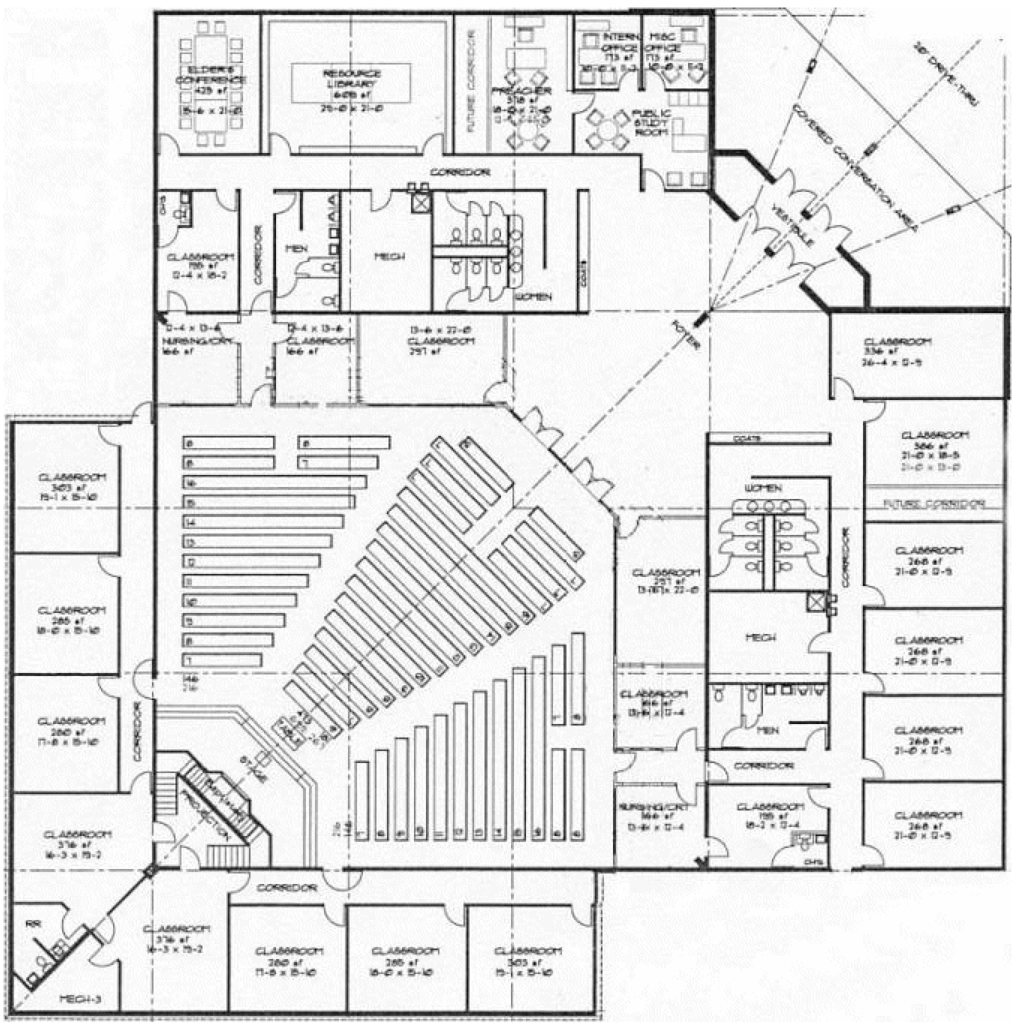
ACCESS CONTROL BASICS COURSE



Sponsored by
Limited Energy Resource Center

TABLE of CONTENTS

I. LETS GET STARTED **5**
- Introduction
- Glossary

II. ACCESS CONTROL SYSTEMS – The Basics **9**
- Breakdown of Equipment Groups
- Types of Systems
- Add-on Equipment Sub-Systems

III. ENTRANCE IDENTIFICATION TECHNOLOGIES **11**
- Access Control Systems
- Keypad Entry
- Card/Token Reader
- Cart Technologies
  - Magnetic Stripe
  - Wiegand
  - Barium Farris
  - Bar Code
  - Optical Storage
  - Hollerith
  - Proximity
  - Smart Card
- Biometric Readers
  - Fingerprint
  - Hand/Palm
  - Handwriting
  - Voice Recognition
  - Retinal Scanner

IV. POWER SUPPLIES **17**
- Primary Power Supply
  - Dedicated Branch Circuit
  - Mechanical Protection
  - Overcurrent Protection
  - Transient Voltage Surge Protection
  - Capacity
- Secondary Power Operation

V. ELEMENTS OF SYSTEM DESIGN **21**
System Design
Guidelines – By Facility Usage
Campus Systems
Health Care Systems
Lodging Systems
Office
Parking Lots

VI. INSTALLATION REQUIREMENTS **24**
Fundamentals
Equipment
Portal
Reader
Locking Systems
Position Sensors
Portal Egress
Free Egress
RTE
Manual.
Automatic.
Controlled Egress
Controllers
Power Supplies
Administrative Tools/Interface
NFPA 5000

VII. INSTALLATION **28**
System Installation
Power Supplies
Installation
Equipment Location
Interconnecting Control Units
Protection
Wiring
General
Termination
Circuit Identification
Strain Relief
Service Loops
Wire Gauge vs, Distance
Routing of Cables
Splicing of Interconnections

Building-to-Building Wiring
Transient Protection
Signal Loss
Testing
Voltage Drop
Leakage in Patient Rooms

VIII. PROPER CONNECTIONS **32**
Types of Connections and Their Uses
Wire-Nut Connector
Crimp-Type Closed-End Connector
Power Connections
Proper Ground Connections
System Terminations
Connections for Supervised Circuits
Regulatory Compliance for Connections
Labeling System Connections

