NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

Installation of Electronic Access Control System

Graduation Project
EE - 400

Student: Shadi I. Al-Khatib (991247)

Supervisor: Asst Prof. Dr Doğan Haktanır

Lefkoşa - 2001

ACKNOWLEDGMENT

First of all, I want to pay my regards to all persons who have contributed in preparation of my project to complete it successfully. I am thankful to my supervisor " Dr Doğan Haktanır ", who helped me a lot in my crises, and gave me full support toward completion of my project.

I would like to thank my parents who gave there ever lasting encouragement in my studies, so that I could be successful in my lifetime.

I am also thankful to my beloved friends "Khaldun, Mohammed, Saif, and Rizwan" they are always tried their best in giving me valuable help toward preparation of my project.

Further I am thankful to the Near East University academic staff and all those persons who helped me or encouraged me in complete my project.

ABSTRACT

As technology advanced the trade secrets increases in line with this advancement. Many companies, in order to prevent the leakage of there trade secrets out of the establishment; they employ complex entry system at the entrances and within the establishments. This project shows how to construct an electronic access system (EAC), which is discussed in details within this project, this project is about installing of EAC system, this system has many equipments, these equipments includes doors and controlling components.

Within this project, I shall speak in details about each parts alone, then I shall combine these equipments together within on system, this system is applied on a building, this building related to software company, this company contains many rooms and the important rooms are computer and information rooms, in these rooms we applied on there doors high security level and for the other rooms we applied different types of security with respect to there importance. By applying high level of security in the main entrance I can keep unauthorized persons outside, I shall apply some other system within the building so that I can increase system efficiency and the system can work fluently.

The whole system is connected to the supervisory computer in the security room, and from there the security man can control and monitor all operations from there, the computer is connected to the other equipments through LAN this network is connected to the main computer and control panels, but the other equipments are connected to the control panels these equipments are responsible from the control panel this panel translate all information coming from the supervisory computer into the right equipment and with suitable standard and from there to the supervisory computer again. These panels can work in some cases without need to supervisory computer but not for long time. All these systems have been introduce with different plan, these plans emphasize its parts. Also it is emphasize security levels, also I shall speak how the whole system work and how does each equipment work In this project I shall use two different types of credentials one is the smart card and the other is the hand of that user (biometric credential) to have very high security in my building, within this project I shall speak about different types of credentials and I shall speak about there readers.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

1.1 Introduction to EAC system

While we have faced increasing in competition between company, it become more and more important to protect the companies information, and improve security in preventing the trade secret reaching to any one but not the dedicated personnel. For that reason or for any other reason protecting the buildings now days become very important.

Through this project I tried to give more obvious idea, clarify and in the same time provides the reader with some specification that is needed, the Electronics Access System that is responsible for our access (entering). This project will assist the reader to get more information easily about this system, which include monitoring system, entrance system, and others, this equipments -card system- will help our security system to activate, actually this part of security system allowed only for authorized person to access, and just to the region which allowed to him. And in order to improve our system these equipments should work fluently and without any bottleneck.

1.1.1 PROJECT OVER VIEW

This project contains three chapters the first chapter includes the introduction to these chapters and introduction to access control system, and how the system is working.

In chapter two I shall speak about *five* different parts. First: Credentials, this includes credential type like smart card that become one of the most important card in the whole world and it's get this speared from the high security that the card can provides, also there are explanations of different kind of reader such as normal card reader and biometrics reader.

The second part, explain Barriers (doors, doors closer, locks, fire exit and doors), here I shall give brief explanations about doors, and doors locks magnetic and electromagnetic.

In the third part I shall show Sensors (types, technology used and standard). Here I focus on Technology Glossary, I speak about many types such infrared sensors, heat sensors…etc. and how system is working and what is there affectivity in the system.

In part number four I shall give introduction to Computer that able to be use in EAC system that include many parts like software, hardware, network and technical information.

In the last part I shall speak about Communication (wired and wireless) in wire I speak about connection, cable types, cable jackets, such as coaxial cable, Fiber Optics and other, in wireless part I shall speak about communication media such as radio frequencies, analog to digital transmission, and digital transmission.

In Chapter number three I shall talk about project designing, in this chapter I have five plans first two is about security zones, the third explain system connections, and how to connect these parts to the main computer, the fourth plan is talking about communication system and CCTV system, the fifth plan shows what can be found in the security room from EAC equipments, then I shall speak about system components and how dose the system work.

At the end, I shall give my conclusion after writing this project, which are about the future of this system nowadays, efficiency and benefit behind using such system and the ability to improve such systems.

1.1.2 ACCESS CONTROL

Not too very long ago, access control was regarded as the art of keeping people out of building. If a stranger did gain access to a facility as, let's say. A guest of a manager, others might regard him or her suspiciously until they team who let this person in.

In modem society, however, transportation allows people from diverse backgrounds to gather in ways never before known in history. Our places of employment have become gigantic social) mixing machines where, in some cases, several new employees are being introduced on a monthly basis, in addition to many visitors.

The result of this is that as our organizations grow larger, people lose their ability to fully know and trust one another. If a problem occurs, such as a theft or physical threat, people feel scared, intimidated and depressed.

Electronic access control (EAC) is one component of a security system and it is best known for its ability to issue ID cards that replace keys. It is more than a security system, however. EAC provides an element of social engineering by quickly and securely introducing strangers into a facility in a way that they can almost instantly be trusted.

Figure 1.1.1 Most people think of EAS credentials as being cards. In fact, a credential can be any number of things, including biometrics, which analyzes physical characteristics such as palm prints. These motion detectors can be less than 3 inches tall. Yet they can sense intrusion over very wide areas.

An Access Control System consists basically of the following components:

- **Central Processing Unit:**

  Monitors and controls the system, including programming and operation.

- **Control Unit Stores and conducts programmed authorization data:**

  All access inquiries are checked and authorized from this unit.

- **Access Control Reader:**

  Being the preliminary control station of the system, it converts magnetic information (encoded in the cards) into electrical signals and directs them to the control unit.

1.1.3 How Does EAC Work?

This project describes EAC components; an overview of security needs and provides examples of real-life applications. Consequently, the following very brief description of how EAC works barely touches the subject, but it should provide an introduction.

EAC describes an electronic system in which information is collected and analyzed by computers. Once the information is digested, these computers issue instructions to various components, such as electronic and electromagnetic locks.

The computers have the ability to remember more information about large numbers of people than is humanly possible. The result of this is that they electronically issue commands based on the combined knowledge of:

- Security profile data
- Time and place
- Sensory data
- Management needs

In a well-designed system, security guards find these computers easy to manage. Through the use of a computer monitor, guards know who and why people are accessing the facility. They are also alerted when problems crop up and can instantly respond from their computer station by canceling an individual's access credential and/or by locking otherwise unlocked doors.

Figure 1.1.3 This is an example of a control panel. It is a circuit board and is often housed in an electrical utility box. The panel is a specialized computer that supervises access. It is capable of making decisions based on input, issuing commands and reporting all transactions to a computer at a central location, such as in a security office.

There are times during the day when facilities need more or less access monitoring. Depending on needs, the freedom of public access might reduce the amount of monitoring during business hours, while evenings and weekends might demand more. EAC systems are programmed to adjust to these needs. They are flexible systems that take into account human behavior.

Access Points: A door monitored by an EAC system has at least one credential reader and possibly two. One for either side, It also has an electronic or electromagnetic lock and at least one sensor that tells the computer when the door is completely closed.

This door might be surrounded with other security components, too. These include additional sensors, the most common type being motion detectors, and a CCTV system with videotaping. All these electronic devices report information (data) that helps control access and provide a history of events for later investigation. This project provides information about:

- EAC credentials. Which most people think of as ID cards.
- Electronic devices, such as locks and credential readers.
- Sensing devices, which provide electronic feedback about what is going on at strategic points throughout the facility and its grounds.
- Computers, which supervise the system.
- Control panels, which are specialized computers that control the electronic devices, receive feedback and issue commands.
- Communications, which carry the electronic data between computers, control panels and the devices they manage.
- System design concerns, which deal with the technicalities of setting up a system.
- Security concerns, which deal with concepts involved in integrating all the aspects of electronic surveillance into one coherent system.

Although issues surrounding closed circuit TV (CCTV) are an extremely important aspect of monitoring access, they are only touched upon briefly in this project. CCTV is a highly complex technology and experts, such as Charlie Pierce, have written clearly and extensively on the subject.

CHAPTER TWO: SYSTEM COMPONENTS

2.1 Credentials

2.1.1 CARDS, CODES, AND BIOMETRICS

The term "*Credentials*" refers to documents that verify a person's identity. People who present their credentials to officials or check points are regarded as being *authentic* . . . They are who they say they are. In electronic access control (EAC), credentials refer to cards, tokens and physical patterns, such as fingerprints, that identify people. Cards and tokens are presented to media readers for authentication, while physical patterns, such at fingerprints, are verified. When a credential is validated, access is granted. A credential is regarded as secure if it strongly resists alteration and/or duplication through forgery, or illegal use gained through spying. A secure credential when used by itself, however, does not resist use by an unauthorized person.

To increase the likelihood of truthful authentication, a single access transaction requires a multiple-step verification process. This process often combines a card with other identifiers, such as a personal identification number (PIN), biometric feature (such as fingerprints) and even photo/video identification. Not all access events require the same level of security. Exterior doors, for example, usually require more validation transactions than do interior doors.

> Example: in a highly secure chemical plant, guards monitor check-in. Employees display and use their proximity photo ID cards. Punch in their PINs, and have their palm prints read and verified. All these transactions take around 27 seconds per person, including a bit of gossip.

Once inside the plant, however, employees wearing their proximity cards move unhampered from monitored area to monitored area. This is because their proximity cards provide hands-free validation. The purpose of the internal EAC system, then, is to track "who goes there" and when they do it. It is not intrusive. The most common cards or tokens used throughout the world are based on Wiegand, magnetic stripe and proximity technologies in conjunction with PINs. These technologies, plus more, are described later.

Figure 2.1.1 Cards often require personal identification numbers in order to verify the authenticity of the user. Cards that are more secure can be used in multiple applications. The reader/keypad unit illustrated is part of a system designed to collect time and attendance information by using a standard EAC card.

2.1.2 MANAGEMENT PROCEDURES

No matter what credential technology you use, a facility is only as secure as its credential users' honesty. To manage a well-run system, then, you need to establish procedures that will verify identification, credential usage and termination, as the following overview describes:

2.1.2.1 ENROLLMENT PROCEDURES:

These let you enter data on access entitlements for users of the system. Time zones, access levels and geographical controls (identifying buildings and doors). Periodically, you'll need to update your information, including addresses, promotions, etc.

2.1.2.2 TRACKING PROCEDURES:

These check to make sure that the credential or your users are still in the system and are not altered or worn in any way. Plan on reissuing credentials and PINs at staged intervals. In a large system, for example. It would be disastrous to discover that all magnetic stripe cards wore out around the same time.

2.1.2.3 TERMINATION PROCEDURES:

These make sure that EAC authorization can be stopped the moment the user is terminated. In addition, they make provisions to retrieve outstanding credentials even though those credentials are no longer active in the system. This reduces chances for counterfeiting.

2.1.3 ENROBING CREDENTIAL USERS

A dishonest person with the best credential will cause harm to the facility. An honest person, free to roam is a blessing. Screening people prior to issuing credentials is important.

Validation: The very lowest level of screening is a visitor's pass issued on the say-so of another person in your organization. These passes do not unlock doors, but they do provide a way of identifying a stranger who is walking through the halls.

The more cautious you wish to be the more verified information you need to corset and maintain. The information you gather is only as accurate as your ability to ***double-check its authenticity.*** Failure to check information, even when a well-ordered portfolio is easily at hand, can have disastrous results.

Enrollment Time: Depending on your needs, the time it takes to enroll new people into your system is a factor in deciding what types of credentials you need to issue. It fakes longer, for example, to customize a magnetic stripe card with a color photo than it does to issue a card from a stockpile. Your enrolment procedures must calculate this processing time—minutes or days—so that you can keep up with your enrollment volume.

Encoding Considerations: Although most people think of credentials in terms of names and identity, computerized EAC systems associate people with code numbers. When used in cards or tokens, these codes are hidden from people (they are not PINs). Of the most popular cards, the user can customize magnetic stripe, proximity and bar-coded cards. But Wiegand cards cannot. With regard to codes, you need to:

- Know the total number of codes available in your system and how that total affects your future needs.
- Decide whether you want to customize those codes or accept standard numbers from the credential manufacturer.
- Know whether you can link PIN codes to your card or token codes.

Figure 2.1.2 Card Types (Smart, Wiegand, proximity and Mix Technology cards)

When you depend on manufacturer-encoded cards, you must keep a sufficient number of those cards on-hand to meet your enrollment demands. If you do not customize these cards with the user's name or photo, these cards can be reassigned until worn out.

For a number of reasons, most systems impose restrictions on the total number of codes available. Keypad systems, if not chosen with care, can be quite restrictive. Coding is dependent on the electronic circuitry of the media-reading mechanisms, memory, software, and in the case of keypads, available keys and internal switches. To increase the number of codes available, some cards provide a *facility code*. This code is placed before every single number in a standard range of codes, thereby increasing the total number of codes available.

> Example: Codes 1 through 9.999 are available to approximately 10,000 users. By using three facility codes with this range (say. 1001. 1002 and 1003), you increase the total to approximately 30.000 available codes.

Control panels validate the facility code first, then the credential code. When designing a system, you want your control panels to interpret the facility and card code whether or not that panel is linked to a main computer. When a control panel is dependent on a main computer and the communications link between them is broken, that panel might accept all valid facility codes without checking card codes. Worse, the panel might not function at all.

2.1.4 CREDENTIAL READERS

Credential readers (as well as scanners, keypads, etc.) act as the "middle man" between the credential user and the control panel. They are stationed at one or both sides of a protected door. When two readers are used to protect both sides of a door, the system enforces *antipassback* procedures, which discourage people from sneaking into areas, If a credential user fails to use the readers in the right sequence on both sides of the door, an alarm is sounded and guards are notified with a message displayed on their control monitor announcing who made the mistake.

All readers send credential codes to a control panel. The control panel compares the code it just received to existing databases. Depending on what the panel finds, it issues instructions to open a lock, sounds an alarm, or does nothing. If the control panel is dependent on a main computer, the computer checks the code, then sends validation information back to the panel and the panel takes it from there. Readers can take many forms. The most common are card swipe or insertion devices, proximity devices (based on radio frequencies), keypads (usually 4-key or 10-key), scanning devices (also called "optical readers"), and sensing devices (used in biometrics).

With the exception of biometric scanners, most readers are used for a variety of commercial applications in addition to EAC. Bar code readers, for example, automate pricing and stocking information in department and grocery stores. Magnetic swipe readers are used in charge and debit card transactions. One increasingly popular use of readers is to *track time and attendance* for payroll. The same credential that lets an employee access a facility also aids in calculating his or her paycheck—and docs so far more accurately than payroll systems compiled by time clocks and cards! The result can be very cost effective.

EAC readers differ from commercial readers because they require *temper resistant* monitoring. Access to wiring by removing a poorly mounted reader can render an electronic lock useless. Tampering and vandalism, not card duplication or fraud, account for a significant percentage of reader failures! Proximity readers, which can be completely hidden within a wait, are the most tamper-resistant. Others, depending upon decorating needs, can be surface mounted or embedded, but must not have exposed

screws or prying areas. Fortunately, reader tampering can be detected by attaching sensors to the reader mount. Once an EAC system detects tampering, it can ring bells and signal authorities.

2.1.5 CARDS AND PHOTO IDS

The increased speed and storage capacity of computers, coupled with decreasing prices for computer equipment, printers, video cameras and digital cameras is making the creation of computerized image databases and photo ID cards easy and inexpensive. White traditional photos and Polaroid technology are still being used to apply photos to cards, digital imaging provides:

1. Truly instant image creation (no chemicals or waiting period).
2. Instant computer files (no scanning necessary when the camera is connected to the computer).
3. Tamperproof, easily produced ID cards in color or black and white that don't require lamination.

Complete control over the design and processing of ID cards. Full color photo ID cards provide better security because they contain more visual information than black and white images. In addition, in full color image database on a computer provides excellent verification resources for the authorities that need to make visual comparisons. At this writing, photo ID cards are most commonly produced by the following methods:

Lamination: In this process, a photo (traditional or Polaroid) is cut out of a background and parted on a card, which is then covered by sheets of clear plastic.

***Dye sublimation*:** In this process, a full color digital image is printed on a card through a process called *dye sublimation,* which works as follows:

The image is reproduced by placing a tightly spaced series of dots on a vinyl card reproduces the image. If color is used, these dots are made through cyan, magenta, yellow, and black ribbons. Print processing uses variable heat temperatures to melt the colored dots, blending their hues and producing a wide range of colors. When these dots cool, they permanently bond to the card surface, making the card tamper resistant.

Black and white laser: In this process, special properties in the cards' material bonds with Mack laser printer toner.

2.1.6 CARD SIZE

What you put on a card, of course, is limited by the size of the card itself. To increase cost-effectiveness and to promote multiple technology cards, the EAC industry is striving to standardize all cards in terms of size and thickness. Two standards, which were developed by the banking industry, are:

- CR-80: most common credit-card sizes (2.125" tall by 3.375" wide by 0.03" thick)
- CR-60: slightly taller than the CR 80 (2.375" tail by 3.25" wide by .03" thick)

CR-80 is the most common size and fits all card swipe and insertion readers. CR-60. However, fits all card swipe readers, but not insertion readers. As swipe and insertion readers perform exactly the same tasks, it is important to be aware of the CR-60's reader limitations when designing a system. These two types shown in figure below.

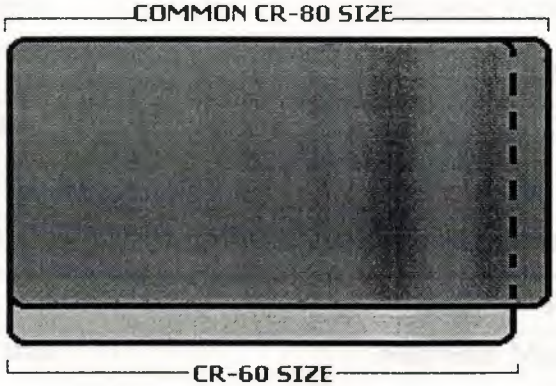


Figure 2.1.4 This figure show the difference between the two card types

2.1.7 CREDENTIAL TYPES

The following pages provide a background on 12 basic credential types, which are listed alphabetically below. Some credentials can be easily customized — important for facilities that want a lot of control over information — others depend on supplier issued ID codes.

The credentials you select depend on your need for easy customization and your overall security goals. Supplier encoding, while often being regarded as highly secure, is not necessarily the best. Combining technologies (such as photo identification, magnetic stripe and a PIN) can result in very satisfactory credential security.

2.1.7.1 BAR CODED CARDS AND OBJECTS

Bar codes are seen as a set of parallel thick and thin black lines. These tines form a light/dark pattern that is interpreted by an optical reader or scanner as a code number. Currently, there are more than 13 different bar code symbol sets, plus variations on these. The most popular codes include the Uniform Pricing Codes (UPC-A, which is a 12-digit code, and UPC-E, which is a 6-digit code).

Table 2.2.1 Credential Types and Related Technology

Credential Types	**Related Technology**
Bar Coded Cards And Objects	Light And Dark Patterns Interpreted By Optics
Barium Ferrite Cards	Magnetic Pattern
Biometrics	Physiological Pattern Interpreted By Various Means
Hollerith Cards	Holes That Allow The Passage Of Light Or Electrical Current
Infrared Cards	Light And Dark Patterns Interpreted By Optics
Keypads	Keyboard Input
Magnetic Stripe Cards	Magnetic Media
Mixed-Technology	Combined Technologies
Optical Cards	Light And Dark Patterns Interpreted By Optics
Proximity Cards And Objects	Radio Transmission And Computer Chips
Smart Cards	Computer Chips
Wiegand Cards	Magnetic Patterns

Code 39, and Post net, which is used exclusively for the U.S. mail. Code 39 is the most popular code used outside the retail industry and the one most likely to be used in EAC. It handles up to 44 characters that can include any of the 225 ASCII characters as well

as leading and trailing spaces. The spaces allow two or more bar codes to be scanned as one very long bar code.

Bar codes, which can be printed directly on cards or objects, provide the least expensive, easiest to use system of EAC identification. The software necessary to create bar codes is sold in computer stores and catalogs as well as through industry-specific sources. Readers, which include optical wands, guns, and scanners, are all commonly available.

Unfortunately, although bar codes are convenient for record keeping, they do not provide an adequate level of security for valuable assets or high security clearance. A photocopier or computer can easily duplicate bar codes. Because they are easy to create, bar codes can be successfully used for time and attendance reporting and casual EAC. Unlike magnetic encoding, printed bar codes cannot be destroyed by radio frequencies or magnetic field interferences. Placing a special translucent patch over the code can prevent easy duplication via a photocopier or computer scanner. Some patches contain patterns and even logos. No matter what they contain, they blacken the bar code when copied, but still allow optical reading.

Figure 2.1.5 The labels on the roll above are made out of translucent red masking material. Typically, this tape is placed on the bar code before the card is laminated

The accuracy of bar code reading depends more on the quality and condition of the optical readers used, than the quality of the printed bar code itself. This means that regular reader servicing is required to avoid problems caused by dirty or scratched optical surfaces. Although bar codes are seldom used alone in EAC. They are often

laminated onto more secure credentials, such as Wiegand, magnetic stripe, and proximity cards, to enhance information gathering.

2.1.7.2 BARIUM FERRITE (BAFE) CARDS

Magnetically encoded barium ferrite cards, which were in the forefront of FAC technology during the 1970s, have declined in popularity, although they are still being used. The first barium ferrite card readers were magnetic and mechanical, with many easy-to-damage parts. They worked as follows:

> At setup, a program cartridge, containing a pre-coded array of magnetized spots, was installed in a reader. Between the program cartridge and the access card insertion area were individual magnets, a movable slider and a metal plate. The slider contained holes through which magnets could fall. The metal plate below the slider stopped the fall of those magnets. The program cartridge attracted a predetermined array of reader magnets upward and out of the slider holes. The remaining non-attracted magnets stayed in the holes (resting on the plate), thereby jamming the slider in place.
>
> The access card contained magnets positioned to match the pattern of those resting on the metal plate. When this card was inserted, the resting magnets were magnetically repotted (pushed upward), releasing the slider, which slid forward, tripped a micro switch, and released the latch.

At one time, the same code array was used by all the access cards issued in a system, if a card was lost, the program cartridge and the remaining cards had to be reissued. As time went on, additional magnetic spots were added to the main array, forming unique ID numbers that could be interpreted by microprocessors.

The original readers required a great deal of maintenance. As they wore out, many were replaced with competing technologies. Still, as of 1980, there were many barium ferrite cards in circulation, providing the market for a few manufacturers to develop 100% microprocessor-based readers that could interpret other manufacturers' cards as well as produce low-cost proximity-like systems.

Magnetic barium ferrite codes are difficult to duplicate because they are factory-embedded, making them highly secure. They hold up especially well to problems caused by harsh weather and hostile environments, and can be used in mixed technology applications. Like all magnetically encoded cards, however, they can be erased or distorted by strong magnetic fields and tend to wear out over time.

2.1.7.3 BIOMETRICS

While the security level of credentials is determined by whether or not they can be easily duplicated, unauthorized use can occur when credentials are shared, stolen and/or PINs are exposed. Biometric credentials were developed to defeat this problem by verifying that the unique personal features of the credential user, such as their palm print or eye, match a copy of those features, called a "*template*," stored in a computer. Biometrics, which began as an offshoot of the study of genetics and disease, are used when the need for a highly secure identification system offsets the cost of that system.

Various biometric systems have been available for decades, including an attempt by IBM in the 1970s to promote a signature recognition system. Many of these systems,

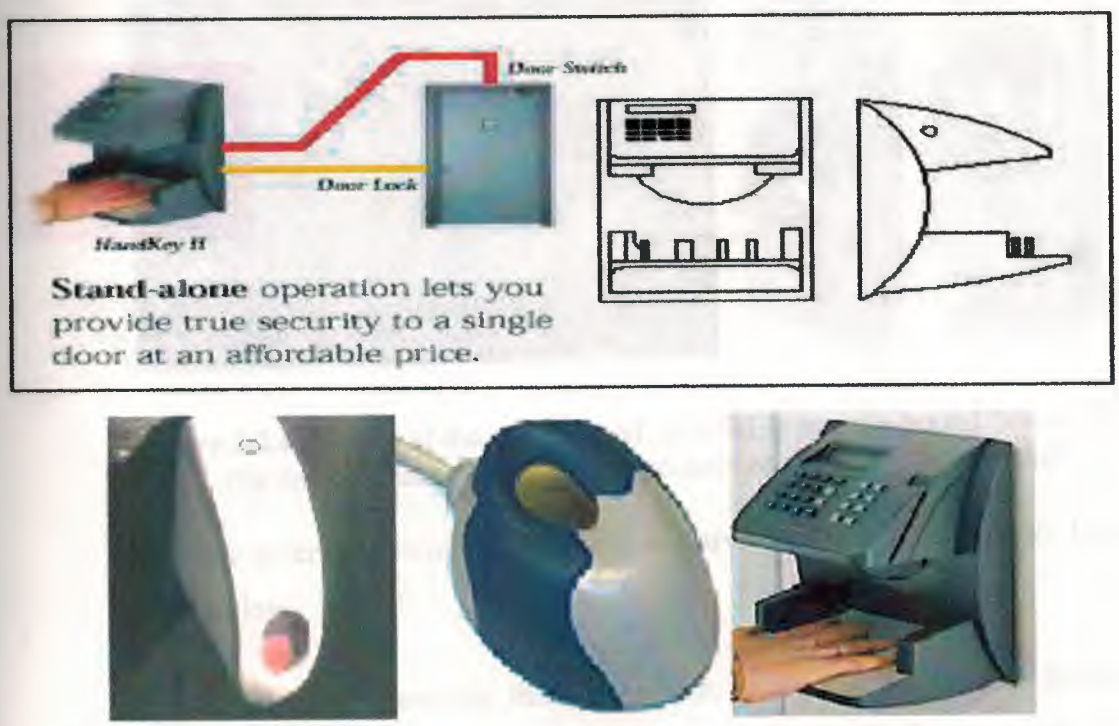


Figure 2.1.6 Reading palm prints checks the length, width and thickness of the hand and almost use for high security and time and attendance points of unique information can be encoded in this way. Also we can see below it fingerprint.

However, were no popular because of high costs, the high rate of verification errors, and verification slowness.

2.1.7.3.1 Body odor:

Senses odors by using chemical processes that are similar to the processes that take place in the nose and brain.

In early 1995, researchers at Leeds University in England announced that they developed a process that can differentiate between people by their smell. Perfumes do not mask this process because perfumes scenes are very different in chemical composition than body odor. Smart card manufacturers hope to eventually embed this technology in their chips in order to compete with finger printing systems.

Before they do that, of course, body odor technology must improve its current identification accuracy of 90%.

2.1.7.3.2 Eye identification:

Figure 2.2.6 Potions of the eye are read by looking into the hound "view" area. The device illustrated is a retinal scanner combined with a keypad

There are several ways of using the eye to provide unique identification, two of which follow:

Iris identification measures the iris, which, according to product literature distributed by Iris can, can identify 4,000 points in less than three seconds. They

claim that iris patterns are fixed at birth and there are no two alike, including those of identical twins.

Retinal scans read the surface behind the eyeball through a tow-intensity infrared fight that tracks 320 points in the retina and records associated blood-vessel patterns.

2.1.7.3.3 Facial recognition:

Verifies facial features by comparing a living face scanned by a camera to older images in a database. Because it is easy to change appearance, there are several systems under development that seek to reduce validation time and increase accuracy. This type of technology is far more sophisticated than having a guard check an image database and then determining the similarity between the picture and the living subject.

2.1.7.3.4 Multiple biometric patterns:

Assures that a severed body part, such as a finger, cannot be used for falsifying identification by requiring that two different biometric readings be taken at the same time. A blood-oxygen saturation reading taken with a fingerprint scan is an example.

2.1.7.3.5 Random voice interrogation:

Assures that a tape recorder cannot be used to bypass a voiceprint system, which compares speech patterns, it does this by recording several spoken phrase templates for each person. When identification is requested, the person is asked to recite only one of the prerecorded phrases. Once the phrase is recited, the voice is compared to the appropriate template.

2.1.7.3.6 Signature identification:

Measures time and pressure used to create a signature as well as the signature pattern itself.

2.1.7.3.7 Voice identification:

Identifies the unique voice characteristics of a freshly spoken phrase to one stored in a template. These comparisons include air pressure and vibrations over the larynx.

2.1.7.3.8 Weight measurement:

Although weight is not a biometric measure because it cannot pinpoint specific traits, weight is often used to determine the presence of an individual or thing and consequently, can be used in the authentication processes.

Weight checkpoints are often found in enclosed rooms called "mantraps" as well as around "invisibly" protected objects, such as might be seen in a museum.

2.1.7.3.9 Hand and fingerprint identification:

Uses various techniques, among which is a three-dimensional digital image that is captured and measured to create a template Between 10,000 to 250,000 points of unique information can be encoded in this way.

While biometrics generally provides a highly accurate verification system, especially when combined with a PIN, users are sometimes concerned about the possibility of physical invasion, harm or discrimination during the credential-reading process. The following considerations describe a few of their concerns:

- A biometric x-ray system, for example, would not be viewed as accept able because x-rays harm the body with regular use.
- People with certain types of physical disabilities, such as those who have artificial hands or who are blind, might not be able to use the system.
- Blood tests are generally considered too intrusive to do on a regular basis. In addition, there are many regulations governing their use.

2.1.7.4 HOLLERITH CARDS

Hollerith cards are modeled after cardboard computer cards that were first used in 1890 by the U. S. Census Bureau to automate the national census. These cards featured a uniform pattern of small rectangles arranged in 80 columns, 12 rows high, and held up to 80 alphanumeric characters of information per card.

To encode these original computer cards, keypunch operators punched out selected rectangles, leaving holes that represented values. These cards were then placed in electronic readers, which passed current through the holes. The resulting pattern of "on's" and "off's" were electronically translated by a computer into data for number crunching. Copying the above principle on a simple scale, Hollerith cards also have holes punched in them, but not as many. These thin plastic cards, which can be manufactured in a variety of rectangular sixes, are read optically by passing a light through the holes, or electronically, by allowing metallic brushes to touch contacts exposed through the holes. Unfortunately, Hollerith cards can be easily duplicated and are only used in low-security applications- Hotels and motels, for example, often use Hollerith cards. When a card is lost, the code can be quickly changed and a new card issued with minimal expense

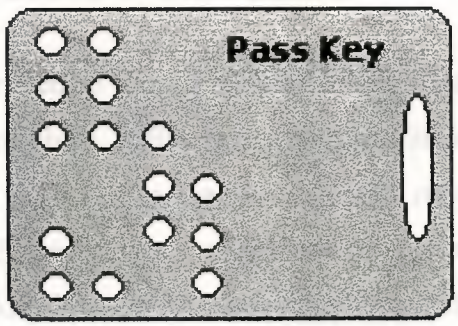


Figure 2.1.7 This Hollerith card is typical of those used in the hotel industry.

2.1.7.5 INFRARED CARDS

Light sensitive infrared card technology, also referred to as "Transmissive infrared" and "differential optics." appeared in the 1970s and uses bar code principles to encode information.

Embedded in the card is a bar code that is coated in a way that allows predetermined amounts of infrared light to pass through. Electronic infrared sensors detect this internal pattern as reduced energy level infrared light. The bar code pattern itself cannot be seen by the human eye. Like bar coded cards, the accurate reading of an infrared card is dependent on the quality and maintenance of its light-sensitive infrared reader. Unlike bar coded cards, these infrared codes cannot be easily duplicated because they are made in a factory and are, therefore, very secure. In addition, they are not subject to erasure by stray magnetic fields as are magnetic stripe, Wiegand, and barium ferrite cards.

2.1.7.6 KEYPADS

Keypad devices provide the means to link a PIN with a credential use a PIN by itself and/or program various devices connected to the system. In all, they are extremely versatile. Some keypads are part of the locking mechanism. This type of keypad might be programmed to respond to a single PIN that's assigned to everyone, or else, it can be linked to a sophisticated control panel, which provides the means to track many codes and time zones. In most mediums to large EAC systems, keypads are linked to powerful control panels and verity cards through use of a PIN. Some keypads even have secret containers in their mountings. These provide a secure storage area in which to place standard keys (for locked cabinets) or other valuables.

Generally, keypads are limited to four-or ten-digit codes, regardless of how many keys appear on the devices themselves. Software, memory and internal circuitry impose these limits; consequently, it is important to examine your PIN requirements before selecting a keypad system. In addition, keypads might not comply with the Americans With Disabilities Act, as their location and PIN usage might be difficult for physically and/or mentally challenged people.

Still, keypads are highly durable and are fairly inexpensive to replace. Systems based exclusively on keypads are easy to maintain because they do not require any card or token inventory or related encoding hardware such as is required for magnetic stripe cards. Unfortunately, keypad systems are not highly secure. For one thing, some keypads contain all the wiring necessary to open a door, which means that unauthorized removal can make the lock useless. Another problem is that PINs can be stolen through

spying or even casual observation. The spying issue has been addressed by the Scramble Pad, patented by Hirsch Electronics. This keypad reduces the chance of spying success by randomly changing its key top labels.

On a Scramble Pad, the keys labeled 123 might become 976 or 485. Consequently, the finger pattern used to punch in the code 6735 is different with every event. Even if a spy sees the motion, he or she would not know what it stands for. This keypad further reduces spying by shielding its key top tables and preview window with view-restricting material. In summary, keypads in combination with card and token, systems, play a very important role in EAC and are in common use.

Figure 2.1.8 **a.** Intelligent locksets like, which seen above can function independently, or be linked to a sophisticated EAC system.
b. This is a typical card reader combination.

2.1.7.7 MAGNETIC STRIPE CARDS

Most people have seen and used a magnetic stripe card of some type. These cards are the most widely used cards in the world and proliferate as bank credit and, of course. EAC cards. They are inexpensive, can carry alphanumeric information, are quickly produced and can be encoded at the user's site.

Each card contains a Mack plastic stripe of magnetically sensitive oxide, which is the same material used to make audio/video tapes. Unlike tapes, however, magnetic stripe cards are subjected to frequent rubbing and bending. Despite their lack of protective housing, their ability to retain magnetically encoded information is quite good. The risk

of magnetic erasure, however, is always a problem. Their resistance to erasure is known as their coercive force rating.

Coercive force ratings indicate the strength of a magnetic force required to erase magnetic material. A card with a low coercively rating, therefore, is fairly easy to erase, and a high coercively rating means that the card is more protected from stray magnetic fields. Needless to say, disposable cardboard cards are more likely to have a lower coercively rating than more permanent plastic varieties. According to the American National Standards Institute, Inc., magnetic stripes must contain four tracks available for encoding, however, specific encoding standards have only been defined for tracks one and two:

Track one: Stores up to 79 alphanumeric characters (210 bits per inch). This information might include the user's name and maybe a title.

Track two: Stores up to 75 bits per inch, with 40 numeric characters. This is the track most commonly used for access control codes.

Track three: This track can contain a facility code (also known as a *water mark*), which is described later in this section. Access to track three requires a special dual-head reader.

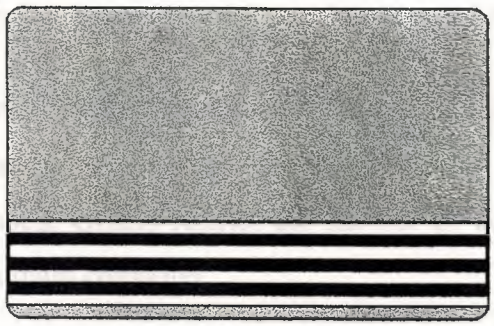


Figure 2.1.9 Magnetic Strip Card

Magnetic stripe cards store more characters of information than associated with bar coding or magnetic particle embedding and are far easier to customize. All encoding can be done at the end user's facilities by manual or automatic equipment. Manual encoders, of course, are more cost-effective for organizations that issue only a few cards. Automatic encoders speed up the process for issuing multiple-cards, plus provide

more control features. These include assigning sequential issue numbers and printing images on the Cards, in addition to the encoding process itself.

Unfortunately, with the right equipment, unauthorized duplication of magnetic stripe information is possible, rendering their security somewhat low. It is common, however, to see magnetic stripes on mixed-technology cards, which increases their security level. One very new development, for example, encodes highly secure, machine-readable, hologram patterns and a magnetic stripe on a single card. The combined use of PINs with magnetic stripe cards, of course, is well known. Magnetic stripe information is read by means of a swipe (moving the magnetic stripe along a track that passes a reader head) or insertion. Swipe readers, with their exposed reader heads, should only be used in environmentally clean areas. Insertion readers are less affected by environmental dust and are suitable for outside installations.

Motorized insertion readers regulate the speed at which the card passes the reader head and may increase reading accuracy. Like tape recorders and VCR's, however, the quality of the information transfer under any circumstance is largely dependent on the strength of the magnetic properties in the magnetic stripe and the cleanness and orientation of the card reader head. Magnetic stripe cards can be individualized by photos and/or bar codes through lamentation, printing, or dye sublimation. Care must be taken to make sure that bulky lamination does not jam up card travel in the reader.

Facility Codes and Water Marks: For a variety of reasons, some systems restrict the number of characters that can be used in a card code, thereby limiting the total number of codes that can be issued. Others restrict the number of codes a control panel can interpret before polling a main computer.

To increase the number of card codes available, a special code, called *facility coded* or *watermark* is permanently fixed in Track Three by the card manufacturer. This is done through a proprietary system that positions magnetic oxide particles on Track Three via wet slurry. When the slurry dries, the information is secure.

The result of applying a facility code is that a range of card codes, such as from 0001 to 9,999, can he duplicated. In the following example, a 10.000 card code range is expanded to approximately 30,000 possibilities.

- Facility Code 1002 - range 1-9,999
- Facility Code 1003 - duplicate
- Facility Code 1004 - duplicate

In addition to increasing the number of available codes, facility codes can be used to detect tampering and unauthorized card duplication.

2.1.7.8 MIXED-TECHNOLOGY

The ideal credential should be capable of combining a variety of technologies, including proximity, magnetic stripe, microprocessor (smart card), Wiegand, infrared, and keypad. In addition, users should be able to inexpensively apply customized designs, photos, and/or bar codes to cards for further individualization.

One advantage of using mixed-technology is that a single card can be read by different types of readers. This makes retrofitting (updating) existing card systems more cost effective because it doesn't require replacement of hardware or wiring. Another advantage is that it reduces the number of cards a person needs to carry.

Figure 2.1.10 Mixed technology card

Many universities are taking advantage of mixed-technology card systems:

> *Example:* In one college, a student photo ID card uses proximity technology to unlock dorms, bar codes to track library books, and a magnetic stripe with PIN to access the debit system used by the cafeteria and ticket agents. As shown in figure 2.1.10.

The three most common credential technologies are magnetic stripe, Wiegand, and proximity. Wiegand and proximity cards offer an exceptionally high degree of security.

Magnetic stripe cards carry a great deal of information and are easily encoded. Proximity cards, which do not touch their readers, improve traffic flow and reduce reader maintenance costs. Combining the three technologies mentioned above into a single credential requires:

1. A standard card size (CR-80 or CR-60 as mentioned earlier in this chapter).
2. A card thin enough (.03") to fit through a magnetic stripe swipe or insertion reader.
3. Sufficient voltage to drive Wiegand and/or proximity systems.

