KLAZIN FUTURE TECHNOLOGY

INTRODUCTION TO ACCESS SYSTEMS FUNDAMENTALS

BASIC TRAINING MANUAL

ACKNOWLEDGEMENT

This document was created to aid Klazin Future Technology technicians in training to get a deeper grasp in Access System Technology and basic electronics fundamentals.

CONTENTS

BASIC ELECTRONICS

Electricity is the flow of free electrons in a conductor from one atom to the next atom in the same general direction. This flow of electrons is referred to as current and is designated by the symbol "I". Electrons move through a conductor at different rates and electric current has different values.

Electricity is the energy that makes a work through the ordered flow of electrons. It is the product of Current, Voltage and time. The amount of useful work that is done, and conversely of energy that is lost as heat, depends on the resistance of the medium through which electrons flow.

What are the two major types of electricity?

There are two kinds of current electricity: direct current (DC) and alternating current (AC). With direct current, electrons move in one direction. Batteries produce direct current.

I=V/R
R= V/I
V = I x R

ELECTRONICS COMPONETS

RESISTORS
CAPACITORS
DIODES
INDUCTORS
TERMINALS

FUNDAMENTALS OF A POWER SUPPLY

AC/ DC
AMPERAGE

ACCESS BASIC TRAINING

ACCESS CONTROL SYSTEMS –

The Basics

As a result of increased security awareness, there has been a move away from the traditional key and lock systems to more sophisticated access control systems. The technology used in access control systems ranges from simple push-button locks to computerized access control systems integrated with video surveillance systems. Regardless of the technology used, all access control systems have one primary objective — they are designed to screen or identify individuals prior to allowing entry. Since identification is the foundation of all access control systems, they generally require that the user be in possession of an identification credential.

TYPES OF ACCESS CONTROL SYSTEMS.

Access control systems can be either of the standalone type or the multiple-portal type. While each type may perform essentially the same functions, stand-alone systems are limited in data storage and system features. Access control systems can range from a small, relatively simple one-door system to highly complex, computer-operated systems capable of handling hundreds of doors and tens of thousands of individually encoded identification credentials.

A basic system usually consists of the following:

1. a central processing unit (CPU),
2. a input device at each protected door,
3. a identification credential assigned to each user.
4. and a locking device.

A printer is often included to provide a record of all activity. The CPU is the brains of the system and is programmed with data on each user. The data can include an access level, which determines which doors may be entered by the user, and time zones, which define the hours of the day and days of the week a user may enter a door at a particular access level.

IN GENERAL.

When the identification credential is presented to the reader, the requester's identification number is relayed to the CPU. The requester's access level and time zone are instantly checked by the computer. For a valid identification, the door lock, which can be an electronic or electro-magnetic lock or an electric strike, is released. If entry is attempted with a card that is not valid or if a card is used outside of its authorized time zone or at an unauthorized door, entry is denied, and an alarm is immediately generated.

Reader types are either swipe, in which the card is passed along an open slot; insertion, in which the card is pushed into the reader and withdrawn; or proximity, which requires that the card be moved within a certain distance of the reader. In some card access control systems, improved security is achieved by requiring the user to present the card to a reader, as well as enter a unique passcode, a personal identification number (PIN), on a keypad. With this enhancement, the loss of a card will not compromise the system, since an unauthorized user

would also need to know the PIN. The added security afforded by the card/PIN combination more than offsets the delay that results from the user having to enter a PIN.

CARD TECHNOLOGIES.

There are at least nine different card-encoding technologies available:

1. Magnetic stripe,
2. Wiegand,
3. Proximity,
4. Barium ferrite,
5. Infrared,
6. Bar code,
7. Hollerith,
8. "Smart" card,
9. Optical storage.

To the basic four parts of the system we next need to look at "the add-ons" that complete the system. We, up to this point, have been dealing with "getting in". Now how do you get back out of the controlled area?

There are as many types of RTE devices as there is types of I.D. technologies to gain entrance. These fall into two basic groups:

1. RTE buttons
2. another reader to enter your card again to leave OK!

We have now designed a basic access system, it has the entry reader, processer, locking device, and RTE device, the person gaining entry has the I.D. device. NOW when we say the person has the I.D. device, that device could be as simple as a numerical code to enter on a keypad, it does not have to be a physical device like a card or fob. Now let's look at some other items that are normally included in a access control system.

