage level. Some locksets use AC voltage, although that is less common.

What is an Electrified Locking Device? (cont'd)

There are two main types of door strikes in regard to whether power is required to lock the door or power is required to unlock the door.

- A lockset that requires power to lock the door is referred to as "**Fail Safe**"; this means that if there was a loss of power to the strike, the door could be opened manually.
- A lockset that requires power to unlock the door is referred to as "**Fail Secure**"; this means that if there was a loss of power to the strike, the door could not be opened manually.
- A Maglock is a very powerful locking mechanism and is rated in the pounds required to forcibly pull the door open (*break the magnetic connection between the electrified Maglock and the plate attached to the top of the door*).
  - Make sure you are aware of local and state fire alarm regulations

Types of Electrified Locking Devices

Frame and Door Mounted Electrified Door Strikes

Frame and Door Mounted Electromagnetic Locks (*Maglocks*)

Cabling Specifications

Name	Max Distance	Cable Type	Code
PoE Cable	100m (328')	Twisted pair, 4 pairs	Cat5 100Base-T or better
Reader Cable	152m (500')	6 conductor stranded (not twisted), 24 AWG or thicker; overall shielded	Overall shielded Belden 9537 or equivalent
Door Strike Cable	152m (500')	2 conductor stranded 18 AWG	Belden 9740 or equivalent
Output Cable	152m (500')	2 conductor stranded 22 AWG	Belden 8740 or equivalent
Input Cable	152m (500')	2 conductor stranded 22 AWG	Belden 8740 or equivalent

How Does Access Control Work?

Access control is a collaboration of schedules and processes to manage and monitor access points and control who can pass through an access point when and by what means.

There are 4 main components to the above process:

- Door Times Zones, which control when a door is secure or public and, when it is secure, what means of credential presentation is required to gain access (*elevator floors are managed the same way*)
- User Time Zones, which control when a user (*cardholder*) can be granted access through a secure door (*or elevator floor*) and when they are denied access
- Access Privilege Groups, also commonly called rules, which are a collection of dedicated doors (*or elevator floors*) assigned to a user that they can gain access through based on the User Time Zone applied to each door/floor
- Users, who are the cardholders that are assigned and the Access Privilege Group defining which doors and when they can access and by what credential means

How Does Access Control Work? (cont'd)

Door Time Zones: This is a schedule that determines the state (secure or public) of the door during times of the day and days of the week. The Vicon software includes a very versatile collection of access modes that can be applied to a door time zone schedule. Up to 20 zones can be applied to a single day in any mix or combination of modes listed below:

- **Card Only** - When door is locked, a valid card will grant access
- **Card or PIN** - When a door is locked, a valid card or valid PIN number entered via keypad will grant access
- **Card And PIN** - When a door is locked, both a valid card and valid PIN associated with the same user are presented in sequence via a keypad/prox combo reader to grant access
- **PIN Only** - When a door is locked, a valid PIN number entered via keypad will grant access
- **First Credential In** - When a door is locked and the time moves into a public period (door to be unlocked), the door will not automatically unlock at that time until the first valid card is presented
- **Dual Credential** – When a door is locked, it requires 2 cardholders to present their cards in sequence to grant access. It can also be configured that one of the two users must have a Supervisor privilege activated in their user account.
- **Unlock** – State of a door when it is public and free access can occur both directions
- **Lockdown** – State of door that is locked and can only be accessed by a cardholder with Master privileges activated in their user account. Often applied in emergency situations.

How Does Access Control Work? (cont'd)

Access Privilege Groups (APG): This is the glue that associates the Door or Floor Time Zone schedule (based on access mode) and the Users Time zone schedule given to the user for that door/floor to create the where, when and who of access control.

- Access Privilege Groups are generally assigned to collections of like users that require the same access through certain access points at the same times of day. This could be personnel such as employees, tenants, cleaning staff, etc.; the possibilities are endless.

- Often the naming of an APG gives clear inference as to its purpose such as "Engineers" or "West Tower – Tenants Only". Designing of the APGs requires a clear understanding of the customers site and personnel movement.

- The Vicon VAX software has no limitations on the number of time zones or access privilege groups that can be created and it does permit a user (cardholder) to possess more than one APG as long as no door/floor is duplicated in any of the rules.