Other combinations are possible, too. Biometrics, for example, often requires a huge computer file (template) for each authorized person. Verification might take an excessive amount of time if the biometric reader has to check against templates held in a distant computer. Smart cards, however, can easily hold these large files. This allows the use of a biometric system for personal identification without being tied to a distant database, thus avoiding problems associated with slow or poor telecommunication connections.

2.1.7.9 OPTICAL CARDS

Optical cards are very new and are not widely used for EAC. This type of card was first developed by Canon U.S.A., Inc., and can store between 3.42 to 4.20 Mbytes of data on the size of a credit card. The amount of storage space it contains depends on the sensitivity of the card reader itself. The benefit to such a credential is that it can carry an enormous amount of information, thus reducing the telecommunications time a reader might require seeking details from a distant computer. The disadvantage is that this information must be entered on the card at the factory.

Optical cards are created by a solid-state, high intensity, laser beam that bums tiny pits on the card's surface. To read this data, a low intensity laser beam directs light on the pits, the reflection of which varies in accordance with the data that was initially etched. The Cannon system writes information on 2,500 tracts, some with multiple sectors, using the same write-once-read-many-times (WORM) techniques as for creating CD disks.

2.1.7.10 PROXIMITY CARDS AND TOKENS

Popular proximity cards or tokens do not need to touch a reader in order to validate a transaction. Their radio-wave transmission technology is highly secure and their readers can be hidden behind walls, in clean, maintenance-free, vandal-proof locations- Best, because proximity readers don't require contact, they speed the flow of human and vehicular traffic through check points.

These cards and tokens can remain in pockets, purses, or even on the front seats of vehicles and still be read by the system.

Figure 2.1.11 These proximity tokens contain a magnetic coil. Memory chip and a battery. Slim cards contain everything but the battery. The bracelet token is commonly used in hospitals and key chain tokens for garage applications. The flat panel token can be kept in a car or else attached to a cup for wearing.

Electrical power is always a big EAC concern and. prior to 1993; a typical proximity reader drew a great deal of current (400 mA at 12 volts). Today, readers can operate, with current as law as 40 mA at 5 volts, which is the same range, used for Wiegand and magnetic stripe readers. Each proximity card contains a coil of wire that acts as both the receiving and transmitting antenna and a small, integrated circuit that is programmed with a unique ID code.

The cards are powered by the voltage generated from a reader's magnetic field in relation card's antenna coil. Once energized by a reader, the card transmits its ID information Transmission is so fast that access verification takes place in less than a quarter second.

There are two types of proximity cards or tokens:

Active:

Has a range measured between touch to 100 feet. Its transmission is powered by a small, lithium battery. Due to battery thickness, active proximity carriers are manufactured as tokens or thick plastic containers that look somewhat like cards. The battery loses power over time and requires systematic replacement, although its average life is from five to seven years.

Passive:

Has a range measured between touch to 30 inches. Its transmission is powered by magnetic properties embedded in a very thin, maintenance-free card. The technological trend is to extend its transmission distance through the use of space technology that was originally developed to receive faint signals from distant stars.

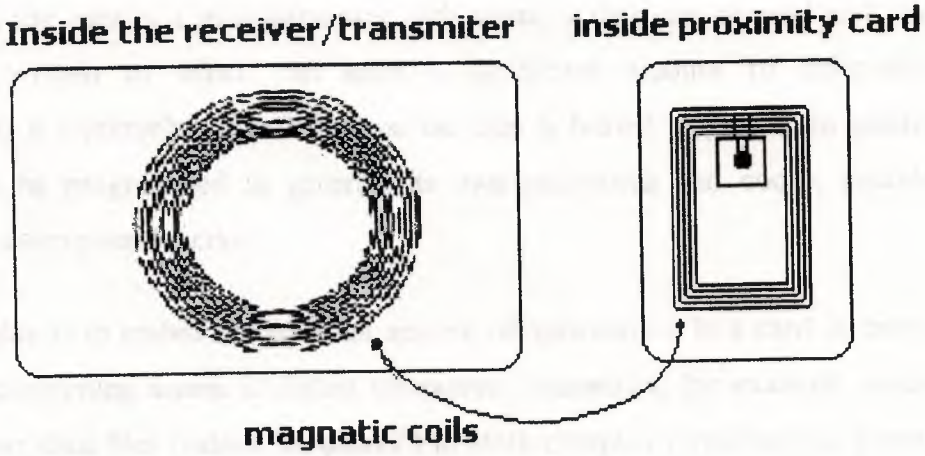


Figure 2.1.12 Both proximity card and reader.

Proximity technology is secure, reasonably priced and becoming increasingly used in mixed-technology cards. Readers have been miniaturized to fit into spaces less than 1.75" square and are getting smaller every day. Being convenient, they comply very well with regulations defined by the Americans With Disabilities Act.

HOW PROXIMITY WORKS

1. A receiver/transmitter (R/T) is either buried in a wall or contained in a slim cabinet hung on a wall.

2. The magnetic coil in the R/T excites the magnetic coil in a card when that card is in range. This range is extended when the card or token contains a battery.
3. Once it is excited, the magnetic coil in the card generates a crisp, magnetic pattern that represents a code contained in its memory chip.
4. The R/T receives the magnetic pattern and responds by amplifying and transmitting it to the processor — a control panel or other unit.

2.1.7.11 SMART CARDS

Although smart cards are currently uncommon in America, that may soon be changing. European companies (telephone systems and banking) have been using smart cards extensively since the early 1990s. A smart card is essentially a credit-card sized computer that was invented over 20 years ago.

Embedded in the card is a microprocessor with memory that can be read and. more importantly, written to which can store a significant amount of information. Counterfeiting is extremely difficult because the chip is buried in plastic. In addition, the chip can be programmed to generate its own passwords and codes, including sophisticated encryption functions.

The trend today is to embed a significant amount of information in a card in order to reduce time-consuming access to distant computers. Biometrics, for example, requires large computer data files (called "*templates*") to store complex physiological patterns. By keeping that information on a smart card, identification time is greatly reduced and worldwide check-in sites (such as used in the military) are not subject to long-distance communication problems. There are three types of smart cards:

- **Memory only:** Has less than 400 bits of memory and are often used for disposable "prepaid card systems."
- **Memory circuits with some hard-wired security logic:** Contains between 1K to 4K of memory and can be erased and rewritten. These are designed to allow encryption and PIN comparisons.
- **Full-Hedged microcomputers:** Contains a complete computer system with an operating system and the ability to be programmed to meet a

wide range of applications. The computer system includes a processor, nonvolatile read/write memory of 1 K to 8K, a small amount of random access memory, and read-only memory, which contains the operating system and the place where security functions are hidden.

Although a smart card looks similar to a standard credit card, it differs by having five to eight metallic contacts displayed on its surface. These contacts connect directly to a computer terminal when the card is inserted. To make sure that contacts is good, smart cards must be stored flat at all times and malignance is needed to make sure that terminal readers are clean.

To increase the potential markets for smart cards, information held in the chip can now be transferred through proximity technology. Although contact less and radio communication methods have not yet been standardized, systems are available.

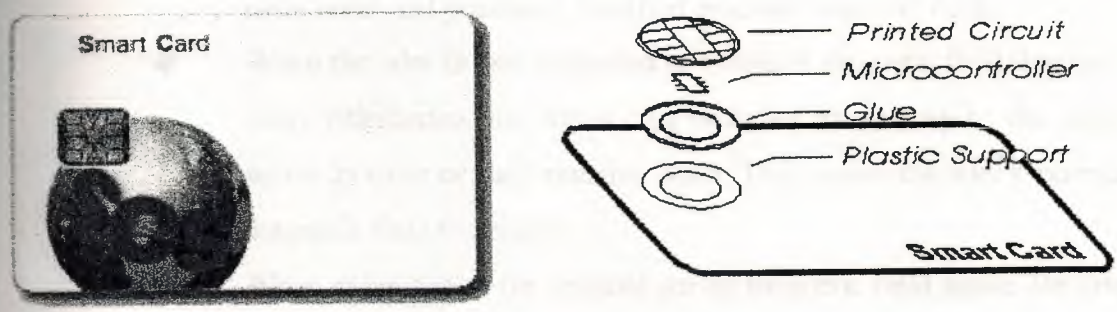


Figure 2.1.13 Smart cards look like common charge cards and can even have a magnetic stripe, bar code and/or id photo present. You can identify a smart card by a metallic design similar to the white one seen on the card above.

New uses for smart cards are being invented every day. Several states, for example, are replacing food stamps and other voucher systems with smart cards. These cards reduce paperwork and theft; white increasing reliability and ease of benefit transfer.

Hospitals are also using smart cards for EAC as well as for sharing patient records. Updating a smart card from a single computer source, as opposed to transferring information from numerous charts and records, improves communications, increases accuracy, and decreases costs associated with paperwork.

2.1.7.12 *WIEGAND CARDS*

Wiegand cards are based on patented technology held by the Sensor Engineering Corporation that embeds an array of magnetic wires in a card that is very difficult to duplicate. Wiegand technology combines several patented processes and a special metal alloy to create unique magnetic properties not found in common ferromagnetic (iron) wires.

Through manipulation and heat-treatment, the core of a Wiegand wire acquires a different magnetic property than its shell. This result in a condition called *magnetic action.*

Bistable magnetic action creates an electrical pulse:

- When first subjected to a strong magnetic field, the wire has a magnetic north and possesses a unified external magnetic field.
- When the wire is then subjected to a weaker magnetic field that has a south orientation, the wire's core switches its polarity to the south, while its exterior shell remains north. This causes the wire's external magnetic field to collapse.
- When subjected to the original strong magnetic field again, the core reverses its polarity to match that of its exterior shell. This change in polarity creates a crisp, discrete electrical pulse.

The only energy input required to create the electrical pulse is the bistable action of the wire in relationship to variations in magnetic fields produced by the reader. Although the pulse it regarded as analog, it is so crisp that it can be read as a digital output. Every Wiegand wire segment embedded in a card represents a magnetized pulse generating "bit." Up to 56 bits are allowed per card, although in reality, not alt the bits are required.

These bits are arranged in two parallel rows. Bits in the top row are referred to as *zero bits*, and in the bottom, *one bits*. The placement of these bits in relation to one another generates a binary pattern that represents a unique code. Wiegand readers have two reading heads, one for each row that read the electrical pulses generated by the bistable magnetic wires.

Manufacturing presses: All Wiegand wire is tested three times before it is cut into .33" strips and placed on vinyl adhesive tape in a pattern determined by computer-controlled machinery. For each order, the wire-encoded tape is spooled onto a tape feeder, and then fed to a tape-cutting-and-placing machine. This machine automatically cuts and places 12 strips of tape in appropriate locations on vinyl sheets (which are eventually cut into 12 cards), continuing with new sheets until the order is complete.

Once a vinyl sheet is prepared by the encoded tape and topped with artwork and lamination, it is pressure-temperature seated, die cut, and inspected- Depending on the order, and some cards also receive a special hot stamped card number. Before being shipped to the customer, the cards are inspected. Cards not meeting the inspection criteria are discarded and remanufactured.

Change in technology: The original Wiegand cards were somewhat thick. New credit-card thin sizes now allow Wiegand technology to be combined with other popular technologies, such as magnetic stripes; in addition, other manufacturers are developing proximity readers that can pick up Wiegand's low voltage power output (5 volt, 25 mA), while Sensor Engineering Corporation itself has also developed proximity technology.

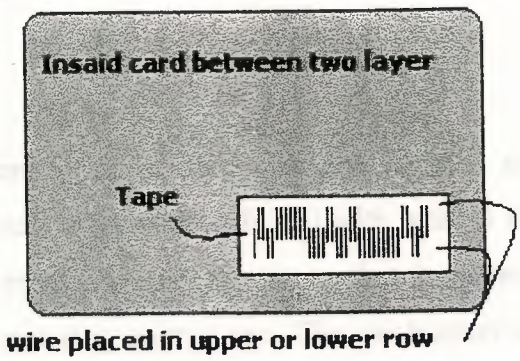


Figure 2.1.14 Wiegand Cards

Wiegand cards are regarded as very durable, secure, and reasonably priced. Unfortunately, because Wiegand cards are grafted at the factory, they take longer to manufacturer than other cards, forcing some EAC system managers to use other technologies because of lead-time considerations.

2.2 Barriers

2.2.1 DOORS

Function, governmental regulations, appearance needs, and cost alt determine a door's style and materials. Beyond these factors, doors controlled by EAC have the following in common:

- A door closing mechanism
- An electronically or magnetically activated lock
- Sensors (switches) that determine whether or not the door is properly closed
- Computerized control either in the locking device itself, or in a nearby, hidden control panel.

EAC requires that doorways, waits, and ceilings have a power source nearby and. in most cases, have adequate conduit and ducts in the walls or ceilings to hold electrical wiring. In areas where placing wire is difficult or prohibitively expensive, such as in an old elevator shaft, wireless EAC is substituted. EAC systems at so require wait or ceiling cavities large enough to contain control panels or wiring closets.

2.2.2 DOOR CLOSERS

Mechanical door closers are as important to an EAC system as the electronics that power the tocks. Door closers are spring-activated with tension strong enough to pull, doors completely shut after use, yet not so strong that it makes opening the door a struggle, or warps the door during normal use. The mechanism attached to the spring that guides the door shut is called the *arm.* Door closers fall into two main categories: concealed and surface mounted, a sample of which is seen on the next pages.

Concealed closer are usually used on doors designed for a clean, "no-hardware" look because the arm is hidden from view.

They can be difficult to adjust and service, however, because they are embedded into the top or bottom of the frame and door itself, requiring the door and frame to be

perfectly balanced. Hardware replacement is usually manufacturer-specific and requires exacting specifications.

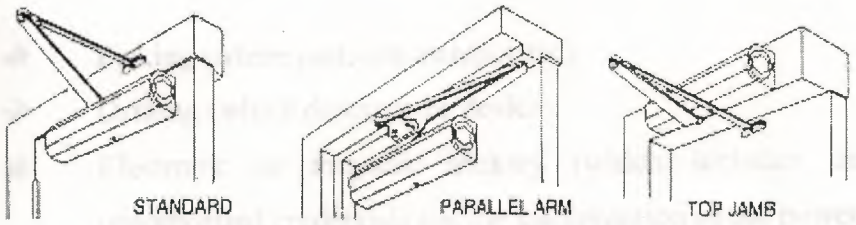


Figure 2.2.1 Door Closer

Surface mounted door closers are the most popular and fall into three main categories:

1. Regular-arm mounted
2. Top-jamb mounted
3. Parallel mounted

The most popular are the regular-arm and top-jamb styles, the latter of which is simply the regular-arm style installed upside down. The regular-arm and top-jamb door closers can stand the greatest deviation in door play. They are usually installed on the interior-side to reduce tampering, reduce weather damage such as rusting, and enhance the exterior appearance of the door. These types are shown in figure 2.2.1 above.

The *parallel style* is less popular. The arm on this closer slides parallel to the door, rattier than perpendicular to it. Unfortunately, it is difficult to service because it requires a very well balanced door. This type of closer is usually used when a jamb mounted closer must be installed on the weather-side of a door. It is thought to be more weather-resistant because its arm does not stick out and it can be shielded by a roof of some sort.

The series of illustrations on the next page show where door closers are commonly positioned on doors. Your understanding of these mechanisms can be greatly enhanced by observing the doors in public and private buildings.

2.2.3 ELECTRONIC AND ELECTROMAGNETIC LOCKS

The four most common types of locks used in EAC systems are the magnetic lock, the eclectic strike lock, the electric lockset, and the electric dead bolt. The strength of any

tock is determined by the way in which it can stop unauthorized entry that uses cleverness or force. Electronic or electromagnetic locks, therefore, must be strong enough to guard against:

- Picking (where parts are manipulated)
- Drifting (which destroys the device)
- Electronic or magnetic trickery (which includes the use of unauthorized credentials and the manipulation of the power supply).

EAC electronic and electromagnetic tocks are regarded as being either fail-safe or fail-secure and both have an important role in overall security:

Fail-safe:

The lock is **unlocked** when the power is off. This type of lock is usually used on a fire door. In the event of a fire, the locks can be released through the fire system or, if the power system fails, they unlock automatically.

Fail-secure:

The lock **remains locked** when the power is off. Power is required to unlock this type of lock and is usually used for normal locking situations.

2.2.3.1 MAGNETIC LOCKS

Magnetic locks secure doors through magnetic force and are always, fail-safe devices. They are ideal for high-frequency access control usage because they are totally free of moving parts, which reduces wear and tear.

Every magnetic lock consists of two components:

- Electromagnet
- Strike plate

The electromagnet is installed on the doorframe and the strike plate on the door itself. When energized, the electromagnet attracts the strike plate with a holding force ranging between 500 lbs. to 3,000 lbs.

All EAC systems require that some form of sensor reports whether a door is open or closed. Conveniently, many magnetic locks have that sensor built in, eliminating the necessity for a secondary sensor or switch.

The two basic magnetic lock styles are called:

- Direct hold, which is surface mounted on the secure-side of the doorframe and door.
- Shear (also called *concealed*), which is completely embedded within the doorframe and the door itself.

The large, *direct hold,* magnetic lock is ideal for use on poorly fitted doors and unframed glass doors because the two lock parts can be installed in rough proximity to each other. When energized, the electromagnet positioned on the frame attracts the strike plate on the door flush to its surface. This strong attraction doesn't require perfect horizontal or vertical alignment between the parts.

Smaller share magnetic locks, which are less than door thickness wide, are totally invisible to the eye when the door is closed. They are used when design and aesthetic considerations dictate that the lock be completely hidden. Concealing reduces the potential for tampering because the electrical wiring is completely enclosed within the doorframe. The narrow surfaces on the shear electromagnet and the strike plate require precise alignment. A small bracket is often used on the frame to stop door travel so that these surfaces line up.

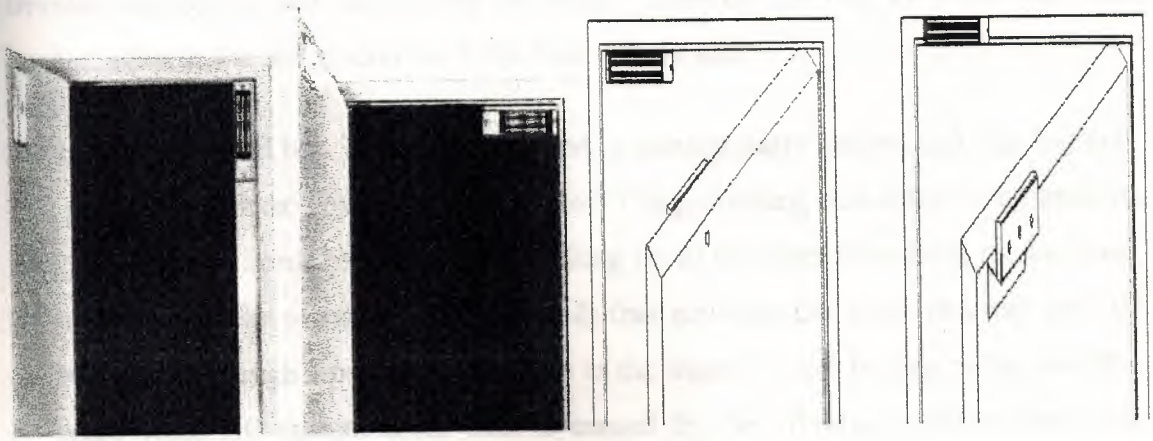


Figure 2.2.3 Magnetic lock

ANSI standards have defined three grades of magnetic locks. Grade one, which holds 1,500 pounds, is designed for medium security. Grade two, at 1,000 pounds, is for light security, and grades three. 500 pounds, simply holds a door shut. Most 180-pound men can force open a door equipped with an 850-pound magnetic lock.

As the holding attraction increases to 2,000 or more pounds, a magnetic lock will stay joined even when the force of a blow is strong enough to shatter the door it secures. Consequently, in addition to the strength of the lock itself, the material strength of the door, frame, and wall must also be considered when planning a high security door.

2.2.3.2 ELECTRIC STRIKE LOCK

The electric strike lock is the most popular EAC locking device on the market and can be set up as either fail-safe or fail-secure. Its popularity stems from the fact that it comes in a wide variety of sizes and can replace existing mechanical locks without a great deal of difficulty. The strike, which is the eclectically controlled portion of the lock mechanism, is mounted in a doorframe (jamb) and does not require wiring through the door itself.

The electronic strike contains a bolt pocket, which is the indent that holds the protruding latch bolt or dead bolt secure in the frame. To open, the strike rotates away from the pocket, providing a path for the bolt to escape. This rotating side is called a *pivoting lip or keeper.* The latch bolt or dead bolt housing itself is mortised (embedded) in the door.

Latch Bolt: The latch is a spring-loaded, beveled bolt. When the door closes, the beveled-side of the bolt slides over the strike, allowing the bolt to retract and then expand again in the bolt pocket once the door is fully shut.

Dead bolt: The dead bolt is a solid metal rod or rectangularly shaped bolt that has only two possible positions: protruding or retracted. The protruding bolt enters or escapes the bolt pocket in the frame only when the pivoting lip of the electric strike is rotated away from the frame. The solenoid (magnetic coil) that activates the strike receives low AC or DC current through a power cord hidden in the frame. A soft buying noise can often be heard when AC current used. This is caused by the vibrations of the alternating current pushing and pulling the solenoid 60 times per second.

Figure 2.2.4 Door Locks

Electric strikes and their rotated latch boils come in a variety of styles suitable for installation on wood and metal frames. Each frame type, however, poses its own demands. A few of the many things to consider include:

Wood frames can be weakened from the hollowing out required for installation of the electric strike and need additional anchors or brackets to protect the took itself against forced-entry attempts.

Tubular aluminum frames might be too shallow to accept an electric strike assembly. Hollow metal frames might be too weak to resist a forced entry, or else were filled with cement or plaster when installed, prohibiting the installation of the electric strike at a later date.

2.2.3.3 ELECTRIC LOCKSET

The electric lockset is very similar to a mechanical lockset and is available in cylindrical and mortise styles. The difference is that an electric solenoid (magnetic coil) replaces the mechanical action provided by a standard key. In addition, only the electric lock has fail-safe or fail-secure operational modes.

- *Cylindrical Lockset:* These are characterized by a doorknob or handle on each side of the door, which are joined by a cylinder that controls the locking mechanism.

- *Mortise-style Lockset*: These are characterized by a lock, which is housed in a rectangular metal container that is embedded at the edge of the door and is often enclosed within the door's thickness.

Electric power is brought to the lock by threading wire from the frame through the door. Electric hinges (or pivots) completely conceal the wiring path when aesthetics are a consideration. Flexible cable loops are used when a seamless appearance isn't necessary and must only be exposed on the secure side of the door.

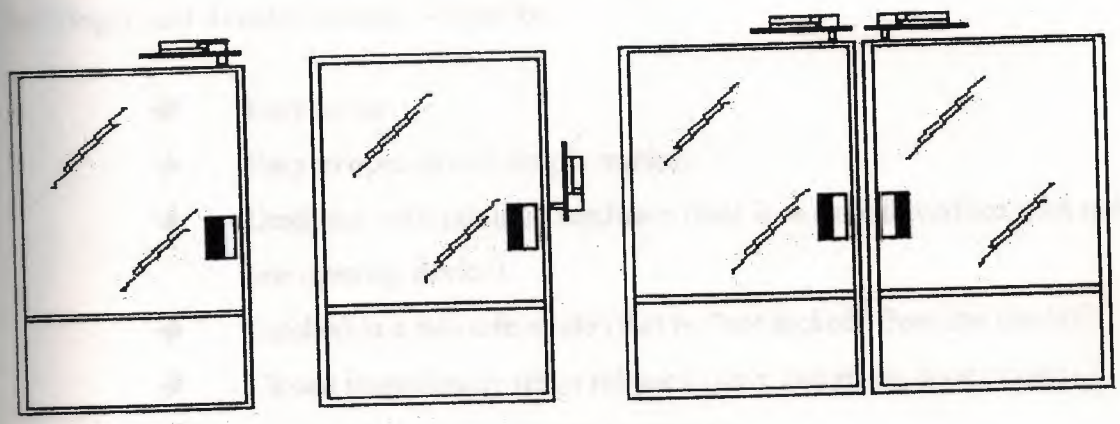


Figure 2.2.5 Electrical Lock locations

2.2.3.4 ELECTRIC DEAD BOLT LOCK

The electric dead bolt refers to the blot design and is used as an alternative to a magnetic shear lock for doors that swing in two directions and double-doors. The electrically powered dead bolt is fitted into either the jamb or the door itself and when activated, it protrudes (shown on previous page) or swings (below) into a mortised strike plate on the adjoining surface.

To increase holding strength, more than one set of electric dead bolts can be installed per door. Dual sets are common on large doors, as well as on both double-hung doors that swing away from each other from a center point. By installing electric dead bolts in the door header (top) and at the base, each door is secured and resistant to force.

The dead bolt does not give way with a spring action. Once it is clicked in place, it stays in place until unlocked. Although electric dead bolts can be set in fail-safe or fail-secure modes, the majority of building and safety codes prohibit them for egress path use in high-rise buildings. Manufacturers have developed standard-compliant locks, but they are not in common use for these applications.

2.2.4 FIRE EXITS AND ADA RULES

The rules surrounding fife exits sometimes conflict with the purpose of EAC. No one wants to be trapped inside of a building during an emergency. This means that specific exits—doors leading to and from stairwells, between firewalls (and adjoining buildings), and directly outside — must be:

- Easy to see
- Easy to open in one simple motion
- Designed with minimal hardware (that is, a smooth surface with only one opening device)
- Latched in a fail-safe mode (that is, "not locked" from the inside)
- Closed immediately when released (have automatic door closers)
- Constructed out of fire-rated materials

Here is how fire codes effect EAC: In this simple example, the door is secured by a magnetic lock that can sense when the door is closed. To enter, a card is swiped through a card reader, which sends the information found on the card to a control panel. If the card is valid, the control panel sends the instructions to unlatch the lock.

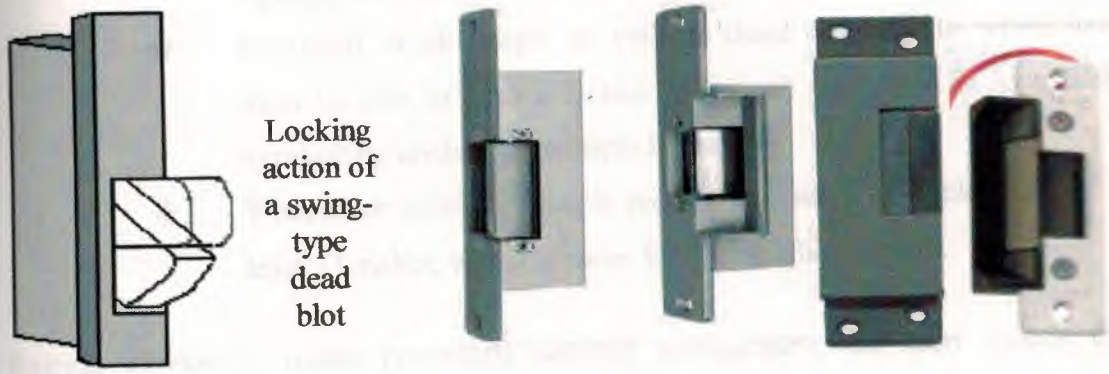


Figure 2.2.6 Door Strikes

After the door is opened, the "door closed" sensor tells the control panel whether or not the door returned to the closed position. If the door does not close within a predetermined amount of time, the control panel triggers an alarm. Whether or not the door closes as scheduled, the EAC database saves the pass code user's name as well as date and time of his or her access. This creates an important trail of information! Exiting, however, creates a different set of circumstances.

NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

Installation of Electronic Access Control System

Graduation Project
EE - 400

Student: Shadi I. Al-Khatib (991247)

Supervisor: Asst Prof. Dr Doğan Haktanır

Lefkoşa - 2001

ACKNOWLEDGMENT

First of all, I want to pay my regards to all persons who have contributed in preparation of my project to complete it successfully. I am thankful to my supervisor " Dr Doğan Haktanır ", who helped me a lot in my crises, and gave me full support toward completion of my project.

I would like to thank my parents who gave there ever lasting encouragement in my studies, so that I could be successful in my lifetime.

I am also thankful to my beloved friends "Khaldun, Mohammed, Saif, and Rizwan" they are always tried their best in giving me valuable help toward preparation of my project.

Further I am thankful to the Near East University academic staff and all those persons who helped me or encouraged me in complete my project.

ABSTRACT

As technology advanced the trade secrets increases in line with this advancement. Many companies, in order to prevent the leakage of there trade secrets out of the establishment; they employ complex entry system at the entrances and within the establishments. This project shows how to construct an electronic access system (EAC), which is discussed in details within this project, this project is about installing of EAC system, this system has many equipments, these equipments includes doors and controlling components.

Within this project, I shall speak in details about each parts alone, then I shall combine these equipments together within on system, this system is applied on a building, this building related to software company, this company contains many rooms and the important rooms are computer and information rooms, in these rooms we applied on there doors high security level and for the other rooms we applied different types of security with respect to there importance. By applying high level of security in the main entrance I can keep unauthorized persons outside, I shall apply some other system within the building so that I can increase system efficiency and the system can work fluently.

The whole system is connected to the supervisory computer in the security room, and from there the security man can control and monitor all operations from there, the computer is connected to the other equipments through LAN this network is connected to the main computer and control panels, but the other equipments are connected to the control panels these equipments are responsible from the control panel this panel translate all information coming from the supervisory computer into the right equipment and with suitable standard and from there to the supervisory computer again. These panels can work in some cases without need to supervisory computer but not for long time. All these systems have been introduce with different plan, these plans emphasize its parts. Also it is emphasize security levels, also I shall speak how the whole system work and how does each equipment work In this project I shall use two different types of credentials one is the smart card and the other is the hand of that user (biometric credential) to have very high security in my building, within this project I shall speak about different types of credentials and I shall speak about there readers.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

1.1 Introduction to EAC system

While we have faced increasing in competition between company, it become more and more important to protect the companies information, and improve security in preventing the trade secret reaching to any one but not the dedicated personnel. For that reason or for any other reason protecting the buildings now days become very important.

Through this project I tried to give more obvious idea, clarify and in the same time provides the reader with some specification that is needed, the Electronics Access System that is responsible for our access (entering). This project will assist the reader to get more information easily about this system, which include monitoring system, entrance system, and others, this equipments -card system- will help our security system to activate, actually this part of security system allowed only for authorized person to access, and just to the region which allowed to him. And in order to improve our system these equipments should work fluently and without any bottleneck.

1.1.1 PROJECT OVER VIEW

This project contains three chapters the first chapter includes the introduction to these chapters and introduction to access control system, and how the system is working.

In chapter two I shall speak about *five* different parts. First: Credentials, this includes credential type like smart card that become one of the most important card in the whole world and it's get this speared from the high security that the card can provides, also there are explanations of different kind of reader such as normal card reader and biometrics reader.

The second part, explain Barriers (doors, doors closer, locks, fire exit and doors), here I shall give brief explanations about doors, and doors locks magnetic and electromagnetic.

In the third part I shall show Sensors (types, technology used and standard). Here I focus on Technology Glossary, I speak about many types such infrared sensors, heat sensors…etc. and how system is working and what is there affectivity in the system.

In part number four I shall give introduction to Computer that able to be use in EAC system that include many parts like software, hardware, network and technical information.

In the last part I shall speak about Communication (wired and wireless) in wire I speak about connection, cable types, cable jackets, such as coaxial cable, Fiber Optics and other, in wireless part I shall speak about communication media such as radio frequencies, analog to digital transmission, and digital transmission.

In Chapter number three I shall talk about project designing, in this chapter I have five plans first two is about security zones, the third explain system connections, and how to connect these parts to the main computer, the fourth plan is talking about communication system and CCTV system, the fifth plan shows what can be found in the security room from EAC equipments, then I shall speak about system components and how dose the system work.

At the end, I shall give my conclusion after writing this project, which are about the future of this system nowadays, efficiency and benefit behind using such system and the ability to improve such systems.

1.1.2 ACCESS CONTROL

Not too very long ago, access control was regarded as the art of keeping people out of building. If a stranger did gain access to a facility as, let's say. A guest of a manager, others might regard him or her suspiciously until they team who let this person in.

In modem society, however, transportation allows people from diverse backgrounds to gather in ways never before known in history. Our places of employment have become gigantic social) mixing machines where, in some cases, several new employees are being introduced on a monthly basis, in addition to many visitors.

The result of this is that as our organizations grow larger, people lose their ability to fully know and trust one another. If a problem occurs, such as a theft or physical threat, people feel scared, intimidated and depressed.

Electronic access control (EAC) is one component of a security system and it is best known for its ability to issue ID cards that replace keys. It is more than a security system, however. EAC provides an element of social engineering by quickly and securely introducing strangers into a facility in a way that they can almost instantly be trusted.

Figure 1.1.1 Most people think of EAS credentials as being cards. In fact, a credential can be any number of things, including biometrics, which analyzes physical characteristics such as palm prints. These motion detectors can be less than 3 inches tall. Yet they can sense intrusion over very wide areas.

An Access Control System consists basically of the following components:

- **Central Processing Unit:**

  Monitors and controls the system, including programming and operation.

- **Control Unit Stores and conducts programmed authorization data:**

  All access inquiries are checked and authorized from this unit.

- **Access Control Reader:**

  Being the preliminary control station of the system, it converts magnetic information (encoded in the cards) into electrical signals and directs them to the control unit.

1.1.3 How Does EAC Work?

This project describes EAC components; an overview of security needs and provides examples of real-life applications. Consequently, the following very brief description of how EAC works barely touches the subject, but it should provide an introduction.

EAC describes an electronic system in which information is collected and analyzed by computers. Once the information is digested, these computers issue instructions to various components, such as electronic and electromagnetic locks.

The computers have the ability to remember more information about large numbers of people than is humanly possible. The result of this is that they electronically issue commands based on the combined knowledge of:

- Security profile data
- Time and place
- Sensory data
- Management needs

In a well-designed system, security guards find these computers easy to manage. Through the use of a computer monitor, guards know who and why people are accessing the facility. They are also alerted when problems crop up and can instantly respond from their computer station by canceling an individual's access credential and/or by locking otherwise unlocked doors.

Figure 1.1.3 This is an example of a control panel. It is a circuit board and is often housed in an electrical utility box. The panel is a specialized computer that supervises access. It is capable of making decisions based on input, issuing commands and reporting all transactions to a computer at a central location, such as in a security office.

There are times during the day when facilities need more or less access monitoring. Depending on needs, the freedom of public access might reduce the amount of monitoring during business hours, while evenings and weekends might demand more. EAC systems are programmed to adjust to these needs. They are flexible systems that take into account human behavior.

Access Points: A door monitored by an EAC system has at least one credential reader and possibly two. One for either side, It also has an electronic or electromagnetic lock and at least one sensor that tells the computer when the door is completely closed.

This door might be surrounded with other security components, too. These include additional sensors, the most common type being motion detectors, and a CCTV system with videotaping. All these electronic devices report information (data) that helps control access and provide a history of events for later investigation. This project provides information about:

- EAC credentials. Which most people think of as ID cards.
- Electronic devices, such as locks and credential readers.
- Sensing devices, which provide electronic feedback about what is going on at strategic points throughout the facility and its grounds.
- Computers, which supervise the system.
- Control panels, which are specialized computers that control the electronic devices, receive feedback and issue commands.
- Communications, which carry the electronic data between computers, control panels and the devices they manage.
- System design concerns, which deal with the technicalities of setting up a system.
- Security concerns, which deal with concepts involved in integrating all the aspects of electronic surveillance into one coherent system.

Although issues surrounding closed circuit TV (CCTV) are an extremely important aspect of monitoring access, they are only touched upon briefly in this project. CCTV is a highly complex technology and experts, such as Charlie Pierce, have written clearly and extensively on the subject.

CHAPTER TWO: SYSTEM COMPONENTS

2.1 Credentials

2.1.1 CARDS, CODES, AND BIOMETRICS

The term "*Credentials*" refers to documents that verify a person's identity. People who present their credentials to officials or check points are regarded as being *authentic* . . . They are who they say they are. In electronic access control (EAC), credentials refer to cards, tokens and physical patterns, such as fingerprints, that identify people. Cards and tokens are presented to media readers for authentication, while physical patterns, such at fingerprints, are verified. When a credential is validated, access is granted. A credential is regarded as secure if it strongly resists alteration and/or duplication through forgery, or illegal use gained through spying. A secure credential when used by itself, however, does not resist use by an unauthorized person.

To increase the likelihood of truthful authentication, a single access transaction requires a multiple-step verification process. This process often combines a card with other identifiers, such as a personal identification number (PIN), biometric feature (such as fingerprints) and even photo/video identification. Not all access events require the same level of security. Exterior doors, for example, usually require more validation transactions than do interior doors.

> Example: in a highly secure chemical plant, guards monitor check-in. Employees display and use their proximity photo ID cards. Punch in their PINs, and have their palm prints read and verified. All these transactions take around 27 seconds per person, including a bit of gossip.

Once inside the plant, however, employees wearing their proximity cards move unhampered from monitored area to monitored area. This is because their proximity cards provide hands-free validation. The purpose of the internal EAC system, then, is to track "who goes there" and when they do it. It is not intrusive. The most common cards or tokens used throughout the world are based on Wiegand, magnetic stripe and proximity technologies in conjunction with PINs. These technologies, plus more, are described later.

Figure 2.1.1 Cards often require personal identification numbers in order to verify the authenticity of the user. Cards that are more secure can be used in multiple applications. The reader/keypad unit illustrated is part of a system designed to collect time and attendance information by using a standard EAC card.

2.1.2 MANAGEMENT PROCEDURES

No matter what credential technology you use, a facility is only as secure as its credential users' honesty. To manage a well-run system, then, you need to establish procedures that will verify identification, credential usage and termination, as the following overview describes:

2.1.2.1 ENROLLMENT PROCEDURES:

These let you enter data on access entitlements for users of the system. Time zones, access levels and geographical controls (identifying buildings and doors). Periodically, you'll need to update your information, including addresses, promotions, etc.

2.1.2.2 TRACKING PROCEDURES:

These check to make sure that the credential or your users are still in the system and are not altered or worn in any way. Plan on reissuing credentials and PINs at staged intervals. In a large system, for example. It would be disastrous to discover that all magnetic stripe cards wore out around the same time.

2.1.2.3 TERMINATION PROCEDURES:

These make sure that EAC authorization can be stopped the moment the user is terminated. In addition, they make provisions to retrieve outstanding credentials even though those credentials are no longer active in the system. This reduces chances for counterfeiting.

2.1.3 ENROBING CREDENTIAL USERS

A dishonest person with the best credential will cause harm to the facility. An honest person, free to roam is a blessing. Screening people prior to issuing credentials is important.

Validation: The very lowest level of screening is a visitor's pass issued on the say-so of another person in your organization. These passes do not unlock doors, but they do provide a way of identifying a stranger who is walking through the halls.

The more cautious you wish to be the more verified information you need to corset and maintain. The information you gather is only as accurate as your ability to ***double-check its authenticity.*** Failure to check information, even when a well-ordered portfolio is easily at hand, can have disastrous results.

Enrollment Time: Depending on your needs, the time it takes to enroll new people into your system is a factor in deciding what types of credentials you need to issue. It fakes longer, for example, to customize a magnetic stripe card with a color photo than it does to issue a card from a stockpile. Your enrolment procedures must calculate this processing time—minutes or days—so that you can keep up with your enrollment volume.