1. Door ajar alarm
2. Forced door alarm
3. Clock timing device (for restricting entry to specific times of the day)
4. Duress alarm (a different code to enter that lets someone enter but alerts the security personnel that they are being forced by a second person).
5. Integration with CCTV, burglar and fire alarm systems for a complete security system

ENTRANCE IDENTIFICATION TECHNOLOGIES ACCESS CONTROL SYSTEMS.

Access control systems can range from small, relatively simple one-door affairs to highly complex, computer-operated systems capable of handling hundreds of doors and tens of thousands of individually encoded identification credentials.

A basic system usually consists of a central processing unit (CPU), a input device at each protected door, and an identification credential assigned to each user. A printer is often included to provide a record of all activity.

The CPU is the brains of the system and is programmed with data on each user. The data can include an access level, which determines which doors may be entered by the user, and time zones, which define the hours of the day and days of the week a user may enter a door at a particular access level. The two types of systems indicated above fall into these categories: Stand-Alone Systems. Stand-alone systems are used to control access at a single entry point and are available either as one integral unit or as two separate components — a reader/keypad and a controller. While stand-alone systems can be networked, they generally do not require a CPU. Data for the entire user population is stored within the unit. The installation of a stand-alone system is simple, and thus cheaper, since there is no need to run wires to connect the unit(s) to the CPU.

Multiple-Portal Systems. Multiple-portal systems are part of a large network of readers and controllers that are connected to a CPU and that can regulate activities at more than one entry point at a time. Some systems are directly under the control of the CPU, while others are programmed to receive only periodic programming updates or to upload data according to a preprogrammed schedule. Installation costs for these systems are relatively high because of the need to interconnect the units to the CPU. Now that we have taken a fast look at the overall systems parts let's look at, probably the most fascinating part of the system, the different types of input devices used in today's systems.

We will start with breaking these devices down into groups.

1. Keypads
2. Card/Token readers
3. Biometric readers

Now let's take a closer look at each of these technologies. -11-

KEYPAD ENTRY

The keypad entry system is the oldest and can be the simplest type of entry system. It can range, on the low end, from a simple keypad where all employees have the same code to enter, to a keypad that requires not only the code but some other type of ID to enter. If you remember the James Bond movie "For your eyes only" you saw during the very first part of the movie, the parts of, what then was, were the two systems required to enter NATO security areas. The movie was true, in part. In the movie it showed a keypad that was completely blank, no numbers. To activate the keypad the person had to push the bottom left ENTER button. This caused the keypad to light up. Each time the keypad lights up the numbers show up in a different order (e.g. the 1 shows up in the 5 spot and the 5 in the 3 spot etc.). This "scramble" type keypad existed then as it still does now. So let's recap. Keypads can be as simple as a

single code entry type, to one that excepts individual codes for each person, to one that has individual codes and scrambles the numbers so someone looking from the side can't figure out what the code was, and finely add any of these to a secondary type of ID requirement to enter.

CARD/TOKEN READERS

Reader types are either swipe, in which the card is passed along an open slot; insertion, in which the card is pushed into the reader and withdrawn; or proximity, which requires that the card be moved within a certain distance of the reader. In some card access control systems, improved security is achieved by requiring the user to present the card to a reader, as well as enter a unique passcode, a personal identification number (PIN), on a keypad. With this enhancement, the loss of a card will not compromise the system, since an unauthorized user would also need to know the PIN. The added security afforded by the card/PIN combination more than offsets the delay that results from the user having to enter a PIN.

CARD TECHNOLOGIES.

There are at least nine different card-encoding technologies available:

Magnetic stripe,

Wiegand,

proximity,

barium ferrite,

infrared, bar code,

Hollerith, "smart" card,

and optical storage.

The magnetically based technologies include magnetic stripe, Wiegand, and barium ferrite. The optically based technologies are infrared, bar code, optical storage, and Hollerith. Proximity cards and some smart cards use radio signals to communicate with the reader. Surveys indicate that magnetic stripe, Weigand, and proximity technologies control over 80 percent of the market in terms of usage. Selection of a technology involves several factors: encoding security, susceptibility of the reader to environmental hazards, resistance of the reader to vandalism, initial cost, and long-term cost, including card and reader replacement and reader maintenance costs. Magnetic Stripe. This was the first card technology incorporated into access control systems and is the most commonly used today. It is the same technology that finds application in credit cards, ATM cards, debit cards, and a host of other uses. The cards are produced with a narrow strip of magnetic material fused to the back.