How to Assess a Site: Vicon VAX Components for Door Access Control

The following is a suggested series of questions that will allow the Sales professional to adequately assess the site's needs in regard to access control components and peripherals:

1. How many doors or access points require access control?
2. Are any of these points parking areas that would use a gate or garage door?
3. Of the doors, how many require Request to Exit Motion?
4. Of the doors, how many require Back-to-Back reader configuration?
5. Of the doors, how many require the implementation of handicap or auto-opener implementation?
6. Of the doors, will there be use of Door Contacts? If so, at which doors and what type of device (*surface or concealed*)?
7. Of the doors, what type of proximity reader will be used, standard prox or keypad/prox combo readers?
8. Of the doors, will there be use of Exit Buttons and/or Handicap buttons (*or other means of egress*)?

How to Assess a Site...(cont'd)

9. Of the parking areas, if applicable, what will be used to control access, Prox reader or keypad on a pedestal or Long Range RF Receivers using handheld remotes?
10. Of the parking areas, will gates or doors be credential in/REX out or require credential both ways?
11. Of the doors, what locking mechanisms are being used, Strikes or Maglocks?
12. If strikes are being used, do they meet the output requirements of the Vicon VAX controller (*12VDC @ 500mA / 24VDC @ 250mA*) or will external lock power supplies be required?
13. Will the strikes be "Fail Safe" or "Fail Secure"?
14. If Maglocks are being used, is there provision for interfacing with Fire Safety System and use of external power supplies?
15. Review the door controller locations and configurations and identify if any groups of two VAX-1Ds, which are relatively close in location to each other, can be switched to a single VAX-2D controller.
16. Are the controllers going to be mounted at or near the doors or back in an equipment/maintenance room with cabling home running back to doors?

How to Assess a Site: Topology

Now with the raw hardware identified, the next step is to review the topology of the site and how the controllers are going to be connected to the network and its PoE sources.

1. Does the site already have a wired LAN infrastructure/network and will the access control system be integrated into it or will there be the creation of a separate network for the access control and cameras?
2. Is the site a single building self-contained or a multiple building site in multiple geographical locations?
3. Identify PoE cable spans from controllers back to switches to optimize number of PoE sources, ensuring spans don't exceed maximum runs (*Midspans are an option to extend ranges*).
4. Identify number of PoE sources required to power controllers, ensuring each device is capable of maintaining 15.4 watts per PoE port full time.
5. Depending on resources required for PoE power, identify and calculate battery backup/UPS requirements.
6. Will the customer be supplying a PC/Server for the Vicon VAX access control software and database? If so, ensure it meets minimum specifications.
7. Can you sell them a preconfigured network controller (*server*) with software installed dedicated for the Vicon VAX system only?

How to Assess a Site: Credentials

To complete the site assessment, the final topic for discussion and required responses from the customer is in regard to credential types.

1. Is this a new installation or a takeover/retrofit of another 3rd party access system?
2. If it is a takeover/retrofit, is the intent to reuse existing readers and credentials?
3. If intent is to reuse, it must be verified the credential type and Wiegand format is compatible with supported formats offered by the Vicon VAX system. The same holds true with readers; are they compatible with the VAX system and what cabling type is used?
4. If it is a takeover/retrofit and the intent is to reuse credentials, does the existing system permit a data extract of cardholder information (*in CSV format*) so that it can be imported in the VAX system?
5. Assuming the above are not the case and it is a new installation, identify what type or types of credentials are required for use, standard clamshell prox cards, proximity key tags, printable graphic quality proximity cards, or magstripe cards?
6. If the customer is going with printable graphics quality proximity cards, do they have a preference on card thickness (*31MIl or 46MIL*)?
7. If printing cards, do they require Photobadging software and a Photobadging printer (*printer specs must match card thickness specified*)?

Glossary of Terms

Glossary of Terms

125 kHz - Radio transmission operating at 125 thousand cycles per second. This technology has historically been the standard for proximity cards/readers.

13.56 MHz - Radio transmission operating at 13.56 million cycles per second. This technology has historically been the standard for smart cards/readers.

26-Bit Standard Format - The most common data format for RFID badges. It consists of 4 components: Even Parity (1 Bit), Facility Code (8 Bits), Card # (16 Bits) and Odd Parity (1 Bit).

Access Level - A logical group of doors paired with a time schedule used to determine when and where a card is granted access.

Access Point - A place along the perimeter of a secure area where there is a door/gate/portal and some type of access control method to screen users attempting entry to the area.