IX. SEPARATION FROM OTHER CIRCUITS AND EQUIPMENT **34**
Conduit and Cable-Tray Systems
Other Equipment

X. AS BUILT DOCUMENTATION **35**
Risers
Interconnect Drawings
Marking Home-Run Cables
System Programming Records
Test Records
In-Service Training
Service Procedures

XI. INSPECTION AND SYSTEM TESTING **37**
Electrical Inspection
Electrical Testing
Functional Testing
Load Testing

XII. MAINTANCE AND SERVICE **38**
Documentation and Parts
Test Equipment Required
Periodic Testing
Problem Investigation
Corrective Action
Technical Assistance
Summery

INTRODUCTION

This manual was written using the outline set forth in NFPA 731. We have concentrated on specific areas of that document dealing directly with Access Control Systems. Those areas are Chapter 3 for Definitions, Chapter 4 on Power Supplies, and of course Chapter 6 on Access Control Systems.

Although we used NFPA 731 as the base document for this course we have noted the following other NFPA standards and there necessity if design and building of Access Control Systems.

NFPA 1	Fire Prevention Code
NFPA 70	National Electric Code – the standard for all electrical installations
NFPA 72	Fire Alarm Code
NFPA 101	Life Safety Code
NFPA 110	Standard for Emergency and Standby Power Systems
NFPA 730	Guide to Premises Security
NFPA 5000	Building Construction and Safety Code

Whenever we have quoted NFPA standards we have re-worded them, hopefully, to make them easier to understand.

Additionally, we have integrated information from other authoritative sources to round out the course.

GLOSSARY

The following glossary has been compiled from the National Fire Protection Association (NFPA) publications used to write this manual.

DEFINITIONS USED IN ALL THE CODE LANGUAGE.

Approved. Acceptable to the authority having jurisdiction.

Authority Having Jurisdiction. The organization, office, or individual responsible for approving equipment, materials, an installation, or a procedure.

Labeled. Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that the equipment, material, or services either meets appropriate designated standards or has been tested and found suitable for a specified purpose.

Shall. Indicates a mandatory requirement.

Should. Indicates a recommendation or that which is advised but not required.

Standard. A document, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and which is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Non-mandatory provisions shall be located in an appendix or annex, footnote, or fine-print note and are not to be considered a part of the requirements of a standard.

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 non-intrusion 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. Asystem 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.

II. 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 stand-alone 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

III. 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 lets 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.

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.

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.

IV. POWER SUPPLIES

Systems will be provided with at least two independent and reliable power supplies, one primary and one secondary (standby), each of which will be of adequate capacity for the application.

Where direct current (dc) voltages are employed, they will be limited to no more than 350 volts above earth ground.

PRIMARY POWER SUPPLY

Dedicated Branch Circuit. One of the following dedicated branch circuits will supply primary power:

(1) Commercial light and power

(2) An engine-driven generator or equivalent in accordance with this section (See Engine-Driven Generator Installation), where a person specifically trained in its operation is on duty at all times

(3) An engine-driven generator or equivalent arranged for cogeneration with commercial light and power in accordance with this section under Engine-Driven Generator Installation , where a person specifically trained in its operation is on duty at all times

The primary supply will have a high degree of reliability and adequate capacity for the intended service.

Mechanical Protection. Circuit disconnecting means are required to have a blue marking, it will be accessible only to authorized personnel, and will be identified as "PREMISES SECURITY CIRCUIT."

The location of the circuit disconnecting means will be permanently identified at the premises security control unit.

Overcurrent Protection. An overcurrent protective device of suitable current carrying capacity and capable of interrupting the maximum short-circuit current to which it can be subjected to will be provided in each ungrounded conductor.

Transient Voltage Surge Protection. A transient voltage surge protection device or circuit will be installed at or incorporated into the primary power supply for the following:

(1) Microprocessor-based control units

(2) Microprocessor-based sub-panels

(3) Microprocessor-based annunciators

(4) Other microprocessor-based equipment

Capacity. Under maximum quiescent load (system functioning in a non-alarm condition), the secondary supply will have sufficient capacity to operate an electronic premises security system for a minimum of 24 hours and, at the end of that period, shall be capable of operating all alarm sounding devices for 15 minutes, where required.

SECONDARY POWER OPERATION

Operation of secondary power will not affect the required performance of an electronic premises security system. The secondary (standby) power supply will supply energy to the system in the event of total failure of the primary (main) power supply or when the primary voltage drops to a level insufficient to maintain functionality of the control equipment and system components.

When primary power is lost or incapable of providing the minimum voltage required for proper operation, the secondary supply will automatically supply the energy to the system without loss of signals or causing transmission of an alarm.

For an integrated system, the secondary supply capacity described in this section will include the load of all premises security–related equipment, functions, or features that are not automatically disconnected upon transfer of operating power to the secondary supply.

The secondary supply will consist of one of the following:

(1) A storage battery dedicated to the electronic premises security system arranged in accordance with Storage Battery – Marking requirements

(2) A dedicated branch circuit of an automatic-starting engine driven generator arranged in accordance with **NFPA 70** ***National Electrical Code,*** **Article 700**, and **NFPA 110,** ***Standard for Emergency and Standby Power Systems***, and, storage batteries dedicated to the electronic premises security system with 15 minutes of capacity under maximum alarm load

(3) An emergency generating system as defined in **NFPA 70,** ***National Electrical Code,*** **Article 700**

The secondary power system will produce the same alarm and trouble signals and indications, excluding the ac power indicator, when operating from the standby power source as are produced when the unit is operating from the primary power source.

Continuity of Power Supplies. The secondary power supply will automatically provide power to the electronic premises security system within 10 seconds, whenever the primary power supply fails to provide the minimum voltage required for operation.

Required signals will not be lost, interrupted, or delayed by more than 10 seconds as a result of the primary power failure.