Encoding Considerations: Although most people think of credentials in terms of names and identity, computerized EAC systems associate people with code numbers. When used in cards or tokens, these codes are hidden from people (they are not PINs). Of the most popular cards, the user can customize magnetic stripe, proximity and bar-coded cards. But Wiegand cards cannot. With regard to codes, you need to:

- Know the total number of codes available in your system and how that total affects your future needs.
- Decide whether you want to customize those codes or accept standard numbers from the credential manufacturer.
- Know whether you can link PIN codes to your card or token codes.

Figure 2.1.2 Card Types (Smart, Wiegand, proximity and Mix Technology cards)

When you depend on manufacturer-encoded cards, you must keep a sufficient number of those cards on-hand to meet your enrollment demands. If you do not customize these cards with the user's name or photo, these cards can be reassigned until worn out.

For a number of reasons, most systems impose restrictions on the total number of codes available. Keypad systems, if not chosen with care, can be quite restrictive. Coding is dependent on the electronic circuitry of the media-reading mechanisms, memory, software, and in the case of keypads, available keys and internal switches. To increase the number of codes available, some cards provide a *facility code*. This code is placed before every single number in a standard range of codes, thereby increasing the total number of codes available.

> Example: Codes 1 through 9.999 are available to approximately 10,000 users. By using three facility codes with this range (say. 1001. 1002 and 1003), you increase the total to approximately 30.000 available codes.

Control panels validate the facility code first, then the credential code. When designing a system, you want your control panels to interpret the facility and card code whether or not that panel is linked to a main computer. When a control panel is dependent on a main computer and the communications link between them is broken, that panel might accept all valid facility codes without checking card codes. Worse, the panel might not function at all.

2.1.4 CREDENTIAL READERS

Credential readers (as well as scanners, keypads, etc.) act as the "middle man" between the credential user and the control panel. They are stationed at one or both sides of a protected door. When two readers are used to protect both sides of a door, the system enforces *antipassback* procedures, which discourage people from sneaking into areas, If a credential user fails to use the readers in the right sequence on both sides of the door, an alarm is sounded and guards are notified with a message displayed on their control monitor announcing who made the mistake.

All readers send credential codes to a control panel. The control panel compares the code it just received to existing databases. Depending on what the panel finds, it issues instructions to open a lock, sounds an alarm, or does nothing. If the control panel is dependent on a main computer, the computer checks the code, then sends validation information back to the panel and the panel takes it from there. Readers can take many forms. The most common are card swipe or insertion devices, proximity devices (based on radio frequencies), keypads (usually 4-key or 10-key), scanning devices (also called "optical readers"), and sensing devices (used in biometrics).

With the exception of biometric scanners, most readers are used for a variety of commercial applications in addition to EAC. Bar code readers, for example, automate pricing and stocking information in department and grocery stores. Magnetic swipe readers are used in charge and debit card transactions. One increasingly popular use of readers is to *track time and attendance* for payroll. The same credential that lets an employee access a facility also aids in calculating his or her paycheck—and docs so far more accurately than payroll systems compiled by time clocks and cards! The result can be very cost effective.

EAC readers differ from commercial readers because they require *temper resistant* monitoring. Access to wiring by removing a poorly mounted reader can render an electronic lock useless. Tampering and vandalism, not card duplication or fraud, account for a significant percentage of reader failures! Proximity readers, which can be completely hidden within a wait, are the most tamper-resistant. Others, depending upon decorating needs, can be surface mounted or embedded, but must not have exposed

screws or prying areas. Fortunately, reader tampering can be detected by attaching sensors to the reader mount. Once an EAC system detects tampering, it can ring bells and signal authorities.

2.1.5 CARDS AND PHOTO IDS

The increased speed and storage capacity of computers, coupled with decreasing prices for computer equipment, printers, video cameras and digital cameras is making the creation of computerized image databases and photo ID cards easy and inexpensive. White traditional photos and Polaroid technology are still being used to apply photos to cards, digital imaging provides:

1. Truly instant image creation (no chemicals or waiting period).
2. Instant computer files (no scanning necessary when the camera is connected to the computer).
3. Tamperproof, easily produced ID cards in color or black and white that don't require lamination.

Complete control over the design and processing of ID cards. Full color photo ID cards provide better security because they contain more visual information than black and white images. In addition, in full color image database on a computer provides excellent verification resources for the authorities that need to make visual comparisons. At this writing, photo ID cards are most commonly produced by the following methods:

Lamination: In this process, a photo (traditional or Polaroid) is cut out of a background and parted on a card, which is then covered by sheets of clear plastic.

***Dye sublimation*:** In this process, a full color digital image is printed on a card through a process called *dye sublimation,* which works as follows:

The image is reproduced by placing a tightly spaced series of dots on a vinyl card reproduces the image. If color is used, these dots are made through cyan, magenta, yellow, and black ribbons. Print processing uses variable heat temperatures to melt the colored dots, blending their hues and producing a wide range of colors. When these dots cool, they permanently bond to the card surface, making the card tamper resistant.

Black and white laser: In this process, special properties in the cards' material bonds with Mack laser printer toner.

2.1.6 CARD SIZE

What you put on a card, of course, is limited by the size of the card itself. To increase cost-effectiveness and to promote multiple technology cards, the EAC industry is striving to standardize all cards in terms of size and thickness. Two standards, which were developed by the banking industry, are:

- CR-80: most common credit-card sizes (2.125" tall by 3.375" wide by 0.03" thick)
- CR-60: slightly taller than the CR 80 (2.375" tail by 3.25" wide by .03" thick)

CR-80 is the most common size and fits all card swipe and insertion readers. CR-60. However, fits all card swipe readers, but not insertion readers. As swipe and insertion readers perform exactly the same tasks, it is important to be aware of the CR-60's reader limitations when designing a system. These two types shown in figure below.

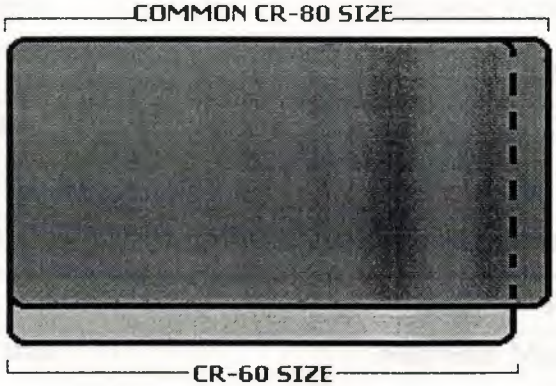


Figure 2.1.4 This figure show the difference between the two card types

2.1.7 CREDENTIAL TYPES

The following pages provide a background on 12 basic credential types, which are listed alphabetically below. Some credentials can be easily customized — important for facilities that want a lot of control over information — others depend on supplier issued ID codes.

The credentials you select depend on your need for easy customization and your overall security goals. Supplier encoding, while often being regarded as highly secure, is not necessarily the best. Combining technologies (such as photo identification, magnetic stripe and a PIN) can result in very satisfactory credential security.

2.1.7.1 BAR CODED CARDS AND OBJECTS

Bar codes are seen as a set of parallel thick and thin black lines. These tines form a light/dark pattern that is interpreted by an optical reader or scanner as a code number. Currently, there are more than 13 different bar code symbol sets, plus variations on these. The most popular codes include the Uniform Pricing Codes (UPC-A, which is a 12-digit code, and UPC-E, which is a 6-digit code).

Table 2.2.1 Credential Types and Related Technology

Credential Types	**Related Technology**
Bar Coded Cards And Objects	Light And Dark Patterns Interpreted By Optics
Barium Ferrite Cards	Magnetic Pattern
Biometrics	Physiological Pattern Interpreted By Various Means
Hollerith Cards	Holes That Allow The Passage Of Light Or Electrical Current
Infrared Cards	Light And Dark Patterns Interpreted By Optics
Keypads	Keyboard Input
Magnetic Stripe Cards	Magnetic Media
Mixed-Technology	Combined Technologies
Optical Cards	Light And Dark Patterns Interpreted By Optics
Proximity Cards And Objects	Radio Transmission And Computer Chips
Smart Cards	Computer Chips
Wiegand Cards	Magnetic Patterns

Code 39, and Post net, which is used exclusively for the U.S. mail. Code 39 is the most popular code used outside the retail industry and the one most likely to be used in EAC. It handles up to 44 characters that can include any of the 225 ASCII characters as well

as leading and trailing spaces. The spaces allow two or more bar codes to be scanned as one very long bar code.

Bar codes, which can be printed directly on cards or objects, provide the least expensive, easiest to use system of EAC identification. The software necessary to create bar codes is sold in computer stores and catalogs as well as through industry-specific sources. Readers, which include optical wands, guns, and scanners, are all commonly available.

Unfortunately, although bar codes are convenient for record keeping, they do not provide an adequate level of security for valuable assets or high security clearance. A photocopier or computer can easily duplicate bar codes. Because they are easy to create, bar codes can be successfully used for time and attendance reporting and casual EAC. Unlike magnetic encoding, printed bar codes cannot be destroyed by radio frequencies or magnetic field interferences. Placing a special translucent patch over the code can prevent easy duplication via a photocopier or computer scanner. Some patches contain patterns and even logos. No matter what they contain, they blacken the bar code when copied, but still allow optical reading.

Figure 2.1.5 The labels on the roll above are made out of translucent red masking material. Typically, this tape is placed on the bar code before the card is laminated

The accuracy of bar code reading depends more on the quality and condition of the optical readers used, than the quality of the printed bar code itself. This means that regular reader servicing is required to avoid problems caused by dirty or scratched optical surfaces. Although bar codes are seldom used alone in EAC. They are often

laminated onto more secure credentials, such as Wiegand, magnetic stripe, and proximity cards, to enhance information gathering.

2.1.7.2 BARIUM FERRITE (BAFE) CARDS

Magnetically encoded barium ferrite cards, which were in the forefront of FAC technology during the 1970s, have declined in popularity, although they are still being used. The first barium ferrite card readers were magnetic and mechanical, with many easy-to-damage parts. They worked as follows:

> At setup, a program cartridge, containing a pre-coded array of magnetized spots, was installed in a reader. Between the program cartridge and the access card insertion area were individual magnets, a movable slider and a metal plate. The slider contained holes through which magnets could fall. The metal plate below the slider stopped the fall of those magnets. The program cartridge attracted a predetermined array of reader magnets upward and out of the slider holes. The remaining non-attracted magnets stayed in the holes (resting on the plate), thereby jamming the slider in place.
>
> The access card contained magnets positioned to match the pattern of those resting on the metal plate. When this card was inserted, the resting magnets were magnetically repotted (pushed upward), releasing the slider, which slid forward, tripped a micro switch, and released the latch.

At one time, the same code array was used by all the access cards issued in a system, if a card was lost, the program cartridge and the remaining cards had to be reissued. As time went on, additional magnetic spots were added to the main array, forming unique ID numbers that could be interpreted by microprocessors.

The original readers required a great deal of maintenance. As they wore out, many were replaced with competing technologies. Still, as of 1980, there were many barium ferrite cards in circulation, providing the market for a few manufacturers to develop 100% microprocessor-based readers that could interpret other manufacturers' cards as well as produce low-cost proximity-like systems.

Magnetic barium ferrite codes are difficult to duplicate because they are factory-embedded, making them highly secure. They hold up especially well to problems caused by harsh weather and hostile environments, and can be used in mixed technology applications. Like all magnetically encoded cards, however, they can be erased or distorted by strong magnetic fields and tend to wear out over time.

2.1.7.3 BIOMETRICS

While the security level of credentials is determined by whether or not they can be easily duplicated, unauthorized use can occur when credentials are shared, stolen and/or PINs are exposed. Biometric credentials were developed to defeat this problem by verifying that the unique personal features of the credential user, such as their palm print or eye, match a copy of those features, called a "*template*," stored in a computer. Biometrics, which began as an offshoot of the study of genetics and disease, are used when the need for a highly secure identification system offsets the cost of that system.

Various biometric systems have been available for decades, including an attempt by IBM in the 1970s to promote a signature recognition system. Many of these systems,

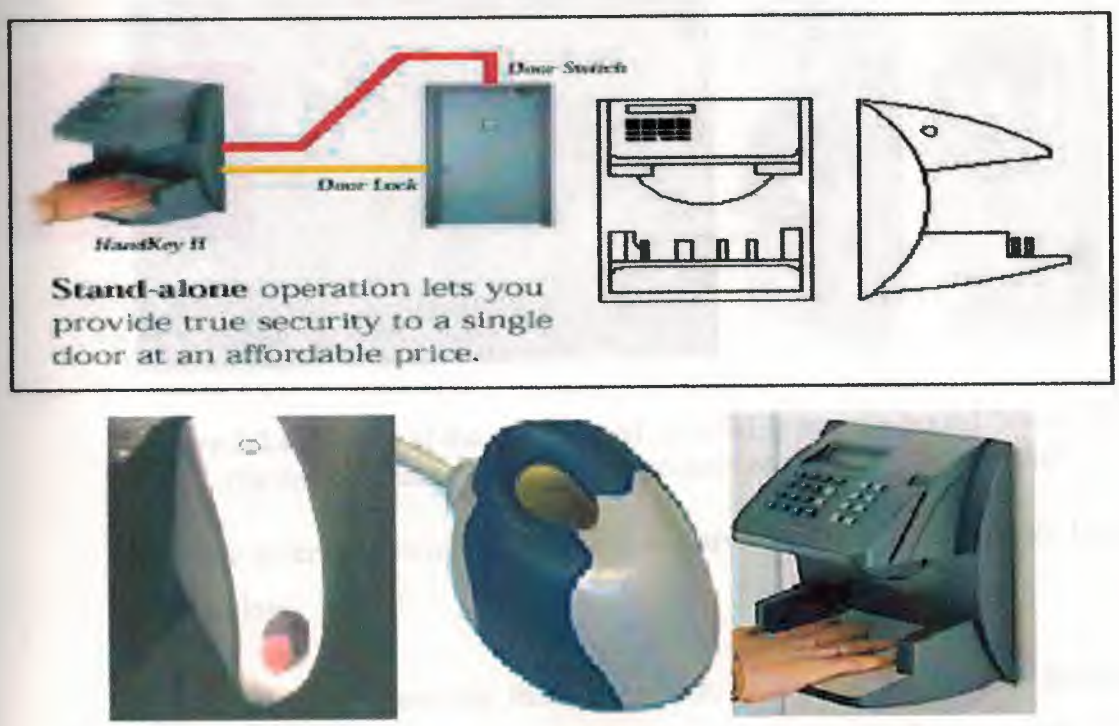


Figure 2.1.6 Reading palm prints checks the length, width and thickness of the hand and almost use for high security and time and attendance points of unique information can be encoded in this way. Also we can see below it fingerprint.

However, were no popular because of high costs, the high rate of verification errors, and verification slowness.

2.1.7.3.1 Body odor:

Senses odors by using chemical processes that are similar to the processes that take place in the nose and brain.

In early 1995, researchers at Leeds University in England announced that they developed a process that can differentiate between people by their smell. Perfumes do not mask this process because perfumes scenes are very different in chemical composition than body odor. Smart card manufacturers hope to eventually embed this technology in their chips in order to compete with finger printing systems.

Before they do that, of course, body odor technology must improve its current identification accuracy of 90%.

2.1.7.3.2 Eye identification:

Figure 2.2.6 Potions of the eye are read by looking into the hound "view" area. The device illustrated is a retinal scanner combined with a keypad

There are several ways of using the eye to provide unique identification, two of which follow:

Iris identification measures the iris, which, according to product literature distributed by Iris can, can identify 4,000 points in less than three seconds. They

claim that iris patterns are fixed at birth and there are no two alike, including those of identical twins.

Retinal scans read the surface behind the eyeball through a tow-intensity infrared fight that tracks 320 points in the retina and records associated blood-vessel patterns.

2.1.7.3.3 Facial recognition:

Verifies facial features by comparing a living face scanned by a camera to older images in a database. Because it is easy to change appearance, there are several systems under development that seek to reduce validation time and increase accuracy. This type of technology is far more sophisticated than having a guard check an image database and then determining the similarity between the picture and the living subject.

2.1.7.3.4 Multiple biometric patterns:

Assures that a severed body part, such as a finger, cannot be used for falsifying identification by requiring that two different biometric readings be taken at the same time. A blood-oxygen saturation reading taken with a fingerprint scan is an example.

2.1.7.3.5 Random voice interrogation:

Assures that a tape recorder cannot be used to bypass a voiceprint system, which compares speech patterns, it does this by recording several spoken phrase templates for each person. When identification is requested, the person is asked to recite only one of the prerecorded phrases. Once the phrase is recited, the voice is compared to the appropriate template.

2.1.7.3.6 Signature identification:

Measures time and pressure used to create a signature as well as the signature pattern itself.

2.1.7.3.7 Voice identification:

Identifies the unique voice characteristics of a freshly spoken phrase to one stored in a template. These comparisons include air pressure and vibrations over the larynx.

2.1.7.3.8 Weight measurement:

Although weight is not a biometric measure because it cannot pinpoint specific traits, weight is often used to determine the presence of an individual or thing and consequently, can be used in the authentication processes.

Weight checkpoints are often found in enclosed rooms called "mantraps" as well as around "invisibly" protected objects, such as might be seen in a museum.

2.1.7.3.9 Hand and fingerprint identification:

Uses various techniques, among which is a three-dimensional digital image that is captured and measured to create a template Between 10,000 to 250,000 points of unique information can be encoded in this way.

While biometrics generally provides a highly accurate verification system, especially when combined with a PIN, users are sometimes concerned about the possibility of physical invasion, harm or discrimination during the credential-reading process. The following considerations describe a few of their concerns:

- A biometric x-ray system, for example, would not be viewed as accept able because x-rays harm the body with regular use.
- People with certain types of physical disabilities, such as those who have artificial hands or who are blind, might not be able to use the system.
- Blood tests are generally considered too intrusive to do on a regular basis. In addition, there are many regulations governing their use.

2.1.7.4 HOLLERITH CARDS

Hollerith cards are modeled after cardboard computer cards that were first used in 1890 by the U. S. Census Bureau to automate the national census. These cards featured a uniform pattern of small rectangles arranged in 80 columns, 12 rows high, and held up to 80 alphanumeric characters of information per card.

To encode these original computer cards, keypunch operators punched out selected rectangles, leaving holes that represented values. These cards were then placed in electronic readers, which passed current through the holes. The resulting pattern of "on's" and "off's" were electronically translated by a computer into data for number crunching. Copying the above principle on a simple scale, Hollerith cards also have holes punched in them, but not as many. These thin plastic cards, which can be manufactured in a variety of rectangular sixes, are read optically by passing a light through the holes, or electronically, by allowing metallic brushes to touch contacts exposed through the holes. Unfortunately, Hollerith cards can be easily duplicated and are only used in low-security applications- Hotels and motels, for example, often use Hollerith cards. When a card is lost, the code can be quickly changed and a new card issued with minimal expense

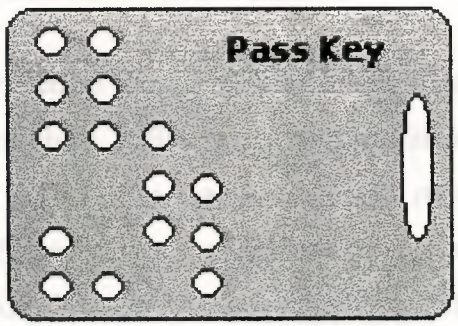


Figure 2.1.7 This Hollerith card is typical of those used in the hotel industry.

2.1.7.5 INFRARED CARDS

Light sensitive infrared card technology, also referred to as "Transmissive infrared" and "differential optics." appeared in the 1970s and uses bar code principles to encode information.

Embedded in the card is a bar code that is coated in a way that allows predetermined amounts of infrared light to pass through. Electronic infrared sensors detect this internal pattern as reduced energy level infrared light. The bar code pattern itself cannot be seen by the human eye. Like bar coded cards, the accurate reading of an infrared card is dependent on the quality and maintenance of its light-sensitive infrared reader. Unlike bar coded cards, these infrared codes cannot be easily duplicated because they are made in a factory and are, therefore, very secure. In addition, they are not subject to erasure by stray magnetic fields as are magnetic stripe, Wiegand, and barium ferrite cards.

2.1.7.6 KEYPADS

Keypad devices provide the means to link a PIN with a credential use a PIN by itself and/or program various devices connected to the system. In all, they are extremely versatile. Some keypads are part of the locking mechanism. This type of keypad might be programmed to respond to a single PIN that's assigned to everyone, or else, it can be linked to a sophisticated control panel, which provides the means to track many codes and time zones. In most mediums to large EAC systems, keypads are linked to powerful control panels and verity cards through use of a PIN. Some keypads even have secret containers in their mountings. These provide a secure storage area in which to place standard keys (for locked cabinets) or other valuables.

Generally, keypads are limited to four-or ten-digit codes, regardless of how many keys appear on the devices themselves. Software, memory and internal circuitry impose these limits; consequently, it is important to examine your PIN requirements before selecting a keypad system. In addition, keypads might not comply with the Americans With Disabilities Act, as their location and PIN usage might be difficult for physically and/or mentally challenged people.

Still, keypads are highly durable and are fairly inexpensive to replace. Systems based exclusively on keypads are easy to maintain because they do not require any card or token inventory or related encoding hardware such as is required for magnetic stripe cards. Unfortunately, keypad systems are not highly secure. For one thing, some keypads contain all the wiring necessary to open a door, which means that unauthorized removal can make the lock useless. Another problem is that PINs can be stolen through

spying or even casual observation. The spying issue has been addressed by the Scramble Pad, patented by Hirsch Electronics. This keypad reduces the chance of spying success by randomly changing its key top labels.

On a Scramble Pad, the keys labeled 123 might become 976 or 485. Consequently, the finger pattern used to punch in the code 6735 is different with every event. Even if a spy sees the motion, he or she would not know what it stands for. This keypad further reduces spying by shielding its key top tables and preview window with view-restricting material. In summary, keypads in combination with card and token, systems, play a very important role in EAC and are in common use.

Figure 2.1.8 **a.** Intelligent locksets like, which seen above can function independently, or be linked to a sophisticated EAC system.
b. This is a typical card reader combination.

2.1.7.7 MAGNETIC STRIPE CARDS

Most people have seen and used a magnetic stripe card of some type. These cards are the most widely used cards in the world and proliferate as bank credit and, of course. EAC cards. They are inexpensive, can carry alphanumeric information, are quickly produced and can be encoded at the user's site.

Each card contains a Mack plastic stripe of magnetically sensitive oxide, which is the same material used to make audio/video tapes. Unlike tapes, however, magnetic stripe cards are subjected to frequent rubbing and bending. Despite their lack of protective housing, their ability to retain magnetically encoded information is quite good. The risk

of magnetic erasure, however, is always a problem. Their resistance to erasure is known as their coercive force rating.

Coercive force ratings indicate the strength of a magnetic force required to erase magnetic material. A card with a low coercively rating, therefore, is fairly easy to erase, and a high coercively rating means that the card is more protected from stray magnetic fields. Needless to say, disposable cardboard cards are more likely to have a lower coercively rating than more permanent plastic varieties. According to the American National Standards Institute, Inc., magnetic stripes must contain four tracks available for encoding, however, specific encoding standards have only been defined for tracks one and two:

Track one: Stores up to 79 alphanumeric characters (210 bits per inch). This information might include the user's name and maybe a title.

Track two: Stores up to 75 bits per inch, with 40 numeric characters. This is the track most commonly used for access control codes.

Track three: This track can contain a facility code (also known as a *water mark*), which is described later in this section. Access to track three requires a special dual-head reader.

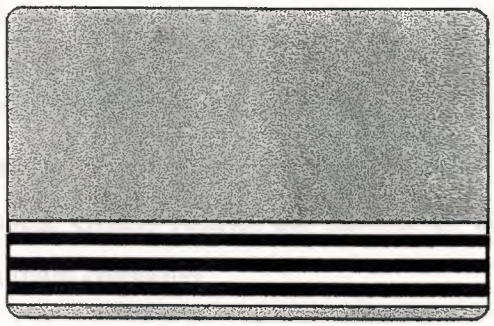


Figure 2.1.9 Magnetic Strip Card

Magnetic stripe cards store more characters of information than associated with bar coding or magnetic particle embedding and are far easier to customize. All encoding can be done at the end user's facilities by manual or automatic equipment. Manual encoders, of course, are more cost-effective for organizations that issue only a few cards. Automatic encoders speed up the process for issuing multiple-cards, plus provide

more control features. These include assigning sequential issue numbers and printing images on the Cards, in addition to the encoding process itself.

Unfortunately, with the right equipment, unauthorized duplication of magnetic stripe information is possible, rendering their security somewhat low. It is common, however, to see magnetic stripes on mixed-technology cards, which increases their security level. One very new development, for example, encodes highly secure, machine-readable, hologram patterns and a magnetic stripe on a single card. The combined use of PINs with magnetic stripe cards, of course, is well known. Magnetic stripe information is read by means of a swipe (moving the magnetic stripe along a track that passes a reader head) or insertion. Swipe readers, with their exposed reader heads, should only be used in environmentally clean areas. Insertion readers are less affected by environmental dust and are suitable for outside installations.

Motorized insertion readers regulate the speed at which the card passes the reader head and may increase reading accuracy. Like tape recorders and VCR's, however, the quality of the information transfer under any circumstance is largely dependent on the strength of the magnetic properties in the magnetic stripe and the cleanness and orientation of the card reader head. Magnetic stripe cards can be individualized by photos and/or bar codes through lamentation, printing, or dye sublimation. Care must be taken to make sure that bulky lamination does not jam up card travel in the reader.

Facility Codes and Water Marks: For a variety of reasons, some systems restrict the number of characters that can be used in a card code, thereby limiting the total number of codes that can be issued. Others restrict the number of codes a control panel can interpret before polling a main computer.

To increase the number of card codes available, a special code, called *facility coded* or *watermark* is permanently fixed in Track Three by the card manufacturer. This is done through a proprietary system that positions magnetic oxide particles on Track Three via wet slurry. When the slurry dries, the information is secure.

The result of applying a facility code is that a range of card codes, such as from 0001 to 9,999, can he duplicated. In the following example, a 10.000 card code range is expanded to approximately 30,000 possibilities.

- Facility Code 1002 - range 1-9,999
- Facility Code 1003 - duplicate
- Facility Code 1004 - duplicate

In addition to increasing the number of available codes, facility codes can be used to detect tampering and unauthorized card duplication.

2.1.7.8 MIXED-TECHNOLOGY

The ideal credential should be capable of combining a variety of technologies, including proximity, magnetic stripe, microprocessor (smart card), Wiegand, infrared, and keypad. In addition, users should be able to inexpensively apply customized designs, photos, and/or bar codes to cards for further individualization.

One advantage of using mixed-technology is that a single card can be read by different types of readers. This makes retrofitting (updating) existing card systems more cost effective because it doesn't require replacement of hardware or wiring. Another advantage is that it reduces the number of cards a person needs to carry.

Figure 2.1.10 Mixed technology card

Many universities are taking advantage of mixed-technology card systems:

> *Example:* In one college, a student photo ID card uses proximity technology to unlock dorms, bar codes to track library books, and a magnetic stripe with PIN to access the debit system used by the cafeteria and ticket agents. As shown in figure 2.1.10.

The three most common credential technologies are magnetic stripe, Wiegand, and proximity. Wiegand and proximity cards offer an exceptionally high degree of security.

Magnetic stripe cards carry a great deal of information and are easily encoded. Proximity cards, which do not touch their readers, improve traffic flow and reduce reader maintenance costs. Combining the three technologies mentioned above into a single credential requires:

1. A standard card size (CR-80 or CR-60 as mentioned earlier in this chapter).
2. A card thin enough (.03") to fit through a magnetic stripe swipe or insertion reader.
3. Sufficient voltage to drive Wiegand and/or proximity systems.

Other combinations are possible, too. Biometrics, for example, often requires a huge computer file (template) for each authorized person. Verification might take an excessive amount of time if the biometric reader has to check against templates held in a distant computer. Smart cards, however, can easily hold these large files. This allows the use of a biometric system for personal identification without being tied to a distant database, thus avoiding problems associated with slow or poor telecommunication connections.

2.1.7.9 OPTICAL CARDS

Optical cards are very new and are not widely used for EAC. This type of card was first developed by Canon U.S.A., Inc., and can store between 3.42 to 4.20 Mbytes of data on the size of a credit card. The amount of storage space it contains depends on the sensitivity of the card reader itself. The benefit to such a credential is that it can carry an enormous amount of information, thus reducing the telecommunications time a reader might require seeking details from a distant computer. The disadvantage is that this information must be entered on the card at the factory.

Optical cards are created by a solid-state, high intensity, laser beam that bums tiny pits on the card's surface. To read this data, a low intensity laser beam directs light on the pits, the reflection of which varies in accordance with the data that was initially etched. The Cannon system writes information on 2,500 tracts, some with multiple sectors, using the same write-once-read-many-times (WORM) techniques as for creating CD disks.

2.1.7.10 PROXIMITY CARDS AND TOKENS

Popular proximity cards or tokens do not need to touch a reader in order to validate a transaction. Their radio-wave transmission technology is highly secure and their readers can be hidden behind walls, in clean, maintenance-free, vandal-proof locations- Best, because proximity readers don't require contact, they speed the flow of human and vehicular traffic through check points.

These cards and tokens can remain in pockets, purses, or even on the front seats of vehicles and still be read by the system.

Figure 2.1.11 These proximity tokens contain a magnetic coil. Memory chip and a battery. Slim cards contain everything but the battery. The bracelet token is commonly used in hospitals and key chain tokens for garage applications. The flat panel token can be kept in a car or else attached to a cup for wearing.

Electrical power is always a big EAC concern and. prior to 1993; a typical proximity reader drew a great deal of current (400 mA at 12 volts). Today, readers can operate, with current as law as 40 mA at 5 volts, which is the same range, used for Wiegand and magnetic stripe readers. Each proximity card contains a coil of wire that acts as both the receiving and transmitting antenna and a small, integrated circuit that is programmed with a unique ID code.

The cards are powered by the voltage generated from a reader's magnetic field in relation card's antenna coil. Once energized by a reader, the card transmits its ID information Transmission is so fast that access verification takes place in less than a quarter second.

There are two types of proximity cards or tokens:

Active:

Has a range measured between touch to 100 feet. Its transmission is powered by a small, lithium battery. Due to battery thickness, active proximity carriers are manufactured as tokens or thick plastic containers that look somewhat like cards. The battery loses power over time and requires systematic replacement, although its average life is from five to seven years.

Passive:

Has a range measured between touch to 30 inches. Its transmission is powered by magnetic properties embedded in a very thin, maintenance-free card. The technological trend is to extend its transmission distance through the use of space technology that was originally developed to receive faint signals from distant stars.

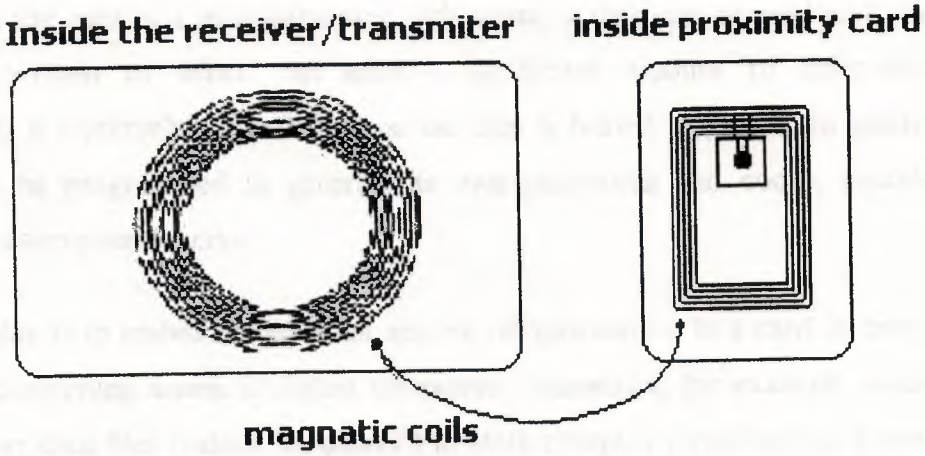


Figure 2.1.12 Both proximity card and reader.

Proximity technology is secure, reasonably priced and becoming increasingly used in mixed-technology cards. Readers have been miniaturized to fit into spaces less than 1.75" square and are getting smaller every day. Being convenient, they comply very well with regulations defined by the Americans With Disabilities Act.

HOW PROXIMITY WORKS

1. A receiver/transmitter (R/T) is either buried in a wall or contained in a slim cabinet hung on a wall.

2. The magnetic coil in the R/T excites the magnetic coil in a card when that card is in range. This range is extended when the card or token contains a battery.
3. Once it is excited, the magnetic coil in the card generates a crisp, magnetic pattern that represents a code contained in its memory chip.
4. The R/T receives the magnetic pattern and responds by amplifying and transmitting it to the processor — a control panel or other unit.

2.1.7.11 SMART CARDS

Although smart cards are currently uncommon in America, that may soon be changing. European companies (telephone systems and banking) have been using smart cards extensively since the early 1990s. A smart card is essentially a credit-card sized computer that was invented over 20 years ago.

Embedded in the card is a microprocessor with memory that can be read and. more importantly, written to which can store a significant amount of information. Counterfeiting is extremely difficult because the chip is buried in plastic. In addition, the chip can be programmed to generate its own passwords and codes, including sophisticated encryption functions.

The trend today is to embed a significant amount of information in a card in order to reduce time-consuming access to distant computers. Biometrics, for example, requires large computer data files (called "*templates*") to store complex physiological patterns. By keeping that information on a smart card, identification time is greatly reduced and worldwide check-in sites (such as used in the military) are not subject to long-distance communication problems. There are three types of smart cards:

- **Memory only:** Has less than 400 bits of memory and are often used for disposable "prepaid card systems."
- **Memory circuits with some hard-wired security logic:** Contains between 1K to 4K of memory and can be erased and rewritten. These are designed to allow encryption and PIN comparisons.
- **Full-Hedged microcomputers:** Contains a complete computer system with an operating system and the ability to be programmed to meet a

wide range of applications. The computer system includes a processor, nonvolatile read/write memory of 1 K to 8K, a small amount of random access memory, and read-only memory, which contains the operating system and the place where security functions are hidden.

Although a smart card looks similar to a standard credit card, it differs by having five to eight metallic contacts displayed on its surface. These contacts connect directly to a computer terminal when the card is inserted. To make sure that contacts is good, smart cards must be stored flat at all times and malignance is needed to make sure that terminal readers are clean.

To increase the potential markets for smart cards, information held in the chip can now be transferred through proximity technology. Although contact less and radio communication methods have not yet been standardized, systems are available.

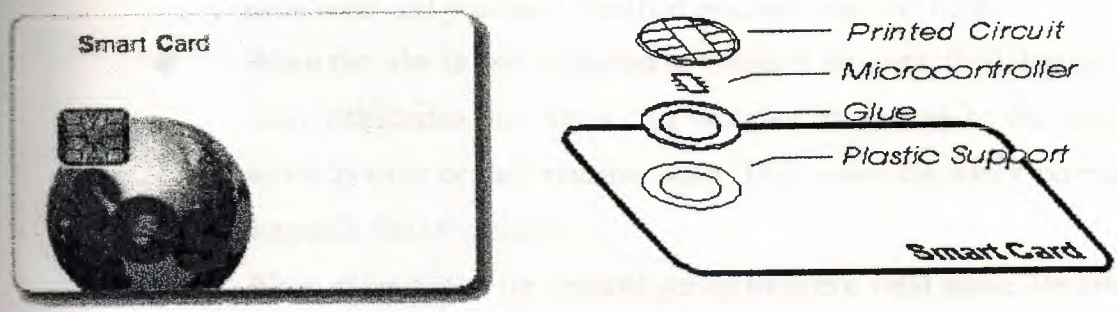


Figure 2.1.13 Smart cards look like common charge cards and can even have a magnetic stripe, bar code and/or id photo present. You can identify a smart card by a metallic design similar to the white one seen on the card above.

New uses for smart cards are being invented every day. Several states, for example, are replacing food stamps and other voucher systems with smart cards. These cards reduce paperwork and theft; white increasing reliability and ease of benefit transfer.

Hospitals are also using smart cards for EAC as well as for sharing patient records. Updating a smart card from a single computer source, as opposed to transferring information from numerous charts and records, improves communications, increases accuracy, and decreases costs associated with paperwork.

2.1.7.12 *WIEGAND CARDS*

Wiegand cards are based on patented technology held by the Sensor Engineering Corporation that embeds an array of magnetic wires in a card that is very difficult to duplicate. Wiegand technology combines several patented processes and a special metal alloy to create unique magnetic properties not found in common ferromagnetic (iron) wires.

Through manipulation and heat-treatment, the core of a Wiegand wire acquires a different magnetic property than its shell. This result in a condition called *magnetic action.*

Bistable magnetic action creates an electrical pulse:

- When first subjected to a strong magnetic field, the wire has a magnetic north and possesses a unified external magnetic field.
- When the wire is then subjected to a weaker magnetic field that has a south orientation, the wire's core switches its polarity to the south, while its exterior shell remains north. This causes the wire's external magnetic field to collapse.
- When subjected to the original strong magnetic field again, the core reverses its polarity to match that of its exterior shell. This change in polarity creates a crisp, discrete electrical pulse.

The only energy input required to create the electrical pulse is the bistable action of the wire in relationship to variations in magnetic fields produced by the reader. Although the pulse it regarded as analog, it is so crisp that it can be read as a digital output. Every Wiegand wire segment embedded in a card represents a magnetized pulse generating "bit." Up to 56 bits are allowed per card, although in reality, not alt the bits are required.

These bits are arranged in two parallel rows. Bits in the top row are referred to as *zero bits*, and in the bottom, *one bits*. The placement of these bits in relation to one another generates a binary pattern that represents a unique code. Wiegand readers have two reading heads, one for each row that read the electrical pulses generated by the bistable magnetic wires.

Manufacturing presses: All Wiegand wire is tested three times before it is cut into .33" strips and placed on vinyl adhesive tape in a pattern determined by computer-controlled machinery. For each order, the wire-encoded tape is spooled onto a tape feeder, and then fed to a tape-cutting-and-placing machine. This machine automatically cuts and places 12 strips of tape in appropriate locations on vinyl sheets (which are eventually cut into 12 cards), continuing with new sheets until the order is complete.

Once a vinyl sheet is prepared by the encoded tape and topped with artwork and lamination, it is pressure-temperature seated, die cut, and inspected- Depending on the order, and some cards also receive a special hot stamped card number. Before being shipped to the customer, the cards are inspected. Cards not meeting the inspection criteria are discarded and remanufactured.

Change in technology: The original Wiegand cards were somewhat thick. New credit-card thin sizes now allow Wiegand technology to be combined with other popular technologies, such as magnetic stripes; in addition, other manufacturers are developing proximity readers that can pick up Wiegand's low voltage power output (5 volt, 25 mA), while Sensor Engineering Corporation itself has also developed proximity technology.