Alarm Point - A defined location that is being monitored by a sensor. In a typical door access control system, a specific door may be defined as an alarm point; through the use of resistors, they may also monitor a normal/alarm/short/open.

Glossary of Terms (cont'd)

Annunciator - An audible and/or visual signaling device.

Anti-Pass-Back Control - The ability to control, via an application, multiple uses of a card to access a door or facility. A typical anti-pass-back control includes both entry and exit card readers and requires the card to be swiped to exit, before being swiped again for entrance. Anti-pass-back controls may also include a time period between swipes (*e.g., once a card is swiped for entry, that same card cannot be swiped again for 30 minutes*).

API - Application Programming Interface is a source code interface that is provided in order to support requests to be made by other computer programs and/or allow data to be exchanged.

Audit Trail - A record of transactions that can be used by an interested party to trace an access control activities during a specific time period.

Badging Software - Security software that is capable of creating Photo Identification badges.

Bandwidth - The amount of data a network can transport in a given time period.

Glossary of Terms (cont'd)

Bar Code - A series of narrow bars of varying widths combined into group that represents unique numbers, letters or characters. Barcodes are read by a beam of light from a bar code reader, translated into electrical signals, and then converted into specific numbers, letters or characters for use by card readers and POS terminal scanners.

Bar Code Reader - A device that identifies and decodes bar codes for use by card readers and POS terminals. Bar code readers use lasers to scan the bar codes.

Battery Backup - A secondary energy source used to power devices in the event the primary energy source fails. Battery Backup typically provides power for a short period of time, allowing for immediate action, system protection, and system shutdown before the battery reaches a drained state.

Biometric Lock - A lock that is controlled by a biometric scanner, such as fingerprint, hand geometry, retina identification, etc.

Biometrics - Establishing personal identity verification using technology to measure a physical or behavioral trait – for example, a fingerprint.

Glossary of Terms (cont'd)

Cardholder - Any individual who is issued a campus card and participates in the plans, services, and activities regulated by the program.

Card Reader - A device that interprets coding resident on or in a credential.

Card Stock - Plastic stock used to create ID cards, usually with dye sublimation printers. Card stock can be manufactured with different types of plastic, which can affect durability and performance (see below). Card stock can be blank or fully or partially pre-printed during manufacturing. Pre-printing of some elements can be desirable in that offset printing delivers a higher print quality than most dye sublimation printers. Also, the card core can be pre-printed and coated with a clear plastic overlay, improving durability. The plastic stock can also be ordered in a variety of colors and incorporating various technologies, including magnetic stripes, radio frequency (RF) antennas, and/or integrated circuit chips. Card stock that is delivered with a pre-encoded magnetic stripe, an RF chip, or integrated circuit is serialized with a unique identifier printed or engraved into the plastic.

Glossary of Terms (cont'd)

Contactless Cards - Any variety of ID cards that use radio frequency (RF) to communicate with a card reader and do not have to come in direct physical contact with the reader. Although proximity cards are technically contactless, the term *contactless cards* is commonly used when referring to smart cards with integrated circuits that also use RF communications.

Credential - A medium that contains encoded information, such as ID cards, key fobs, and smart chips.

Controller - A microprocessor based circuit board that manages access to a secure area. The controller receives information that it uses to determine through which doors and at what times cardholders are granted access to secure areas. Based on that information, the controller can lock/unlock doors, sound alarms and communicate status to a host computer.

Data0 - (DO) One of two data lines in Wiegand communications. Data0 (D0) represents the binary "0".

Data1 - (D1) One of two data lines in Wiegand communications. Data1 (D1) represents the binary "1".

Glossary of Terms (cont'd)

Distributed Access Control - Access control systems in which all control decisions are made at the local controllers, independent from a host computer. Local Controller events are uploaded to a host computer periodically for review and storage.

Door Access Control/Access Control System - Any system used to monitor, regulate and report on access to entrances and exits to facilities. Such systems may use a variety of techniques to perform these functions: card readers, monitoring of door positions and locks, as well as alarms that report on unusual conditions such as held-open doors or forced entries. The ID card can act as the authorization device for entry into a building or room. These systems also have extensive logging and reporting capabilities. Increasingly, video surveillance systems are being integrated with card access systems to record video of persons entering and exiting facilities. Video surveillance may be integrated in such a way as to activate recording when cards are used to enter a building or the door controller senses an exit signal. Door access systems maybe dedicated systems or a module of a broader card system.