Storage batteries dedicated to the electronic premises security system or an uninterruptible power supply (UPS) arranged in accordance with the provisions of **NFPA 111,** ***Standard on Stored Electrical Energy Emergency and Standby Power Systems,*** and will be permitted to supplement the secondary power supply to ensure required operation during the transfer period.

Where a UPS is employed, as in the above paragraph, a positive means for disconnecting the input and output of the UPS system while maintaining continuity of the power supply to the load will be provided.

Storage Batteries. Marking. Batteries will be permanently marked with the month and year of manufacture.

Replacement. Batteries will be replaced in accordance with the recommendations of the electronic premises security equipment manufacturer.

Sealed lead-acid batteries will be replaced within 5 years of manufacture.

Location. Storage batteries will be located so that the premises security equipment, including overcurrent devices, are not adversely affected by battery gases and shall conform to the requirements of **NFPA 70*, National Electrical Code*, Article 480**.

Cells will be insulated against grounds and crosses and shall be mounted securely in such a manner so as not to be subject to mechanical injury.

Racks will be protected against deterioration.

If not located in or adjacent to the electronic premises security system control unit, the batteries and their charger location will be permanently identified at the premises security control unit. In-line overcurrent protection will be located between the secondary power supply batteries and the secondary power supply.

Battery Charging. A means shall be provided to automatically maintain the battery fully charged under all conditions of normal operation.

A means shall be provided to recharge batteries within 24 hours after fully charged batteries have been subject to discharge.

Upon attaining a fully charged condition, the charge rate shall not result in battery damage.

Overcurrent Protection. The batteries will be protected against excessive load current by overcurrent devices.

The batteries will be protected from excessive charging current by overcurrent devices or by automatic current limiting design of the charging source.

Charger Supervision. Supervision means appropriate for the batteries and charger employed will be provided to detect a failure of battery charging and initiate a trouble signal in accordance with ***NFPA 731 Section 5.1.1.1.***

Engine-Driven Generator Installation. The installation of engine-driven generators shall conform to the provisions of **NFPA 70*, National Electrical Code*, Article 700**, and **NFPA 110*, Standard for Emergency and Standby Power Systems*.**

SYSTEM FUNCTIONS.

Electronic Premises Security System. Electronic premises security system functions will be permitted to be performed automatically.

The performance of electronic premises security system functions will not interfere with power for fire alarms, lighting, or operation of elevators or other building control systems.

The performance of electronic premises security system functions will not preclude the combination of other services requiring monitoring of operations.

Time Delay. The time delays will be determined by other sections of this standard.

Distinctive Signals. Electronic premises security system alarms, supervisory signals, and trouble signals will be distinctively and descriptively annunciated.

PREFORMANCE & LIMITEATIONS.

Voltage, Temperature, and Humidity Variation. Equipment will be designed so that it is capable of performing its intended functions under the following conditions:

(1) At 85 percent and at 110 percent of the nameplate primary (main) and secondary (standby) input voltage(s)

(2) At ambient temperatures of 0°C (32°F) and 49°C (120°F)

(3) At a relative humidity of 85 percent and an ambient temperature of 30°C (86°F)

Damp, Wet, or Exterior Environments. Equipment intended for use in damp, wet, or exterior environments is required to be listed for its use and location.

V. ELEMENTS OF SYSTEM DESIGN

SYSTEM DESIGN

Persons who are experienced in the design, application, installation, and testing of electronic premises security systems will develop plans and specifications in accordance with **NFPA 731 Standard for the Installation of Electronic Premises Security Systems**.

The system designer will be identified on the system design documents. Evidence of qualifications will be provided when requested by the authority having jurisdiction (AHJ).

Qualified personnel will include, but not be limited to, the following:

(1) Equipment manufacturer trained and certified personnel
(2) Personnel licensed and certified by state or local authority
(3) Personnel certified by an accreditation program acceptable to the authority having jurisdiction (AHJ)

AHJ Approval. All systems will be installed in accordance with the specifications and standards approved by the AHJ.

Site Inspection. The site will be inspected for environmental factors that affect the operation of the electronic premises security system.

Environment. The devices installed will perform their intended functions in the environmental conditions at the protected premises.

Equipment Mounting. Devices, appliances, and control units will be located and mounted so that accidental operation or failure is not caused by vibration or jarring.

GUIDELINES BY PREMISES USAGE

Campus Access Control Systems. With the increased security awareness on campuses, there has been a move away from the traditional key and lock systems to more sophisticated access control systems. One of the major advantages of access control systems is the ease with which codes can be changed to delete lost or stolen identification credentials from the system.

These access control systems can range from basic systems that operate a single lock on a door to computer-operated systems that electronically tie together hundreds of locks. In these systems, an identification credential serves as a key to operate the lock on a door. Because of this, the same principles of key control apply to the issuance of identification credentials.

New technologies are available with cards that can perform a variety of functions. In addition to being a photo ID and access card, the card can also function as library card, debit card, meal-plan card, and long-distance telephone card.

Health Care Facilities. Building access control measures should include those described herein:

(A) Every consideration should be given to establishing a program to control access by personnel, vendors, and visitors.

(B) Identification cards need to be issued to all employees, physicians, volunteers, students, and contract staff in accord with the hospitals security assessment. The cards should have, as a minimum, a photograph of the bearer, at least the bearer's first name, and the bearer's position title. Employees should be required to display their identification cards at all times.

I Visitors should not be able to access patient areas without passing the reception area. Facilities should consider the use of visitor logs or badges.

(D) Access to uniforms, such as for maintenance workers, and, if possible, patients' gowns, and doctors' scrubs should be controlled. When intruders are able to obtain such garments, they are able to blend in with health care staff.

(E) A messenger center for packages, flowers, and other deliveries should be established. Messengers should not be allowed to roam the building freely.