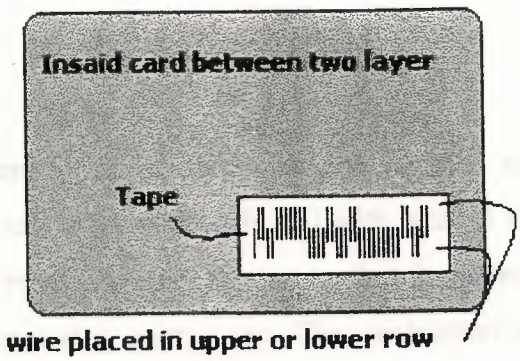


Figure 2.1.14 Wiegand Cards

Wiegand cards are regarded as very durable, secure, and reasonably priced. Unfortunately, because Wiegand cards are grafted at the factory, they take longer to manufacturer than other cards, forcing some EAC system managers to use other technologies because of lead-time considerations.

2.2 Barriers

2.2.1 DOORS

Function, governmental regulations, appearance needs, and cost alt determine a door's style and materials. Beyond these factors, doors controlled by EAC have the following in common:

- A door closing mechanism
- An electronically or magnetically activated lock
- Sensors (switches) that determine whether or not the door is properly closed
- Computerized control either in the locking device itself, or in a nearby, hidden control panel.

EAC requires that doorways, waits, and ceilings have a power source nearby and. in most cases, have adequate conduit and ducts in the walls or ceilings to hold electrical wiring. In areas where placing wire is difficult or prohibitively expensive, such as in an old elevator shaft, wireless EAC is substituted. EAC systems at so require wait or ceiling cavities large enough to contain control panels or wiring closets.

2.2.2 DOOR CLOSERS

Mechanical door closers are as important to an EAC system as the electronics that power the tocks. Door closers are spring-activated with tension strong enough to pull, doors completely shut after use, yet not so strong that it makes opening the door a struggle, or warps the door during normal use. The mechanism attached to the spring that guides the door shut is called the *arm.* Door closers fall into two main categories: concealed and surface mounted, a sample of which is seen on the next pages.

Concealed closer are usually used on doors designed for a clean, "no-hardware" look because the arm is hidden from view.

They can be difficult to adjust and service, however, because they are embedded into the top or bottom of the frame and door itself, requiring the door and frame to be

perfectly balanced. Hardware replacement is usually manufacturer-specific and requires exacting specifications.

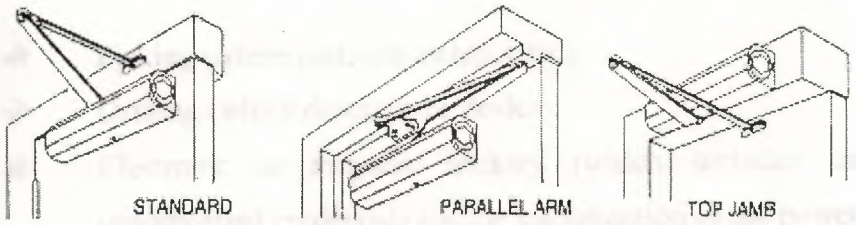


Figure 2.2.1 Door Closer

Surface mounted door closers are the most popular and fall into three main categories:

1. Regular-arm mounted
2. Top-jamb mounted
3. Parallel mounted

The most popular are the regular-arm and top-jamb styles, the latter of which is simply the regular-arm style installed upside down. The regular-arm and top-jamb door closers can stand the greatest deviation in door play. They are usually installed on the interior-side to reduce tampering, reduce weather damage such as rusting, and enhance the exterior appearance of the door. These types are shown in figure 2.2.1 above.

The *parallel style* is less popular. The arm on this closer slides parallel to the door, rattier than perpendicular to it. Unfortunately, it is difficult to service because it requires a very well balanced door. This type of closer is usually used when a jamb mounted closer must be installed on the weather-side of a door. It is thought to be more weather-resistant because its arm does not stick out and it can be shielded by a roof of some sort.

The series of illustrations on the next page show where door closers are commonly positioned on doors. Your understanding of these mechanisms can be greatly enhanced by observing the doors in public and private buildings.

2.2.3 ELECTRONIC AND ELECTROMAGNETIC LOCKS

The four most common types of locks used in EAC systems are the magnetic lock, the eclectic strike lock, the electric lockset, and the electric dead bolt. The strength of any

tock is determined by the way in which it can stop unauthorized entry that uses cleverness or force. Electronic or electromagnetic locks, therefore, must be strong enough to guard against:

- Picking (where parts are manipulated)
- Drifting (which destroys the device)
- Electronic or magnetic trickery (which includes the use of unauthorized credentials and the manipulation of the power supply).

EAC electronic and electromagnetic tocks are regarded as being either fail-safe or fail-secure and both have an important role in overall security:

Fail-safe:

The lock is **unlocked** when the power is off. This type of lock is usually used on a fire door. In the event of a fire, the locks can be released through the fire system or, if the power system fails, they unlock automatically.

Fail-secure:

The lock **remains locked** when the power is off. Power is required to unlock this type of lock and is usually used for normal locking situations.

2.2.3.1 MAGNETIC LOCKS

Magnetic locks secure doors through magnetic force and are always, fail-safe devices. They are ideal for high-frequency access control usage because they are totally free of moving parts, which reduces wear and tear.

Every magnetic lock consists of two components:

- Electromagnet
- Strike plate

The electromagnet is installed on the doorframe and the strike plate on the door itself. When energized, the electromagnet attracts the strike plate with a holding force ranging between 500 lbs. to 3,000 lbs.

All EAC systems require that some form of sensor reports whether a door is open or closed. Conveniently, many magnetic locks have that sensor built in, eliminating the necessity for a secondary sensor or switch.

The two basic magnetic lock styles are called:

- Direct hold, which is surface mounted on the secure-side of the doorframe and door.
- Shear (also called *concealed*), which is completely embedded within the doorframe and the door itself.

The large, *direct hold,* magnetic lock is ideal for use on poorly fitted doors and unframed glass doors because the two lock parts can be installed in rough proximity to each other. When energized, the electromagnet positioned on the frame attracts the strike plate on the door flush to its surface. This strong attraction doesn't require perfect horizontal or vertical alignment between the parts.

Smaller share magnetic locks, which are less than door thickness wide, are totally invisible to the eye when the door is closed. They are used when design and aesthetic considerations dictate that the lock be completely hidden. Concealing reduces the potential for tampering because the electrical wiring is completely enclosed within the doorframe. The narrow surfaces on the shear electromagnet and the strike plate require precise alignment. A small bracket is often used on the frame to stop door travel so that these surfaces line up.

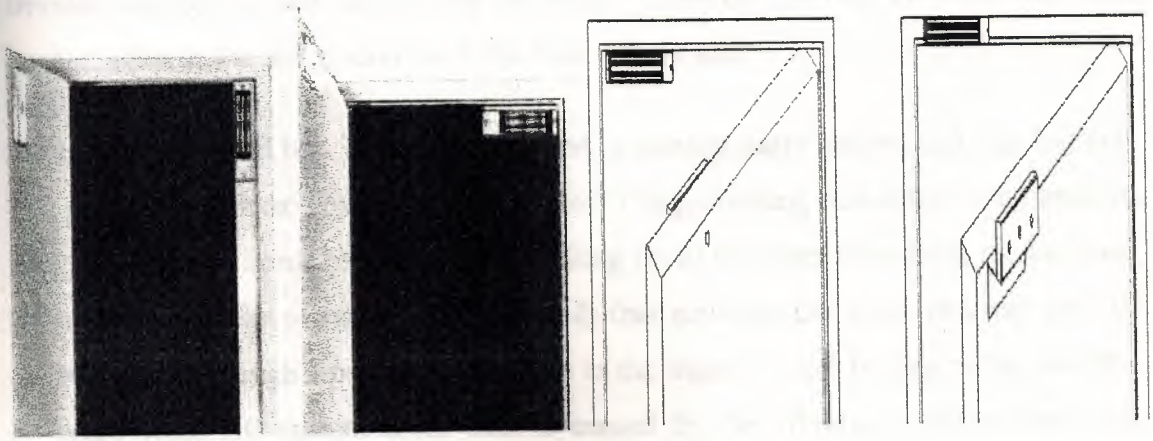


Figure 2.2.3 Magnetic lock

ANSI standards have defined three grades of magnetic locks. Grade one, which holds 1,500 pounds, is designed for medium security. Grade two, at 1,000 pounds, is for light security, and grades three. 500 pounds, simply holds a door shut. Most 180-pound men can force open a door equipped with an 850-pound magnetic lock.

As the holding attraction increases to 2,000 or more pounds, a magnetic lock will stay joined even when the force of a blow is strong enough to shatter the door it secures. Consequently, in addition to the strength of the lock itself, the material strength of the door, frame, and wall must also be considered when planning a high security door.

2.2.3.2 ELECTRIC STRIKE LOCK

The electric strike lock is the most popular EAC locking device on the market and can be set up as either fail-safe or fail-secure. Its popularity stems from the fact that it comes in a wide variety of sizes and can replace existing mechanical locks without a great deal of difficulty. The strike, which is the eclectically controlled portion of the lock mechanism, is mounted in a doorframe (jamb) and does not require wiring through the door itself.

The electronic strike contains a bolt pocket, which is the indent that holds the protruding latch bolt or dead bolt secure in the frame. To open, the strike rotates away from the pocket, providing a path for the bolt to escape. This rotating side is called a *pivoting lip or keeper.* The latch bolt or dead bolt housing itself is mortised (embedded) in the door.

Latch Bolt: The latch is a spring-loaded, beveled bolt. When the door closes, the beveled-side of the bolt slides over the strike, allowing the bolt to retract and then expand again in the bolt pocket once the door is fully shut.

Dead bolt: The dead bolt is a solid metal rod or rectangularly shaped bolt that has only two possible positions: protruding or retracted. The protruding bolt enters or escapes the bolt pocket in the frame only when the pivoting lip of the electric strike is rotated away from the frame. The solenoid (magnetic coil) that activates the strike receives low AC or DC current through a power cord hidden in the frame. A soft buying noise can often be heard when AC current used. This is caused by the vibrations of the alternating current pushing and pulling the solenoid 60 times per second.

Figure 2.2.4 Door Locks

Electric strikes and their rotated latch boils come in a variety of styles suitable for installation on wood and metal frames. Each frame type, however, poses its own demands. A few of the many things to consider include:

Wood frames can be weakened from the hollowing out required for installation of the electric strike and need additional anchors or brackets to protect the took itself against forced-entry attempts.

Tubular aluminum frames might be too shallow to accept an electric strike assembly. Hollow metal frames might be too weak to resist a forced entry, or else were filled with cement or plaster when installed, prohibiting the installation of the electric strike at a later date.

2.2.3.3 ELECTRIC LOCKSET

The electric lockset is very similar to a mechanical lockset and is available in cylindrical and mortise styles. The difference is that an electric solenoid (magnetic coil) replaces the mechanical action provided by a standard key. In addition, only the electric lock has fail-safe or fail-secure operational modes.

- *Cylindrical Lockset:* These are characterized by a doorknob or handle on each side of the door, which are joined by a cylinder that controls the locking mechanism.

- *Mortise-style Lockset*: These are characterized by a lock, which is housed in a rectangular metal container that is embedded at the edge of the door and is often enclosed within the door's thickness.

Electric power is brought to the lock by threading wire from the frame through the door. Electric hinges (or pivots) completely conceal the wiring path when aesthetics are a consideration. Flexible cable loops are used when a seamless appearance isn't necessary and must only be exposed on the secure side of the door.

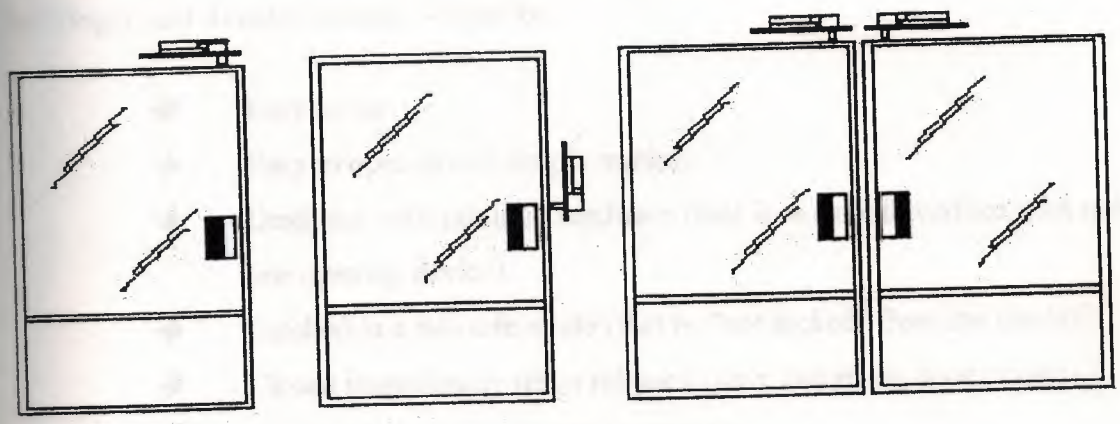


Figure 2.2.5 Electrical Lock locations

2.2.3.4 ELECTRIC DEAD BOLT LOCK

The electric dead bolt refers to the blot design and is used as an alternative to a magnetic shear lock for doors that swing in two directions and double-doors. The electrically powered dead bolt is fitted into either the jamb or the door itself and when activated, it protrudes (shown on previous page) or swings (below) into a mortised strike plate on the adjoining surface.

To increase holding strength, more than one set of electric dead bolts can be installed per door. Dual sets are common on large doors, as well as on both double-hung doors that swing away from each other from a center point. By installing electric dead bolts in the door header (top) and at the base, each door is secured and resistant to force.

The dead bolt does not give way with a spring action. Once it is clicked in place, it stays in place until unlocked. Although electric dead bolts can be set in fail-safe or fail-secure modes, the majority of building and safety codes prohibit them for egress path use in high-rise buildings. Manufacturers have developed standard-compliant locks, but they are not in common use for these applications.

2.2.4 FIRE EXITS AND ADA RULES

The rules surrounding fife exits sometimes conflict with the purpose of EAC. No one wants to be trapped inside of a building during an emergency. This means that specific exits—doors leading to and from stairwells, between firewalls (and adjoining buildings), and directly outside — must be:

- Easy to see
- Easy to open in one simple motion
- Designed with minimal hardware (that is, a smooth surface with only one opening device)
- Latched in a fail-safe mode (that is, "not locked" from the inside)
- Closed immediately when released (have automatic door closers)
- Constructed out of fire-rated materials

Here is how fire codes effect EAC: In this simple example, the door is secured by a magnetic lock that can sense when the door is closed. To enter, a card is swiped through a card reader, which sends the information found on the card to a control panel. If the card is valid, the control panel sends the instructions to unlatch the lock.

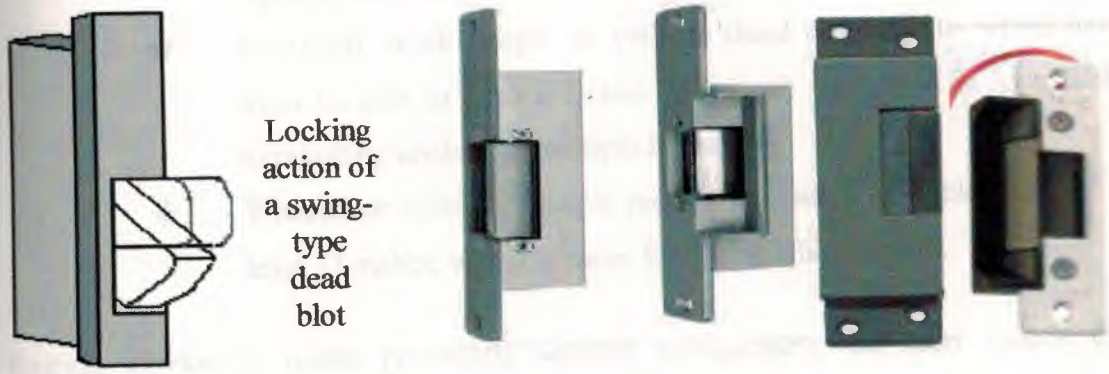


Figure 2.2.6 Door Strikes

After the door is opened, the "door closed" sensor tells the control panel whether or not the door returned to the closed position. If the door does not close within a predetermined amount of time, the control panel triggers an alarm. Whether or not the door closes as scheduled, the EAC database saves the pass code user's name as well as date and time of his or her access. This creates an important trail of information! Exiting, however, creates a different set of circumstances.

The Exit Bar in this example sends a signal to the control panel. The control panel then releases the magnetic lock. Unfortunately, this action leaves no record of the person who pushed the door open, because exiting bypasses the EAC recording system.

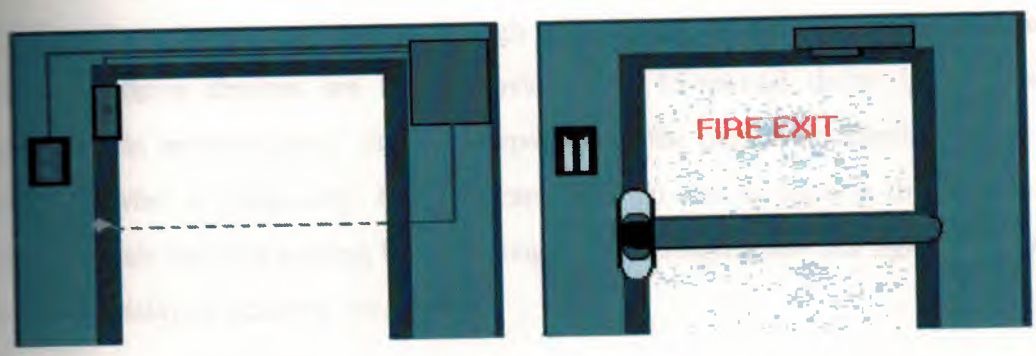


Figure 2.2.7 Door interior and Exterior View

The Americans with Disability Act (ADA) imposes additional restrictions on door design, lighting, and usage. ADA requires that:

- Blind and sight-impaired people must be able to touch specific types of door hardware and understand what to do next.
- Hearing and sight impaired people must be able to easily see exits. Consequently, there are rules regarding the size and color of exit signage, including the use of strobe lights.
- Physically weak people as well as those confined to wheelchairs must be able to push a locked door open with little or no trouble, eliminating knobs and multiple latches.
- Wheelchair confined people require doorways with clearings of at least 32 inches, which is room for a wheelchair to pass.

Exiting, obviously, opens previously secured passageways. To alert guards that someone is leaving, an egress button is sometimes found on the opposite side of a door protected by EAC.

When pushed, this button disarms an alarm and tell the control panel that door usage is in compliance with the system. Egress buttons, unlike card readers, are subject to fire code regulations that forbid them to control locks. Egress buttons, therefore, can be bypassed without hampering travel, although doing so will trigger an alarm.

A "delayed egress" device on a fire exit door, however, postpones unlocking for up to 15 seconds. Pressing this device sends an alarm to a guard station and informs the guard that an exit attempt is being made. At this point, the guard can see the exit event on CCTV, talk to the person leaving through an intercom, or simply run to the scene if neither of those devices are there. Obviously, a 15-second delay in exit can be frightening in an emergency situation, especially if the person attempting egress does not know what is happening. Extreme care must go into designing this type of exit system, which includes posting bold warning signs. *A single-push bar egress is required even when delayed action is used.*

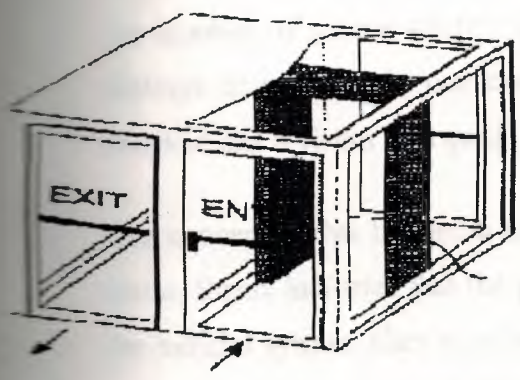
It is very common to see fire code violations and when you do, it if our strong recommendation that you immediately report them to the fire department. The National Fire Protection Association (NFPA) code clearly states that only one action can be used to unlock a door with exit or fire exit hardware. Many companies, unfortunately, install additional locks, if the fights fail during an emergency, the extra burden of finding those locks could cause confusion, panic, and death. Double-exit doors, where one door must be opened before the other is released, are forbidden, in the case where the doors have an overlapping astragal (center strip), which normally requires one door to open, before the other, hardware must be installed that allows either door to open quickly.

Locking arrangement on double-exit doors is tricky and mistakes are often made during installation. Always check to see that each door can be opened quickly, regardless of the other's position. If one doesn't open, the setup is in violation of fire code. Heavy double exit doors are commonly seen in shipping and receiving areas. The temptation is to install additional handles to better distribute the weight of the door in order to make opening easier. This solution, however, would be in violation of fire codes, in the event of an emergency; it might not be obvious which handle is associated with the latch, which could, in turn, cause confusion and panic.

Stairwells pose additional security concerns. Fire codes require that people in stairwells be able to exit freely at any floor. Unfortunately, in some high-rise buildings, these exits open into unrelated businesses. The temptation is to bar the exits to stairwell doors so that uninvited guests don't get in, which, of course, is in violation of fire code. As you

see from this brief overview, building codes, fire regulations, and ADA requirements are detailed and complex.

2.2.5 MANTRAPS (SECURE VESTIBULES AND TURNSTILES)



Mantraps-Double Vestibule Style

Many devices may be present including motion and weight sensors as well as CCTV and an enunciation (intercom) system

Figure 2.2.8 Metal Detector

Tight access control is obviously very desirable in high crime areas. Financial institutions, hit hard by increased robberies, are exploring ways to quickly screen visitors. Many European and South American banks, for example, are using glassed-in mantraps, called "double vestibule (hall) portals," as seen in the illustration. These are used to unobtrusively examine visitors prior to admission, keep nonconforming people out, and make sure that two people do not enter at one time (piggybacking) as described in the following procedure:

2.2.4.1.1 Entering a building:

With the exterior (outside) door unlocked and the interior door locked, sensors and a metal detector determine whether one person is present in the "enter hall" and is free of weapons. When access is granted, the exterior door locks and simultaneously, the interior door unlock.

This allows the occupant to enter into the building while at the same time preventing piggybacking. The system resets itself when the interior door is shut, allowing the next person to enter from the outside.

2.2.4.1.2 Leaving a building:

The person exits through the "exit hall." which reverses the door locking and unlocking process as reported above: however, does not include a weapon detection sensor. Strict access control in this housing project has greatly reduced the number of people freely roaming the halls and has increased the tenants' feelings of security. In one case where a rape did occur, EAC records were cheeked and a visitor was quickly identified, found, and hauled off to jail.

One concern is that biometric scanning might interfere with American civil liberties. Smart indicates that the palm prints used by this system are not used in the judicial system. Care must be taken when installing a mantrap, however, to make sure that it meets alt fire and safety regulations and it does not interfere with the public's civil rights.

Revolving Doors: Revolving doors can also be used to reduce piggybacking and pose as mantraps. Used with or without an EAC pass code, one section of the area can be set up to sense for metal detection and other conditions. If all conditions are met, a person can pass through the system. If conditions aren't met, the interior doors remain locked and the person is directed back to the outside. As revolving doors are confining and have been known to cause feelings of panic, extreme care must be taken when using this type of system to meet all fire and ADA regulations.

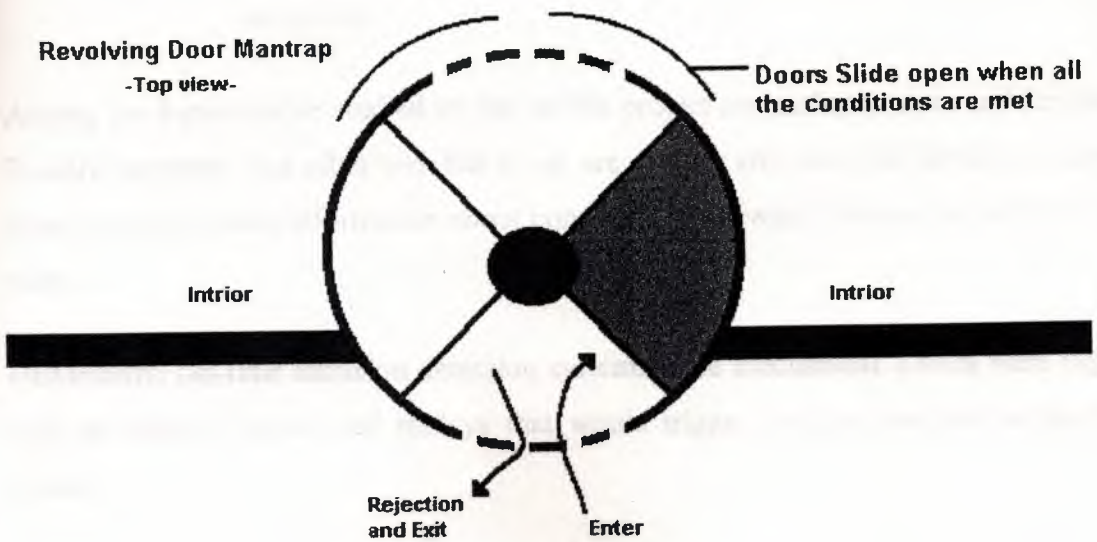


Figure 2.2.9 Revolving Door

2.3 Sensor (Information Reporting Devices)

2.3.1 SENSORS PROVIDE INPUT FOR ELECTRONIC DECISIONS

The "control" in electronic access control (EAC) is accomplished by the relationship between three types of devices, which are:

Detection Devices: These devices detect and report changes in one or more conditions. They are regarded as *inputs* because they report "into" a management device.

A Management Device: This is a specialized computer that receives information from detection devices, compares that information against programmed information, and decides what to do. Then issues instructions to action devices.

Action Devices: These devices carry out the instructions provided by the management device. They are regarded as *outputs* because the management device sends information "out to" them.

In a large EAC system, detection and action are managed electronically through control panels. These panels:

- Accept input from many detection devices.
- Issue instructions to many action devices (outputs).
- Communicate with other control panels and computers throughout the system.

Among the inputs we've studied so far in this project are authenticators and keypads. Equally important, but often invisible to us, are *sensors* and *detection device*. In secret, these devices provide information about conditions upon which electronic decisions are made.

Historically, old-time intrusion detection systems were mechanical. Doors were rigged with all kinds of levers and pulleys that would trigger bells and/or start a chain of events:

Example: To deter intrusion in castles, stones would drop through shoots, spears would fly out of walls and trap doors would open up, tumbling unauthorized people into pits full of snakes (or bodies).

Fortunately, electronically powered intrusion detection systems (also called *burglary detection systems*) alert guards to a wide variety of issues without destroying an unaware visitor. Today. EAC uses the information reported by sensors to make informed decisions.

Example: When an EAC controller receives a signal from a door contact sensor, it knows that a door was opened. If that signal was received after a proper signal from an authenticator, the controller regards the situation as being OK. If the contact sensor does not close within a specified time, the controller signals an alarm, which can include ringing bells, flashing lights and warnings seen on central station monitors.

Here are a few examples of how controllers use sensors to monitor situations:

- Elevator Door: An EAC authenticator determines who can select a given floor. Contact switches determine whether an elevator door is completely opened or closed. While closing, one or more photo electronic sensors determine whether people and/or objects are between the sliding door and the frame. Finally, pressure-sensitive sensors determine whether someone or something is attempting to hold the door open.
- Exterior Door in a Chemical Plant: An EAC authenticator determines who can access this door. One or more contact switches in a doorframe determine whether the door is opened or closed. A contact switch that is part of the latch determines whether the latch is fully extended. Chemical and/or oxygen sensors inside the plant sense whether a chemical spill has taken place. If one has, the door will not unlock, even for an authorized person trying to enter. Photoelectric sensors around the door determine when people or objects are in the area. These sensors start a video recorder and/or turn lights on so the camera and visitor can see well.

The ways sensors are used in a facility depend on overall security requirements and management needs. At minimum, a door controlled by an EAC system requires at least

one door contact sensor (input), an authentication device (input), and an electronically activated lock (output).

2.3.2 SENSOR CATEGORIES

2.3.2.1 SENSORS ARE EITHER ACTIVE OR PASSIVE.

Active sensors introduce energy into an area, which is interpreted by a receiver. When the receiver senses a change in energy, it registers an alarm. Break-beam sensors are a good example of this type. Here, a transmitter focuses light, which is energy, into a receiver. When the receiver notes a change in light, such as when someone passes by and "breaks the beam." it triggers an event.

Passive sensors measure changes in an environment over time. A good example of this type of sensor is a thermostat which, when the temperature drops, triggers a furnace. Likewise, passive sensors can detect noise and vibration levels within an area and indicate when those levels are outside a given range.

Sensing devices commonly used for EAC generally fall into the following categories. (Check the sensor glossary at the end of this chapter for specific types of sensors.):

- *Mechanical sensors* have simple levers or rods that, when pulled or pushed, move a switch that reports an event.
  Example: An *egress* (exit) button used on the secure side of a door controlled by an authenticator is a mechanical switch that, when pushed, creates a electrical circuit that tells a control panel that opening the door is legal. If the door is opened, but the button isn't pushed, other sensors in the system announce an alarm.
- *Electromechanical* sensors depend on a specific flow of current to activate a mechanical device.
- Capacitance sensors generate an evenly charged electrical field between two antennas. When the energy level in that field changes due to an intrusion in the area, an alarm is triggered.
- Vibration sensors measure subtle environmental motion, which, when motion reaches a predefined level, register an alarm.

- *Audio sensors are similar to vibration sensors, except they measure* sound waves (audible, which we can hear and ultrasonic and microwave, which we can't).
- Light sensors measure the degree of light in a given area. Active light sensors are used in break-beam devices wherein the interruption of the light beam between a transmitter and receiver results in an alarm. Passive light sensors measure environmental light.

Additional sensor categories exist for environmental monitoring, such as for fire, flood, humidity, oxygen and chemical detection, to name a few. All these sensors can be tied into a controller of some type (including some EAC controllers) to automate a chain of events. Sensor applications can be quite complex. In fact, many systems maintain redundancies, which means that one variety of sensor checks on another in order to double-check intrusion reports. With that in mind, the brief list that follows shows what types of sensors are commonly used within specific areas.

Yards - External Perimeter: Fence alarms (conductive wire sensors), photoelectric beams and microwaves.

Building Perimeter: Exterior door contacts and overhead door contacts (contact switches) and glass break detectors.

Interior Detection: Passive infrared, microwave, dual motion technology, photoelectric beams, interior door contacts, mantrap components, and glass break sensors.

The section that follows is a Sensor Glossary, which provides an overview of the types of sensors used in EAC and security systems.

2.3.3 SENSOR TECHNOLOGY GLOSSARY

This glossary is meant to provide an overview of sensing technology terminology commonly related to EAC and intrusion detection systems. Within a sensor type, there can be many variations. Check with sensor manufacturers for details. There are many sensor systems not mentioned in this glossary that are commonly used in industry. We recommend that you become aware of them. The more you know, the more resourceful you'll become when designing a system.

2.3.3.1 ACTIVE SYSTEM

(*Example:* Capacitance Detector) The word "active" refers to a sensing system that introduces energy through a transmitter into an area for interpretation by a receiver. The receiver is set up to expect a specific energy level. Any changes to that energy level indicate a change in the environment caused by an invasion of some type. The opposite is a passive system, which simply reads the environment "as is" and makes decisions based on a range of outcomes, such as increased noise or impulse.

2.3.3.1.1 Audio Sensors

These sensors are similar to ultrasonic and microwave sensors, except that the receiver bases its judgment on sounds that can be heard by the human ear, rather than a high frequency pitch. Reception sensitivity can be set to detect explosions, gunshots and even human conversation. (See *Ultrasonic and Microwave sensor).*Audio sensors are usually used in connection with intercom systems and can amplify low noise, such as whispering, for transmission to remote guard stations. Two types of audio sensors exist. The first is sensitive to sound at any frequency within a range. The second is sensitive to sound at a specific frequency. In high background noise applications where vibration sensors are used, *discriminator sensors* are also installed as a redundant backup. These devices sense common noise and cancel the effect of these vibrations, reducing false alarms based on common occurrences. (See *Vibration sensors*. Page 55)

2.3.3.1.2 Capacitance Detectors (Proximity & Capacitance Detectors)

This type of sensor is used to monitor large areas by maintaining a consistent energy level, called an *electrical field*, between two electrically charged antennas. The air in the electrical field becomes a *dielectric space*, meaning that it has a constant, predefined energy level. When the energy level changes due to an intrusion, an alarm is sounded. While capacitance sensors are not affected by noise or vibration, they are very sensitive to atmospheric changes and consequently, are most commonly used indoors. This type of sensor is relatively easy to set up by taping antennas of copper tubing or wiring to windows, walls, doorframes, etc. As long as the energy within the room between these

antennas remains constant, the area is secure. Intruders, however, absorb part of the radiated energy, causing a difference in *capacitance* (electrical charge), which, in turn, triggers an alarm.

2.3.3.1.3 Conductive Wire Sensors and Fiber Optics

Metallic tape, once commonly seen on glass doors and large windows, carries a *current* (indicting conduction) that completes a circuit. If the tape is broken, an alarm results. Unfortunately, although it is easy to apply tape to glass surfaces, it is also very easy to scratch through the tape, causing a complete split that breaks the electronic circuit. This renders the system useless and in need of continual repairs. Another type of conductive wire sensor is a fine, hard-drawn copper wire that is woven into screens, grids and other lacings (such as used in fencing) and mats. Changes in tension on the wire, such as caused by someone pressing on a surface, changes current flow, triggering an alarm. In newer systems, fiber optic filaments are used, with light transmission replacing electrical conduction. The principle, however, is the same as with conductive wire. Fiber optics eliminates corrosion problems common with metallic materials and is especially useful in outside applications.

2.3.3.1.4 Discriminator Sensors

See *Vibration Sensors*. Also see *Audio sensor, page 55 & 49.*

2.3.3.1.5 Dual Motion Detectors

This refers to a redundant system in which one type of motion detection system backs up another. Either system can be used by itself, but when used together, they provide a broader, more complex range of coverage. Generally a dual motion detection system combines passive infrared (PIR) and microwave (MW) motion detectors, or PIR and ultrasonic (US) motion detectors.

2.3.3.1.6 Fiber Optic Sensors

See *Conductive wire sensors and Fiber Optics, page 50.*

2.3.3.1.7 Fire and Environmental Sensors

Environmental sensors can be tied into electronic access control systems; however, local fire, building and police authorities determine usage and insurance companies may insist on additional requirements. Among common sensors used for environmental purposes are smoke detectors. Heat/temperature sensors, chemical spill detectors, water flow monitors and moisture detectors.

2.3.3.1.8 Flexible Cable Sensors

See *Conductive Wire Sensors and Fiber Optics, page50.*

2.3.3.1.9 Foil

See *Conductive Wire Sensors and Fiber Optics, page 50.*

2.3.3.1.10 Glass Break Sensors

The original glass break sensors used conductive foil taped along the side areas of the glass. As this type of sensor was easy to scratch, it caused many false alarms and is now considered obsolete. (See *Conductive Wire Sensors and Fiber Optics, page 50.*) Today, a popular sensor used to detect glass breaking is a small capsule containing liquid Mercury (a conductive metal), which is glued to the glass. Once the glass breaks, vibrations and/or dropping causes the Mercury to flow across the capsule, closing a circuit, which, in turn, sends an alarm. Sensors that fall in the sound and vibration categories are also used for glass. These sensors can be tuned to audible or vibratory frequencies that match the frequencies of glass breaking. (See *Vibration Sensors, page 55.*)

2.3.3.1.11 Infrared

This refers to the part of radiation within the full radiation spectrum that falls below visible light. It can't be seen by the human eye, but it can be felt as heat. Sensors that detect infrared heat detect the presence of warmth, such as that radiated by a human being or animal.

2.3.3.1.12 Infrasonic Sensors

There are sound sensors that detect sound below that detectable by ear. They can, for example, "hear" the sound of air moving into a room when a door is opened. They are not widely used today, however, because of false alarms.

2.3.3.1.13 Intrusion Switches (Balanced Magnetic Switches, Magnetic Switches, and Electrical Intrusion Switches)

This type of sensor can be mechanical (similar in concept to a rocker switch used to turn on lights) or electrical. It has two parts, typically one that moves or changes state and one that interprets the change. *Electrical intrusion switches* are commonly installed on the secure-side of windows, doors and other openings. Under normal conditions, both parts of the sensor touch, creating a circuit through which current flows. When separated, such as happens when a window is illegally opened, the flow of current is broken, signaling an alarm. A variation of this type of switch is the *magnate switch.* This switch, which is an electrified plate, is mounted on a fixed frame, while a non-electrified metal plate is mounted on a moveable object, such as a door or window. When the two plates contact, a stable magnetic field registers. When separated, the magnetic field is disturbed, causing an alarm.

2.3.3.1.14 Light Sensors (Break-Beam Sensors, Infrared Sensors, and Laser Sensors Photoelectric Sensors)

The "photo" in the word "photoelectric" refers to light. Light sensors respond to changes in light level and are used in a wide variety of industrial applications in addition to EAC. One type, called an *ambient light sensor*, measures daylight. When this sensor detects that daylight is dimming, a controller responds by turning on lamps. If timing devices do not control lamps, then ambient light sensors are most likely being used. You usually can tell when one is present on a light pole by seeing a small dome on the very top of the lamp fixture. In security applications, photoelectric sensors are commonly used. Known as *break-beam sensors*, they consist of two parts: A transmitter and a receiver. The transmitter beams a tightly focused beam of light at the receiver.

When someone passing between the transmitter and receiver breaks the beam, the receiver notes the change, and then triggers an event. These events can include sounding an intrusion alarm, triggering video recording, or opening a gate when someone or thing approaches, then shutting the gate as soon as it's clear.

Photoelectric sensors use specific types of light. These include light generated from specially designed incandescent bulbs. Infrared light or laser light. No matter what source is used, the light transmitter is adjusted to tightly focus the light beam on the receiver. Depending on the type of sensor, intruders can defeat break-beam sensors by fixing a flashlight on the receiver. To solve this problem, light transmission is commonly *modulated* (pulsed) in a way that cannot be duplicated by a constant light beam from a flashlight. Technology is improving the way photoelectric sensors work. Zigzagged light paths rigged through a system of mirrors can track intruders, for example. In addition, laser beam sensors are increasingly replacing infrared due to greater beam strength and focusing capability.

2.3.3.1.15 Metallic Tape

See *Conductive Wire Sensors and Fiber Optics, page 50.*

2.3.3.1.16 Microwave Sensors

See Ultrasonic and Microwave Sensors, page 54.

2.3.3.1.17 Motion Detectors

See Ultrasonic and Microwave Sensors. Also see Video Motion Detectors and Dual Motion Detectors, page 54, 55 & 50.

2.3.3.2 PASSIVE SYSTEM

(*Example:* Passive Infrared.) The word "passive" refers to a sensing system that measures changes in the environment over time. This could include changes in infrared light, temperature and humidity normally found within an environment. The opposite is

an *active system*, which actively introduces energy into the environment through a transmitter for interpretation by a receiver

2.3.3.2.1 Pressure Mat SENSORS (Mats (pressure))

This type of sensor mat is used in mantraps, entrances and exterior yards. They trigger an alarm when a specific weight (from 5 to 20 pounds per square foot) presses on the surface. Fiber-Optic mats are preferred for outdoor or moist applications. Also see *Conductive Wire Sensors and Fiber Optics, page 50.*

2.3.3.2.2 Sonic Sensors

See *Ultrasonic and Microwave sensor*; also see *Audio Sensor, and Infrasonic Sensors, page 54,49 & 52.*

Timed Applications

When a control panel receives an alarm from a sensor, it may time how long the sensor regains in an alarm state. If a sensor returns to normal within a predetermined time span, no alarm is sounded. Timing is used to measure the travel time a person or vehicle requires when passing through an access point. If the time set is too short, false alarms occur. If the time is set too long. It does not become obvious when a door or gate is improperly held opened.