Glossary of Terms (cont'd)

Door Position Switch - A magnetic switch, usually mounted in the door jamb, that reports the position of the door (either open or closed) to an access control board.

Double Swipe/Triple Swipe - The act of swiping a card multiple times in quick succession. In some access control systems, specific cards can be programmed to perform specific door functions when multi-swiped (e.g., override the door schedule and manually lock or unlock a door for a period of time).

Dye Sublimation Printing - The common process of printing ID cards with a printer that uses heat to transfer dye directly onto the plastic card stock. Dye sublimation printers use multi-panel ribbons with cyan (C), magenta (M), yellow (Y), and black (K) and may also include clear overlay panels (T) or laminates adhered overtop of the printing for protection. Ribbons are designated by number of panels and the corresponding letters. A CMYK ribbon would have four panels, whereas a CMYKT would have five panels (addition of the clear overlay). Used ribbons from dye sublimation printing of IDs need to be disposed of securely because they will show the information that was printed on the ID cards, including names and ID numbers.

Glossary of Terms (cont'd)

Egress - The act of going out.

Electric Strike - An electric door locking device (usually solenoid-operated) that will unlock the door when electrical power is applied to it. A fail-safe configuration will operate in the reverse condition (i.e., normally locked when power is applied and unlocked when power is interrupted).

Electromagnetic Interference (EMI) - Excess electromagnetic energy radiated by an electrical device that may affect the operation of other electrical devices.

Encryption - The process of using an algorithm to transform information from plain text to a format that is readable only by someone possessing a key or password. Sensitive financial information is commonly encrypted in databases and in transmission across open networks. Standard magnetic stripe cards used for financial transactions do not encrypt data on the magnetic stripe and are therefore easily read and copied.

Facial Geometry - One of the physical traits that can be measured by biometric technology – the relative position of eyes, nose and mouth on the face.

Glossary of Terms (cont'd)

False Acceptance - In biometric identification, the erroneous result of identifying someone who isn't in the database of known people. It is one of two ways biometric identification can fail; the other is false rejection.

False Rejection - In biometric identification, the erroneous result of failure to recognize a known person. It is one of two ways biometric identification can fail; the other is false acceptance.

Fail-Secure - A term used to describe an electric lock that has a mechanical state of being locked and requires power to unlock it. Also known as electrically unlocked.

Fail-Safe - A term used to describe an electric lock that has a mechanical state of being unlocked and requires power to lock it. Also known as electrically locked.

Forced Door Alarm, Forced Alarm - The condition created by a door access control system when a door is opened without a valid card read signal or request to exit signal being received by the door controller, indicating that the door may have been forced open.

Format - The way that the information (parity bits, facility code and card #) is organized on the credential.

Glossary of Terms (cont'd)

Hand Scan - A technique for biometric identification that measures three-dimensional hand geometry – the shape of the fingers and the thickness of the hand.

Held Alarm - The condition created by a door access control system when the door controller senses that the door has been opened longer than the programmed held time.

Held Time - The defined length of time, usually in seconds, that a door can be open before the door controller registers a held alarm. Each door in an access control system can be configured with a door held time. The held time must be long enough to allow for a normal entrance or exit and door closure sequence.

Homerun - A wiring method in which each device has a separate wiring run to the control panel.

Glossary of Terms (cont'd)

ID Card – A plastic card that is used to ascertain identity of the cardholder and that may be used in a variety of card system applications. ID cards should clearly identify the cardholder and the issuing institution and include basic information such as photo, name, and status. Many ID cards also print an identification number and a card number on the face of the card. ID cards commonly include one or more technologies that allow the card to be read by a card reader. Technologies may include a bar code, magnetic stripe, radio frequency antenna, or integrated circuit. Some of these technologies require the card to come in physical contact with a reader, while other technologies may only require the card to be close to the reader (contactless).

Infrared Motion Sensor - A sensing unit that detects motion based on the disruption of infrared light waves.

I/O - Input/output.

Glossary of Terms (cont'd)

Inrush - The initial surge of current through a load when power is first applied. Electrified locks, maglocks, lamp loads, inductive motors, solenoids and capacitive load types all have inrush or surge currents higher than the normal running or steady state currents. Resistive loads, such as heater elements, have no inrush.