Data are stored on the strips as a binary code in the form of narrow bars, some of which are magnetized and others not. The card is inserted or swiped through the reader and the code is read.

(A) There are two types of magnetic cards on the market today: the 300 Oersted and the 4000 Oersted, high coercivity card. The code on a 300 Oersted card can become scrambled when subjected to a magnetic field. The 4000 Oersted card is the preferred card, since the material

that comprises, the magnetic stripe retains data better and is almost invulnerable to magnetic fields.

(B) Although relatively inexpensive and widely used, magnetic stripe cards are one of the most insecure cards in use. The card can be encoded with readily available encoding devices and, as such, should only be used in low-security applications. For higher security applications, the card should be used in combination with a passcode. © Since there is direct contact between the card and reader, both components are subject to wear.

The readers are vulnerable to weather and the environment, as well as vandalism, and need regular maintenance.

Wiegand. (A) The operation of the Wiegand card is based on the use of short lengths of small diameter, ferro-magnetic wires that have been subjected to a patented twisting process that imparts unique magnetic properties to the wires. When exposed to a magnetic field in a reader, a current is induced in the wires that generate a signal for the reader to pick up.

(B) The Wiegand card provides a very high degree of security, since it is factory-encoded and extremely difficult to counterfeit or alter. It is also immune to electromagnetic (EM) and radio-frequency (RF) fields. The reader is completely sealed, which protects the working parts from the elements, and is capable of operating over wide temperature ranges. Weigand cards are relatively expensive when compared to other cards. They can only be encoded once, since the wires within them can only be magnetized one time.

Barium Ferrite. The barium ferrite card uses magnetized spots to create a code on the card that must match magnets in a reader to close a micro switch. The card has generally been used in high volume, high-turnover applications, such as parking lots. It affords high encoding security and is relatively inexpensive to produce and encode. Older readers were of the insertion type and subject to high maintenance costs due to wear and the environment. Newer, state-of-the-art readers are of the proximity or “touch” type and use an array of electronic sensor devices installed behind a touch plate to read the magnetic spot patterns on the card.

Infrared. (A) Data is stored on this card by means of a bar code written between layers of plastic. The card is read by passing infrared light through it. The bar code within the card casts a shadow on the other side that is read by an array of infrared light sensors. Encoding security is high because duplication is almost impossible.

(B) Although they provide a high degree of security, infrared cards are not in widespread use for access control because of high card and maintenance costs. The optical reader comes in both swipe and insertion styles and is subject to wear and contamination from the environment, requiring regular maintenance.

Bar Code. (A) The bar code card also is not widely used for access control because encoding security is very low and the bar code strip can be easily damaged. Card encoding is accomplished at relatively low cost. Because the bar code card is an optical system, periodic cleaning and servicing of the reader is necessary.

(B) Bar code labels can be applied to magnetic stripe, Weigand, and other types of cards by simply affixing the label to an area of the card that does not contain information. These types of cards are called dual technology cards. -13-

Optical Storage. (A) Information is written to an optical storage card by etching small pits into the surface of a reflective layer of plastic using a solid-state infrared laser. The reflective layer is sandwiched between two protective layers of plastic. More than four Mega Bytes of information can be written on the card. The data is secure from compromise, since the information on the card is usually in an encrypted format. (B) The reader is equipped with a solid-state laser and generally a transport system that moves the card past the reader at a steady speed. Generally, the users are required to enter a passcode before inserting the card. Data is read from the card by systematically striking its surface with an infrared beam of light from the laser in the reader.

A photo sensor reads the data from fluctuations in the reflected light. While relatively expensive as compared with other card technologies, optical storage cards are reusable. The readers and transport systems are initially expensive and require regular maintenance.

Hollerith. The Hollerith card is the oldest technology in use. Data is written on the card by punching holes in the card. The card is read by either passage of light through the holes or by fine contact brushes that connect with an electrical contact on the other side of the card through the holes. The plastic or paper card is very inexpensive, but the security is low. This optical-type card is commonly used in hotels as a replacement for key systems.

Proximity.

Proximity identification credentials are of two types—active and passive. Both types of proximity identification credentials have a micro-miniature electronic tuned circuit and a switching mechanism buried within them, while active identification credentials also have a power source.