2.3.3.2.3 Ultrasonic (US) and Microwave (MW) Sensors

These sensors measure ultrasonic sound and microwave energy. Ultrasonic sonic is lower on the Frequency scale. But above our threshold of hearing. While microwave energy is higher than ultrasonic and is regarded as electromagnetic energy. Ultrasonic and microwave sensors work on a similar principle. They broadcast sound at a specific frequency, which is picked up by a preset receiver. As the broadcast is spread over a specific area. Anything moving within that area disturbs the frequency pattern. If the receiver picks up a frequency that is different from what it experts, an alarm is sounded. The broadcast frequency can be adjusted to allow for probable disturbances. Such us

small animals or birds. It can also be set to distinguish the stride fate of a moving person, sounding an alarm within four consecutive steps. Ultrasonic servers are normally used to monitor interior spaces because their frequencies are easily disturbed by the environment. Their frequencies must be adjusted with regard to the presence or absence of furniture, as materials absorb sound and alter frequency wavelengths. Generally, interior ultrasonic sensors are stable. Air currents caused by air conditioners, however, can set off false alarms. Microwave sensors are better suited for outdoor use and are employed in sensing the sky at airports as well as sensing land use around remote prisons and military bases.

2.3.3.2.4 Vibration Sensors

In stable environments, this type of sensor samples vibration rates. Should the normal atmospheric vibration rate change, such as caused by cutting, chiseling, or ripping, an alarm is rounded. This type of sensor is well suited for installation on masonry walls because masonry is naturally low in vibratory properties, thus reducing the probability of false alarms. In applications with higher vibratory background noise, *discriminator sensors* are also installed. These devices sense common noise and cancel the effect of these vibrations, reducing false alarms based on common occurrences. (See *Audio Sensors, page49.*)

2.3.3.2.5 Video Motion Detectors (VMD)

This sensor electronically analyses CCTV camera images. It detects changes that are judged large enough to warrant an alarm. In a digital system, this detector notes changes light level from one set of *digital pixels* (square units) in a TV frame to similarly placed pixels in the next. An intruder casting a shadow over the area, wearing clothing with a different light refraction than the background materials and/or illuminating the area with a flashlight would cause this detector to sound an alarm. In an analog CCTV system, the detector compares large areas in one frame to the same areas in the next. Analog comparison is mere susceptible to false alarms caused by lighting changes and camera vibration than in a digital system, however, and is not recommended for outdoor applications.

2.4 Computer (Software, Hardware And Intelligent Networks)

2.4.1 WHY YOU SHOULD UNDERSTAND COMPUTERS

Many devices used in electronic access control (EAC) systems are controlled by microprocessor chips. The most useful microprocessor-driven devices; allow us to customize their behavior through software instructions. They can also communicate with other devices and calculate a wide range of information. We commonly call these devices *computer*.

The three main types of computers used in a large EAC system are the:

Supervisory Computer is a personal computer (PC), with monitor and keyboard, used to manage an EAC network. It issues information and instructions to other computers on the network, receives reports from those devices and stores information about ongoing events.

Controller (or Control panel) The controller provides a direct link to electronic authenticators, locks, sensors, gates, etc., installed at the site. When connections permit, it can communicate with the supervisory computer, hut does not normally have a dedicated monitor or keyboard.

Switcher The switcher controls closed circuit TV cameras and video taping activities and are commonly linked to sensing devices. Like a controller, it can communicate with the supervisory computer, but does not normally have a dedicated monitor or keyboard.

Few security professionals, unfortunately, have a formal education in computer technology, even though they've alt used software. This forces them to rely on advice about computer hardware from non-security professionals; advice that may be at odds with actual needs.

2.4.2 THE GRAPHICAL USER INTERFACE

The GUI presents vital information to the user in a simplified form without losing the importance or impact of the message. By using the mouse, an operator can select activities or options from context-sensitive menu pads located at the left-hand portion of the screen. The menu pads change from a light gray to dark gray when they are selected and are organized in a descending hierarchy to keep the operator from becoming "lost"

in the system and to present only the necessary actions on screen. On screen options can vary depending on the access level of an operator. This enables the System Administrator to "block out" options and actions for those operators who do not possess a "need to know". Such control is discreet since these "blocked" areas will never appear on screen for an operator who is excluded from working with them.

An instruction line at the top of the screen provides a brief explanation of the action that will result when a highlighted menu pad is picked. Every menu pad pick and all fields in the data forms offer a more thorough explanation of their function and use by accessing the on-line help feature with one keystroke. The workspace area, located in the center of the screen, permits a user to enter data into the system using reconfigured forms or monitor the facility using site-specific maps with interactive icons.

The EAC software offers object oriented hardware solutions to devices in the field through an operation's actions at the workstation. In the monitoring mode, icons represent Card Access or Site Security devices. The state of these devices is indicated by the color of the icon. (e.g. green for secured, red for alarm or orange for a broken device). An operator is apprised of a change in the state of a hardware device by the change in color of an icon. Action can then be taken using the mouse and the on-screen icon and appropriate menu pad picks appearing on the screen.

Incoming alarms are displayed at the bottom of the screen and site-specific maps, which contain the icon in alarm, will appear automatically simplifying the steps an operator must take to address the situation. In the event of multiple alarms, the system relies on a user-generated list of priorities to determine the order in which alarms are reported to an operator. The system stores in memory a list of the last 500 events to assist an operator in searching or past events.

The concept of simply tracking the status of alarms in the field through interactive icons is carried into the system software itself through the self-diagnostic feature. The EAC relies on a network of workstations and processors in the field to carry out its functions. These devices reside on a LAN. The integrity of the LAN as well as the various software programs that support the system and allow it to carry out commands are also represented through graphical icons on the screen. Should a link between two

processors become broken or a segment of the software fail, an operator is notified and appropriate steps can be taken to maintain security while the situation is rectified. Therefore, the internal software integrity is assured in the same manner as the field devices.

The software supports the capability to simulate various events such as an alarm, tamper, void card or valid card. Such simulations can be used to verify whether a point programmed into the system, such as a card access door, will function as planned. An operation can verify the function without having to be physically at the door. In the case of a card access system, however, it is often necessary to determine if a certain card is valid at a given door. With the simulation tools, an operator can "present" a card to a door by inputting the card number in a form that appears on screen.

The system permits any number of icons to be grouped together and given their own specific icon. For instance, a group of doors could be gathered together and with one-operator actions, they could be locked or unlocked. An individual item could be present in several different groups depending on what categories the system operator desires to control. These groupings can include communications links, field processors and software programs as well as doors or card readers.

The EAC also supports a graphical drawing program, which enables users to build their own site maps and icons as well as determine their location. Thus, a representation of the site or area to be monitored and controlled is created using the internal line drawing package or by importing CAD/DXF files into the system.

The GUI simplifies data entry by providing data forms for the various system functions. These forms contain spaces, which are filled in using the keyboard to add Card Access Doors to the site, create Access Levels or enroll personnel into the database. The forms serve as a template to insure information is correctly entered into the system and to avoid duplicate entries. The EAC uses this information to determine relationships between system components and personnel. The data entered into these forms is entered into the system directly and needs no further modification by the operator. These forms also assist an operator searching for records by allowing for specific values for descriptors to be entered into the appropriate spaces. For instance, if an operator wished

to locate all personnel in a specific department or building who were C.P.R. certified, he could limit his search by filling in the fields indicating department worked and specific skills.

2.4.3 ACCESS CONTROL

The EAC excels in its task of Access Control and Facility Management through the use of its speed and flexibility to carry out multiple tasks at once. Access Control is simply granting access to personnel depending on their relationship to certain parameters such as the need for personnel to gain access to an area versus the needs to limit access to areas for security or other reasons. These relationships present a complex matrix of options and actions for which the EAC is well suited.

In addition to determining who can access an area at what time and on what days, the system is capable of employing more sophisticated levels of control such as Area Control, *AntiPassback* and the Two Man Rule. Area Control is simply the establishment of an area that a cardholder must present a card to both enter and exit. Typically two or more card readers are used and a specific access level is often established for the area. A cardholder is not permitted to reenter an area if he did not present his card to exit. This can assist in keeping track of personnel in an area would an evacuation become necessary.

Area Control also can be used to create an Anti-Pass back atmosphere that essentially prohibits a cardholder from entering an area and then "passing" his card back to someone else to present to the card reader to gain access. Such positive "one man, one card" control limits unauthorized access to secured areas. The Two Man Rule option can also be chosen which requires the presentation of two access cards before access is granted to a door or area. All Area Control, Anti-Pass back and Two Man Rule decision-making is carried out at the field processor level for instant response.

The backbone of the Card Access component of the system is made up of the system hardware and firmware that stores the software and interprets its commands.

The EAC utilizes a network of a host machine and any quantity of workstations necessary to serve a site. These workstations at PCs can store system maps, data,

captured video images and the operating software. They are, in turn, linked to processors in the field, which relay data from the field devices, such as card access doors to the workstations and carry out commands from them to the devices in the field. The capacity of these field processors and the direct transmission of data to them on the LAN, however, mean they can store system data sufficient enough to allow them to operate independently of any one workstation. In other words, the processors are "smart" enough to open doors for valid cardholders themselves without having to verify access with a workstation. The System Administrator can choose when that stored data be updated for a processor. Such "smart" devices provide distributed intelligence, which allows for greater capacity within the system and foster decision-making. Distributed intelligence also makes the system invulnerable to single point failures.

The EAC has integrated Video Badging into its system as a means of better tracking and monitoring personnel and enhancing site security. A video image is issued to create an access card, which personnel can use throughout the site to gain entry and use as identification. The cardholder's image is captured by a video camera linked with one of the system's workstations and entered into the database. An access badge can be printed at that time or stored for later use.

The badges can be configured by the user to discourage forgery and the use of personalized badges with the picture of a cardholder discourages the swapping or unauthorized use of badges. Because the cardholder's image is stored in the database, printing additional badges to replace lost or expired badges are simplified.

The step of entering information into the on-screen forms to create a badge automatically enrolls a cardholder into the database, thus saving time for the operator. The cardholder's image can be "called up" by other terminals in the system to visually verify the identity of the person presenting the access card if necessary. Just as monitoring a premises for intrusion and allowing access are necessary component of a Card Access system, so too is the logging of the events into a database to create a record. These records are typically maintained for a time deemed appropriate by the system operator and can be used to evaluate the performance or effectiveness of the system configuration and usage by personnel.

2.4.4 DATABASE MANAGEMENT AND REPORT GENERATION

The entry of data through completion of on-screen forms or by site activity records builds a system database that is used internally to support access control and facilities automation functions. As mentioned previously, the data can be retrieved by traveling to a specific form and entering the appropriate data to limit the search of requesting the system list all records. A simplified Structured Query Language format can be employed to limit the search criteria and search the database more efficiently.

System operators can also tailor reports to address specific site needs and applications. These reports can be created for onetime use or they can be recalled as frequently as desired. Such reports can track the usage of doors or track a certain cardholder. Denied Access events, those times a cardholder is denied access to a door, can highlight seemingly discreet attempts by a cardholder to gain access to an unauthorized area.

In the present time, security is a prerequisite for the functioning of modern organizations. Access Control Systems are compulsory components of such intelligent safety precautions.

Access Control Systems provide:

- Overall item protection
- Differentiated operational protection
- Classified coded protection
- Comprehensive protection of specific security zones and data areas

The main targets of an Access Control System are the following:

- Controlling and defining access points
- Grouping of identified persons as authorized or unauthorized
- Securing that access is restricted only to the authorized persons at the specific access points
- An Access Control System consists basically of the following components:

NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

Installation of Electronic Access Control System

Graduation Project
EE - 400

Student: Shadi I. Al-Khatib (991247)

Supervisor: Asst Prof. Dr Doğan Haktanır

Lefkoşa - 2001

ACKNOWLEDGMENT

First of all, I want to pay my regards to all persons who have contributed in preparation of my project to complete it successfully. I am thankful to my supervisor " Dr Doğan Haktanır ", who helped me a lot in my crises, and gave me full support toward completion of my project.

I would like to thank my parents who gave there ever lasting encouragement in my studies, so that I could be successful in my lifetime.

I am also thankful to my beloved friends "Khaldun, Mohammed, Saif, and Rizwan" they are always tried their best in giving me valuable help toward preparation of my project.

Further I am thankful to the Near East University academic staff and all those persons who helped me or encouraged me in complete my project.

ABSTRACT

As technology advanced the trade secrets increases in line with this advancement. Many companies, in order to prevent the leakage of there trade secrets out of the establishment; they employ complex entry system at the entrances and within the establishments. This project shows how to construct an electronic access system (EAC), which is discussed in details within this project, this project is about installing of EAC system, this system has many equipments, these equipments includes doors and controlling components.

Within this project, I shall speak in details about each parts alone, then I shall combine these equipments together within on system, this system is applied on a building, this building related to software company, this company contains many rooms and the important rooms are computer and information rooms, in these rooms we applied on there doors high security level and for the other rooms we applied different types of security with respect to there importance. By applying high level of security in the main entrance I can keep unauthorized persons outside, I shall apply some other system within the building so that I can increase system efficiency and the system can work fluently.

The whole system is connected to the supervisory computer in the security room, and from there the security man can control and monitor all operations from there, the computer is connected to the other equipments through LAN this network is connected to the main computer and control panels, but the other equipments are connected to the control panels these equipments are responsible from the control panel this panel translate all information coming from the supervisory computer into the right equipment and with suitable standard and from there to the supervisory computer again. These panels can work in some cases without need to supervisory computer but not for long time. All these systems have been introduce with different plan, these plans emphasize its parts. Also it is emphasize security levels, also I shall speak how the whole system work and how does each equipment work In this project I shall use two different types of credentials one is the smart card and the other is the hand of that user (biometric credential) to have very high security in my building, within this project I shall speak about different types of credentials and I shall speak about there readers.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

1.1 Introduction to EAC system

While we have faced increasing in competition between company, it become more and more important to protect the companies information, and improve security in preventing the trade secret reaching to any one but not the dedicated personnel. For that reason or for any other reason protecting the buildings now days become very important.

Through this project I tried to give more obvious idea, clarify and in the same time provides the reader with some specification that is needed, the Electronics Access System that is responsible for our access (entering). This project will assist the reader to get more information easily about this system, which include monitoring system, entrance system, and others, this equipments -card system- will help our security system to activate, actually this part of security system allowed only for authorized person to access, and just to the region which allowed to him. And in order to improve our system these equipments should work fluently and without any bottleneck.

1.1.1 PROJECT OVER VIEW

This project contains three chapters the first chapter includes the introduction to these chapters and introduction to access control system, and how the system is working.

In chapter two I shall speak about *five* different parts. First: Credentials, this includes credential type like smart card that become one of the most important card in the whole world and it's get this speared from the high security that the card can provides, also there are explanations of different kind of reader such as normal card reader and biometrics reader.

The second part, explain Barriers (doors, doors closer, locks, fire exit and doors), here I shall give brief explanations about doors, and doors locks magnetic and electromagnetic.

In the third part I shall show Sensors (types, technology used and standard). Here I focus on Technology Glossary, I speak about many types such infrared sensors, heat sensors…etc. and how system is working and what is there affectivity in the system.

In part number four I shall give introduction to Computer that able to be use in EAC system that include many parts like software, hardware, network and technical information.

In the last part I shall speak about Communication (wired and wireless) in wire I speak about connection, cable types, cable jackets, such as coaxial cable, Fiber Optics and other, in wireless part I shall speak about communication media such as radio frequencies, analog to digital transmission, and digital transmission.

In Chapter number three I shall talk about project designing, in this chapter I have five plans first two is about security zones, the third explain system connections, and how to connect these parts to the main computer, the fourth plan is talking about communication system and CCTV system, the fifth plan shows what can be found in the security room from EAC equipments, then I shall speak about system components and how dose the system work.

At the end, I shall give my conclusion after writing this project, which are about the future of this system nowadays, efficiency and benefit behind using such system and the ability to improve such systems.

1.1.2 ACCESS CONTROL

Not too very long ago, access control was regarded as the art of keeping people out of building. If a stranger did gain access to a facility as, let's say. A guest of a manager, others might regard him or her suspiciously until they team who let this person in.

In modem society, however, transportation allows people from diverse backgrounds to gather in ways never before known in history. Our places of employment have become gigantic social) mixing machines where, in some cases, several new employees are being introduced on a monthly basis, in addition to many visitors.

The result of this is that as our organizations grow larger, people lose their ability to fully know and trust one another. If a problem occurs, such as a theft or physical threat, people feel scared, intimidated and depressed.

Electronic access control (EAC) is one component of a security system and it is best known for its ability to issue ID cards that replace keys. It is more than a security system, however. EAC provides an element of social engineering by quickly and securely introducing strangers into a facility in a way that they can almost instantly be trusted.

Figure 1.1.1 Most people think of EAS credentials as being cards. In fact, a credential can be any number of things, including biometrics, which analyzes physical characteristics such as palm prints. These motion detectors can be less than 3 inches tall. Yet they can sense intrusion over very wide areas.

An Access Control System consists basically of the following components:

- **Central Processing Unit:**

  Monitors and controls the system, including programming and operation.

- **Control Unit Stores and conducts programmed authorization data:**

  All access inquiries are checked and authorized from this unit.

- **Access Control Reader:**

  Being the preliminary control station of the system, it converts magnetic information (encoded in the cards) into electrical signals and directs them to the control unit.

1.1.3 How Does EAC Work?

This project describes EAC components; an overview of security needs and provides examples of real-life applications. Consequently, the following very brief description of how EAC works barely touches the subject, but it should provide an introduction.

EAC describes an electronic system in which information is collected and analyzed by computers. Once the information is digested, these computers issue instructions to various components, such as electronic and electromagnetic locks.

The computers have the ability to remember more information about large numbers of people than is humanly possible. The result of this is that they electronically issue commands based on the combined knowledge of:

- Security profile data
- Time and place
- Sensory data
- Management needs

In a well-designed system, security guards find these computers easy to manage. Through the use of a computer monitor, guards know who and why people are accessing the facility. They are also alerted when problems crop up and can instantly respond from their computer station by canceling an individual's access credential and/or by locking otherwise unlocked doors.

Figure 1.1.3 This is an example of a control panel. It is a circuit board and is often housed in an electrical utility box. The panel is a specialized computer that supervises access. It is capable of making decisions based on input, issuing commands and reporting all transactions to a computer at a central location, such as in a security office.

There are times during the day when facilities need more or less access monitoring. Depending on needs, the freedom of public access might reduce the amount of monitoring during business hours, while evenings and weekends might demand more. EAC systems are programmed to adjust to these needs. They are flexible systems that take into account human behavior.

Access Points: A door monitored by an EAC system has at least one credential reader and possibly two. One for either side, It also has an electronic or electromagnetic lock and at least one sensor that tells the computer when the door is completely closed.

This door might be surrounded with other security components, too. These include additional sensors, the most common type being motion detectors, and a CCTV system with videotaping. All these electronic devices report information (data) that helps control access and provide a history of events for later investigation. This project provides information about:

- EAC credentials. Which most people think of as ID cards.
- Electronic devices, such as locks and credential readers.
- Sensing devices, which provide electronic feedback about what is going on at strategic points throughout the facility and its grounds.
- Computers, which supervise the system.
- Control panels, which are specialized computers that control the electronic devices, receive feedback and issue commands.
- Communications, which carry the electronic data between computers, control panels and the devices they manage.
- System design concerns, which deal with the technicalities of setting up a system.
- Security concerns, which deal with concepts involved in integrating all the aspects of electronic surveillance into one coherent system.

Although issues surrounding closed circuit TV (CCTV) are an extremely important aspect of monitoring access, they are only touched upon briefly in this project. CCTV is a highly complex technology and experts, such as Charlie Pierce, have written clearly and extensively on the subject.

CHAPTER TWO: SYSTEM COMPONENTS

2.1 Credentials

2.1.1 CARDS, CODES, AND BIOMETRICS

The term "*Credentials*" refers to documents that verify a person's identity. People who present their credentials to officials or check points are regarded as being *authentic* . . . They are who they say they are. In electronic access control (EAC), credentials refer to cards, tokens and physical patterns, such as fingerprints, that identify people. Cards and tokens are presented to media readers for authentication, while physical patterns, such at fingerprints, are verified. When a credential is validated, access is granted. A credential is regarded as secure if it strongly resists alteration and/or duplication through forgery, or illegal use gained through spying. A secure credential when used by itself, however, does not resist use by an unauthorized person.

To increase the likelihood of truthful authentication, a single access transaction requires a multiple-step verification process. This process often combines a card with other identifiers, such as a personal identification number (PIN), biometric feature (such as fingerprints) and even photo/video identification. Not all access events require the same level of security. Exterior doors, for example, usually require more validation transactions than do interior doors.

> Example: in a highly secure chemical plant, guards monitor check-in. Employees display and use their proximity photo ID cards. Punch in their PINs, and have their palm prints read and verified. All these transactions take around 27 seconds per person, including a bit of gossip.

Once inside the plant, however, employees wearing their proximity cards move unhampered from monitored area to monitored area. This is because their proximity cards provide hands-free validation. The purpose of the internal EAC system, then, is to track "who goes there" and when they do it. It is not intrusive. The most common cards or tokens used throughout the world are based on Wiegand, magnetic stripe and proximity technologies in conjunction with PINs. These technologies, plus more, are described later.

Figure 2.1.1 Cards often require personal identification numbers in order to verify the authenticity of the user. Cards that are more secure can be used in multiple applications. The reader/keypad unit illustrated is part of a system designed to collect time and attendance information by using a standard EAC card.

2.1.2 MANAGEMENT PROCEDURES

No matter what credential technology you use, a facility is only as secure as its credential users' honesty. To manage a well-run system, then, you need to establish procedures that will verify identification, credential usage and termination, as the following overview describes:

2.1.2.1 ENROLLMENT PROCEDURES:

These let you enter data on access entitlements for users of the system. Time zones, access levels and geographical controls (identifying buildings and doors). Periodically, you'll need to update your information, including addresses, promotions, etc.

2.1.2.2 TRACKING PROCEDURES:

These check to make sure that the credential or your users are still in the system and are not altered or worn in any way. Plan on reissuing credentials and PINs at staged intervals. In a large system, for example. It would be disastrous to discover that all magnetic stripe cards wore out around the same time.

2.1.2.3 TERMINATION PROCEDURES:

These make sure that EAC authorization can be stopped the moment the user is terminated. In addition, they make provisions to retrieve outstanding credentials even though those credentials are no longer active in the system. This reduces chances for counterfeiting.

2.1.3 ENROBING CREDENTIAL USERS

A dishonest person with the best credential will cause harm to the facility. An honest person, free to roam is a blessing. Screening people prior to issuing credentials is important.

Validation: The very lowest level of screening is a visitor's pass issued on the say-so of another person in your organization. These passes do not unlock doors, but they do provide a way of identifying a stranger who is walking through the halls.

The more cautious you wish to be the more verified information you need to corset and maintain. The information you gather is only as accurate as your ability to ***double-check its authenticity.*** Failure to check information, even when a well-ordered portfolio is easily at hand, can have disastrous results.

Enrollment Time: Depending on your needs, the time it takes to enroll new people into your system is a factor in deciding what types of credentials you need to issue. It fakes longer, for example, to customize a magnetic stripe card with a color photo than it does to issue a card from a stockpile. Your enrolment procedures must calculate this processing time—minutes or days—so that you can keep up with your enrollment volume.

Encoding Considerations: Although most people think of credentials in terms of names and identity, computerized EAC systems associate people with code numbers. When used in cards or tokens, these codes are hidden from people (they are not PINs). Of the most popular cards, the user can customize magnetic stripe, proximity and bar-coded cards. But Wiegand cards cannot. With regard to codes, you need to:

- Know the total number of codes available in your system and how that total affects your future needs.
- Decide whether you want to customize those codes or accept standard numbers from the credential manufacturer.
- Know whether you can link PIN codes to your card or token codes.

Figure 2.1.2 Card Types (Smart, Wiegand, proximity and Mix Technology cards)

When you depend on manufacturer-encoded cards, you must keep a sufficient number of those cards on-hand to meet your enrollment demands. If you do not customize these cards with the user's name or photo, these cards can be reassigned until worn out.

For a number of reasons, most systems impose restrictions on the total number of codes available. Keypad systems, if not chosen with care, can be quite restrictive. Coding is dependent on the electronic circuitry of the media-reading mechanisms, memory, software, and in the case of keypads, available keys and internal switches. To increase the number of codes available, some cards provide a *facility code*. This code is placed before every single number in a standard range of codes, thereby increasing the total number of codes available.

> Example: Codes 1 through 9.999 are available to approximately 10,000 users. By using three facility codes with this range (say. 1001. 1002 and 1003), you increase the total to approximately 30.000 available codes.

Control panels validate the facility code first, then the credential code. When designing a system, you want your control panels to interpret the facility and card code whether or not that panel is linked to a main computer. When a control panel is dependent on a main computer and the communications link between them is broken, that panel might accept all valid facility codes without checking card codes. Worse, the panel might not function at all.

2.1.4 CREDENTIAL READERS

Credential readers (as well as scanners, keypads, etc.) act as the "middle man" between the credential user and the control panel. They are stationed at one or both sides of a protected door. When two readers are used to protect both sides of a door, the system enforces *antipassback* procedures, which discourage people from sneaking into areas, If a credential user fails to use the readers in the right sequence on both sides of the door, an alarm is sounded and guards are notified with a message displayed on their control monitor announcing who made the mistake.

All readers send credential codes to a control panel. The control panel compares the code it just received to existing databases. Depending on what the panel finds, it issues instructions to open a lock, sounds an alarm, or does nothing. If the control panel is dependent on a main computer, the computer checks the code, then sends validation information back to the panel and the panel takes it from there. Readers can take many forms. The most common are card swipe or insertion devices, proximity devices (based on radio frequencies), keypads (usually 4-key or 10-key), scanning devices (also called "optical readers"), and sensing devices (used in biometrics).

With the exception of biometric scanners, most readers are used for a variety of commercial applications in addition to EAC. Bar code readers, for example, automate pricing and stocking information in department and grocery stores. Magnetic swipe readers are used in charge and debit card transactions. One increasingly popular use of readers is to *track time and attendance* for payroll. The same credential that lets an employee access a facility also aids in calculating his or her paycheck—and docs so far more accurately than payroll systems compiled by time clocks and cards! The result can be very cost effective.

EAC readers differ from commercial readers because they require *temper resistant* monitoring. Access to wiring by removing a poorly mounted reader can render an electronic lock useless. Tampering and vandalism, not card duplication or fraud, account for a significant percentage of reader failures! Proximity readers, which can be completely hidden within a wait, are the most tamper-resistant. Others, depending upon decorating needs, can be surface mounted or embedded, but must not have exposed

screws or prying areas. Fortunately, reader tampering can be detected by attaching sensors to the reader mount. Once an EAC system detects tampering, it can ring bells and signal authorities.

2.1.5 CARDS AND PHOTO IDS

The increased speed and storage capacity of computers, coupled with decreasing prices for computer equipment, printers, video cameras and digital cameras is making the creation of computerized image databases and photo ID cards easy and inexpensive. White traditional photos and Polaroid technology are still being used to apply photos to cards, digital imaging provides:

1. Truly instant image creation (no chemicals or waiting period).
2. Instant computer files (no scanning necessary when the camera is connected to the computer).
3. Tamperproof, easily produced ID cards in color or black and white that don't require lamination.

Complete control over the design and processing of ID cards. Full color photo ID cards provide better security because they contain more visual information than black and white images. In addition, in full color image database on a computer provides excellent verification resources for the authorities that need to make visual comparisons. At this writing, photo ID cards are most commonly produced by the following methods:

Lamination: In this process, a photo (traditional or Polaroid) is cut out of a background and parted on a card, which is then covered by sheets of clear plastic.

***Dye sublimation*:** In this process, a full color digital image is printed on a card through a process called *dye sublimation,* which works as follows:

The image is reproduced by placing a tightly spaced series of dots on a vinyl card reproduces the image. If color is used, these dots are made through cyan, magenta, yellow, and black ribbons. Print processing uses variable heat temperatures to melt the colored dots, blending their hues and producing a wide range of colors. When these dots cool, they permanently bond to the card surface, making the card tamper resistant.

Black and white laser: In this process, special properties in the cards' material bonds with Mack laser printer toner.

2.1.6 CARD SIZE

What you put on a card, of course, is limited by the size of the card itself. To increase cost-effectiveness and to promote multiple technology cards, the EAC industry is striving to standardize all cards in terms of size and thickness. Two standards, which were developed by the banking industry, are:

- CR-80: most common credit-card sizes (2.125" tall by 3.375" wide by 0.03" thick)
- CR-60: slightly taller than the CR 80 (2.375" tail by 3.25" wide by .03" thick)

CR-80 is the most common size and fits all card swipe and insertion readers. CR-60. However, fits all card swipe readers, but not insertion readers. As swipe and insertion readers perform exactly the same tasks, it is important to be aware of the CR-60's reader limitations when designing a system. These two types shown in figure below.

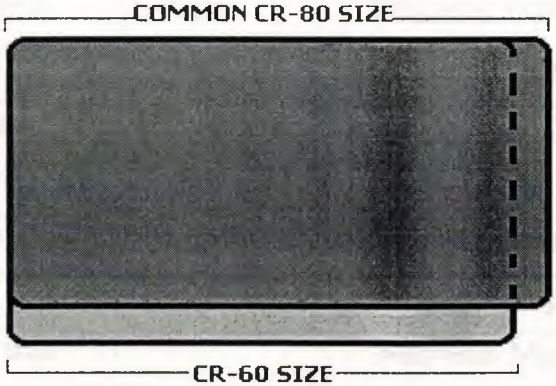


Figure 2.1.4 This figure show the difference between the two card types

2.1.7 CREDENTIAL TYPES

The following pages provide a background on 12 basic credential types, which are listed alphabetically below. Some credentials can be easily customized — important for facilities that want a lot of control over information — others depend on supplier issued ID codes.

The credentials you select depend on your need for easy customization and your overall security goals. Supplier encoding, while often being regarded as highly secure, is not necessarily the best. Combining technologies (such as photo identification, magnetic stripe and a PIN) can result in very satisfactory credential security.

2.1.7.1 BAR CODED CARDS AND OBJECTS

Bar codes are seen as a set of parallel thick and thin black lines. These tines form a light/dark pattern that is interpreted by an optical reader or scanner as a code number. Currently, there are more than 13 different bar code symbol sets, plus variations on these. The most popular codes include the Uniform Pricing Codes (UPC-A, which is a 12-digit code, and UPC-E, which is a 6-digit code).

Table 2.2.1 Credential Types and Related Technology

Credential Types	**Related Technology**
Bar Coded Cards And Objects	Light And Dark Patterns Interpreted By Optics
Barium Ferrite Cards	Magnetic Pattern
Biometrics	Physiological Pattern Interpreted By Various Means
Hollerith Cards	Holes That Allow The Passage Of Light Or Electrical Current
Infrared Cards	Light And Dark Patterns Interpreted By Optics
Keypads	Keyboard Input
Magnetic Stripe Cards	Magnetic Media
Mixed-Technology	Combined Technologies
Optical Cards	Light And Dark Patterns Interpreted By Optics
Proximity Cards And Objects	Radio Transmission And Computer Chips
Smart Cards	Computer Chips
Wiegand Cards	Magnetic Patterns

Code 39, and Post net, which is used exclusively for the U.S. mail. Code 39 is the most popular code used outside the retail industry and the one most likely to be used in EAC. It handles up to 44 characters that can include any of the 225 ASCII characters as well

as leading and trailing spaces. The spaces allow two or more bar codes to be scanned as one very long bar code.

Bar codes, which can be printed directly on cards or objects, provide the least expensive, easiest to use system of EAC identification. The software necessary to create bar codes is sold in computer stores and catalogs as well as through industry-specific sources. Readers, which include optical wands, guns, and scanners, are all commonly available.

Unfortunately, although bar codes are convenient for record keeping, they do not provide an adequate level of security for valuable assets or high security clearance. A photocopier or computer can easily duplicate bar codes. Because they are easy to create, bar codes can be successfully used for time and attendance reporting and casual EAC. Unlike magnetic encoding, printed bar codes cannot be destroyed by radio frequencies or magnetic field interferences. Placing a special translucent patch over the code can prevent easy duplication via a photocopier or computer scanner. Some patches contain patterns and even logos. No matter what they contain, they blacken the bar code when copied, but still allow optical reading.

Figure 2.1.5 The labels on the roll above are made out of translucent red masking material. Typically, this tape is placed on the bar code before the card is laminated

The accuracy of bar code reading depends more on the quality and condition of the optical readers used, than the quality of the printed bar code itself. This means that regular reader servicing is required to avoid problems caused by dirty or scratched optical surfaces. Although bar codes are seldom used alone in EAC. They are often

laminated onto more secure credentials, such as Wiegand, magnetic stripe, and proximity cards, to enhance information gathering.

2.1.7.2 BARIUM FERRITE (BAFE) CARDS

Magnetically encoded barium ferrite cards, which were in the forefront of FAC technology during the 1970s, have declined in popularity, although they are still being used. The first barium ferrite card readers were magnetic and mechanical, with many easy-to-damage parts. They worked as follows:

> At setup, a program cartridge, containing a pre-coded array of magnetized spots, was installed in a reader. Between the program cartridge and the access card insertion area were individual magnets, a movable slider and a metal plate. The slider contained holes through which magnets could fall. The metal plate below the slider stopped the fall of those magnets. The program cartridge attracted a predetermined array of reader magnets upward and out of the slider holes. The remaining non-attracted magnets stayed in the holes (resting on the plate), thereby jamming the slider in place.
>
> The access card contained magnets positioned to match the pattern of those resting on the metal plate. When this card was inserted, the resting magnets were magnetically repotted (pushed upward), releasing the slider, which slid forward, tripped a micro switch, and released the latch.

At one time, the same code array was used by all the access cards issued in a system, if a card was lost, the program cartridge and the remaining cards had to be reissued. As time went on, additional magnetic spots were added to the main array, forming unique ID numbers that could be interpreted by microprocessors.

The original readers required a great deal of maintenance. As they wore out, many were replaced with competing technologies. Still, as of 1980, there were many barium ferrite cards in circulation, providing the market for a few manufacturers to develop 100% microprocessor-based readers that could interpret other manufacturers' cards as well as produce low-cost proximity-like systems.

Magnetic barium ferrite codes are difficult to duplicate because they are factory-embedded, making them highly secure. They hold up especially well to problems caused by harsh weather and hostile environments, and can be used in mixed technology applications. Like all magnetically encoded cards, however, they can be erased or distorted by strong magnetic fields and tend to wear out over time.

2.1.7.3 BIOMETRICS

While the security level of credentials is determined by whether or not they can be easily duplicated, unauthorized use can occur when credentials are shared, stolen and/or PINs are exposed. Biometric credentials were developed to defeat this problem by verifying that the unique personal features of the credential user, such as their palm print or eye, match a copy of those features, called a "*template*," stored in a computer. Biometrics, which began as an offshoot of the study of genetics and disease, are used when the need for a highly secure identification system offsets the cost of that system.

Various biometric systems have been available for decades, including an attempt by IBM in the 1970s to promote a signature recognition system. Many of these systems,

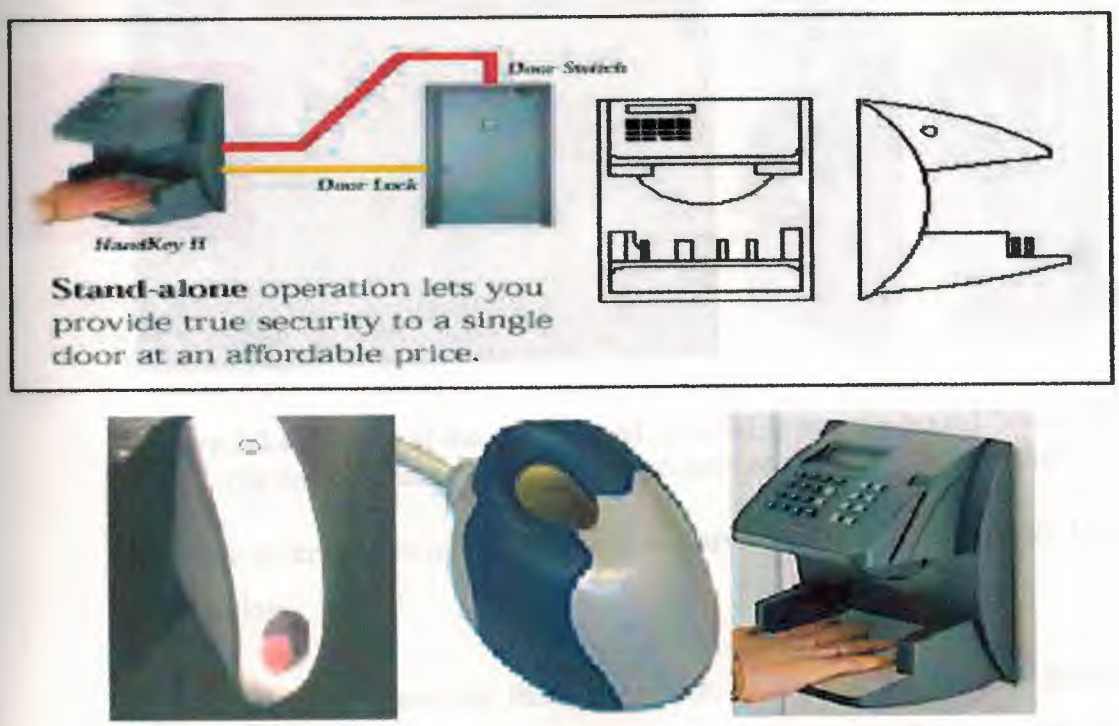


Figure 2.1.6 Reading palm prints checks the length, width and thickness of the hand and almost use for high security and time and attendance points of unique information can be encoded in this way. Also we can see below it fingerprint.

However, were no popular because of high costs, the high rate of verification errors, and verification slowness.

2.1.7.3.1 Body odor:

Senses odors by using chemical processes that are similar to the processes that take place in the nose and brain.

In early 1995, researchers at Leeds University in England announced that they developed a process that can differentiate between people by their smell. Perfumes do not mask this process because perfumes scenes are very different in chemical composition than body odor. Smart card manufacturers hope to eventually embed this technology in their chips in order to compete with finger printing systems.

Before they do that, of course, body odor technology must improve its current identification accuracy of 90%.

2.1.7.3.2 Eye identification:

Figure 2.2.6 Potions of the eye are read by looking into the hound "view" area. The device illustrated is a retinal scanner combined with a keypad

There are several ways of using the eye to provide unique identification, two of which follow:

Iris identification measures the iris, which, according to product literature distributed by Iris can, can identify 4,000 points in less than three seconds. They

claim that iris patterns are fixed at birth and there are no two alike, including those of identical twins.

Retinal scans read the surface behind the eyeball through a tow-intensity infrared fight that tracks 320 points in the retina and records associated blood-vessel patterns.

2.1.7.3.3 Facial recognition:

Verifies facial features by comparing a living face scanned by a camera to older images in a database. Because it is easy to change appearance, there are several systems under development that seek to reduce validation time and increase accuracy. This type of technology is far more sophisticated than having a guard check an image database and then determining the similarity between the picture and the living subject.