Lodging Facilities. Although they are open to the general public, a lodging facility is a private property. Management should monitor and, when necessary, control the access of persons onto the premises. The following should be considered:

(1) Building access should be limited to authorized people only.

(2) All exterior entry points to the facility, except the lobby entrance, should be equipped with automatic door closers and locks.

(3) A program to ensure, that during nighttime hours, every remote and/or unattended entrance is locked. This cannot conflict with fire and emergency exit requirements.

Office Facilities. All exterior entrances into the facility should be equipped with automatic door closers and secure locks.

Perimeter entrances during non-business hours, should be secured. Only certain entry points should be designated for after-hours access. A program should exist to ensure that entrances that are not needed for entry or exit are secured. That program **cannot** conflict with fire and building code exit requirements.

It is best if all exterior entrances to the building be adequately illuminated.

Identification credentials should be issued to all employees and tenants. The cards should have, as a minimum, a photograph of the bearer and the bearer's name. Identification credentials should have the bearer's signature and the signature of the individual authorized to issue the card. Employees and tenants should be required to display their I.D. cards at all times; at the very least, they should be required to display them on demand. For large facilities, the use of color codes on identification cards should be considered and a code established for specific buildings, floors, or areas. The stock for the cards should be controlled to ensure that the system cannot be compromised.

Custodial personnel reporting to the building after the end of the normal business day, whether employees or a contract service, should be required to check in and check out with security personnel. Custodial personnel should display an identification credential acceptable to facility management.

Contractors and other vendors should display an identification credential acceptable to facility management.

Parking Facilities. For private facilities, a solid overhead garage door, operated by an access control system, should be provided. Once a car has entered or exited, the door should close automatically. Tenants or employees should be advised to wait until the garage door has closed completely before proceeding, to deter furtive attempts at entry by unauthorized individuals. Issuance of identification credentials should be controlled.

VI. INSTALLATION REQUIREMENTS

FUNDAMENTALS
This section applies to physical electronic access control systems only.

Equipment. Electronic access control equipment will be listed in accordance **with UL 294, *Standard for Access Control System Units*.**

Portal. The system will be designed to control the unauthorized access of people, vehicles, and/or property through a portal as prescribed by the AHJ.

Reader. Readers will be mounted in accordance with adopted local codes and the requirements of the AHJ.

When the portal is a door, readers will be mounted on the latch side.

Clearance between the reader and the portal will be provided for the portal action appropriate for its application.

Access to the readers will not be obstructed when manual presentation is required.

When manual presentation of access credentials is required for a vehicle, the reader will be readily accessible from the operator's position of vehicles common to the site.

All readers will provide a visual or audible indication that the credential has been recognized.

The maximum interval of time between the recognition of a valid credential and the unlocking of a portal will not exceed 10 seconds.

Locking Systems. Access control systems will utilize electric locking systems to control the use of portals.

Control of egress will comply with the requirements of the applicable codes and standards based on the occupancy and usage of the facility.

Locking systems will be installed in accordance with the manufacturer's instructions.

Portals will automatically close and lock when the portal is supervised by the access control system.

Where delayed egress function is used in conjunction with an access control system, equipment will be listed for the purpose and be installed in accordance with the applicable codes and standards based on the occupancy and usage of the facility.

When a portal is a required means of egress and is provided with an active lock, a manual means, independent of the access control system, will be provided that directly releases the active lock.

The manual means of release required for emergency egress portals in the above paragraph will not be required if approved by the AHJ.

Position Sensor. A position sensor will be required on all controlled portals.

A position sensor will monitor the position of the portal for held-open or forced-open conditions.

The position sensor will be mounted such that no portion of the portal can be opened greater than 15.24 cm (6 in.) before activating the sensor.

Position sensors will be monitored as applicable by the head end controller or an integrated intrusion detection system so as to notify the system users of an event.

PORTAL EGRESS.

Free Egress. Free egress will employ the use of a request-to-exit (RTE) device.

When the RTE controls the portal lock, the lock will open on loss of power.

When activated, RTE devices will prevent the position sensor from reporting a forced-open alarm.

The RTE will be either manual or automatic.

Manual.

(A) The RTE device will not require any special instruction or knowledge to use.

(B) If a manual RTE device is used as a fail-safe for an automatic RTE device, it will be installed so as to directly release the locking mechanism.

Automatic.

(A) If the RTE device is a motion detector, it will be listed for its purpose.

(B) When automatic RTE devices are used to unlock portals, they will be installed so that only intentional requests are executed.

Controlled Egress. Controlled egress will require the use of access credentials to be presented to a reader that is installed on the secured side of the portal in accordance with 6.1.3.

Active locks used for controlled egress will meet the requirements of this chapter.

Controllers. A controller will be listed for its purpose.

A controller shall be installed per manufacturer's instructions.

A controller shall be installed in a space that protects it from damage, tampering, and access by unauthorized personnel.

Power Supplies. All power supplies will meet the requirements of **NFPA 731** ***Standard for the Installation of Electronic Premises Security Systems Chapter 4.***

Power supplies will be sized based upon the application and manufacturer's requirements.

The voltage and current of the power supply will be the same as required by the associated field devices.

Power supplies will be installed in a space that protects them from damage, tampering, and access by unauthorized personnel.

AC POWER INPUT

General Requirements. The system central equipment requires dedicated, computer-grade 120 volt, 60 Hz, 20 amp power.

Earth Ground. Central equipment and the power supply must be properly grounded for proper operation of the system. This dedicated grounding wire should be as short as possible and at least #10AWG or larger.

Line Conditioners. Each AC power input to the system should have a line conditioner to maintain a clean, regulated power source. These conditioners must be UL Listed and be rated for the correct load.