(A) Active identification credentials transmit a coded signal when they come within range of a proximity reader or when someone manually activates them. Other identification credentials transmit a signal continuously. Generally, a long-life lithium battery is used as the power source.

(B) Passive identification credentials rely on an electrostatic field generated by the proximity reader to cause them to transmit a unique coded signal that is received by the reader.

(C) Proximity technology has grown in popularity because of its convenient “hands-free” feature. An identification credential is simply waved in front of a reader to transmit the code. Operating ranges are usually from 2 in. to 12 in. The identification credential is factory encoded and difficult to copy or counterfeit and affords good encoding security. Since there is no contact with the reader, identification credential life is generally long, and the reader can be installed inside, behind a wall or glass partition, to afford protection from the elements and vandals.

The electronic circuits in the identification credentials, however, can be damaged if handled roughly.

Smart Card.

“Smart card” is a generic term for a single card that serves many functions. The smart card is the state-of-the-art in access control technology. The basic card provides access control and can double as a photo I.D. card or debit card, as well as serving other functions.

(A) The card contains an integrated circuit in which can be stored all the information needed to identify and permit access, eliminating the necessity for a CPU. To function, a passcode must be provided before the card can be read. Some smart cards are powered by their own battery,

while others rely on the reader to power them either directly by a set of external contacts or electromagnetically.

(B) Because of their relatively high cost, at present, the smart cards find limited application. Their use is expected to grow substantially, since they provide a high level of security and can serve many other applications. BIOMETRIC SYSTEMS Establishing a person's identity can be based on three methods: something known by an individual (a password), something possessed by an individual (a card or key), and something physical about an individual (a personal characteristic).

Biometric access control devices, or personal characteristic verification locks, rely on the latter method. Since duplication of individual physical characteristics is very rare, biometric devices, in theory, could offer the highest security possible. Biometric systems measure a unique characteristic of the person seeking access. These systems are classified as fingerprint, hand or palm geometry, handwriting, voice, and retinal verification systems. Typically, biometric readers are connected into a central processor, but can also be used alone.

Fingerprint Verification Systems.

Fingerprint verification systems have been around for more than a decade. These systems identify an individual by matching stored fingerprints with live prints presented on an electro-optical scanner.

(A) Two types of systems have been developed for fingerprint identification. One system stores a laser picture or hologram on the access card and compares the user's print data to that stored on the card. In the other system, the fingerprint data is indexed in a computer and is called up by an access card or code issued to the user. The user places a finger onto the scanner, which optically scans it and compiles, in digital form, a list of significant features (minutiae) of the fingerprint and their locations. The minutiae, which consist of ridge endings and ridge branches, are then compared with the stored data.

(B) Fingerprint verification systems are considered to be very high in their relative resistance to counterfeiting; in more than 60 years of compiling fingerprints, the FBI has never found two sets of identical prints. However, the equipment is very costly and, according to some accounts, can be adversely affected by dirt or grime on the hands. For this reason, most fingerprint verification systems are programmed to give the user a second or third try, or request the use of an alternate finger, before rejection.

Hand or Palm Geometry Verification Systems.

Hand geometry units identify a user by measuring the length and curvature of the fingers of the user's hand together with the degree of translucency of the fingertips and the webbing between the fingers.

These measurements are then compared to that stored in a computer. The translucency test is intended to prevent the use of a synthetic "forged" hand. Palm geometry systems optically scan a section of the palm, recording creases, skin tone, and swirls for minute computer analysis. The disadvantages to the use of these systems are that both are very expensive and can be adversely affected by dirt or grime on the hands.

Handwriting Verification Systems.

Handwriting verification systems are also referred to as signature dynamics verification. These systems are based on an examination of the dynamics of writing, that is, the speed, rhythm, and peculiar flourishes of a pen while writing a signature, rather than the end product of writing the signature itself. While a forger may be able to duplicate a signature, the dynamics of the signature cannot be falsified for the reason that writing is considered a ballistic motion that is done almost "reflexively," requiring very little conscious effort.

(A) Two methods are used in handwriting verification. One method uses a pen containing an accelerometer to record the dynamics of the signature and to compare it to the data stored on a computer. The other method uses a sensitive tablet that measures the pen's acceleration, pressure, and velocity as it sweeps through the signature.