2.1.7.3.4 Multiple biometric patterns:

Assures that a severed body part, such as a finger, cannot be used for falsifying identification by requiring that two different biometric readings be taken at the same time. A blood-oxygen saturation reading taken with a fingerprint scan is an example.

2.1.7.3.5 Random voice interrogation:

Assures that a tape recorder cannot be used to bypass a voiceprint system, which compares speech patterns, it does this by recording several spoken phrase templates for each person. When identification is requested, the person is asked to recite only one of the prerecorded phrases. Once the phrase is recited, the voice is compared to the appropriate template.

2.1.7.3.6 Signature identification:

Measures time and pressure used to create a signature as well as the signature pattern itself.

2.1.7.3.7 Voice identification:

Identifies the unique voice characteristics of a freshly spoken phrase to one stored in a template. These comparisons include air pressure and vibrations over the larynx.

2.1.7.3.8 Weight measurement:

Although weight is not a biometric measure because it cannot pinpoint specific traits, weight is often used to determine the presence of an individual or thing and consequently, can be used in the authentication processes.

Weight checkpoints are often found in enclosed rooms called "mantraps" as well as around "invisibly" protected objects, such as might be seen in a museum.

2.1.7.3.9 Hand and fingerprint identification:

Uses various techniques, among which is a three-dimensional digital image that is captured and measured to create a template Between 10,000 to 250,000 points of unique information can be encoded in this way.

While biometrics generally provides a highly accurate verification system, especially when combined with a PIN, users are sometimes concerned about the possibility of physical invasion, harm or discrimination during the credential-reading process. The following considerations describe a few of their concerns:

- A biometric x-ray system, for example, would not be viewed as accept able because x-rays harm the body with regular use.
- People with certain types of physical disabilities, such as those who have artificial hands or who are blind, might not be able to use the system.
- Blood tests are generally considered too intrusive to do on a regular basis. In addition, there are many regulations governing their use.

2.1.7.4 HOLLERITH CARDS

Hollerith cards are modeled after cardboard computer cards that were first used in 1890 by the U. S. Census Bureau to automate the national census. These cards featured a uniform pattern of small rectangles arranged in 80 columns, 12 rows high, and held up to 80 alphanumeric characters of information per card.

To encode these original computer cards, keypunch operators punched out selected rectangles, leaving holes that represented values. These cards were then placed in electronic readers, which passed current through the holes. The resulting pattern of "on's" and "off's" were electronically translated by a computer into data for number crunching. Copying the above principle on a simple scale, Hollerith cards also have holes punched in them, but not as many. These thin plastic cards, which can be manufactured in a variety of rectangular sixes, are read optically by passing a light through the holes, or electronically, by allowing metallic brushes to touch contacts exposed through the holes. Unfortunately, Hollerith cards can be easily duplicated and are only used in low-security applications- Hotels and motels, for example, often use Hollerith cards. When a card is lost, the code can be quickly changed and a new card issued with minimal expense

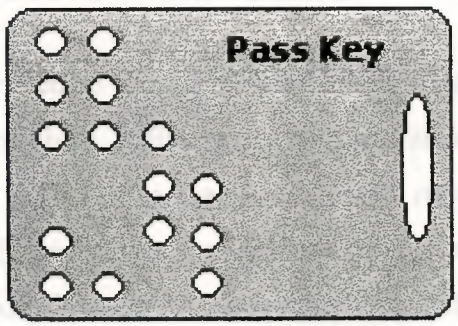


Figure 2.1.7 This Hollerith card is typical of those used in the hotel industry.

2.1.7.5 INFRARED CARDS

Light sensitive infrared card technology, also referred to as "Transmissive infrared" and "differential optics." appeared in the 1970s and uses bar code principles to encode information.

Embedded in the card is a bar code that is coated in a way that allows predetermined amounts of infrared light to pass through. Electronic infrared sensors detect this internal pattern as reduced energy level infrared light. The bar code pattern itself cannot be seen by the human eye. Like bar coded cards, the accurate reading of an infrared card is dependent on the quality and maintenance of its light-sensitive infrared reader. Unlike bar coded cards, these infrared codes cannot be easily duplicated because they are made in a factory and are, therefore, very secure. In addition, they are not subject to erasure by stray magnetic fields as are magnetic stripe, Wiegand, and barium ferrite cards.

2.1.7.6 KEYPADS

Keypad devices provide the means to link a PIN with a credential use a PIN by itself and/or program various devices connected to the system. In all, they are extremely versatile. Some keypads are part of the locking mechanism. This type of keypad might be programmed to respond to a single PIN that's assigned to everyone, or else, it can be linked to a sophisticated control panel, which provides the means to track many codes and time zones. In most mediums to large EAC systems, keypads are linked to powerful control panels and verity cards through use of a PIN. Some keypads even have secret containers in their mountings. These provide a secure storage area in which to place standard keys (for locked cabinets) or other valuables.

Generally, keypads are limited to four-or ten-digit codes, regardless of how many keys appear on the devices themselves. Software, memory and internal circuitry impose these limits; consequently, it is important to examine your PIN requirements before selecting a keypad system. In addition, keypads might not comply with the Americans With Disabilities Act, as their location and PIN usage might be difficult for physically and/or mentally challenged people.

Still, keypads are highly durable and are fairly inexpensive to replace. Systems based exclusively on keypads are easy to maintain because they do not require any card or token inventory or related encoding hardware such as is required for magnetic stripe cards. Unfortunately, keypad systems are not highly secure. For one thing, some keypads contain all the wiring necessary to open a door, which means that unauthorized removal can make the lock useless. Another problem is that PINs can be stolen through

spying or even casual observation. The spying issue has been addressed by the Scramble Pad, patented by Hirsch Electronics. This keypad reduces the chance of spying success by randomly changing its key top labels.

On a Scramble Pad, the keys labeled 123 might become 976 or 485. Consequently, the finger pattern used to punch in the code 6735 is different with every event. Even if a spy sees the motion, he or she would not know what it stands for. This keypad further reduces spying by shielding its key top tables and preview window with view-restricting material. In summary, keypads in combination with card and token, systems, play a very important role in EAC and are in common use.

Figure 2.1.8 **a.** Intelligent locksets like, which seen above can function independently, or be linked to a sophisticated EAC system.
b. This is a typical card reader combination.

2.1.7.7 MAGNETIC STRIPE CARDS

Most people have seen and used a magnetic stripe card of some type. These cards are the most widely used cards in the world and proliferate as bank credit and, of course. EAC cards. They are inexpensive, can carry alphanumeric information, are quickly produced and can be encoded at the user's site.

Each card contains a Mack plastic stripe of magnetically sensitive oxide, which is the same material used to make audio/video tapes. Unlike tapes, however, magnetic stripe cards are subjected to frequent rubbing and bending. Despite their lack of protective housing, their ability to retain magnetically encoded information is quite good. The risk

of magnetic erasure, however, is always a problem. Their resistance to erasure is known as their coercive force rating.

Coercive force ratings indicate the strength of a magnetic force required to erase magnetic material. A card with a low coercively rating, therefore, is fairly easy to erase, and a high coercively rating means that the card is more protected from stray magnetic fields. Needless to say, disposable cardboard cards are more likely to have a lower coercively rating than more permanent plastic varieties. According to the American National Standards Institute, Inc., magnetic stripes must contain four tracks available for encoding, however, specific encoding standards have only been defined for tracks one and two:

Track one: Stores up to 79 alphanumeric characters (210 bits per inch). This information might include the user's name and maybe a title.

Track two: Stores up to 75 bits per inch, with 40 numeric characters. This is the track most commonly used for access control codes.

Track three: This track can contain a facility code (also known as a *water mark*), which is described later in this section. Access to track three requires a special dual-head reader.

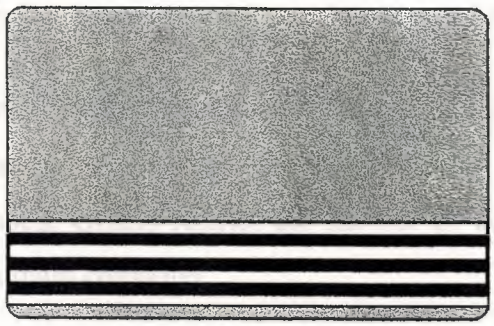


Figure 2.1.9 Magnetic Strip Card

Magnetic stripe cards store more characters of information than associated with bar coding or magnetic particle embedding and are far easier to customize. All encoding can be done at the end user's facilities by manual or automatic equipment. Manual encoders, of course, are more cost-effective for organizations that issue only a few cards. Automatic encoders speed up the process for issuing multiple-cards, plus provide

more control features. These include assigning sequential issue numbers and printing images on the Cards, in addition to the encoding process itself.

Unfortunately, with the right equipment, unauthorized duplication of magnetic stripe information is possible, rendering their security somewhat low. It is common, however, to see magnetic stripes on mixed-technology cards, which increases their security level. One very new development, for example, encodes highly secure, machine-readable, hologram patterns and a magnetic stripe on a single card. The combined use of PINs with magnetic stripe cards, of course, is well known. Magnetic stripe information is read by means of a swipe (moving the magnetic stripe along a track that passes a reader head) or insertion. Swipe readers, with their exposed reader heads, should only be used in environmentally clean areas. Insertion readers are less affected by environmental dust and are suitable for outside installations.

Motorized insertion readers regulate the speed at which the card passes the reader head and may increase reading accuracy. Like tape recorders and VCR's, however, the quality of the information transfer under any circumstance is largely dependent on the strength of the magnetic properties in the magnetic stripe and the cleanness and orientation of the card reader head. Magnetic stripe cards can be individualized by photos and/or bar codes through lamentation, printing, or dye sublimation. Care must be taken to make sure that bulky lamination does not jam up card travel in the reader.

Facility Codes and Water Marks: For a variety of reasons, some systems restrict the number of characters that can be used in a card code, thereby limiting the total number of codes that can be issued. Others restrict the number of codes a control panel can interpret before polling a main computer.

To increase the number of card codes available, a special code, called *facility coded* or *watermark* is permanently fixed in Track Three by the card manufacturer. This is done through a proprietary system that positions magnetic oxide particles on Track Three via wet slurry. When the slurry dries, the information is secure.

The result of applying a facility code is that a range of card codes, such as from 0001 to 9,999, can he duplicated. In the following example, a 10.000 card code range is expanded to approximately 30,000 possibilities.

- Facility Code 1002 - range 1-9,999
- Facility Code 1003 - duplicate
- Facility Code 1004 - duplicate

In addition to increasing the number of available codes, facility codes can be used to detect tampering and unauthorized card duplication.

2.1.7.8 MIXED-TECHNOLOGY

The ideal credential should be capable of combining a variety of technologies, including proximity, magnetic stripe, microprocessor (smart card), Wiegand, infrared, and keypad. In addition, users should be able to inexpensively apply customized designs, photos, and/or bar codes to cards for further individualization.

One advantage of using mixed-technology is that a single card can be read by different types of readers. This makes retrofitting (updating) existing card systems more cost effective because it doesn't require replacement of hardware or wiring. Another advantage is that it reduces the number of cards a person needs to carry.

Figure 2.1.10 Mixed technology card

Many universities are taking advantage of mixed-technology card systems:

> *Example:* In one college, a student photo ID card uses proximity technology to unlock dorms, bar codes to track library books, and a magnetic stripe with PIN to access the debit system used by the cafeteria and ticket agents. As shown in figure 2.1.10.

The three most common credential technologies are magnetic stripe, Wiegand, and proximity. Wiegand and proximity cards offer an exceptionally high degree of security.

Magnetic stripe cards carry a great deal of information and are easily encoded. Proximity cards, which do not touch their readers, improve traffic flow and reduce reader maintenance costs. Combining the three technologies mentioned above into a single credential requires:

1. A standard card size (CR-80 or CR-60 as mentioned earlier in this chapter).
2. A card thin enough (.03") to fit through a magnetic stripe swipe or insertion reader.
3. Sufficient voltage to drive Wiegand and/or proximity systems.

Other combinations are possible, too. Biometrics, for example, often requires a huge computer file (template) for each authorized person. Verification might take an excessive amount of time if the biometric reader has to check against templates held in a distant computer. Smart cards, however, can easily hold these large files. This allows the use of a biometric system for personal identification without being tied to a distant database, thus avoiding problems associated with slow or poor telecommunication connections.

2.1.7.9 OPTICAL CARDS

Optical cards are very new and are not widely used for EAC. This type of card was first developed by Canon U.S.A., Inc., and can store between 3.42 to 4.20 Mbytes of data on the size of a credit card. The amount of storage space it contains depends on the sensitivity of the card reader itself. The benefit to such a credential is that it can carry an enormous amount of information, thus reducing the telecommunications time a reader might require seeking details from a distant computer. The disadvantage is that this information must be entered on the card at the factory.

Optical cards are created by a solid-state, high intensity, laser beam that bums tiny pits on the card's surface. To read this data, a low intensity laser beam directs light on the pits, the reflection of which varies in accordance with the data that was initially etched. The Cannon system writes information on 2,500 tracts, some with multiple sectors, using the same write-once-read-many-times (WORM) techniques as for creating CD disks.

2.1.7.10 PROXIMITY CARDS AND TOKENS

Popular proximity cards or tokens do not need to touch a reader in order to validate a transaction. Their radio-wave transmission technology is highly secure and their readers can be hidden behind walls, in clean, maintenance-free, vandal-proof locations- Best, because proximity readers don't require contact, they speed the flow of human and vehicular traffic through check points.

These cards and tokens can remain in pockets, purses, or even on the front seats of vehicles and still be read by the system.

Figure 2.1.11 These proximity tokens contain a magnetic coil. Memory chip and a battery. Slim cards contain everything but the battery. The bracelet token is commonly used in hospitals and key chain tokens for garage applications. The flat panel token can be kept in a car or else attached to a cup for wearing.

Electrical power is always a big EAC concern and. prior to 1993; a typical proximity reader drew a great deal of current (400 mA at 12 volts). Today, readers can operate, with current as law as 40 mA at 5 volts, which is the same range, used for Wiegand and magnetic stripe readers. Each proximity card contains a coil of wire that acts as both the receiving and transmitting antenna and a small, integrated circuit that is programmed with a unique ID code.

The cards are powered by the voltage generated from a reader's magnetic field in relation card's antenna coil. Once energized by a reader, the card transmits its ID information Transmission is so fast that access verification takes place in less than a quarter second.

There are two types of proximity cards or tokens:

Active:

Has a range measured between touch to 100 feet. Its transmission is powered by a small, lithium battery. Due to battery thickness, active proximity carriers are manufactured as tokens or thick plastic containers that look somewhat like cards. The battery loses power over time and requires systematic replacement, although its average life is from five to seven years.

Passive:

Has a range measured between touch to 30 inches. Its transmission is powered by magnetic properties embedded in a very thin, maintenance-free card. The technological trend is to extend its transmission distance through the use of space technology that was originally developed to receive faint signals from distant stars.

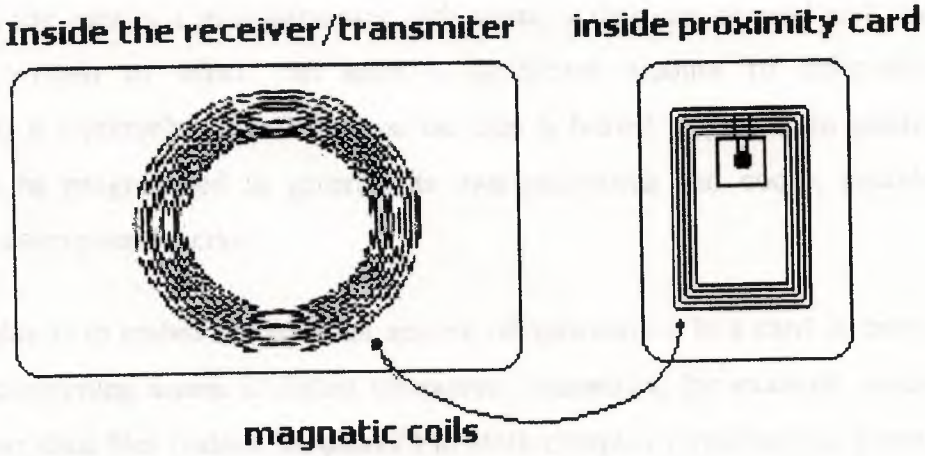


Figure 2.1.12 Both proximity card and reader.

Proximity technology is secure, reasonably priced and becoming increasingly used in mixed-technology cards. Readers have been miniaturized to fit into spaces less than 1.75" square and are getting smaller every day. Being convenient, they comply very well with regulations defined by the Americans With Disabilities Act.

HOW PROXIMITY WORKS

1. A receiver/transmitter (R/T) is either buried in a wall or contained in a slim cabinet hung on a wall.

2. The magnetic coil in the R/T excites the magnetic coil in a card when that card is in range. This range is extended when the card or token contains a battery.
3. Once it is excited, the magnetic coil in the card generates a crisp, magnetic pattern that represents a code contained in its memory chip.
4. The R/T receives the magnetic pattern and responds by amplifying and transmitting it to the processor — a control panel or other unit.

2.1.7.11 SMART CARDS

Although smart cards are currently uncommon in America, that may soon be changing. European companies (telephone systems and banking) have been using smart cards extensively since the early 1990s. A smart card is essentially a credit-card sized computer that was invented over 20 years ago.

Embedded in the card is a microprocessor with memory that can be read and. more importantly, written to which can store a significant amount of information. Counterfeiting is extremely difficult because the chip is buried in plastic. In addition, the chip can be programmed to generate its own passwords and codes, including sophisticated encryption functions.

The trend today is to embed a significant amount of information in a card in order to reduce time-consuming access to distant computers. Biometrics, for example, requires large computer data files (called "*templates*") to store complex physiological patterns. By keeping that information on a smart card, identification time is greatly reduced and worldwide check-in sites (such as used in the military) are not subject to long-distance communication problems. There are three types of smart cards:

- **Memory only:** Has less than 400 bits of memory and are often used for disposable "prepaid card systems."
- **Memory circuits with some hard-wired security logic:** Contains between 1K to 4K of memory and can be erased and rewritten. These are designed to allow encryption and PIN comparisons.
- **Full-Hedged microcomputers:** Contains a complete computer system with an operating system and the ability to be programmed to meet a

wide range of applications. The computer system includes a processor, nonvolatile read/write memory of 1 K to 8K, a small amount of random access memory, and read-only memory, which contains the operating system and the place where security functions are hidden.

Although a smart card looks similar to a standard credit card, it differs by having five to eight metallic contacts displayed on its surface. These contacts connect directly to a computer terminal when the card is inserted. To make sure that contacts is good, smart cards must be stored flat at all times and malignance is needed to make sure that terminal readers are clean.

To increase the potential markets for smart cards, information held in the chip can now be transferred through proximity technology. Although contact less and radio communication methods have not yet been standardized, systems are available.

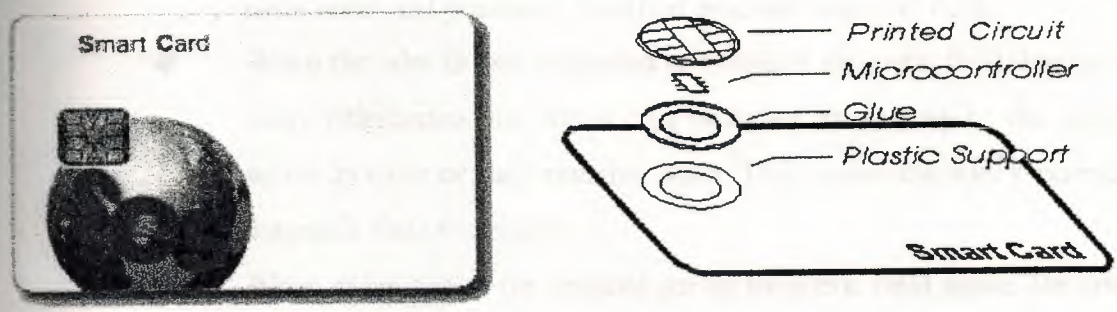


Figure 2.1.13 Smart cards look like common charge cards and can even have a magnetic stripe, bar code and/or id photo present. You can identify a smart card by a metallic design similar to the white one seen on the card above.

New uses for smart cards are being invented every day. Several states, for example, are replacing food stamps and other voucher systems with smart cards. These cards reduce paperwork and theft; white increasing reliability and ease of benefit transfer.

Hospitals are also using smart cards for EAC as well as for sharing patient records. Updating a smart card from a single computer source, as opposed to transferring information from numerous charts and records, improves communications, increases accuracy, and decreases costs associated with paperwork.

2.1.7.12 *WIEGAND CARDS*

Wiegand cards are based on patented technology held by the Sensor Engineering Corporation that embeds an array of magnetic wires in a card that is very difficult to duplicate. Wiegand technology combines several patented processes and a special metal alloy to create unique magnetic properties not found in common ferromagnetic (iron) wires.

Through manipulation and heat-treatment, the core of a Wiegand wire acquires a different magnetic property than its shell. This result in a condition called *magnetic action.*

Bistable magnetic action creates an electrical pulse:

- When first subjected to a strong magnetic field, the wire has a magnetic north and possesses a unified external magnetic field.
- When the wire is then subjected to a weaker magnetic field that has a south orientation, the wire's core switches its polarity to the south, while its exterior shell remains north. This causes the wire's external magnetic field to collapse.
- When subjected to the original strong magnetic field again, the core reverses its polarity to match that of its exterior shell. This change in polarity creates a crisp, discrete electrical pulse.

The only energy input required to create the electrical pulse is the bistable action of the wire in relationship to variations in magnetic fields produced by the reader. Although the pulse it regarded as analog, it is so crisp that it can be read as a digital output. Every Wiegand wire segment embedded in a card represents a magnetized pulse generating "bit." Up to 56 bits are allowed per card, although in reality, not alt the bits are required.

These bits are arranged in two parallel rows. Bits in the top row are referred to as *zero bits*, and in the bottom, *one bits*. The placement of these bits in relation to one another generates a binary pattern that represents a unique code. Wiegand readers have two reading heads, one for each row that read the electrical pulses generated by the bistable magnetic wires.

Manufacturing presses: All Wiegand wire is tested three times before it is cut into .33" strips and placed on vinyl adhesive tape in a pattern determined by computer-controlled machinery. For each order, the wire-encoded tape is spooled onto a tape feeder, and then fed to a tape-cutting-and-placing machine. This machine automatically cuts and places 12 strips of tape in appropriate locations on vinyl sheets (which are eventually cut into 12 cards), continuing with new sheets until the order is complete.

Once a vinyl sheet is prepared by the encoded tape and topped with artwork and lamination, it is pressure-temperature seated, die cut, and inspected- Depending on the order, and some cards also receive a special hot stamped card number. Before being shipped to the customer, the cards are inspected. Cards not meeting the inspection criteria are discarded and remanufactured.

Change in technology: The original Wiegand cards were somewhat thick. New credit-card thin sizes now allow Wiegand technology to be combined with other popular technologies, such as magnetic stripes; in addition, other manufacturers are developing proximity readers that can pick up Wiegand's low voltage power output (5 volt, 25 mA), while Sensor Engineering Corporation itself has also developed proximity technology.

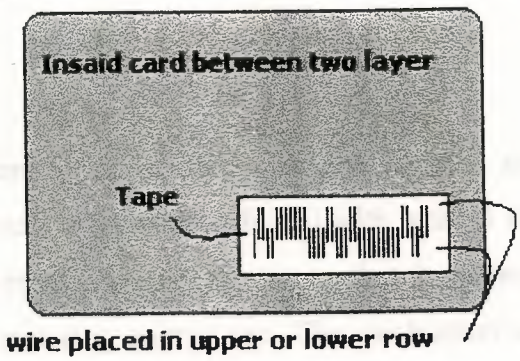


Figure 2.1.14 Wiegand Cards

Wiegand cards are regarded as very durable, secure, and reasonably priced. Unfortunately, because Wiegand cards are grafted at the factory, they take longer to manufacturer than other cards, forcing some EAC system managers to use other technologies because of lead-time considerations.

2.2 Barriers

2.2.1 DOORS

Function, governmental regulations, appearance needs, and cost alt determine a door's style and materials. Beyond these factors, doors controlled by EAC have the following in common:

- A door closing mechanism
- An electronically or magnetically activated lock
- Sensors (switches) that determine whether or not the door is properly closed
- Computerized control either in the locking device itself, or in a nearby, hidden control panel.

EAC requires that doorways, waits, and ceilings have a power source nearby and. in most cases, have adequate conduit and ducts in the walls or ceilings to hold electrical wiring. In areas where placing wire is difficult or prohibitively expensive, such as in an old elevator shaft, wireless EAC is substituted. EAC systems at so require wait or ceiling cavities large enough to contain control panels or wiring closets.

2.2.2 DOOR CLOSERS

Mechanical door closers are as important to an EAC system as the electronics that power the tocks. Door closers are spring-activated with tension strong enough to pull, doors completely shut after use, yet not so strong that it makes opening the door a struggle, or warps the door during normal use. The mechanism attached to the spring that guides the door shut is called the *arm.* Door closers fall into two main categories: concealed and surface mounted, a sample of which is seen on the next pages.

Concealed closer are usually used on doors designed for a clean, "no-hardware" look because the arm is hidden from view.

They can be difficult to adjust and service, however, because they are embedded into the top or bottom of the frame and door itself, requiring the door and frame to be

perfectly balanced. Hardware replacement is usually manufacturer-specific and requires exacting specifications.

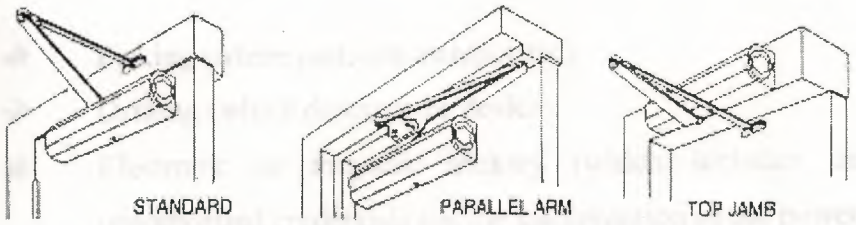


Figure 2.2.1 Door Closer

Surface mounted door closers are the most popular and fall into three main categories:

1. Regular-arm mounted
2. Top-jamb mounted
3. Parallel mounted

The most popular are the regular-arm and top-jamb styles, the latter of which is simply the regular-arm style installed upside down. The regular-arm and top-jamb door closers can stand the greatest deviation in door play. They are usually installed on the interior-side to reduce tampering, reduce weather damage such as rusting, and enhance the exterior appearance of the door. These types are shown in figure 2.2.1 above.

The *parallel style* is less popular. The arm on this closer slides parallel to the door, rattier than perpendicular to it. Unfortunately, it is difficult to service because it requires a very well balanced door. This type of closer is usually used when a jamb mounted closer must be installed on the weather-side of a door. It is thought to be more weather-resistant because its arm does not stick out and it can be shielded by a roof of some sort.

The series of illustrations on the next page show where door closers are commonly positioned on doors. Your understanding of these mechanisms can be greatly enhanced by observing the doors in public and private buildings.

2.2.3 ELECTRONIC AND ELECTROMAGNETIC LOCKS

The four most common types of locks used in EAC systems are the magnetic lock, the eclectic strike lock, the electric lockset, and the electric dead bolt. The strength of any

tock is determined by the way in which it can stop unauthorized entry that uses cleverness or force. Electronic or electromagnetic locks, therefore, must be strong enough to guard against:

- Picking (where parts are manipulated)
- Drifting (which destroys the device)
- Electronic or magnetic trickery (which includes the use of unauthorized credentials and the manipulation of the power supply).

EAC electronic and electromagnetic tocks are regarded as being either fail-safe or fail-secure and both have an important role in overall security:

Fail-safe:

The lock is **unlocked** when the power is off. This type of lock is usually used on a fire door. In the event of a fire, the locks can be released through the fire system or, if the power system fails, they unlock automatically.

Fail-secure:

The lock **remains locked** when the power is off. Power is required to unlock this type of lock and is usually used for normal locking situations.

2.2.3.1 MAGNETIC LOCKS

Magnetic locks secure doors through magnetic force and are always, fail-safe devices. They are ideal for high-frequency access control usage because they are totally free of moving parts, which reduces wear and tear.

Every magnetic lock consists of two components:

- Electromagnet
- Strike plate

The electromagnet is installed on the doorframe and the strike plate on the door itself. When energized, the electromagnet attracts the strike plate with a holding force ranging between 500 lbs. to 3,000 lbs.

All EAC systems require that some form of sensor reports whether a door is open or closed. Conveniently, many magnetic locks have that sensor built in, eliminating the necessity for a secondary sensor or switch.

The two basic magnetic lock styles are called:

- Direct hold, which is surface mounted on the secure-side of the doorframe and door.
- Shear (also called *concealed*), which is completely embedded within the doorframe and the door itself.

The large, *direct hold,* magnetic lock is ideal for use on poorly fitted doors and unframed glass doors because the two lock parts can be installed in rough proximity to each other. When energized, the electromagnet positioned on the frame attracts the strike plate on the door flush to its surface. This strong attraction doesn't require perfect horizontal or vertical alignment between the parts.

Smaller share magnetic locks, which are less than door thickness wide, are totally invisible to the eye when the door is closed. They are used when design and aesthetic considerations dictate that the lock be completely hidden. Concealing reduces the potential for tampering because the electrical wiring is completely enclosed within the doorframe. The narrow surfaces on the shear electromagnet and the strike plate require precise alignment. A small bracket is often used on the frame to stop door travel so that these surfaces line up.

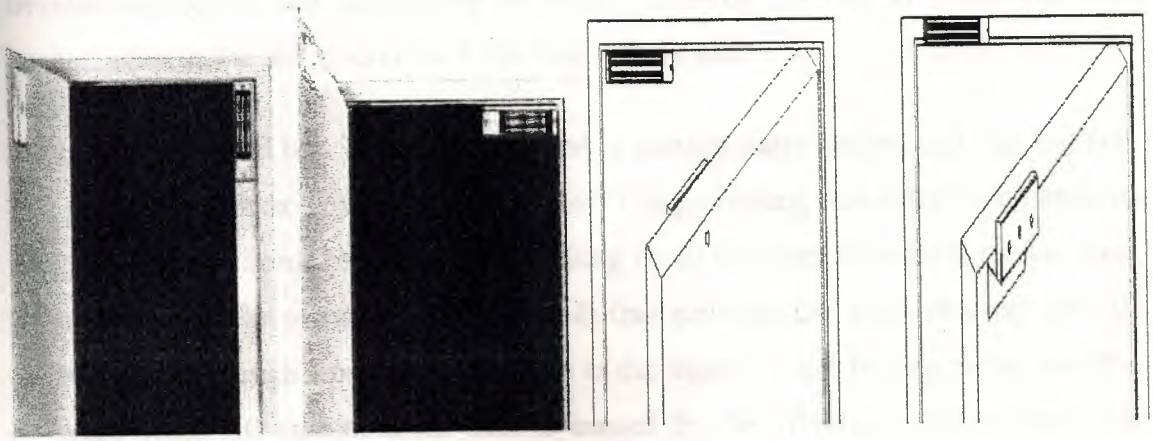


Figure 2.2.3 Magnetic lock

ANSI standards have defined three grades of magnetic locks. Grade one, which holds 1,500 pounds, is designed for medium security. Grade two, at 1,000 pounds, is for light security, and grades three. 500 pounds, simply holds a door shut. Most 180-pound men can force open a door equipped with an 850-pound magnetic lock.

As the holding attraction increases to 2,000 or more pounds, a magnetic lock will stay joined even when the force of a blow is strong enough to shatter the door it secures. Consequently, in addition to the strength of the lock itself, the material strength of the door, frame, and wall must also be considered when planning a high security door.

2.2.3.2 ELECTRIC STRIKE LOCK

The electric strike lock is the most popular EAC locking device on the market and can be set up as either fail-safe or fail-secure. Its popularity stems from the fact that it comes in a wide variety of sizes and can replace existing mechanical locks without a great deal of difficulty. The strike, which is the eclectically controlled portion of the lock mechanism, is mounted in a doorframe (jamb) and does not require wiring through the door itself.

The electronic strike contains a bolt pocket, which is the indent that holds the protruding latch bolt or dead bolt secure in the frame. To open, the strike rotates away from the pocket, providing a path for the bolt to escape. This rotating side is called a *pivoting lip or keeper.* The latch bolt or dead bolt housing itself is mortised (embedded) in the door.

Latch Bolt: The latch is a spring-loaded, beveled bolt. When the door closes, the beveled-side of the bolt slides over the strike, allowing the bolt to retract and then expand again in the bolt pocket once the door is fully shut.

Dead bolt: The dead bolt is a solid metal rod or rectangularly shaped bolt that has only two possible positions: protruding or retracted. The protruding bolt enters or escapes the bolt pocket in the frame only when the pivoting lip of the electric strike is rotated away from the frame. The solenoid (magnetic coil) that activates the strike receives low AC or DC current through a power cord hidden in the frame. A soft buying noise can often be heard when AC current used. This is caused by the vibrations of the alternating current pushing and pulling the solenoid 60 times per second.

Figure 2.2.4 Door Locks

Electric strikes and their rotated latch boils come in a variety of styles suitable for installation on wood and metal frames. Each frame type, however, poses its own demands. A few of the many things to consider include:

Wood frames can be weakened from the hollowing out required for installation of the electric strike and need additional anchors or brackets to protect the took itself against forced-entry attempts.

Tubular aluminum frames might be too shallow to accept an electric strike assembly. Hollow metal frames might be too weak to resist a forced entry, or else were filled with cement or plaster when installed, prohibiting the installation of the electric strike at a later date.

2.2.3.3 ELECTRIC LOCKSET

The electric lockset is very similar to a mechanical lockset and is available in cylindrical and mortise styles. The difference is that an electric solenoid (magnetic coil) replaces the mechanical action provided by a standard key. In addition, only the electric lock has fail-safe or fail-secure operational modes.

- *Cylindrical Lockset:* These are characterized by a doorknob or handle on each side of the door, which are joined by a cylinder that controls the locking mechanism.

- *Mortise-style Lockset*: These are characterized by a lock, which is housed in a rectangular metal container that is embedded at the edge of the door and is often enclosed within the door's thickness.

Electric power is brought to the lock by threading wire from the frame through the door. Electric hinges (or pivots) completely conceal the wiring path when aesthetics are a consideration. Flexible cable loops are used when a seamless appearance isn't necessary and must only be exposed on the secure side of the door.

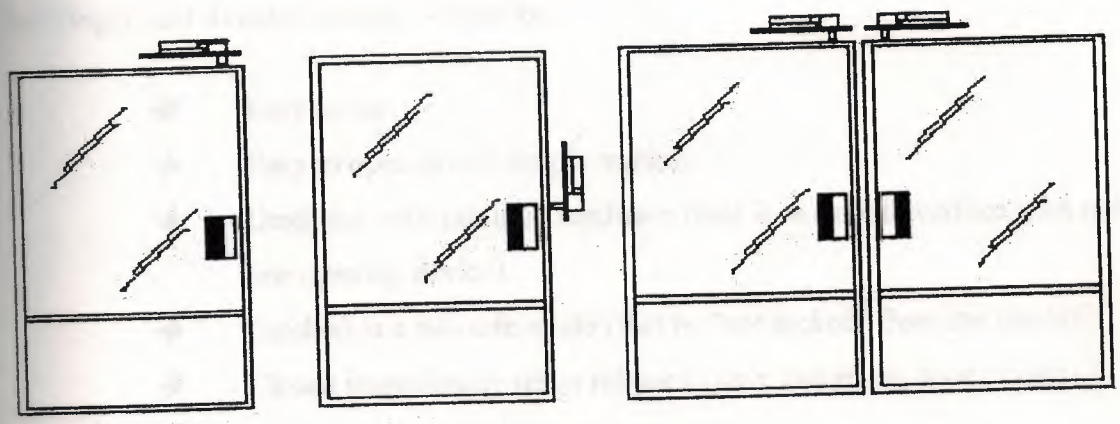


Figure 2.2.5 Electrical Lock locations

2.2.3.4 ELECTRIC DEAD BOLT LOCK

The electric dead bolt refers to the blot design and is used as an alternative to a magnetic shear lock for doors that swing in two directions and double-doors. The electrically powered dead bolt is fitted into either the jamb or the door itself and when activated, it protrudes (shown on previous page) or swings (below) into a mortised strike plate on the adjoining surface.

To increase holding strength, more than one set of electric dead bolts can be installed per door. Dual sets are common on large doors, as well as on both double-hung doors that swing away from each other from a center point. By installing electric dead bolts in the door header (top) and at the base, each door is secured and resistant to force.

The dead bolt does not give way with a spring action. Once it is clicked in place, it stays in place until unlocked. Although electric dead bolts can be set in fail-safe or fail-secure modes, the majority of building and safety codes prohibit them for egress path use in high-rise buildings. Manufacturers have developed standard-compliant locks, but they are not in common use for these applications.

2.2.4 FIRE EXITS AND ADA RULES

The rules surrounding fife exits sometimes conflict with the purpose of EAC. No one wants to be trapped inside of a building during an emergency. This means that specific exits—doors leading to and from stairwells, between firewalls (and adjoining buildings), and directly outside — must be:

- Easy to see
- Easy to open in one simple motion
- Designed with minimal hardware (that is, a smooth surface with only one opening device)
- Latched in a fail-safe mode (that is, "not locked" from the inside)
- Closed immediately when released (have automatic door closers)
- Constructed out of fire-rated materials

Here is how fire codes effect EAC: In this simple example, the door is secured by a magnetic lock that can sense when the door is closed. To enter, a card is swiped through a card reader, which sends the information found on the card to a control panel. If the card is valid, the control panel sends the instructions to unlatch the lock.

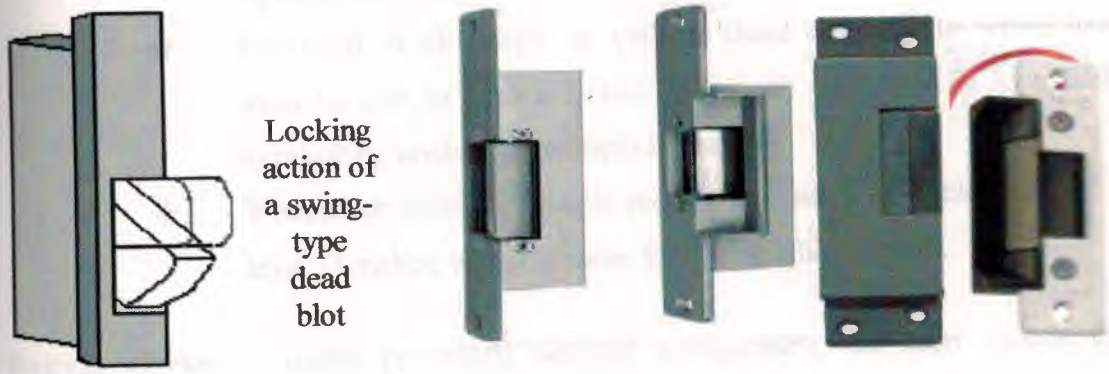


Figure 2.2.6 Door Strikes

After the door is opened, the "door closed" sensor tells the control panel whether or not the door returned to the closed position. If the door does not close within a predetermined amount of time, the control panel triggers an alarm. Whether or not the door closes as scheduled, the EAC database saves the pass code user's name as well as date and time of his or her access. This creates an important trail of information! Exiting, however, creates a different set of circumstances.

The Exit Bar in this example sends a signal to the control panel. The control panel then releases the magnetic lock. Unfortunately, this action leaves no record of the person who pushed the door open, because exiting bypasses the EAC recording system.