Uninterruptible Power Supplies (UPS). A UPS is recommended to provide the nurse call system with back-up power for a maximum amount of time or until the hospital's emergency back-up power come on line. The UPS source must be UL Listed and have the correct rating for the load.

ADMINISTRATION TOOLS/INTERFACE

The configuration of the system operating parameters will be done in accordance with the facility requirements and subject to the approval of the AHJ.

All system operating parameters will be protected from unauthorized changes.

Ancillary functions will not interfere with the security and life safety–related functions.

Interconnections of components of an access control system will be verified for compatibility.

Network Interface Device. In network interface device (NID) configurations, the level of encryption will comply with the applicable level

NFPA 5000 Building Construction and Safety Code, Chapter 11, 11.2.1.6.2 Access-Controlled Egress Doors. Where permitted in Chapter 16 through Chapter 30 (NFPA 5000), doors in the means of egress will be permitted to be equipped with an approved entrance and egress access control system, provided that the following criteria are met:

(1) Either of the following shall be provided:

(a) A sensor will be provided on the egress side and arranged to detect an occupant approaching the doors, and the doors will be arranged to unlock in the direction of egress upon detection of an approaching occupant or loss of power to the sensor.

(b) Listed panic hardware or fire exit hardware that, when operated, unlocks the door will be provided.

(2) Loss of power to the part of the access control system that locks the doors will automatically unlock the doors in the direction of egress.

(3) The doors will be arranged to unlock in the direction of egress from a manual release device located 40 in. to 48 in. (102 cm to 122 cm) vertically above the floor and within 5 ft (1.5 m) of the secured doors.

(4) The manual release device specified in 11.2.1.6.2(3) will be readily accessible and clearly identified by a special sign that complies with 11.10.8.1 and 11.10.8.2 and reads as follows:

PUSH TO EXIT.

(5) When operated, the manual release device specified in 11.2.1.6.2(3) will result in direct interruption of power to the lock—independent of the access control system electronics—and the doors will remain unlocked for not less than 30 seconds.

(6) Activation of the building fire-protective signaling system, if provided, will automatically unlock the doors in the direction of egress, and the doors will remain unlocked until the fire-protective signaling system has been manually reset.

(7) Activation of the building automatic sprinkler or fire detection system, if provided, will automatically unlock the doors in the direction of egress and the doors shall remain unlocked until the fire-protective signaling system has been manually reset.

VII. INSTALLATION

SYSTEM INSTALLATION.
Installation personnel will be supervised by persons who are qualified and experienced in the installation, inspection, and testing of electronic premises security systems. Qualified personnel will include, but not be limited to, the following:

(1) Equipment manufacturer trained and certified personnel
(2) Personnel licensed or certified by federal, state, or local authority
(3) Personnel certified by an accreditation program acceptable to the AHJ
(4) Trained and qualified personnel employed by an organization listed by a national testing laboratory for the servicing of electronic premises security systems

POWER SUPPLIES
Code Conformance. All power supplies will be installed in conformity with the requirements of **NFPA 70*, National Electrical Code***, for such equipment and with the requirements indicated in this subsection.

INSTALLATION
Unless otherwise permitted by the manufacturer, control units, power supplies, and batteries will be mounted in the vertical, upright position.

Manual Resetting. All equipment requiring manual resetting to maintain normal operation will have an indication to the user that the device has not been restored to normal.

Equipment Location.
Equipment will be installed in locations where conditions do not exceed the voltage, temperature, and humidity limits specified below or unless listed for the application.

Voltage, Temperature, and Humidity Variation. Equipment shall be designed so that it is capable of performing its intended functions under the following conditions:

(1) At 85 percent and at 110 percent of the nameplate primary (main) and secondary (standby) input voltage(s)
(2) At ambient temperatures of 0°C (32°F) and 49°C (120°F)
(3) At a relative humidity of 85 percent and an ambient temperature of 30°C (86°F)

Damp, Wet, or Exterior Environments. Equipment intended for use in damp, wet, or exterior environments shall be listed for its use.

Interconnecting Control Units. Control units, sub-controls, and devices that are used to interconnect the control unit to protection devices will be located within the area being protected by the system.

If the enclosures for such equipment are not located in such an area, the enclosures will be protected by one of the following methods:

(1) Continuously under the notice of assigned security personnel
(2) Located in an area that is accessible only to authorized personnel
(3) Supervised to annunciate tampering

Control units and sub-controls will be readily accessible to service personnel.

Protection. To reduce the possibility of damage by induced transients, circuits and equipment will be protected in accordance with the requirements of **NFPA 70, *National Electrical Code,* Article 800.**

WIRING.

General. The installation of all wiring, cable, and equipment will be performed in a workman-like manner in accordance with **NFPA 70, *National Electrical Code***, and specifically with Article 725 or 800, where applicable.

Optical fiber cables will be protected against mechanical injury in accordance with **NFPA 70, *National Electrical Code,* Article 770.**

A conductor will be spliced or joined with a mechanical splicing device listed for this purpose.

Unless specifically allowed by the manufacturer's wiring specifications, low voltage electronic premises security system wiring will be spaced at least 5.08 cm (2 in.) from conductors of any light and power circuits, unless one of the circuits is in metal raceway.

Electronic premises security system wiring and cables will be of the appropriate gauge, strands, insulation, and electrical properties as specified by the equipment manufacturer.

Termination. Connections of conductors to terminal parts will ensure a good connection without damaging the conductors and be made by means of pressure connectors, wire binding screws, or splices to flexible leads.

Conductors will be connected to devices and to fittings so that tension is not transmitted to joints or terminals.

Wires and cables will not be placed in such a manner as to prevent access to equipment.

Terminals for more than one conductor will be identified and intended for the purpose.

Conductors will be of the same size and composition.

Terminals will be marked or colored coded where necessary to indicate the proper connections.