(B) The greatest advantage to the use of handwriting verification systems in access control is that everyone is accustomed to and accepts signing their name to gain a certain privilege, such as cashing a check or paying with a credit card. On the other hand, fingerprint (or palm or hand geometry) verification carries an association with wrongdoing that many people may find objectionable.

(C) The major drawback to the use of handwriting verification is that of inconsistencies in writing one's signature. As was noted earlier, signature writing is a ballistic motion that requires little conscious effort. However, signing in on a verifier could result in a more conscious effort on the part of a legitimate user, resulting in inconsistencies. For this reason, handwriting verification systems use the average of three or four signature dynamics for the data stored in the computer. Inconsistencies would also come about as a result of an injury to the hand or fingers used in signing one's name.

Voice Verification Systems.

Certain features of a person's speech, such as resonance, pitch, and loudness, can be used to identify the person. In voice verification systems, also known as speech recognition systems, the prospective user is enrolled by speaking certain key words or phrases into a microphone connected to a computer that translates features of the spoken words into quantitative terms for storage. To gain entry, the user speaks the same words or phrases into a microphone at the access-control point for comparison with that stored on the computer. However, because the voice can vary due to the weather, a cold (illness), stress, and other factors, voice recognition systems tend to be error-prone, limiting their commercial application.

Retinal Verification Systems.

Retinal verification systems use the pattern of blood vessels within the retina of the eye, which is unique in everyone, as a means of identifying an individual. The user looks into an eyepiece that scans the retina with a safe low-level infrared light. The infrared light reflected back is converted into digital data that is compared to information stored in a computer. The limitation in retinal verification systems is that retinal patterns are not stable and can be altered by injury, illness, alcohol, or drugs. There also may be resistance on the part of an individual to look into the device.

FUNDAMENTALS OF ACCESS SYTEMS

Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data.

There are four (4) fundamentals of access system;

1. Identification
2. Authentication
3. Authorization
4. Auditing

The 4 main access control models are:

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)
- Rule-based access control (RuBAC)

Model	Advantages
Mandatory Access Control Model (MAC)	MAC provides higher security because only a system administrator can access or alter controls.
Discretionary Access Control Model (DAC)	Object access is determined during access control list (ACL) authorization and based on user identification.
Role Based Access Control Model (RBAC)	Increased security of complex organization, reduce complexity and cost.
Attributed-Base Access Control Model (ABAC)	ABAC add additional parameters such as resource information, requested entity, resource and dynamic information such as time and user IP.

The 5 Ds of perimeter security (Deter, Detect, Deny, Delay, Defend) work on the 'onion skin' principle, whereby multiple layers of security work together to prevent access to your site's assets, giving you the time and intelligence, you need to respond effectively.

Types of Access Control

Access control types include the following three that we'll look at one at a time.

1. Administrative Access Control

Administrative access control sets the access control policies and procedures for the whole organization, defines the implementation requirements of both physical and technical access control, and what the consequences of non-compliance will be. Some examples include supervisory structure, staff and contractor controls, information classification, training, auditing, and testing.

2. Physical Access Control

Physical access control is critical to an organization's security and applies to the access or restriction of access to a place such as property, building, or room. Some examples are fences, gates, doors, turnstiles, etc., using locks, badges, biometrics (facial recognition, fingerprints), video surveillance cameras, security guards, motion detectors, man-trap doors, etc. to allow access to certain areas.

3. Technical or Logical Access Control

Technical or logical access control limits connections to computer networks, system files, and data. It enforces restrictions on applications, protocols, operating systems, encryptions, mechanisms, etc.

In today's increasingly digital world, modern access control systems combine both administrative, physical, and technical access control to limit access to sensitive data and physical locations, providing a much higher level of security. Some examples are access control lists, intrusion detection systems, and antivirus software.

Implementing Access Control

A valid access control plan includes the following considerations:

- Security goals: Identify the resources and processes that you want to authorize
- Security risks: Identify the vulnerabilities of the organization and identify security loopholes. These include:
    - Preventing physical or data loss
    - Unauthorized access and modification
    - Incorrectly configured permissions that could lead to security breaches or inability to perform tasks (not enough permissions for the role)

- Security strategies
- Security group descriptions
- Security policies
- Information security strategies
- Administrative policies

The following is a typical access control process:

- Identification of the subject (e.g., person, digital resource, vehicle)

- Authenticate that subject by matching the credentials found in the request with those stored
- Authorization by setting the privileges to be granted using access control lists (ACLs) to allow access to resources for which the subject has permission and preventing access to resources for which they don't have permission
- Auditing and checking via periodic audits of the processes and verification of the access controls

What are the Different Types of Entry Devices?