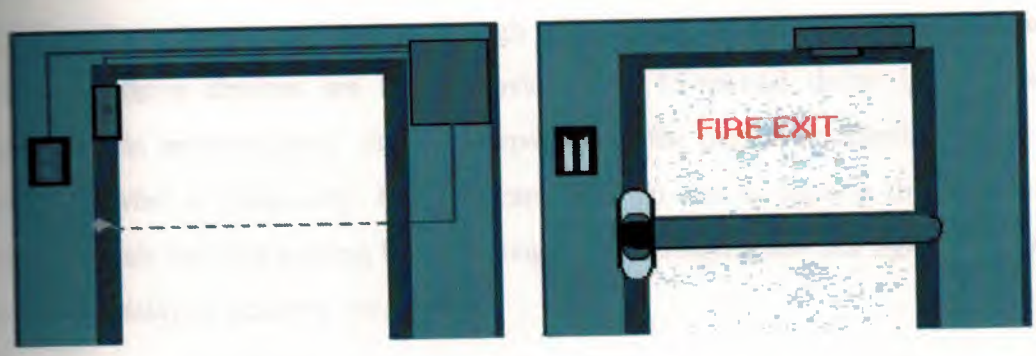


Figure 2.2.7 Door interior and Exterior View

The Americans with Disability Act (ADA) imposes additional restrictions on door design, lighting, and usage. ADA requires that:

- Blind and sight-impaired people must be able to touch specific types of door hardware and understand what to do next.
- Hearing and sight impaired people must be able to easily see exits. Consequently, there are rules regarding the size and color of exit signage, including the use of strobe lights.
- Physically weak people as well as those confined to wheelchairs must be able to push a locked door open with little or no trouble, eliminating knobs and multiple latches.
- Wheelchair confined people require doorways with clearings of at least 32 inches, which is room for a wheelchair to pass.

Exiting, obviously, opens previously secured passageways. To alert guards that someone is leaving, an egress button is sometimes found on the opposite side of a door protected by EAC.

When pushed, this button disarms an alarm and tell the control panel that door usage is in compliance with the system. Egress buttons, unlike card readers, are subject to fire code regulations that forbid them to control locks. Egress buttons, therefore, can be bypassed without hampering travel, although doing so will trigger an alarm.

A "delayed egress" device on a fire exit door, however, postpones unlocking for up to 15 seconds. Pressing this device sends an alarm to a guard station and informs the guard that an exit attempt is being made. At this point, the guard can see the exit event on CCTV, talk to the person leaving through an intercom, or simply run to the scene if neither of those devices are there. Obviously, a 15-second delay in exit can be frightening in an emergency situation, especially if the person attempting egress does not know what is happening. Extreme care must go into designing this type of exit system, which includes posting bold warning signs. *A single-push bar egress is required even when delayed action is used.*

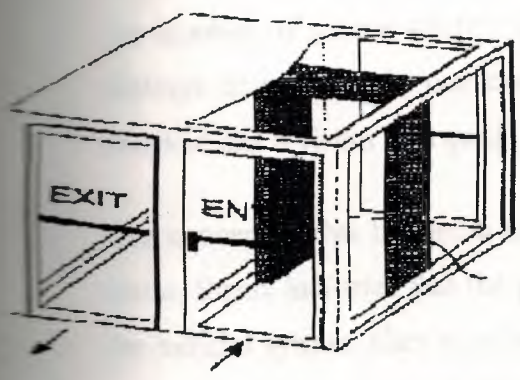
It is very common to see fire code violations and when you do, it if our strong recommendation that you immediately report them to the fire department. The National Fire Protection Association (NFPA) code clearly states that only one action can be used to unlock a door with exit or fire exit hardware. Many companies, unfortunately, install additional locks, if the fights fail during an emergency, the extra burden of finding those locks could cause confusion, panic, and death. Double-exit doors, where one door must be opened before the other is released, are forbidden, in the case where the doors have an overlapping astragal (center strip), which normally requires one door to open, before the other, hardware must be installed that allows either door to open quickly.

Locking arrangement on double-exit doors is tricky and mistakes are often made during installation. Always check to see that each door can be opened quickly, regardless of the other's position. If one doesn't open, the setup is in violation of fire code. Heavy double exit doors are commonly seen in shipping and receiving areas. The temptation is to install additional handles to better distribute the weight of the door in order to make opening easier. This solution, however, would be in violation of fire codes, in the event of an emergency; it might not be obvious which handle is associated with the latch, which could, in turn, cause confusion and panic.

Stairwells pose additional security concerns. Fire codes require that people in stairwells be able to exit freely at any floor. Unfortunately, in some high-rise buildings, these exits open into unrelated businesses. The temptation is to bar the exits to stairwell doors so that uninvited guests don't get in, which, of course, is in violation of fire code. As you

see from this brief overview, building codes, fire regulations, and ADA requirements are detailed and complex.

2.2.5 MANTRAPS (SECURE VESTIBULES AND TURNSTILES)



Mantraps-Double Vestibule Style

Many devices may be present including motion and weight sensors as well as CCTV and an enunciation (intercom) system

Figure 2.2.8 Metal Detector

Tight access control is obviously very desirable in high crime areas. Financial institutions, hit hard by increased robberies, are exploring ways to quickly screen visitors. Many European and South American banks, for example, are using glassed-in mantraps, called "double vestibule (hall) portals," as seen in the illustration. These are used to unobtrusively examine visitors prior to admission, keep nonconforming people out, and make sure that two people do not enter at one time (piggybacking) as described in the following procedure:

2.2.4.1.1 Entering a building:

With the exterior (outside) door unlocked and the interior door locked, sensors and a metal detector determine whether one person is present in the "enter hall" and is free of weapons. When access is granted, the exterior door locks and simultaneously, the interior door unlock.

This allows the occupant to enter into the building while at the same time preventing piggybacking. The system resets itself when the interior door is shut, allowing the next person to enter from the outside.

2.2.4.1.2 Leaving a building:

The person exits through the "exit hall." which reverses the door locking and unlocking process as reported above: however, does not include a weapon detection sensor. Strict access control in this housing project has greatly reduced the number of people freely roaming the halls and has increased the tenants' feelings of security. In one case where a rape did occur, EAC records were cheeked and a visitor was quickly identified, found, and hauled off to jail.

One concern is that biometric scanning might interfere with American civil liberties. Smart indicates that the palm prints used by this system are not used in the judicial system. Care must be taken when installing a mantrap, however, to make sure that it meets alt fire and safety regulations and it does not interfere with the public's civil rights.

Revolving Doors: Revolving doors can also be used to reduce piggybacking and pose as mantraps. Used with or without an EAC pass code, one section of the area can be set up to sense for metal detection and other conditions. If all conditions are met, a person can pass through the system. If conditions aren't met, the interior doors remain locked and the person is directed back to the outside. As revolving doors are confining and have been known to cause feelings of panic, extreme care must be taken when using this type of system to meet all fire and ADA regulations.

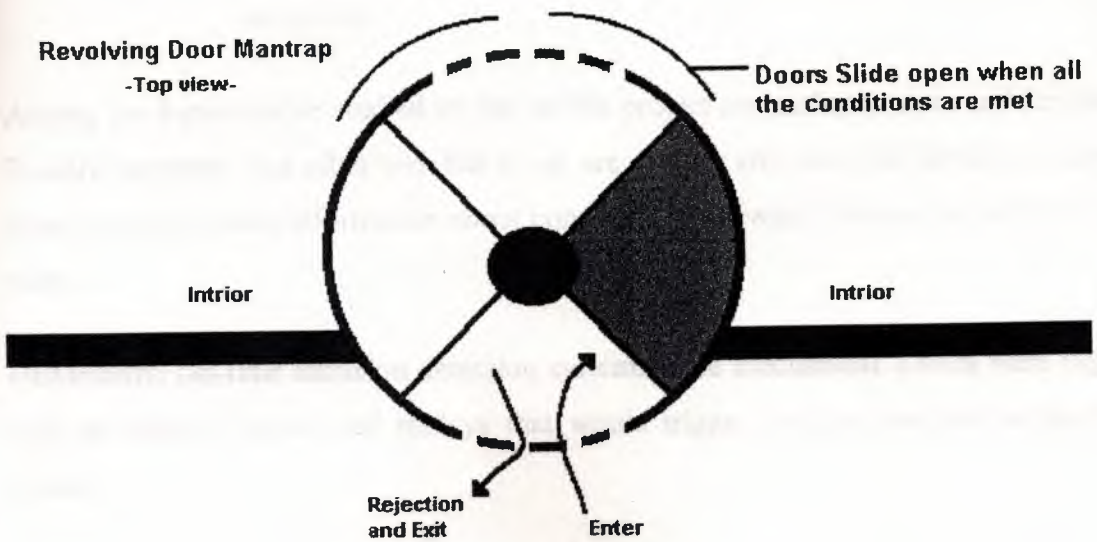


Figure 2.2.9 Revolving Door

2.3 Sensor (Information Reporting Devices)

2.3.1 SENSORS PROVIDE INPUT FOR ELECTRONIC DECISIONS

The "control" in electronic access control (EAC) is accomplished by the relationship between three types of devices, which are:

Detection Devices: These devices detect and report changes in one or more conditions. They are regarded as *inputs* because they report "into" a management device.

A Management Device: This is a specialized computer that receives information from detection devices, compares that information against programmed information, and decides what to do. Then issues instructions to action devices.

Action Devices: These devices carry out the instructions provided by the management device. They are regarded as *outputs* because the management device sends information "out to" them.

In a large EAC system, detection and action are managed electronically through control panels. These panels:

- Accept input from many detection devices.
- Issue instructions to many action devices (outputs).
- Communicate with other control panels and computers throughout the system.

Among the inputs we've studied so far in this project are authenticators and keypads. Equally important, but often invisible to us, are *sensors* and *detection device*. In secret, these devices provide information about conditions upon which electronic decisions are made.

Historically, old-time intrusion detection systems were mechanical. Doors were rigged with all kinds of levers and pulleys that would trigger bells and/or start a chain of events:

Example: To deter intrusion in castles, stones would drop through shoots, spears would fly out of walls and trap doors would open up, tumbling unauthorized people into pits full of snakes (or bodies).

Fortunately, electronically powered intrusion detection systems (also called *burglary detection systems*) alert guards to a wide variety of issues without destroying an unaware visitor. Today. EAC uses the information reported by sensors to make informed decisions.

Example: When an EAC controller receives a signal from a door contact sensor, it knows that a door was opened. If that signal was received after a proper signal from an authenticator, the controller regards the situation as being OK. If the contact sensor does not close within a specified time, the controller signals an alarm, which can include ringing bells, flashing lights and warnings seen on central station monitors.

Here are a few examples of how controllers use sensors to monitor situations:

- Elevator Door: An EAC authenticator determines who can select a given floor. Contact switches determine whether an elevator door is completely opened or closed. While closing, one or more photo electronic sensors determine whether people and/or objects are between the sliding door and the frame. Finally, pressure-sensitive sensors determine whether someone or something is attempting to hold the door open.
- Exterior Door in a Chemical Plant: An EAC authenticator determines who can access this door. One or more contact switches in a doorframe determine whether the door is opened or closed. A contact switch that is part of the latch determines whether the latch is fully extended. Chemical and/or oxygen sensors inside the plant sense whether a chemical spill has taken place. If one has, the door will not unlock, even for an authorized person trying to enter. Photoelectric sensors around the door determine when people or objects are in the area. These sensors start a video recorder and/or turn lights on so the camera and visitor can see well.

The ways sensors are used in a facility depend on overall security requirements and management needs. At minimum, a door controlled by an EAC system requires at least

one door contact sensor (input), an authentication device (input), and an electronically activated lock (output).

2.3.2 SENSOR CATEGORIES

2.3.2.1 SENSORS ARE EITHER ACTIVE OR PASSIVE.

Active sensors introduce energy into an area, which is interpreted by a receiver. When the receiver senses a change in energy, it registers an alarm. Break-beam sensors are a good example of this type. Here, a transmitter focuses light, which is energy, into a receiver. When the receiver notes a change in light, such as when someone passes by and "breaks the beam." it triggers an event.

Passive sensors measure changes in an environment over time. A good example of this type of sensor is a thermostat which, when the temperature drops, triggers a furnace. Likewise, passive sensors can detect noise and vibration levels within an area and indicate when those levels are outside a given range.

Sensing devices commonly used for EAC generally fall into the following categories. (Check the sensor glossary at the end of this chapter for specific types of sensors.):

- *Mechanical sensors* have simple levers or rods that, when pulled or pushed, move a switch that reports an event.
  Example: An *egress* (exit) button used on the secure side of a door controlled by an authenticator is a mechanical switch that, when pushed, creates a electrical circuit that tells a control panel that opening the door is legal. If the door is opened, but the button isn't pushed, other sensors in the system announce an alarm.
- *Electromechanical* sensors depend on a specific flow of current to activate a mechanical device.
- Capacitance sensors generate an evenly charged electrical field between two antennas. When the energy level in that field changes due to an intrusion in the area, an alarm is triggered.
- Vibration sensors measure subtle environmental motion, which, when motion reaches a predefined level, register an alarm.

- *Audio sensors are similar to vibration sensors, except they measure* sound waves (audible, which we can hear and ultrasonic and microwave, which we can't).
- Light sensors measure the degree of light in a given area. Active light sensors are used in break-beam devices wherein the interruption of the light beam between a transmitter and receiver results in an alarm. Passive light sensors measure environmental light.

Additional sensor categories exist for environmental monitoring, such as for fire, flood, humidity, oxygen and chemical detection, to name a few. All these sensors can be tied into a controller of some type (including some EAC controllers) to automate a chain of events. Sensor applications can be quite complex. In fact, many systems maintain redundancies, which means that one variety of sensor checks on another in order to double-check intrusion reports. With that in mind, the brief list that follows shows what types of sensors are commonly used within specific areas.

Yards - External Perimeter: Fence alarms (conductive wire sensors), photoelectric beams and microwaves.

Building Perimeter: Exterior door contacts and overhead door contacts (contact switches) and glass break detectors.

Interior Detection: Passive infrared, microwave, dual motion technology, photoelectric beams, interior door contacts, mantrap components, and glass break sensors.

The section that follows is a Sensor Glossary, which provides an overview of the types of sensors used in EAC and security systems.

2.3.3 SENSOR TECHNOLOGY GLOSSARY

This glossary is meant to provide an overview of sensing technology terminology commonly related to EAC and intrusion detection systems. Within a sensor type, there can be many variations. Check with sensor manufacturers for details. There are many sensor systems not mentioned in this glossary that are commonly used in industry. We recommend that you become aware of them. The more you know, the more resourceful you'll become when designing a system.

2.3.3.1 ACTIVE SYSTEM

(*Example:* Capacitance Detector) The word "active" refers to a sensing system that introduces energy through a transmitter into an area for interpretation by a receiver. The receiver is set up to expect a specific energy level. Any changes to that energy level indicate a change in the environment caused by an invasion of some type. The opposite is a passive system, which simply reads the environment "as is" and makes decisions based on a range of outcomes, such as increased noise or impulse.

2.3.3.1.1 Audio Sensors

These sensors are similar to ultrasonic and microwave sensors, except that the receiver bases its judgment on sounds that can be heard by the human ear, rather than a high frequency pitch. Reception sensitivity can be set to detect explosions, gunshots and even human conversation. (See *Ultrasonic and Microwave sensor).*Audio sensors are usually used in connection with intercom systems and can amplify low noise, such as whispering, for transmission to remote guard stations. Two types of audio sensors exist. The first is sensitive to sound at any frequency within a range. The second is sensitive to sound at a specific frequency. In high background noise applications where vibration sensors are used, *discriminator sensors* are also installed as a redundant backup. These devices sense common noise and cancel the effect of these vibrations, reducing false alarms based on common occurrences. (See *Vibration sensors*. Page 55)

2.3.3.1.2 Capacitance Detectors (Proximity & Capacitance Detectors)

This type of sensor is used to monitor large areas by maintaining a consistent energy level, called an *electrical field*, between two electrically charged antennas. The air in the electrical field becomes a *dielectric space*, meaning that it has a constant, predefined energy level. When the energy level changes due to an intrusion, an alarm is sounded. While capacitance sensors are not affected by noise or vibration, they are very sensitive to atmospheric changes and consequently, are most commonly used indoors. This type of sensor is relatively easy to set up by taping antennas of copper tubing or wiring to windows, walls, doorframes, etc. As long as the energy within the room between these

antennas remains constant, the area is secure. Intruders, however, absorb part of the radiated energy, causing a difference in *capacitance* (electrical charge), which, in turn, triggers an alarm.

2.3.3.1.3 Conductive Wire Sensors and Fiber Optics

Metallic tape, once commonly seen on glass doors and large windows, carries a *current* (indicting conduction) that completes a circuit. If the tape is broken, an alarm results. Unfortunately, although it is easy to apply tape to glass surfaces, it is also very easy to scratch through the tape, causing a complete split that breaks the electronic circuit. This renders the system useless and in need of continual repairs. Another type of conductive wire sensor is a fine, hard-drawn copper wire that is woven into screens, grids and other lacings (such as used in fencing) and mats. Changes in tension on the wire, such as caused by someone pressing on a surface, changes current flow, triggering an alarm. In newer systems, fiber optic filaments are used, with light transmission replacing electrical conduction. The principle, however, is the same as with conductive wire. Fiber optics eliminates corrosion problems common with metallic materials and is especially useful in outside applications.

2.3.3.1.4 Discriminator Sensors

See *Vibration Sensors*. Also see *Audio sensor, page 55 & 49.*

2.3.3.1.5 Dual Motion Detectors

This refers to a redundant system in which one type of motion detection system backs up another. Either system can be used by itself, but when used together, they provide a broader, more complex range of coverage. Generally a dual motion detection system combines passive infrared (PIR) and microwave (MW) motion detectors, or PIR and ultrasonic (US) motion detectors.

2.3.3.1.6 Fiber Optic Sensors

See *Conductive wire sensors and Fiber Optics, page 50.*

2.3.3.1.7 Fire and Environmental Sensors

Environmental sensors can be tied into electronic access control systems; however, local fire, building and police authorities determine usage and insurance companies may insist on additional requirements. Among common sensors used for environmental purposes are smoke detectors. Heat/temperature sensors, chemical spill detectors, water flow monitors and moisture detectors.

2.3.3.1.8 Flexible Cable Sensors

See *Conductive Wire Sensors and Fiber Optics, page50.*

2.3.3.1.9 Foil

See *Conductive Wire Sensors and Fiber Optics, page 50.*

2.3.3.1.10 Glass Break Sensors

The original glass break sensors used conductive foil taped along the side areas of the glass. As this type of sensor was easy to scratch, it caused many false alarms and is now considered obsolete. (See *Conductive Wire Sensors and Fiber Optics, page 50.*) Today, a popular sensor used to detect glass breaking is a small capsule containing liquid Mercury (a conductive metal), which is glued to the glass. Once the glass breaks, vibrations and/or dropping causes the Mercury to flow across the capsule, closing a circuit, which, in turn, sends an alarm. Sensors that fall in the sound and vibration categories are also used for glass. These sensors can be tuned to audible or vibratory frequencies that match the frequencies of glass breaking. (See *Vibration Sensors, page 55.*)

2.3.3.1.11 Infrared

This refers to the part of radiation within the full radiation spectrum that falls below visible light. It can't be seen by the human eye, but it can be felt as heat. Sensors that detect infrared heat detect the presence of warmth, such as that radiated by a human being or animal.

2.3.3.1.12 Infrasonic Sensors

There are sound sensors that detect sound below that detectable by ear. They can, for example, "hear" the sound of air moving into a room when a door is opened. They are not widely used today, however, because of false alarms.

2.3.3.1.13 Intrusion Switches (Balanced Magnetic Switches, Magnetic Switches, and Electrical Intrusion Switches)

This type of sensor can be mechanical (similar in concept to a rocker switch used to turn on lights) or electrical. It has two parts, typically one that moves or changes state and one that interprets the change. *Electrical intrusion switches* are commonly installed on the secure-side of windows, doors and other openings. Under normal conditions, both parts of the sensor touch, creating a circuit through which current flows. When separated, such as happens when a window is illegally opened, the flow of current is broken, signaling an alarm. A variation of this type of switch is the *magnate switch.* This switch, which is an electrified plate, is mounted on a fixed frame, while a non-electrified metal plate is mounted on a moveable object, such as a door or window. When the two plates contact, a stable magnetic field registers. When separated, the magnetic field is disturbed, causing an alarm.

2.3.3.1.14 Light Sensors (Break-Beam Sensors, Infrared Sensors, and Laser Sensors Photoelectric Sensors)

The "photo" in the word "photoelectric" refers to light. Light sensors respond to changes in light level and are used in a wide variety of industrial applications in addition to EAC. One type, called an *ambient light sensor*, measures daylight. When this sensor detects that daylight is dimming, a controller responds by turning on lamps. If timing devices do not control lamps, then ambient light sensors are most likely being used. You usually can tell when one is present on a light pole by seeing a small dome on the very top of the lamp fixture. In security applications, photoelectric sensors are commonly used. Known as *break-beam sensors*, they consist of two parts: A transmitter and a receiver. The transmitter beams a tightly focused beam of light at the receiver.

When someone passing between the transmitter and receiver breaks the beam, the receiver notes the change, and then triggers an event. These events can include sounding an intrusion alarm, triggering video recording, or opening a gate when someone or thing approaches, then shutting the gate as soon as it's clear.

Photoelectric sensors use specific types of light. These include light generated from specially designed incandescent bulbs. Infrared light or laser light. No matter what source is used, the light transmitter is adjusted to tightly focus the light beam on the receiver. Depending on the type of sensor, intruders can defeat break-beam sensors by fixing a flashlight on the receiver. To solve this problem, light transmission is commonly *modulated* (pulsed) in a way that cannot be duplicated by a constant light beam from a flashlight. Technology is improving the way photoelectric sensors work. Zigzagged light paths rigged through a system of mirrors can track intruders, for example. In addition, laser beam sensors are increasingly replacing infrared due to greater beam strength and focusing capability.

2.3.3.1.15 Metallic Tape

See *Conductive Wire Sensors and Fiber Optics, page 50.*

2.3.3.1.16 Microwave Sensors

See Ultrasonic and Microwave Sensors, page 54.

2.3.3.1.17 Motion Detectors

See Ultrasonic and Microwave Sensors. Also see Video Motion Detectors and Dual Motion Detectors, page 54, 55 & 50.

2.3.3.2 PASSIVE SYSTEM

(*Example:* Passive Infrared.) The word "passive" refers to a sensing system that measures changes in the environment over time. This could include changes in infrared light, temperature and humidity normally found within an environment. The opposite is

an *active system*, which actively introduces energy into the environment through a transmitter for interpretation by a receiver

2.3.3.2.1 Pressure Mat SENSORS (Mats (pressure))

This type of sensor mat is used in mantraps, entrances and exterior yards. They trigger an alarm when a specific weight (from 5 to 20 pounds per square foot) presses on the surface. Fiber-Optic mats are preferred for outdoor or moist applications. Also see *Conductive Wire Sensors and Fiber Optics, page 50.*

2.3.3.2.2 Sonic Sensors

See *Ultrasonic and Microwave sensor*; also see *Audio Sensor, and Infrasonic Sensors, page 54,49 & 52.*

Timed Applications

When a control panel receives an alarm from a sensor, it may time how long the sensor regains in an alarm state. If a sensor returns to normal within a predetermined time span, no alarm is sounded. Timing is used to measure the travel time a person or vehicle requires when passing through an access point. If the time set is too short, false alarms occur. If the time is set too long. It does not become obvious when a door or gate is improperly held opened.

2.3.3.2.3 Ultrasonic (US) and Microwave (MW) Sensors

These sensors measure ultrasonic sound and microwave energy. Ultrasonic sonic is lower on the Frequency scale. But above our threshold of hearing. While microwave energy is higher than ultrasonic and is regarded as electromagnetic energy. Ultrasonic and microwave sensors work on a similar principle. They broadcast sound at a specific frequency, which is picked up by a preset receiver. As the broadcast is spread over a specific area. Anything moving within that area disturbs the frequency pattern. If the receiver picks up a frequency that is different from what it experts, an alarm is sounded. The broadcast frequency can be adjusted to allow for probable disturbances. Such us

small animals or birds. It can also be set to distinguish the stride fate of a moving person, sounding an alarm within four consecutive steps. Ultrasonic servers are normally used to monitor interior spaces because their frequencies are easily disturbed by the environment. Their frequencies must be adjusted with regard to the presence or absence of furniture, as materials absorb sound and alter frequency wavelengths. Generally, interior ultrasonic sensors are stable. Air currents caused by air conditioners, however, can set off false alarms. Microwave sensors are better suited for outdoor use and are employed in sensing the sky at airports as well as sensing land use around remote prisons and military bases.

2.3.3.2.4 Vibration Sensors

In stable environments, this type of sensor samples vibration rates. Should the normal atmospheric vibration rate change, such as caused by cutting, chiseling, or ripping, an alarm is rounded. This type of sensor is well suited for installation on masonry walls because masonry is naturally low in vibratory properties, thus reducing the probability of false alarms. In applications with higher vibratory background noise, *discriminator sensors* are also installed. These devices sense common noise and cancel the effect of these vibrations, reducing false alarms based on common occurrences. (See *Audio Sensors, page49.*)

2.3.3.2.5 Video Motion Detectors (VMD)

This sensor electronically analyses CCTV camera images. It detects changes that are judged large enough to warrant an alarm. In a digital system, this detector notes changes light level from one set of *digital pixels* (square units) in a TV frame to similarly placed pixels in the next. An intruder casting a shadow over the area, wearing clothing with a different light refraction than the background materials and/or illuminating the area with a flashlight would cause this detector to sound an alarm. In an analog CCTV system, the detector compares large areas in one frame to the same areas in the next. Analog comparison is mere susceptible to false alarms caused by lighting changes and camera vibration than in a digital system, however, and is not recommended for outdoor applications.

2.4 Computer (Software, Hardware And Intelligent Networks)

2.4.1 WHY YOU SHOULD UNDERSTAND COMPUTERS

Many devices used in electronic access control (EAC) systems are controlled by microprocessor chips. The most useful microprocessor-driven devices; allow us to customize their behavior through software instructions. They can also communicate with other devices and calculate a wide range of information. We commonly call these devices *computer*.

The three main types of computers used in a large EAC system are the:

Supervisory Computer is a personal computer (PC), with monitor and keyboard, used to manage an EAC network. It issues information and instructions to other computers on the network, receives reports from those devices and stores information about ongoing events.

Controller (or Control panel) The controller provides a direct link to electronic authenticators, locks, sensors, gates, etc., installed at the site. When connections permit, it can communicate with the supervisory computer, hut does not normally have a dedicated monitor or keyboard.

Switcher The switcher controls closed circuit TV cameras and video taping activities and are commonly linked to sensing devices. Like a controller, it can communicate with the supervisory computer, but does not normally have a dedicated monitor or keyboard.

Few security professionals, unfortunately, have a formal education in computer technology, even though they've alt used software. This forces them to rely on advice about computer hardware from non-security professionals; advice that may be at odds with actual needs.

2.4.2 THE GRAPHICAL USER INTERFACE

The GUI presents vital information to the user in a simplified form without losing the importance or impact of the message. By using the mouse, an operator can select activities or options from context-sensitive menu pads located at the left-hand portion of the screen. The menu pads change from a light gray to dark gray when they are selected and are organized in a descending hierarchy to keep the operator from becoming "lost"

in the system and to present only the necessary actions on screen. On screen options can vary depending on the access level of an operator. This enables the System Administrator to "block out" options and actions for those operators who do not possess a "need to know". Such control is discreet since these "blocked" areas will never appear on screen for an operator who is excluded from working with them.

An instruction line at the top of the screen provides a brief explanation of the action that will result when a highlighted menu pad is picked. Every menu pad pick and all fields in the data forms offer a more thorough explanation of their function and use by accessing the on-line help feature with one keystroke. The workspace area, located in the center of the screen, permits a user to enter data into the system using reconfigured forms or monitor the facility using site-specific maps with interactive icons.

The EAC software offers object oriented hardware solutions to devices in the field through an operation's actions at the workstation. In the monitoring mode, icons represent Card Access or Site Security devices. The state of these devices is indicated by the color of the icon. (e.g. green for secured, red for alarm or orange for a broken device). An operator is apprised of a change in the state of a hardware device by the change in color of an icon. Action can then be taken using the mouse and the on-screen icon and appropriate menu pad picks appearing on the screen.

Incoming alarms are displayed at the bottom of the screen and site-specific maps, which contain the icon in alarm, will appear automatically simplifying the steps an operator must take to address the situation. In the event of multiple alarms, the system relies on a user-generated list of priorities to determine the order in which alarms are reported to an operator. The system stores in memory a list of the last 500 events to assist an operator in searching or past events.

The concept of simply tracking the status of alarms in the field through interactive icons is carried into the system software itself through the self-diagnostic feature. The EAC relies on a network of workstations and processors in the field to carry out its functions. These devices reside on a LAN. The integrity of the LAN as well as the various software programs that support the system and allow it to carry out commands are also represented through graphical icons on the screen. Should a link between two

processors become broken or a segment of the software fail, an operator is notified and appropriate steps can be taken to maintain security while the situation is rectified. Therefore, the internal software integrity is assured in the same manner as the field devices.

The software supports the capability to simulate various events such as an alarm, tamper, void card or valid card. Such simulations can be used to verify whether a point programmed into the system, such as a card access door, will function as planned. An operation can verify the function without having to be physically at the door. In the case of a card access system, however, it is often necessary to determine if a certain card is valid at a given door. With the simulation tools, an operator can "present" a card to a door by inputting the card number in a form that appears on screen.

The system permits any number of icons to be grouped together and given their own specific icon. For instance, a group of doors could be gathered together and with one-operator actions, they could be locked or unlocked. An individual item could be present in several different groups depending on what categories the system operator desires to control. These groupings can include communications links, field processors and software programs as well as doors or card readers.

The EAC also supports a graphical drawing program, which enables users to build their own site maps and icons as well as determine their location. Thus, a representation of the site or area to be monitored and controlled is created using the internal line drawing package or by importing CAD/DXF files into the system.

The GUI simplifies data entry by providing data forms for the various system functions. These forms contain spaces, which are filled in using the keyboard to add Card Access Doors to the site, create Access Levels or enroll personnel into the database. The forms serve as a template to insure information is correctly entered into the system and to avoid duplicate entries. The EAC uses this information to determine relationships between system components and personnel. The data entered into these forms is entered into the system directly and needs no further modification by the operator. These forms also assist an operator searching for records by allowing for specific values for descriptors to be entered into the appropriate spaces. For instance, if an operator wished

to locate all personnel in a specific department or building who were C.P.R. certified, he could limit his search by filling in the fields indicating department worked and specific skills.

2.4.3 ACCESS CONTROL

The EAC excels in its task of Access Control and Facility Management through the use of its speed and flexibility to carry out multiple tasks at once. Access Control is simply granting access to personnel depending on their relationship to certain parameters such as the need for personnel to gain access to an area versus the needs to limit access to areas for security or other reasons. These relationships present a complex matrix of options and actions for which the EAC is well suited.

In addition to determining who can access an area at what time and on what days, the system is capable of employing more sophisticated levels of control such as Area Control, *AntiPassback* and the Two Man Rule. Area Control is simply the establishment of an area that a cardholder must present a card to both enter and exit. Typically two or more card readers are used and a specific access level is often established for the area. A cardholder is not permitted to reenter an area if he did not present his card to exit. This can assist in keeping track of personnel in an area would an evacuation become necessary.

Area Control also can be used to create an Anti-Pass back atmosphere that essentially prohibits a cardholder from entering an area and then "passing" his card back to someone else to present to the card reader to gain access. Such positive "one man, one card" control limits unauthorized access to secured areas. The Two Man Rule option can also be chosen which requires the presentation of two access cards before access is granted to a door or area. All Area Control, Anti-Pass back and Two Man Rule decision-making is carried out at the field processor level for instant response.

The backbone of the Card Access component of the system is made up of the system hardware and firmware that stores the software and interprets its commands.

The EAC utilizes a network of a host machine and any quantity of workstations necessary to serve a site. These workstations at PCs can store system maps, data,

captured video images and the operating software. They are, in turn, linked to processors in the field, which relay data from the field devices, such as card access doors to the workstations and carry out commands from them to the devices in the field. The capacity of these field processors and the direct transmission of data to them on the LAN, however, mean they can store system data sufficient enough to allow them to operate independently of any one workstation. In other words, the processors are "smart" enough to open doors for valid cardholders themselves without having to verify access with a workstation. The System Administrator can choose when that stored data be updated for a processor. Such "smart" devices provide distributed intelligence, which allows for greater capacity within the system and foster decision-making. Distributed intelligence also makes the system invulnerable to single point failures.

The EAC has integrated Video Badging into its system as a means of better tracking and monitoring personnel and enhancing site security. A video image is issued to create an access card, which personnel can use throughout the site to gain entry and use as identification. The cardholder's image is captured by a video camera linked with one of the system's workstations and entered into the database. An access badge can be printed at that time or stored for later use.

The badges can be configured by the user to discourage forgery and the use of personalized badges with the picture of a cardholder discourages the swapping or unauthorized use of badges. Because the cardholder's image is stored in the database, printing additional badges to replace lost or expired badges are simplified.

The step of entering information into the on-screen forms to create a badge automatically enrolls a cardholder into the database, thus saving time for the operator. The cardholder's image can be "called up" by other terminals in the system to visually verify the identity of the person presenting the access card if necessary. Just as monitoring a premises for intrusion and allowing access are necessary component of a Card Access system, so too is the logging of the events into a database to create a record. These records are typically maintained for a time deemed appropriate by the system operator and can be used to evaluate the performance or effectiveness of the system configuration and usage by personnel.

2.4.4 DATABASE MANAGEMENT AND REPORT GENERATION

The entry of data through completion of on-screen forms or by site activity records builds a system database that is used internally to support access control and facilities automation functions. As mentioned previously, the data can be retrieved by traveling to a specific form and entering the appropriate data to limit the search of requesting the system list all records. A simplified Structured Query Language format can be employed to limit the search criteria and search the database more efficiently.

System operators can also tailor reports to address specific site needs and applications. These reports can be created for onetime use or they can be recalled as frequently as desired. Such reports can track the usage of doors or track a certain cardholder. Denied Access events, those times a cardholder is denied access to a door, can highlight seemingly discreet attempts by a cardholder to gain access to an unauthorized area.

In the present time, security is a prerequisite for the functioning of modern organizations. Access Control Systems are compulsory components of such intelligent safety precautions.

Access Control Systems provide:

- Overall item protection
- Differentiated operational protection
- Classified coded protection
- Comprehensive protection of specific security zones and data areas

The main targets of an Access Control System are the following:

- Controlling and defining access points
- Grouping of identified persons as authorized or unauthorized
- Securing that access is restricted only to the authorized persons at the specific access points
- An Access Control System consists basically of the following components:

- Central Processing Unit: Monitors and controls the system, including programming and operation.
- Control Unit Stores and conducts programmed authorization data: All access inquiries are checked and authorized from this unit.
- Access Control Reader: Being the preliminary control station of the system, it converts magnetic information (encoded in the cards) into electrical signals and directs them to the control unit.
- Regulating Unit Realizes the barring of the door.

2.4.4.1 REDUNDANCY - TAKING EXTRA SPECIAL CARE

Very commonly, the command post for all your security information is a single computer. No matter how many computers you might have in your system, ultimately, one computer oversees the rest. Backing up data on a daily basis is, of course, a must, but what happens when your supervisory computer fails?

White you should contact a top security consultant to determine how you can introduce *redundancy* (duplicated processes and equipment) into your system; most PC-based systems are small enough to enable this simple solution:

- Buy a second computer that duplicates your supervisory computer in every way.
- Duplicate all your software and data on this computer. This can be done through a communications link or through a backup device.
- If a problem occurs with your supervisory computer, substitute your backup computer during the repair process.

Also make sure that your lines of communication are redundant. Having multiple ways of contacting local authorities, such as by modem, direct line and wireless channels, is an important plus. Use battery backup devices (not just surge protectors) to keep your system running during a storm and protect your equipment against damage from electrical spikes, which can damage sensitive electronics.

a supply of fresh, new cables available and label them as to their use. Intermittent system problems can be caused by a single broken wire at a connection

point in what otherwise looks like a strong, thick cable. Breaks can happen unexpectedly, such as when something is accidentally shoved against a plug. Don't jeopardize security in the evening or over the weekend by having to wait until the next day for computer supply stores to open. In addition, do not keep old used cable for replacements. The few dollars saved might cost you hundreds. If not thousands, in headaches.

2.4.5 TECHNICAL INFORMATION

Understanding the components of computers greatly aids the understanding of computerized electronic access control networks.

2.4.5.1 OPERATING SYSTEM AND OTHER SOFTWARE

The microprocessor that manages information flow in your computer or intelligent device is itself managed by instructions. These instructions are either *hardware,* meaning that they are physically embedded in your system, or are issued by *software.* Software is composed of written words, just tike the words you're reading in this project. The actual language of software, however, is like any foreign language. You need to learn it in order to use it, consequently, most people regard software language as *code.*

The information you see on your monitor is an interpretation of software code translated into a readable format. While you might be required to program your EAC system, most likely you'll do so by answering questions with everyday language. Once you enter your choices, the software translates this information into its own code. Computers use many layers of software, most of which is not apparent. The very first piece of software your computer uses is called the operate system, or OS for short.

The acronym DOS refers to *disk operating system*, meaning that the computer supports disk drives. White this may seem obvious, computers were once controlled by tape drives, similar to those used by tape and video recorders. The designation DOS on "new" machines at that time told the public that they were state-of-the-art. There are a number of operating systems available, among which are: MS-DOS or PC-DOS, OS/2, WARP. UNIX and high-end Microsoft Windows products.

Low-end Windows products, such as Windows 3.1 and Windows for Workgroups, require that MS- or PC-DOS be installed before they will run. Essentially, MS-DOS and PC-DOS are the same operating system. MS refers to the software sold by Microsoft and PC to software sold by International Business Machines (IBM).