All raceway connections to junction boxes and at all open ends of raceway or flexible raceway will be protected from abrasion and fixed in position in accordance with **NFPA 70, *National Electrical Code,*** Articles 725 and 800**.**

Circuit Identification. Circuit identification will be within the control panel and enclosures used for wiring connections.

Circuit identification will be at all field terminations. The circuit identification will not be visible to the public.

Strain Relief. Strain relief will be provided for wiring leaving control panels and junction boxes not utilizing raceway.

Service Loop Metallic Conductors. A minimum 15.24 cm (6 in.) service loop will be at control panels and enclosures used for wiring terminations.

A minimum 15.24 cm (6 in.) service loop will be at field terminations. All service loops will be mechanically protected.

Service Loop Optical Fiber Cable. A service loop will be at control panels and enclosures used for terminations.

The radius of the service loop will meet the manufacturer's specifications. If no manufacturer's specifications exist, the radius will not be less than 10 times the cable diameter. Service loops will be mechanically protected.

Routing of Cables. When determining a logical pattern for laying out the low-voltage cables always begin with the manufacturer's recommendation for the maximum number of stations on a single cable run. The pattern should also take into account the physical layout of the rooms along with the ease of trouble-shooting the system cabling. For example, a 'T' shaped floor might tend itself to three runs; (one for each log of the "T') or, if there are a large number of stations in these corridors, six runs (one for each side of each leg).

Splicing of interconnections. NEC recommends using butt splices or equivalent crimp-style connectors for splicing the low-voltage wires. Electric tape and wire nuts are not recommended. Each manufacturer will specify a preferred splicing method.

Building-to-Building Wiring. Special care must be taken in running low-voltage wiring between buildings because its location is subject to potentially large transients and its length may result in large voltage drops. In addition, proper consideration of ground water leakage should be taken. Wiring shall conform to **NFPA 70.**

> ***725.57 Installation of Circuit Conductors Extending Beyond One Building.***
>
> *Where Class 2 or Class 3 circuit conductors extend beyond one building and are run so as to be subject to accidental contact with electric light or power conductors operating over 300 volts to ground, or are exposed to lightning on inter-building circuits on the same premises, the requirements of the following shall also apply:*
>
> ***(1) Sections 800.10, 800.12, 800.13, 800.31, 800.32, 800.33, and 800.40 for other than coaxial conductors***
>
> ***(2) Sections 820.10, 820.33, and 820.40 for coaxial conductors***

Transient Protection. All building-to-building wiring should be run in an underground conduit system. Any wiring in an above-ground conduit system must have transient protectors (as specified by the manufacturer).

Signal Loss. The length of wiring between buildings may contribute to signal losses (voltage drops) or signal degradation (accumulated wire capacitance). Always follow the manufacturers' guidelines regarding the length of such runs.

GROUNDING.
All grounding will be in accordance with **NFPA 70, *National Electrical Code,*** Articles 250 and 800.

Additional grounding will be in accordance with manufacturer's requirements.

All other circuits will test free of grounds.

ZONING & ANNUNCIATION.
General. All required annunciation means will be readily accessible to responding personnel and shall be located as required by the AHJ to facilitate an efficient response to the event.

Visible Zone Indication. When required, the location of an operated initiating device will be visibly indicated by building, floor, or other approved subdivision by annunciation, printout, or other approved means.

When required, the visible indication will not be canceled by the operation of an audible alarm silencing means.

If all locations in alarm are not displayed simultaneously, visual indication will show that other locations are in alarm.

Testing. All electronic premises security systems will be maintained and tested in accordance with **NFPA 731 *Standard for the Installation of Electronic Premises Security Systems*** Chapter 9.

Voltage Drop. Normally, 1-16 rooms will be on a power riser. The voltage drop should be tested on each power cable as follows:

a. Take the measurement at the splice point of the last splice box on the riser.
b. Attach the voltmeter leads across the positive and negative power wires (as specified by the manufacturer).
c. Load the system by placing enough calls to represent 20% of the riser's calling capacity.
d. The voltage measured should be within the specified input range for the station in the room. A reading that is too low indicates the need for additional or higher-gauge power wires.

Software Control. Where required, all software provided with an electronic premises security system shall be listed for use with the equipment on which it is installed.

A record of installed software version numbers will be maintained at the location of the electronic premises security system.

All software will be protected from unauthorized changes.

All changes will be tested in accordance with **NFPA 731 *Standard for the Installation of Electronic Premises Security Systems*** Chapter 9.

VIII. PROPER CONNECTIONS

TYPES OF CONNECTIONS AND THEIR USES

Wire-Nut Connector. This screw-on connector can be removed and reused. Its primary use is for connections to pigtail wires. Although it is not recommended for Class 2 connections, it may be used for Class 1 connections.

Crimp-Type Closed-End Connector. This connector is installed, manually or automatically, with a compression tool. It is not reusable. It is recommended when the equipment is supplied with a pigtailed plug or receptacle. The equipment may be removed without cutting or shortening the wiring.

POWER CONNECTIONS

The most important attribute of a power connection is high conductivity. There must be a large mating surface between conductors, and the connection method must offer both a long-term gas seal and mechanical strength.

A gas seal is assured when the conductors, are brought into contact with enough force to make the wires metal surfaces conform and eliminate air gaps. Long-term seal stability is achieved when the mechanical memory of the connection maintains force on the contact. In making the connection, it is necessary to use abrasive action for breaking through any oxide or other film on the conductors' surfaces.

Since it is not a permanent, insulating, and full covering, the connection must be secured from any condition that would allow spurious contact with another conductor.

High-voltage connections should be completely covered so that they cannot be touched by a person. These covered areas must be labeled as dangerous or be sufficiently difficult to access.

Low-voltage connections should be covered so that they cannot connect with another circuit. They can be made accessible to authorized personnel.