Entry devices are the term used to refer to objects that release the secure lock. That is, they act as keys that open the door control system. Entry devices are usually found on the mullion of the exterior side of the door or the wall near the door. A mullion is the part of a door frame that separates the door from a glass window or panel. It is also the part of the frame between two doors. When the device is mounted on the mullion of the door, it is said to be a mullion mount. When the device is mounted on the wall near the door, it is called a gang mount. The following are some examples of entry devices:

PROXIMITY READERS

Proximity readers are the most commonly used entry devices in businesses. With a **proximity reader**, one can easily deactivate a lost card and issue new ones without stress. They come with sensors that can read cards from up to three feet away. Since there is no contact between the card and the reader, wear and tear are minimal. In addition, it helps to save costs as many businesses today combine it with their staff ID cards.

BIOMETRIC READERS

Biometric access control systems allow users access based on their unique biological identification features like handprints, retinal scans, and fingerprints. These types of systems are the most secure for access control. They also usually cost more than a keypad or proximity reader.

KEY PADS

These are commonly used in many businesses for protecting single doors. They are very affordable and easy to use. However, they do not offer as much security. Anyone with the code can easily share with others, and people also can try to crack the code. The system also lacks extensive audit trails if everyone uses the same code. This issue can be fixed by issuing unique codes to all of your employees.

STAND-ALONE LOCKS

These battery-powered locks are usually used for single doors. They can be accessed with keypads, proximity readers, or a combination of the two. The beauty of the system is that you can install them easily. However, they usually cannot be integrated into a more extensive security network. Some of them, however, have small readers that can show you audit trails.

What are the Different Types of Egress Devices?

Egress devices refer to the security devices that secure the exit of access control systems. Unlike the entry devices, they are usually found near the exits of the building, either on the door or on a wall by the door. The purpose of an egress device is to ensure there is a free and secure passage out of a building. The following are some common types:

PUSH BUTTONS

These are button mounted near the exit point, and they usually carry directions. Pressing such buttons will automatically open the door.

PUSH BARS

These are usually attached to the inside of doors just at the position of the door latch. To exit the door, you need to push the bar. As you push, the latch will be released, and the door will open.

EMERGENCY EXITS

Emergency exit egress devices can either be break glass models or pull-down handle models. They are usually mounted on doors or walls at exit points. To leave the building, users have to either break a glass or pull a handle to release the door.

MOTION SENSORS

This type of egress device automatically opens doors when they detect humans or cars approaching the exit of buildings.

DELAYED EGRESS

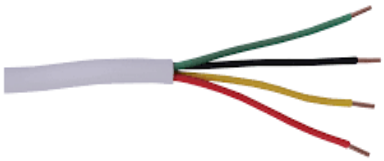
These are devices that come with timers that delay the opening of doors for security reasons. These devices usually have count-down times that count down to when the latch will be released, and the door will open. They also can come with sounds and voice commands that explain when the door will be opened.

POWER SUPPLY

MAGLOCK

KEYPAD

RTE BUTTON (REQUEST TO EXIT)



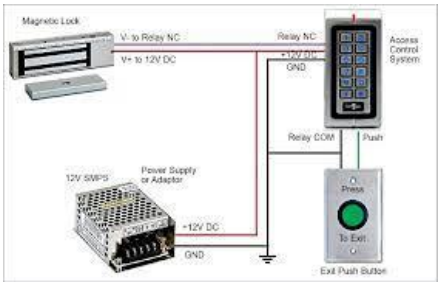
4 WIRE CABLE (22/4)

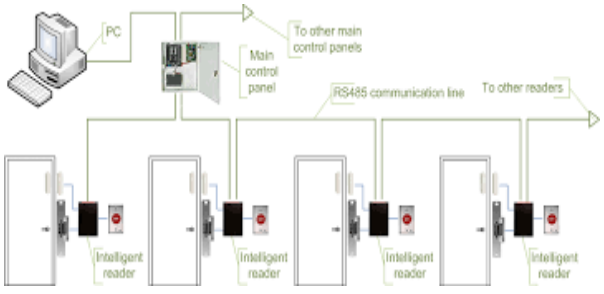
WIRELESS KEYFOB

DOOR STRIKE

SMART LOCK

SCHEMATICS DIAGRAM





GENERAL DEFINITIONS.