Interlock - A system of multiple doors with controlled interaction. Interlocks are also known as mantraps.

Iris Scan - A technique for biometric identification that maps the pattern of colors in the iris of the eye.

ISO-14443 - A series of international vendor independent standards for proximity RFID that establishes guidelines for two types of smart cards (A & B). The most common application requires a read within 4 inches of the reader and includes Classic MIFARE, EV1, DESFire and PIV.

Key fob - A specific form factor of credential that generally refers to a hard plastic disk that is carried on a key chain.

Keypad - An alphanumeric grid which allows a user to enter an identification code.

Glossary of Terms (cont'd)

LCD - The abbreviation for Liquid Crystal Display.

LED - The abbreviation for Light Emitting Diode.

Linking - When an input changes the state of an output.

Lock Relay Output - A relay on the controller that changes its state upon command by the controller, locking or unlocking a secure door.

Magnetic Stripe*, Mag Stripe* - *A strip of magnetic tape embedded on an ID card in a pre-defined location (either conforming to ISO standards or proprietary*) for purposes of data encoding to be read by a card reader. Magnetic stripes are designed to accommodate either high energy or low energy encoding methods. Low coercivity stripes are usually brownish in color, while high coercivity stripes are black. Depending on the width, magnetic stripes can contain 1, 2, or 3 tracks of data.

Magnetic Lock - A door lock made up of an electromagnet and a strike plate. The electromagnet is mounted in the door frame, the strike plate in the door. When power is applied to the electromagnet, the strength of the electromagnet keeps the door locked.

Glossary of Terms (cont'd)

Mantrap - An airlock-style arrangement having secured doors for entry and exit, with room for only one person between the doors. It is a solution to the security loophole called piggybacking or tailgating, in which an unauthorized person freely passes a security checkpoint by following an authorized person through an open door.

Masking - Hiding or suppressing alarms which do not need to be viewed.

MIFARE® - A contactless and dual smart card chip technology that is fully compliant with ISO-14443.

Mil - A unit of 0.001 inch used to specify the thickness of ID card components.

Mission Critical Facility - A facility that must operate 24/7/365 regardless of availability of power/water/fuel/etc. Examples would be corporate data center, 911 dispatch or military facilities.

Multi-Technology Credential - A credential that contains two or more technologies (*i.e., proximity, smart card, magnetic stripe*).

Multi-Technology Reader - A reader with the capability to read two or more card technologies *(i.e., proximity, smart card, magnetic stripe*).

Glossary of Terms (cont'd)

Mylar - A plastic used in the production of laminated magnetic stripe ID cards.

Network - In general, any collection of computers and associated devices connected together in order to share information.

Noise – Technically referred to as electro-magnetic interference (EMI) and radio frequency interference (*RFI*), electrical noise disrupts the smooth sine wave output of electricity expected from utility power sources. Electrical noise can adversely affect the functioning of card reading components and cause information sent over data lines to be garbled or lost. Transmission lines using a serial communications protocol tend to be more susceptible to EMI noise than TCP/IP network cables. Noise can often be combated by using a line conditioner and EMI/RFI filters like those offered by an uninterruptible power supply (*UPS*).

NO/NC - Normally open/normally closed, refers to the normal circuit state of a switch/relay.

Offline - Refers to the state of a card system where transactions are processed in a reader/controller that is not communicating in real-time to the host server. The controller stores a record of the transaction within its memory. The transactions are automatically uploaded once communications are restored.

Glossary of Terms (cont'd)

Online - Refers to a state of a card system where transactions processed in a reader/controller that is validating cardholder information to a central server via real-time communications. Online systems can operate in an offline mode if communications are disrupted, temporarily storing transaction data until communications are restored.

Panic Bar - A quick release door lock allowing the door to be quickly opened in the case of an emergency situation; also known as Crash Bar.

Physical Security - Protecting physical facilities from accidents or sabotage caused by the presence of unauthorized or ill-intentioned people. A physical security system includes access control devices for automated screening at entry points, plus a sensor-based alarm system. Additional protection may include camera surveillance and security guards.

Piggybacking - The security breach that occurs when an authorized person, having unlocked a door using legitimate credentials, holds the door open for an unauthorized person to follow through the checkpoint with no credentials. (A similar breach is tailgating, where the unauthorized user slips through undetected behind the authorized user.)