All connections should be documented with a layout schematic that includes cable identifications and descriptions.

PROPER GROUND CONNECTIONS

Access systems must have proper ground (or earth-ground) connections to provide high-conductivity paths for shunting any charge imbalances that may occur. Ideally, a perfect ground will provide an infinite "sink" for electrical charges and provide a universal reference for zero volts.

A good ground connection at an exposed metal surface may also afford some safety. Should inadvertent voltages become present on the surface, the resulting flow to ground could trigger protection devices.

However, if an exposed metal surface can be absolutely insulated from ground, then it should not be connected to a ground or it will serve as a path for uncontrolled currents introduced from outside the system. Highly conductive discharge paths to ground may attract large currents that could damage the equipment being discharged.

Each system layout should document all the ground connections.

Ground connections should not be used to carry any nurse call signal or power current.

SYSTEM TERMINATIONS

System terminations are the connections between the system's components. They involve Class 2 wiring only. As with all electrical connections, gas-tightness, isolation between circuits, and mechanical stability are essential.

Connections should be enclosed in back boxes, away from view and the possibility of tampering.

If the equipment cannot be mounted in a back box, it should be connected to the system wiling with n connector designed to make multiple connects/disconnects. This connector should make a verifiably positive and retentive connection and incorporate cable strain relief.
Since nurse call system terminations require the use of hand tools by field personnel, the connection location must be easily accessible, facilitating the easy installation and quick replacement of the equipment.

The layout of the facility installation should document all connections within the system. It should give color coding and cable designations for the connecting points and describe each cable (gauge, type, number of wires, etc.).

CONNECTIONS FOR SUPERVISED CIRCUITS

Connections for supervised circuits must be made using screw terminals, locking connectors, or butt splices. Using screw terminals, the wires must be stripped and placed under the screw head or clamp. On other locking connectors, the wires must be stripped and crimped. All unused wires in back boxes should be cut and taped to prevent their being pinched. Cables running outside the conduit should have a strain relief at either end so that cable movement does not affect the connection or the system's operation.

Connections with Equipment. All equipment connections shall comply with NFPA 70 (NEC) and with all requirements of the equipment manufacturer.

IX. SEPARATION FROM OTHER CIRCUITS AND EQUIPMENT

CONDUIT AND CABLE-TRAY SYSTEMS

Article 725.136 of NFPA 70, the National Electrical Code, specifically details the restrictions in proximity between Class 1 circuits being run in the same conduit or cable tray as Class 2 or 3 circuits (most nurse call systems use Class 2 wiring for the load side of the wiring). Although the code does allow other Class 2 circuits in the same conduit or cable tray, this can create unacceptable leakage. (See Section 7 of this guide.)

OTHER EQUIPMENT

Access control systems are often required to be interconnected with other low-voltage systems. However, such interconnections may violate the energy-limited requirement (100va) or cause RFI/EMI leakage problems. The installer must comply with the manufacturer's limitations as stated in their installation manuals.

A manufacturer has two ways of obtaining authorization for interconnecting an external system. The usual method is to have the interface Listed with a NRTL (Nationally Recognized Testing Laboratory). This requires that the interface inputs and outputs will isolate the access control system from any violation of the leakage or energy-limiting standards even if the interconnected systems were to have a 120-VAC fault.

X. AS-BUILT DOCUMENTATION

GENERAL INFORMATION

As-built documentation facilitates proper service over the life of the installed system. This documentation must come from the installer. The manufacturer's installation manuals have only typical connection drawings that do not include cable-routing, colors, and other pertinent information.

It is recommended that all pertinent as-built information be placed in a pouch inside the central processing equipment cabinet of the system.

RISERS

120 VAC Wiring. If the 120 VAC feed breaker trips, this could shut down the system. Even if there is standby power, it will only last a short time. To reset the breaker, the maintenance personnel need to find it. Hence, the location of the breaker box and the number of the breaker should be marked on the central equipment cabinet. In addition, the AC riser should be included in the as-built pouch.

Low-Voltage Wiring. Access systems typically use low-voltage (Class 2 or 3) wiring. In order to trace any future problems, the service personnel need diagrams of the system's physical layout, including the routing of the cable (conduit, cable tray, or open cabling) and the locations of the splice boxes. These low-voltage wiring risers should be included in the as-built pouch.

INTERCONNECT DRAWINGS

The manufacturer will supply typical connection drawings for interconnecting each unit of the system. Typical splice drawings may be included, but they will not give the actual connections or color codes of the spliced wires for a specific site.

The as-built pouch should contain the following typical interconnection drawings specific to a site:

- Terminations and color-coding of the central equipment wiring.
- Typical splice-box interconnections.
- Typical splices at each room (including input device, RTEs, locking devices, controllers).

There should also be an as-built wiring layout and interconnection, sometimes referred to as a point-to-point wiring diagram, which shows:

- How every component in the system is interconnected.
- The physical location of all system components.
- The interconnections that are made at all junction boxes and splice points.
- The physical location of all junction boxes and splice points.

The conduit routing and distances.
The physical location of the central equipment.

MARKING HOME-RUN CABLES
Most installations have multiple low-voltage cables connected to the central equipment or central splice locations. To help the service personnel, the installer should label these cables to identify each run and its corresponding low-voltage riser drawing. (See Low Voltage Section above.)

SYSTEM PROGRAMMING RECORDS
Most microprocessor-based systems can be programmed to match the physical layout of the facility and meet the needs of the users (e.g., with door names, zone assignments, and custom feature configuration). The service personnel may need details of this programming when they service a CPU card (with memory) or central equipment, or when they change the programming.

A record of this programming (either written or in media form, as specified by the manufacturer) should be included in the as-built pouch for each system.

