Access Control Design and Installation Considerations

Planning Considerations

• Request site drawings and building prints, these will be used to indicate where access devices are to be Installed.
• Obtain in writing your customers systems requirements.
• *ALWAYS VERIFY SYSTEM DESIGN WITH LOCAL FIRE OFFICIALS.*
In addition to NFPA standards many cities and towns have their own requirements and codes.
It is essential that you consult with these codes when installing access control systems.
(Consult ANSI/NFPA101 Life Safety Code.)
• If you have not installed locking hardware in the past, you may want to consult a locksmith for the system design and hardware installation.

System Integration Possibilities and Expansion

Add on to the Basic System
• When laying out an access control system, keep in mind that there are many opportunities beyond the initial installation. Many of the Access Control software packages incorporate *CCTV control, Graphical Displays* of a facility incorporating *alarm conditions* etc., as well as *control of gates for parking lots*, and even *elevator control*. When these other technologies are incorporated into the access control system the profit opportunities become very attractive.
Leave Room For Expansion
• Remember that in a typical access installation the customer's requirements often grow with time. This presents opportunities to expand the system for more users, more doors,
additional facilities and protection of inner areas like computer rooms and managers offices.

Access Control Glossary of Terms

Access Card: A coded employee card, usually the size of a credit card, recognizable to the access control system and read by a reader to allow access. It can be used for photo identification of the cardholder and for other data collection purposes. Card technologies include magnetic strips, wiegand-effect, proximity (active/passive), barium ferrite, and smart/intelligent cards.

Access Code: Any system or method which automatically controls the passage of people and vehicles into or out of an area or structure.

Access Level: The door or combination of doors and/or barriers an individual is authorized to pass through.

Access Mask: Electronic alarm masking suppresses the annunciation of an alarm condition that would have been reported in the "secure" mode of operation. Masking does not block the reporting ability of tamper or fault conditions that may not be seen when alarm shunting is used.

Access Point: Each means of entry into a controlled security area, consisting of a card reader, monitor switches and/or latches. Access points are wired to an access control panel.

Access Relay: An electrically operated switch that is activated when access is granted to unlock a door.

Annunciator: An audible and/or visual signaling device.

Anti-Passback (Anti-Tailgating): This feature protects against more than one person using the same card or number. It defines each system card reader and card I.D. number as *IN*, *OUT*, or Other. Once a card is granted access to and *IN* reader, it must be presented to an *OUT* reader before another *IN* reader access is granted. Cards will continue to have access to all authorized *OTHER* readers.

Access Time: The period of time during which an access point is unlocked. (Also see shunt time).

Audit Trail: A listing created which may be created in real time, which may be used to monitor the progress of a person through protected areas.

Badge: To use a card key in a reader to gain access to protected areas; a card key itself, especially one with a photo I.D.

Biometrics: Refers to readers that identify human attributes such as fingerprint, hand geometry, voice recognition or retinal analysis.

Buffer Capacity: Refers to the amount of information the system can store, this may include the users, time of day and specific door.

Coercivity: The property of a magnetic material, as on a magnetic stripe keys, which is a measure of the coercive force. It is used when describing the strength of magnetic saturation when discussing magnetic stripe card keys.

Database: A collection of data used and produced by a computer program. The files created at the host of the access control system forms its database.

Device Address: Value set on an access control device to determine its unique identity.

Distributed Intelligent Devices: Access control devices that make
their own access decisions uploading event messages periodically to the central processing unit for storage.

Door Open Time: The time allowed for a controlled door to remain open after a valid entry. At the expiration of this time, the system records a transaction which may be defined as an alarm. If the alarm bypass relay is used, it would also de-energize at the end of this time.

Egress: Exit, depart, leave (opposite of ingress).

Electric Door Strike: An electric door-locking device, usually solenoid operated, that will unlock a door when electric power is either applied, or removed, depending upon the configuration.

Electromagnetic: Pertaining to combined electric & magnetic fields associated with movements of electrons through conductors

Enclosure: A box or cabinet usually constructed of metal, that houses system components, such as circuit boards and other electronic and electrochemical controls and circuitry.

Erasable Programmable Read-Only Memory (EPROM):
A programmed memory (often in a chip) that cannot only be read, but can be repeatedly erased under high-intensity ultraviolet light and reprogrammed.