Glossary of Terms (cont'd)

PIN - Personal Identification Number, usually a four-digit numeric code known only to the cardholder, which must be entered (*possibly along with a card swipe*) in order to validate access. PINs are primarily used in areas or for access that require greater security.

Proximity Card, Prox Card - An ID card using radio frequency (*RF*) signals to communicate with a reader. Proximity cards do not have to come into physical contact with the reader (*like a magnetic stripe card*) but only have to be held near the reader. Depending on the type of reader, the card must be held within a few inches to a couple of feet to read. Proximity card capabilities can range from the simple transmission of a unique card serial number to the more sophisticated wireless communication found in a contactless smart card. Other non-ID card formats may be used to transmit the same RF signal, such as a key fob or small sticker.

Relay - An electrically controlled device that opens and/or closes electrical contacts.

Glossary of Terms (cont'd)

Request to Exit Switch, Request to Exit Device, RX Switch - A micro switch (*inside a crash bar*) button mounted next to the door or a motion detector that triggers the controller board to unlock the door when someone is exiting. These switches are typically used on the inside or secure side of the door. In some cases, a card reader is placed on both sides of the door (*for entrance and exit*). In this case, the card reader on the inside acts as the request to exit device.

Retinal Scan - A technique for biometric identification that maps the pattern of blood vessels in the retina of the eye.

RFID - Radio frequency identification; communication between card and reader without physical contact. RFID technology is what makes proximity cards, vicinity cards, and contactless smart cards work. The RFID chip is powered by an electromagnetic field from the reader.

Glossary of Terms (cont'd)

Schedules, Door Schedules - Various types of schedules are used in card systems to define how door access systems function. In the case of door access, schedules may be used in a number of ways. For example, schedules could determine when a door is unlocked, when cardholder access plans are active, or when alarm monitoring should occur. In many cases, schedules are defined in a weekly format where time periods (*and corresponding parameters*) are defined each day of the week and the schedule is repeated each week. In other cases, schedules are calendar/date driven and are specific to calendar dates.

Strike (Lock) Position Switch - A micro switch that monitors the position of a door electronic lock strike plate, reporting the condition to the controller board.

Strike Unlock Time, Unlock Time - The amount of time, usually defined in seconds, that a door will unlock after the controller receives a valid signal from the card swipe or proximity reader. Once the door is opened, as reported by the door position switch, the controller board usually sends a signal to reset the strike back to a locked state (*regardless of the unlock time*) to ensure the entrance is secured as soon as the door is returned to the closed position.

Glossary of Terms (cont'd)

Smart Card - According to the Smart Card Alliance, "A smart card is a device that includes an embedded integrated circuit chip (*ICC*) that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (*ISO/IEC 7816 and ISO/IEC 14443*) and is available in a variety of form factors, including plastic cards, fobs, subscriber identity modules (*SIMs*) used in GSM mobile phones, and USB-based tokens." Smart cards may require contact with readers or be contactless.

Swipe - Traditionally a swipe was the act of passing a magnetic stripe ID card through the long, shallow slot and past the read head of the swipe reader of a card reader. With the advent of various RF and proximity technologies, a card swipe may also be the act of passing an ID card close by the reader.

Glossary of Terms (cont'd)

Switch, Maintained (toggled) - A switch that, when activated, maintains its activated position until it is deactivated.

Switch, Momentary (pulsed) - A switch that, when activated, automatically returns to its original position afterwards.

Tailgating - The security breach that occurs when an unauthorized person slips past a checkpoint undetected, by following an authorized user through an open door. (A similar breach is piggybacking, where the authorized user is complicit and holds the door open.)

Tamper - A digital input which monitors the status of a device, typically the door of an enclosure.

Time Schedules - Consists of time ranges that are associated with days of the week or holidays, and are often used with access levels or as trigger events.

Glossary of Terms (cont'd)

Transaction - The record created by and stored on a card system when a card is used to enter a door or facility, or other activity. A transaction record typically records the time and date of the transaction, the cardholder's primary ID number, the card number, the terminal or card reader where the transaction occurred, and an indication if the transaction was valid or denied.

Trigger - An event or manual action that will cause another event or execution of a macro.

Voltage Drop - Voltage loss experienced by electrical circuits due to two principal factors: (1) wire size and (2) length of wire runs.

Wiegand Card - A type of access control card that uses imbedded work-hardened wire (Wiegand wire) to hold information read by swiping it through a reader.

Thank you