Access Control. The monitoring or control of traffic through portals of a protected area by identifying the requestor and approving entrance or exit.

Access Control Portals. Access control portals are doors, gates, turnstiles, and so forth. Controls can be operational, technical, physical, or a combination thereof and can vary depending on type of credential, authorization level, day or time of day.

Active Lock. An electric locking device that holds a portal closed and cannot be opened for egress by normal operation of the door hardware.

Ancillary Functions. Monitored points that are not security points but are incorporated into an electronic premises security system or outputs that are not necessary to the function of the electronic premises security system.

Annunciator. A unit containing one or more indicator lamps, alphanumeric displays, computer monitor, or other equivalent means on which each indication provides status information about a circuit, condition, system, or location.

Closed Circuit Television (CCTV). A video system in which an analog or digital video signal travels from the camera to video monitoring stations at the protected premises.

Control Unit. A system component that monitors inputs and controls outputs through various types of circuits. [72, 2002]

Controller. A control unit used to provide the logic in an access control system.

Detection. Intrusion Detection. The ability to detect the entry or attempted entry of a person or vehicle into a protected area.

Sound Detection. Recognition of an audio pattern indicative of unauthorized activity.

Device. Initiating Device. A system component that originates transmission of a change-of-state condition.

Ambush Alarm Initiating Device. An initiating device or procedure that personnel authorized to disarm the intrusion system at a protected premises can use to transmit a signal indicating a forced disarming of an intrusion detection system.

Duress Alarm Initiating Device. An initiating device intended to enable a person at protected premises to indicate a hostile situation.

Holdup Alarm Initiating Device. An initiating device intended to enable an employee of a protected premises to transmit a signal indicating a robbery has transpired.

Signaling Device. A device that indicates an alarm or abnormal condition by means of audible, visual, or both methods, including sirens, bells, horns, and strobes.

False Alarm. Notification of an alarm condition when no evidence of the event that the alarm signal was designed to report is found. Monitoring Station. A facility that receives signals and has personnel in attendance at all times to respond to these signals.

Position Sensor. A device that indicates whether a portal is open or closed.

Reader. A device that allows an identification credential to be entered into an access control system. Record of Completion. A document that acknowledges the features of installation, operation (performance), service, and equipment with representation by the property owner, system installer, system supplier, service organization, and the authority having jurisdiction.

RTE. Request to Exit sensor.

Safe. An iron, steel, or equivalent container that has its door(s) equipped with a combination lock.

Security Personnel. Employees or contract service personnel charged with duties to aid in the protection at a protected premises.

Signals. Alarm Signals. A signal indicating an unauthorized event at a protected premises.

Supervisory Signals. A signal indicating the need for action in connection with the supervision of guard tours, unverified exterior alarm, or environmental or other nonintrusion monitored point or system.

Trouble Signals. A signal indicating a fault in a monitored circuit or component.

Strain Relief. Cable termination that provides structural rigidity of conductors under conditions of flexure.

System.

Combination System. A system of multiple control units that work together to provide one integrated control.

Digital Imaging System (DIS). A video system in which a digital video signal travels from the camera and can be viewed by any authorized user at or away from the protected premises.

Duress Alarm System. Private Duress Alarm System.

A system or portion thereof in which the action to activate the duress signal is known only to the person activating the device.

Public Duress Alarm System. A system or portion thereof in which the ability to activate a duress signal is available to any person at the protected premises.

Electronic Premises Security System. A system or portion of a combination system that consists of components and circuits arranged to monitor or control activity at or access to a protected premises.

Holdup Alarm System.

Manual Holdup

Alarm System. A system or portion thereof in which the initiation of a holdup signal depends solely on operation of manually operated hand or foot initiating devices installed within the working area.

Semiautomatic

Holdup Alarm System. A system or portion thereof in which the initiation of a holdup signal does not depend solely on operation of manually operated hand or foot initiating devices installed within the working area.

Integrated System. A control unit that includes other types of systems in addition to the electronic premises security system.

Partition System. A part of one control unit that through software acts as a separate control unit.

Vault. A room constructed of iron, steel, brick, concrete, stone, tile, or similar masonry units permanently built into or assembled on the premises and having an iron, steel, or equivalent door and frame with a combination lock