Executive Privilege: An option which allows a cardholder unlimited access to all operational access points. Access may be without the system referring to any other access parameters, or there may be a PIN-code requirement has been enabled.

Exit Switch: A push button, switch mat, proximity detector, or other device that starts a timer in the reader interface electronics when someone is leaving through a controlled entry or exit. The timer bypass (shunts) the door-open detector for a selected period of time.

Facility Code: A numeric code programmed into a cardreader and encoded on the access card/token, which is unique to the one card access systems facility. In a distributed or semi-distributed intelligent card reader system, the facility code will allow access to cardholders with the proper facility code when communications are lost with the CPU.

Fail Safe: On loss of power, access points will automatically unlock allowing free access, and signal the card access system of a device malfunction or loss of power.

Fail - Secure: An electric lock that requires power to unlock. Also called fail-locked.

Fail-Unlocked: An electric lock that automatically unlocks with any power interruption. Also called fail-safe.

Global Linking: An input at one Access Control panel effecting the output at another.

Guard Tour: A defined route of a security guard.

History: A log of system activity that can be recalled by utilizing the report command. Most systems offer a feature that notifies the console operator of the amount of available storage for history information preventing information from being written over. The message will usually alert the operator to archive the information onto a removable magnetic tape.

Ingress: Enter (opposite of egress).

Key Switch: A switch, which must be operated with a key.

Keypad: A flat device, which has buttons that may be pressed in a sequence to send data to a controller, and which differs (said to be "non-QUERTY") from a typewriter-like computer board.

LCD: An acronym for *Liquid Crystal Display*.

LED: An acronym for *Light-Emitting Diode*.

Load: Any device that converts the computer system's digital information into analog information and transmits it over a telephone line. Another modem must be used when the information back from analog to digital.

Magnetic Stripe: A band of ferrous material that is sealed onto or into a card key or credit card.

Modem: Device that converts the computer system's digital information into analog information and transmits it over a telephone line. Another modem must be used when the information is received to convert the information back from analog to digital.

Momentary Switch: A switch that, after being activated, automatically returns to its original position; a spring-loaded contact that, when pressed, closes two contacts, and when pressure is removed, opens the contact.

Output Relays: The auxiliary relays found in access control panels or NODES that control external devices.

Panic Bar: A device, usually a small electrical switch in a mounting plate, used for unlocking a door in an emergency.

Parking Gate: A barrier that can be opened or closed to control vehicular access

Passive Infrared (PIR) Detector: A sensor that detects the changes in the infrared light radiating from.

Reader: Refers to the *"front end"* that a user must interact with to allow access. Readers can be keypads, card readers, and proximity readers.

Shunt: To bypass. When an alarm is bypassed so that it doesn't activate, it is said to be shunted.

Shunt Time: The time in seconds that a door-open alarm is suppressed after the door has been opened.

Standalone: An access control system that makes its own access decisions without communicating with a central controller.

Strike: A plate mortised into or mounted on the doorjamb to accept and restrain a bolt when the door is closed. In some metal installations or with a deadlock, the strike may simply be an opening cut into the jamb. (Synonym: *keeper*)

Strike Plate: A plate, usually of metal, mortised into or mounted on the doorjamb to accept and restrain a bolt
when the door is closed.

Time and Attendance: The ability to utilize the time in and time out information per user, for the purpose of keeping track of employee's hours at a facility. Many time and attendance packages work as stand-alone systems, and interface with most payroll software.

Time Schedules: Allows for Access based on time of day, date and user. Also allows for holidays, etc.

Transaction: A record created that contains pertinent information about an occurrence in the access control and monitoring system.

Transient Suppressor: A device that protects data lines from high transient such as lighting and inductive loads. They are recommended where there are data communications lines between the reader and its electronics that are subject to high-transient situations. Two are required: *one at each end of the exposed communications lines.*

Twisted Pair: A cable composed of two small substantially insulated conductors, twisted together with or without a common covering. Bleden 8720 cable, for instance, contains two twisted shielded pairs of stranded wire.

Underwriters Laboratories Inc. (UL): An independent, not-for-profit organization that tests products in the interests of public safety.

Wiegand Card Key: A plastic card, approximately the shape of a credit card, which has an embedded module of inert, specially treated ferromagnetic wires which generate a voltage pulse that can be sensed by a coil within the card reader.