TEST RECORDS
As part of the installation, the installer must do a walk-through test to verify the safety and operation of the system. Since any significant service may require the service personnel to duplicate these tests, a record of the tests and the test results should be included in the as-built pouch for each system. These records should include:
The door by door walk-through results.
Locking device working verification
Standby power test results.

IN-SERVICE TRAINING
The installing contractor shall ensure in-service training is provided for the security staff. The training shall include any material specified by the manufacturer. These materials should be included in the as-built pouch, together with records of those who have been trained.

SERVICE PROCEDURES
The manufacturers or installer's recommended service procedures should be included in the as-built pouch. In addition, some preliminary information should be posted at or near the security department’s operator console.

This information includes:
A check list of procedures to try for a specific system problem before calling for service.
Who to call for service.
A form on which the user can record pertinent data regarding a system problem for the service personnel.

XI. INSPECTION AND SYSTEM TESTING

GENERAL INFORMATION

All access control system components should be tested by an independent Nationally Recognized Testing Laboratory (NRTL) to assure that they meet the safety and reliability requirements of the appropriate ANSI standards, the completed system must also be tested to verify that it has been installed in accordance with the manufacturer's manual.

This section describes the minimum proper system testing.

ELECTRICAL INSPECTION

Earth Ground. All system power supplies must be grounded in conformance with the manufacturer's installation manual, the appropriate chapters of the National Electrical Code (NFPA 70), and the applicable state and local codes.

AC Supply. Verification is made that the system's power supplies are connected to a dedicated branch circuit that is derived from the appropriate electrical system in the facility, See the requirements in the manufacturer's installation manual and the NEC.

Conformity with the Manufacturer's Installation Manual. The location, application, and wiring of the system components are checked to be sure they comply with the manufacturer's installation manual.

Connected Equipment. Verification is made that all equipment connected to the system is listed and regulatory labeled appropriately for the intended use and shown in the manufacturer's manual.

ELECTRICAL TESTING

AC Input Voltage. The AC input voltage is tested to make sure it is within the ratings of the systems power supplies.

Power-Supply Test. The output voltage of the system's power supply is tested to make sure it lies within the range specified by the manufacturer.

NEC Tests. Tests are made that verify that the installed system conforms to applicable chapters of the National Electrical Code (e.g., 250, 725).

LOAD TESTING

Test in accordance with the instructions in the manufacturer's installation manual, the maximum number of door activations, that the system is specified to support simultaneously, are activated. Verify that the system functions properly under this load.

XII. MAINTENANCE AND SERVICE

GENERAL INFORMATION
It is imperative to follow any manufacturer's instructions for maintenance and service.

The following is a broad outline of general maintenance and servicing procedures that should be followed. These are not intended to replace the manufacturer's documentation.

DOCUMENTATION AND PARTS
To properly maintain and service the system, it is vital that the following be available:

As-Built Documentation. This important documentation combines the manufacturer's general system information with project-specific details on system cabling and interconnections. The creation of this documentation is normally the responsibility of the installer and should be considered an integral part of the installation contract. (See Section 10.)

Manufacturer's Installation Manual. This document provides the installer with product-specific installation information, including: Descriptions of all system devices.
Typical applications of each system device.
Suggested location of each system device.
Typical interconnection diagrams.
Typical block wiring diagrams.
The type and gauge of the system wires and cables that must be used.
The maximum cable lengths, as appropriate.

Manufacturer's User Operation Manual. This manual is normally a two-part document. One part, the *Quick Reference Guide*, will apply only to the normal user functions of the systems normal operation.
The second part will describe the operation of the entire system, including all its peripheral devices. For programmable or user configurable systems, this part of the manual will include all programming and configuration instructions. For other systems, it will include initial set-up instructions.

Manufacturer's Service Manual. This manual will include both system servicing and trouble-shooting instructions as well as a list of spare parts recommended by the manufacturer. It is important to remember that the servicing and troubleshooting portions of this manual are written for trained personnel.

Spare Parts. It is recommended that a facility with a access control system, maintain an inventory of the following spare parts:

Extra Stock of Input devices for new personnel.

One of each type of input reader.
One of each type of locking device.
Controller card or unit ready for installation.
Power Supplies (a sample of each type used at the facility).

As the above list clearly implies, when a system device fails, it must be immediately replaced. Circuit boards should be repaired only by the manufacturer. In most cases, performing circuit-level repairs elsewhere will void the manufacturer's warranty and render any NRTL listing void. It is also important to keep the spare-part inventory current with any changes or updates made to the system.

TEST EQUIPMENT REQUIRED

Every facility should have the following basic test equipment on-hand for system service and trouble-shooting:

Multi-Meter: For checking voltage levels, electrical current measurements, and circuit continuity.

Again, the manufacturer's service manual should be consulted.

PERIODIC TESTING

Each access control system's operations should be tested periodically, and the results should be recorded.

All of the system's components should be tested for proper operation. The manufacturer's operation manual should be used during these tests.

PROBLEM INVESTIGATION

If there is a suspicion that a system failure has occurred, the following procedure should be followed:

1. Confirm that the operation in question has failed: This is especially important, given the diversity of equipment used in these systems. Obviously, making sure that there is a problem before beginning troubleshooting or corrective action will save both time and money.
2. Pinpoint tie problem to a specific area of the system.
3. Locate the Malfunctioning Device.

TECHNICAL ASSISTANCE

Directions for contacting the system's controller manufacturer's representative or the manufacturer's service department should be prominently displayed at the central equipment, and in the facility maintenance department.

Seek technical assistance in the following order:

1. System Installer.
2. System Distributor.
3. System Manufacturer's Representative.
4. System Manufacturer's Service Department.

A contact person should be identified with the company's name and telephone number. Be sure to periodically update this list.

Technician requiring factory support should note equipment model numbers and have that information available when contacting the factory.