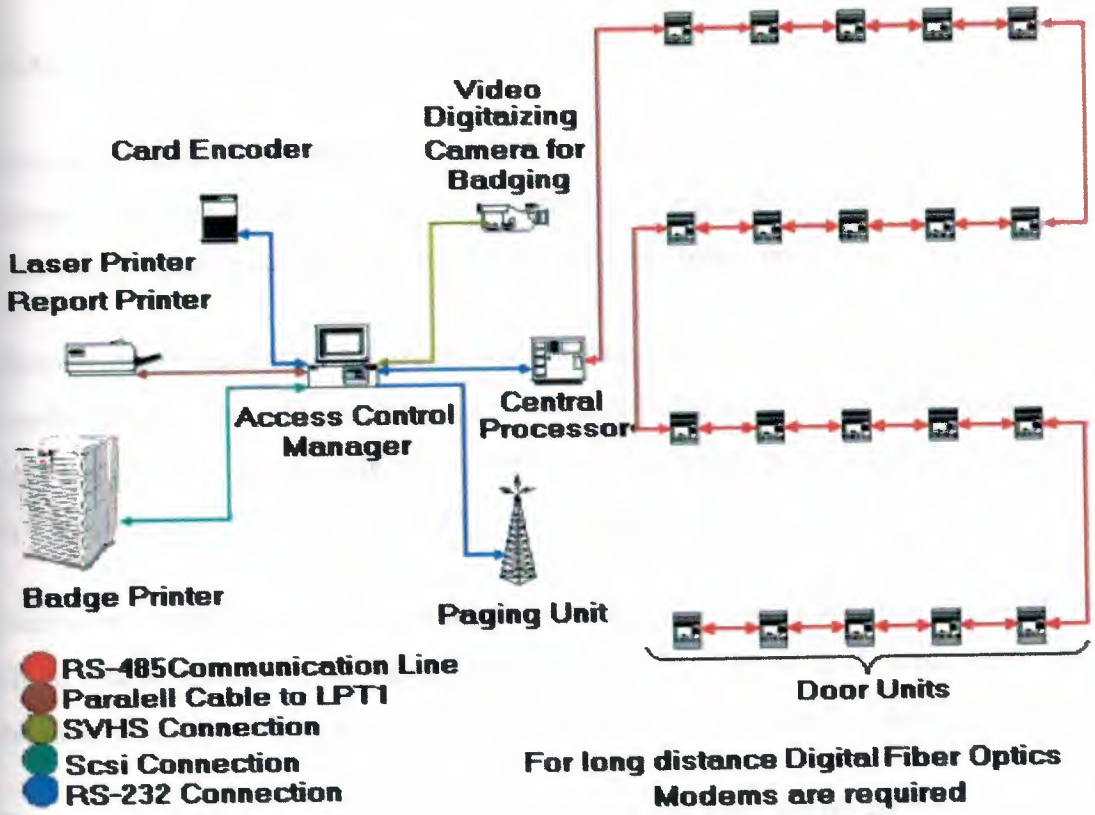


Figure 2.4.1 Computer Network

2.4.5.2 DATABASE SOFTWARE

Next to your computer's operating system, database software is the most common type of software used in EAC. Database software is especially good at:

- Acquiring a history of events.
- Creating and maintaining records related to authentication,
- Holding specialized information related to the way locks, sensors and other devices work, and
- Providing data storage and report generation.

Unfortunately, power failures, static electricity and turning off the computer before properly closing software can cause serious trouble. Database software opens and closes many files. When some files are saved, but others are not due to premature shut down, the database becomes corrupt.

2.4.5.3 CIRCUITS AND CIRCUIT BOARDS

Electrical circuits route electricity to and from a variety of sources. A circuit board increases the number of routes available within a small area by providing a stiff backing upon which ultra-fine wiring and multiple connection points rest.

Microprocessors and other electronic devices are plugged into specially designed circuit boards. At the edges of these boards are *terminals* (also known as connection points or plug sockets), which provide the means to attach wires from other devices. These terminals are usually exposed behind your computer's case.

Computer circuit boards also contain sockets used to connect additional circuit boards. These boards are commonly called "*Add-on boards*" or "*cards*" and sit perpendicular to the main board. Installing a new card is sometimes referred to as "*taking up a slot.*"

The term bus refers to a *group of connections* on the main circuit card that move data between the integrated circuit chips. The type of bus used defines the types of cards that can be plugged in and directs the flow of information through wires in much the same way as a freeway system directs drivers to use traffic lanes.

A 32-bit microprocessor requires a group of 32 wires, called a 32-bit path, on the bus. Other devices use fewer wires, which can cause slowdowns. In a freeway system, switching from many lanes to just a few causes backups when traffic is heavy. The same is true with the flow of information.

Crossover points between different wiring requirements on the bus stow the flow of data, even though a fast computer chip is being used. The following list provides a few examples of common bus names and their wiring capabilities:

8-bit bus: Sends data along 8 wires.

16-bit or ISA bus: Sends data over 8 or 16 wires.

EISA bus: Sends data over 8, 16, or 32 wires.

MCA bus: Limited to sending data over all 32 wires.

Local or PCI bus: A special 32 wire bus that can transfer data at 32 bits to all high speed connections, such as used for the display or disk controllers and fewer bits to other devices, such as the keyboard and mouse, which do not require data transmission speed.

2.4.5.4 PORT TYPES:

In the process of setting up your computer, you will come upon references to various connection types, which sometimes can be confusing. Here are some examples:

A port is another name for a connection.

The names *serial port* and COM port are used interchangeably. The abbreviation "com" stands for "communications." They provide the connection that allows information to be sent or received one-bit-at-a-time to another device or outside source. These ports are commonly used for modems and mice, both of which communicate one-bit-at-a-time through a 9-pin connector, although older computers and a few off-brands use 25-pin connectors.

The names parallel port and LPT port are also interchangeable. LPT used to stand for *line printer terminal* because at one time, only printers were connected to computers in a parallel fashion. This type of connector has 25 pins, which are capable of simultaneously sending or receiving information over 16 wires, 8 bits at a time.

2.4.5.5 INTELLIGENT AND DUMB DEVICE

An intelligent device is one that is controlled by its own microprocessor.

At minimum, an intelligent device requires its own operating system, BIOS and instructions. It can also have DRAM. Flash Memory and other means of storing information. While state-of-the-art, super fast microprocessors might drive the computer, intelligent devices often use slower, less expensive microprocessors, such as those defined by 8-bit and 16-bit chips.

A dumb electronic device operates in a manner similar to an intelligent device, except that it is 100% dependent on another computer for instructions. Dumb devices place an extra burden on, a supervisory computer's capabilities and will fail to work properly when that computer goes down.

Overburdened computers (those that must control numerous dumb devices) send instructions slowly, severely limiting the effectiveness of a dumb device's ability to respond to emergencies.

The ideal devices, then, tend to be intelligent and can work independently of a computer, even though they might use a central computer for its:

- User interface
- Communications ability (information processing and routing)
- Information storage capability

Intelligent devices are more useful, under a wider variety of circumstances, than, dumb devices. This is a very important consideration when selecting devices for a security system.

2.4.9.6 SYSTEMS – NETWORKED AND DISTRIBUTED

An electronic access control network consists of one or more personal computers, control panels and devices, such as electronic authenticators, locks, sensors, etc.

Network control is provided by *network management system* that resides on the supervisory computer. The supervisory computer in a network is commonly referred to as a *server* because it deals out information.

The interconnection and exchange of information between devices in a computer network is referred to as *communication.*

2.4.5.6.1 Distributed System

A distributed system is made up of intelligent control panels that communicate with the supervisory computer.

This means that each control panel acts like an independent computer, even though monitors and keyboards are not present. The supervisory computer and control panels in this type of system communicate with one another as needed. Communication, however, is not always required.

> *Example:* An intelligent control panel might not report common activities, such as granting access to authorized users, but will report attempts at unauthorized use as well its alt alarms.

Intelligent control panels stay up-to-date through software changes, just like personal computers do. In the case of improvements in technology, many intelligent control panels can also have their ROM or EPROM chips replaced. Chip replacement is an economical way to upgrade, especially when compared to replacing an entire system, which might involve rewiring!

Numerous intelligent control panels can be networked within a distributed system, sometimes using repeaters to boost signals between them and me server. All the panels, of course, work independently from one another and none put a strain on the main server.

In the past, dumb control panels were used to control access. This was primarily because of the expense of the microprocessors involved.

Fortunately, microprocessor and memory prices have dropped. Distributed systems and intelligent devices are becoming the standard. This enables EAC systems to stay running no matter what problems may befall any part of them—most certainly a plus for security!

2.4.6 COMPUTER NETWORKS

The EAC computer network is the communication system between the computers used to supervise the EAC system. This may or may not be part of a general-purpose computer network.

Making the EAC computer system part of a general-purpose network can save cabling, equipment costs, and leverage the efforts of people already supporting the network. On

the other hand, the EAC network is sensitive to information delays. As we discuss later in this chapter, you don't want to find out about an alarm minutes or hours after it occurs. Also, combining EAC with a general-purpose network opens the security system to attack from any user on the general network. Many EAC systems use one supervisory computer and would not require a computer network, however, the trend toward computer networks is growing. It have more than one supervisory computer a network is essential.

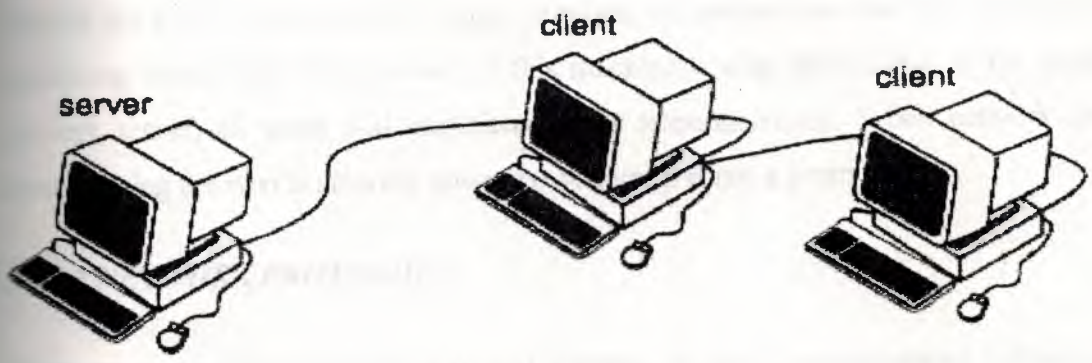


Figure 2.4.2 Server and Clients

2.4.6.1 CLIENT / SERVER

If spending any time around computer networks, you will hear the terms "client" and "server."

- **The client** is the computer requesting a service or data.
- **The server** is the computer supplying it.

Many networks have one or more computers designated as "the server." The primary purpose of a server is to function as a central depository of files and/ or serving. These central services may include supporting printer, providing a connection to the Internet, sending and receiving FAX transmissions, or acting as the post office for electronic mail. The other computers on the network, or clients, are generally regarded as personal workstations and are used for everyday tasks by the people accessing the network.

To make the issue more complex, a server can also function as a personal workstation, but that is typically avoided because the server's processing time is needed to quickly respond to the requests of the network.

2.4.6.2 EAC ADDS CONTROL PANELS TO A NETWORK

As we mentioned, a computer network can have more than one server. An EAC system win typically have a computer designated as the EAC server where the database is kept. The EAC server may or may not be the same computer as the network server.

It is perfectly acceptable, even recommended, that the EAC server actually be one of the machines that functions as a client for the general network. This is recommended because the EAC system can have large numbers of transactions that will consume the processing time of the EAC server. If this machine is also functioning as the general network server, all users will experience stow response times. When network users come looking for who is slowing down the system, it is not a pretty sight.

2.4.6.3 NETWORK PROTOCOLS

There are many different protocol (rules) followed by the communications software for computer networks. Two of these protocols are so common and referred to so often that they deserve mention here:

- **TCP/IP** is the protocol used by the Internet and, as a result, by many other applications as well.
- **IPX/SPX** is the protocol used by Novell networks. Novell has been a longtime leader in the installation of networked systems and many corporate systems depend on this protocol.

These protocols are not compatible in the sense that software designed to use one of the protocols will not be able to make use of the other protocol. They are compatible in the sense that both protocols can exist on the same cable and computers can be set up to respond to both protocols. It is possible to send TCP/IP packets on Novell network provided the sender and receiver have been set up to handle the TCP/IP protocol.

One possible problem with mixed protocols on one network is a device called a router. A router is a dedicated computer that monitors messages being sent from one leg of a network to another. It passes messages that are intended for a node on another leg and does not pass messages that are intended for nodes on the same leg as the sender.

Routers are very helpful in keeping the traffic on a network to a manageable, level. The problem is that routers must know something about the protocol to be able to open a message and determine the destination. A router on a Novell network, for example, may not be able to process TCP/IP messages and therefore not pass them to the next network segment.

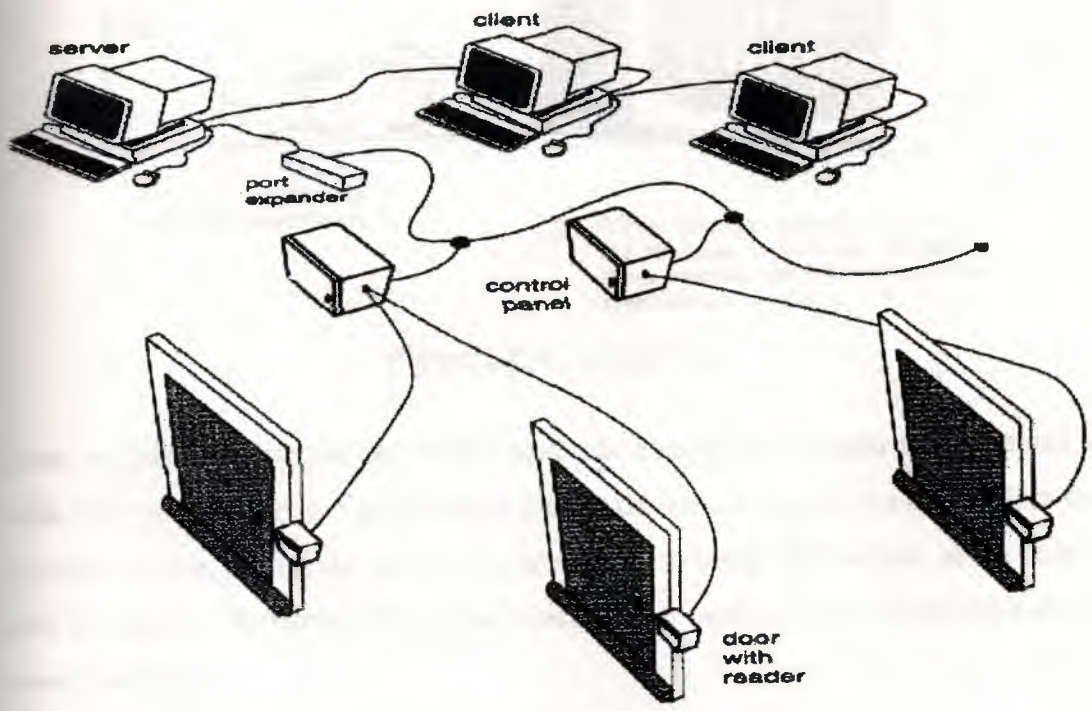


Figure 2.4.3 EAC Network (using a multi-Drop line)

2.4.7 CONTROL NETWORKS

The control panels in an EAC system can be thought of as special purpose computers. As such, many of the same principles used in computer networks also apply to networks connecting the control panels (control networks). Since the control panels are highly specialized, the protocols tend to be proprietary, or specific to that manufacturer.

Computers from different manufacturers communicate over most computer networks. In *proprietary network* such as those used by EAC panels, only equipment limit by the manufacturer of the network will function property. In recent years standards for control network protocols have been proposed which will allow equipment from different manufacturers to communicate over the same network. These universal control network protocols are slowly achieving acceptance.

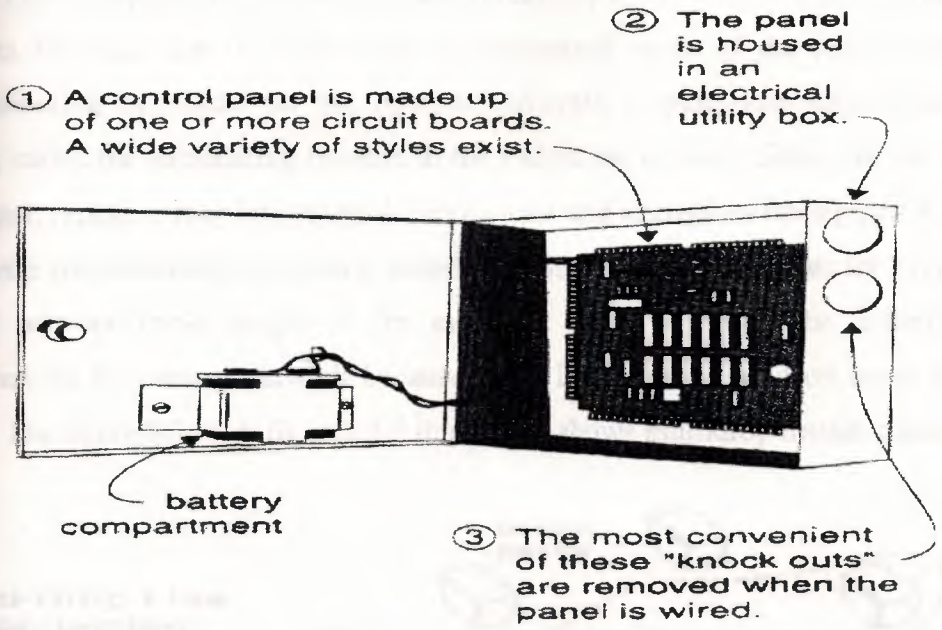


Figure 2.4.4 Control Panel

When we talk about connecting control panels to a network, we refer to each panel as a node. The word "node" is a generic term for any device connected to a network. In order to communicate, each node has a transmitter, used to send information, and a receiver, used to receive information. There are typically two methods for connecting a *node* in control networks:

Multi-Drop and Daisy-Chain.

In a **multi-drop** system, the transmitter and receiver of each node are connected over a common conductor with the transmitter and receiver of every other node.

The Daisy-Chain, or "loop." method has the transmitter of the first node connected to the receiver of the second node. The transmitter of the second node is then connected to the receiver of the third node and soon until the transmitter of the last node is connected back to the receiver of the first node completing the "loop."

2.4.7.1 A MULTI-DROP

The multi-drop method is popular because it is easy to add or remove a node from the network. Because all the transmitters and receivers share a common conductor, the multi-drop method requires a means of insuring that only one transmitter is operating at

a time. This is bandied by the network communications software and is invisible to the user, but knowing that it exists helps to understand some of the requirements and troubleshooting techniques for this method. Generally a multi-drop scheme requires a resistor, called the terminating resistor, at the end of the network cable. As the network gets larger, repeaters may be needed to rebroadcast and strengthen the signal. A popular multi-drop communication standard, caned RS-485, calls for a repeater for every 4,000 feet of network cable length or for every 32 nodes. Consult the manufacturer's specifications for control network because these limits can depend on many different factors. The figure below & figure2.4.3 in page 71 shows multidrop lines& connections.

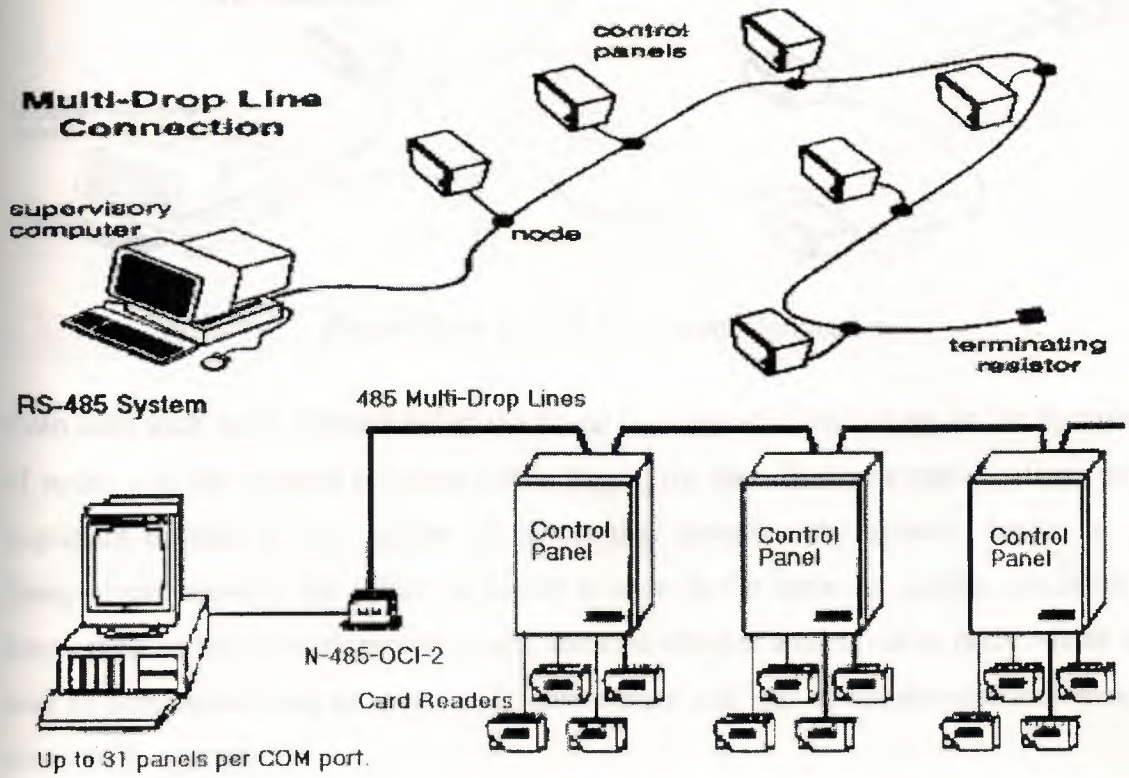


Figure 3.1.4 Multi-Drop Line Connection

When a node in a multi-drop network fails, only communications to that node is lost. The network will continue to function normally minus that node. When the cable is cut, all nodes downstream, from the cut to the terminating resistor, are lost along with the terminating resistor. The loss of the terminating resistor degrades the performance of the network and may result in slow or lost communications. Usually some communication remains with the nodes upstream of the cut.

2.4.7.2 *DAISY-CHAIN*

With the Daisy-Chain method each transmitter can transmit whenever it pleases because the information it sends is picked up by only one receiver. In a multi-drop system, a repeater is required to strengthen the signal over long distances. Since each transmission between nodes in the daisy-chain method is a rebroadcast of the signal, there is much less need for a repeater.

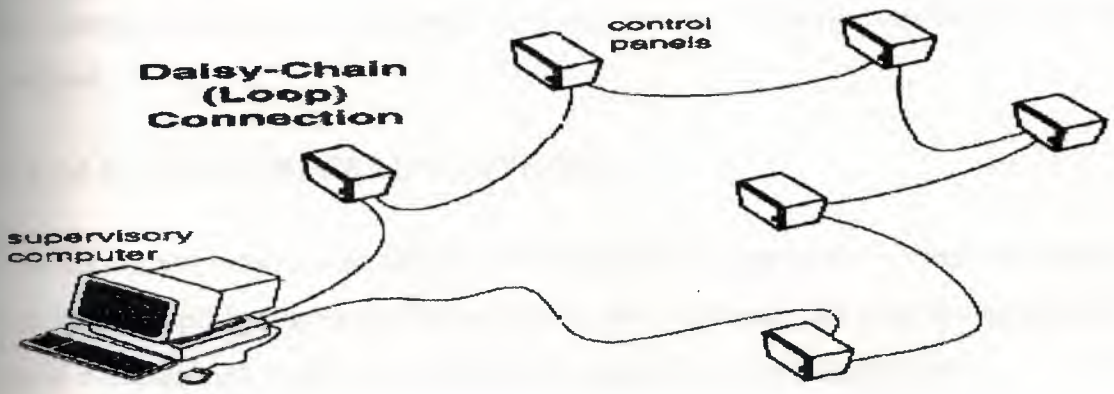


Figure 2.4.6 Daisy-Chain (loop) Connection

Even with each node rebroadcasting the signal there are still limitations on the number of nodes and the distance between nodes. Again, the manufacturer's specifications are important because of the number of factors that determine the network limits. In a Daisy-chain network the effect of losing a node is the same as cutting the cable. Depending on the network protocol used, the least effect of a cable cut or node failure is loss of communications to every node downstream and loss of communications from every node upstream.

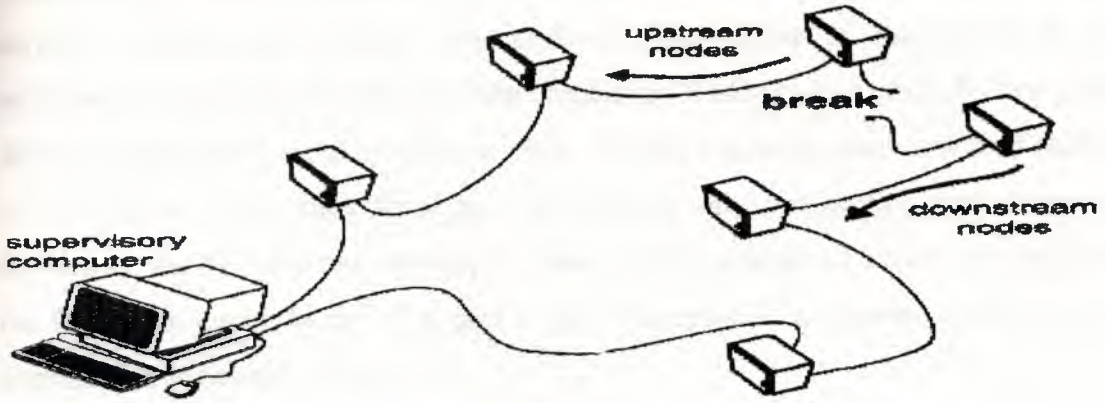


Figure 2.4.7 Daisy-Chain Problem

2.4.7.3 CONTROL NETWORK SAFEGUARDS

For both the multi-drop and the daisy-chain methods, it is possible to add redundant paths to keep the network fully functional in the case of a cable cut, but this is more expensive.

The benefit of distributed systems is that even with the loss of communications, intelligent control panels continue to provide access control. They also store a record of the events monitored by the panel in a memory buffer until communications are restored.

2.4.7.4 INTER-NETWORK CONNECTIONS

The connection between the Control Network and the supervisory Computer Network can be accomplished in many different ways. Due to the fact that most computers have serial communication ports, the connection is generally made through those.

2.4.7.4.1 Serial Connections

Serial ports, also called COM port ("com" stands for communications) are the typical means of connecting various computer-based devices. Serial ports on personal computers, workstations, and most mini-computers use the RS-232 standard for serial communications. This standard has been around for a long time and many devices have been built to use it.

The RS-232 standard only defines the electrical and mechanical characteristics of the connection. It does not insure that two devices, each using an RS-232 connection, can actually communicate property- Successful communication is determined by the software in the devices at each end of the connection. EAC systems typically have many devices that require a serial connection while personal computers have a limited number of serial ports. Since each serial port can support only one device, port expansion devices for the PC have been developed. These devices consist of a card that plugs into the PC's main circuit board. This card is then connected to a separate utility box that contains the additional serial ports.

Another standard for serial communications is RS-485. It is possible to connect a Control Network, for example, using RS-485 directly to the computer, but most computers do not come equipped with hardware that supports the RS-485 standard. To connect devices using RS-485 to a personal computer, a compatible interface board will need to be installed. You must also make sure that the software on the computer can support the interface board.

2.4.7.4.2 Modems

It is not always possible to directly connect the Control Network to the Computer Network. Multiple Control Networks as well as long distances sometimes dictate the use of "temporary" connections through dial-up telephone lines or the use of long-distance communication systems leased from a third party.

> *Example:* Global Manufacturing, Inc. is located in a large city and all EAC functions are monitored by a central security computer, this company also has a storage facility in another country, where EAC traffic is tight.
>
> The control panels at the remote facility are hooked up to a modem. Periodically the security computer uses its own modem to connect with the modem at the remote facility. Once the connection is made, the security computer polls (contacts) each control panel at that site for a report of activity.
>
> In case of an emergency, the Control Network at the remote site makes use of the modem to dial the security computer and report the situation.

A modem is a special circuit card that controls the flow of information over commercial telephone tines. These tines were designed to transfer the analog signals that are produced by telephones carrying voice messages. The modem converts the digital signal from the computer into an analog signal for the telephone line. The modem on the other end converts the analog signal back into a digital form for use by the receiving device.

There is also a device known as a codec that transmits and receives digital signals over the telephone lines. It is possible in many areas to request an ISDN hue which is a telephone tine designed to carry digital signals, but again, because it is not yet common, the cost it significantly higher.

2.4.7.4.3 Other Connections

There are many other communications standards other than RS-232 and RS-485. These other standards require specific internee boards and supporting software to create a functional system. The supplier of the Control Network will provide the interface hardware and software fur the supervisory computer.

It is possible for the Computer Network and the Central Network to be the same network, fn this case the control panels and other devices on the Central Network are connected directly to the Computer Network and only the software determines whether messages are between the supervisory computers, between the central panels, or between the control panels and the supervisor computers. This type of connection for control panels is more expensive and is generally only cost effective if the Computer Network already exists everywhere control panels are needed and the Computer Network is not heavily used.

2.4.7.4.4 Network Recommendations

We highly recommend that the Control Network be separate from the Computer Network to insure that the report of a significant security event is not delayed by heavy network traffic and to make it more difficult for computer hackers to compromise the security system. For these same reasons we also recommend the Computer Network that connects the supervisory computers for the security system be separate from the corporate or enterprise-wide network. If these networks are combined careful attention must be paid to traffic volume and security concerns.

2.4.7.4.5 Connections in General

The quality of cables and their connections are as important as the computers and EAC devices in the system. The following items are very important when designing any electronic system:

- Cables should be well labeled and installed with care. Make sure that installers know and follow the appropriate electrical codes. Poorly installed

cable can create electrical short circuits or breaks in the wire that are very difficult to diagnose and locate.

- Unless fiber-optic are using cables take care to avoid sources of electromagnetic interference (EMI). Typical sources of this electrical noise are motors, fluorescent lighting ballast, and transformers. Avoid running cables carrying data signals in the same conduit as those conducting power. If data cables must cross power cables, do so at right angles to minimize the interference.
- Pay attention to Specifications. A manufacturer's specification sheet indicates the limits to which a piece of equipment has been tested. Failure to follow specifications may appear to work for a while, but chances are conditions will eventually occur that will cause the system to fail. Finding problems in a system that are caused by failure to follow specifications is difficult and usually very expensive.

2.4.8 SOFTWARE

The supervision of every system has three components. These components are defined in the software so they are not always easy to separate. Understanding that every system has these three components, prepares to understand and compare different implementations. These three components are:

- The user interface
- The database, and
- Communication.

All three of these components can exist on the same computer, but in very large applications each of these components might require a separate computer.

2.4.8.1 USER INTERFACE

The user interface determines how software is seen and used by people. This includes everything from the way information is presented in reports and on the screen, to the selection of which information and options are presented to the user and when. Many software packages today include a Graphical User Interface (GUI, pronounced

"gooey"), which can improve the ease of use. A GUI also requires a more powerful computer and better monitor than a standard text-based interface.

Don't let the color and flash of fancy graphics determine choice of a software package. Pay close attention to the information conveyed and compare it to the way will use the system. Elaborate interfaces that are confusing detract from the usefulness of the software. Colors or animation that are pretty, but don't convey information will eventually annoy and distract the operator from the information needed to use the system.

When evaluating software, spend some time with the user interface looking for clarity. Information that is used regularly should require a minimum number of keystrokes or mouse clicks to access. This is where an integrated system is most helpful because the user does not need to leave one software package and start another to accomplish a task. Also evaluate typical operator actions in an EAC system which include:

- Alarm monitoring,
- System control,
- Report generation,
- And Operator security levels.

Systems with higher levels of integration may also include the creation of credentials or badges and the automatic control of CCTV cameras and other equipment within the user interface.

2.4.8.2 ALARM MONITORING

Even if there are no general-purpose intrusion detection devices in the system, almost every EAC system monitors the doors for forced entry. The alarm-monitoring screen should clearly indicate to the operator, which inputs are in the alarm state both visually and by a sound that is not easily ignored. Typically this is how it works:

Each alarm requires the operator to acknowledge the event by pressing a key or clicking a mouse on an ACK (acknowledge) icon. Many times the operator receives instructions on what to do when this alarm occurs and may be required to enter a description of the event and the operator's response.

Acknowledging the alarm should change its display and make it less obvious than alarms that have not been acknowledged. After the operator has acknowledged the alarm and handled its cause, the alarm may be cleared from me display, but is stored permanently in a history file. In addition to "alarm" and "normal." Supervised input may indicate a "trouble" state.

A supervised input is one that is electrically monitored to prevent tampering. If an attempt is made to bypass a supervised input or if something happens to damage the circuit, the display will indicate that point in a trouble state.

2.4.8.3 OPERATOR CENTRAL

Most EAC systems operate automatically; reading credentials and making decisions about granting or denying access. From time to time human intervention is required, such as when someone forgets their access credentials or an event occurs that was not covered in the system's automatic programming. In these cases it is important that the operator be able to easily and smoothly control the system in a manual fashion. Consequently, the operator must be able to unlock and/or open doors, shunt alarms, and perhaps activate other devices such as cameras or lights.

Shunting an alarm is a term used to indicate that the alarm input is to be ignored. For example, the open door alarm is automatically "shunted" when access is granted to allow the door to be opened without falsely signaling an alarm. Other control terms used in these systems are energize, de-energized, and pulse. If a device is energized, it will stay that way until de-energized. Whether "energizing" locks or unlocks the door is defined by each system. If a device is pulsed it will be energized for some defined time period and then automatically be de-energized. Pulsing is convenient if wish to allow one person through a dour. Pulsing the lock allows the door to be unlocked for that person, but does not require the operator to remember to re-lock the door after the person enters because the output is returned to the original state automatically.

2.4.8.4 ACCESS DEFINITION

- Access control is managed by three concepts:
- Access Level

- Time Zone
- Access Area

EAC systems determine when an individual can enter an area by assigning an access level. An access level is a combination of n time /one and one or more access areas- Access areas group the use of specific readers. Time is managed in an EAC system through the creation of time zone. Time zones are periods of time given a label so they can be referred to in a systematic fashion.

Example: The First Shift time zone may refer to the time periods between 7:00 am and 5:00 pm on Monday through Friday. Time zones must take into account the time, the day of the week, and holidays. The controlled areas in a facility are referred to as access area. Each access area is defined by the credential readers assigned to it, therefore, access areas and physics moms may not necessarily coincide or they may overlap. If the computer room supervisor's office it inside the computer room and both moms are contused by the EAC system, the definition of the access area is determined by the assignment of the specific readers.

Example 1: If the reader for the computer room and the supervisor's office were both included in one access area, a person in the supervisor's office would be considered inside the computer room access area.

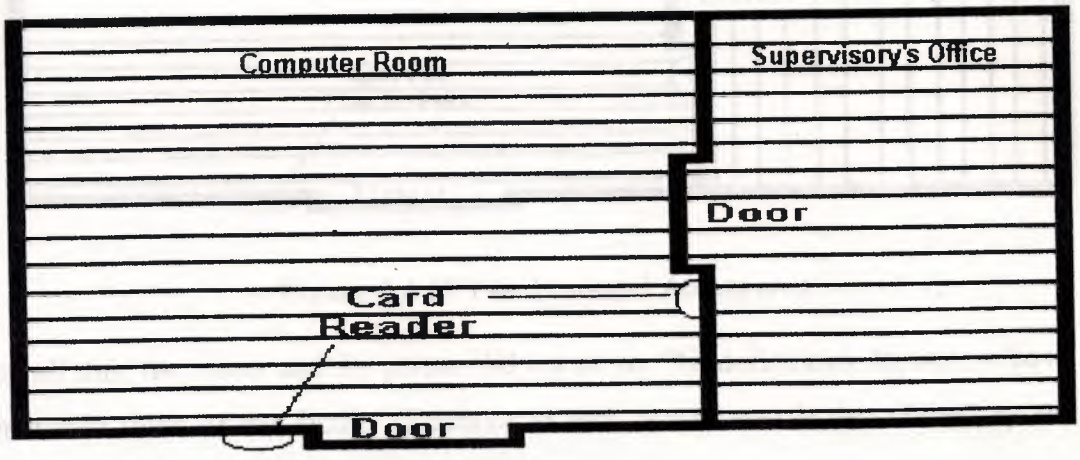


Figure 2.4.8 Example 1-One Access area

Example 2: If an additional access area were created for only the supervisor's office, the person in that office would be considered to be in both access areas at the same time.

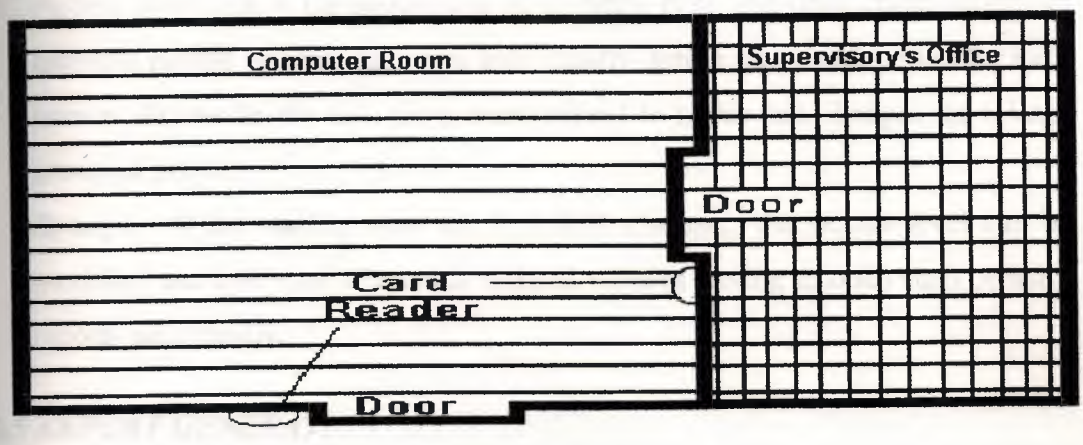


Figure 2.4.9 Example 2 This room-within-room creates overlapping access area

Example: It the reader for the supervisor's office is then removed from the definition of the computer room access area, the person in that office is considered to be in the office access area, but not in the computer room access area.

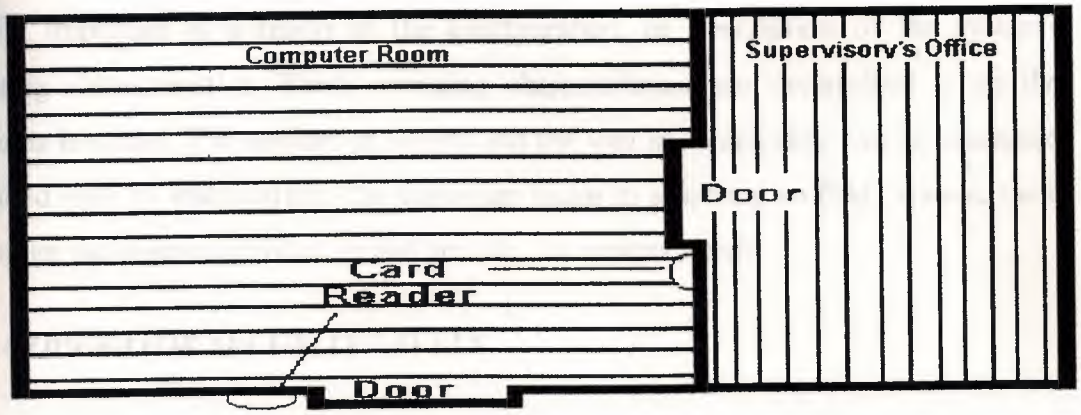


Figure 2.4.10 Two Unrelated Access area

During all this, the rooms and the person did not move. The definitions depend on how the operators think of the facility. Entrance to each access area is determined by an access level.

Example: George may be assigned the access level of Supervisor, which entitles him to enter any door on weekdays except the Executive Washroom. Sam, on

the other hand, is assigned the access level of janitor, which allows him access to every door including the Executive Washroom but only between the hours of 8:00 pm and midnight.

Access levels allow the assignment of common time and door combinations to multiple people without having to individually define that combination for each person. Access levels also allow management to make fast changes for a large group of people.

Example: If the starting time for first shift changes, the access level can be modified and everyone affected is updated without having to open each person's record individually.

2.4.8.5 REPORT GENERATION

When evaluating a system, determine the kinds of reports are going to need. Creating a history report of the events that occurred is one of the reasons many people installing EAC in the first place. Creating a report of the people who hold or held credentials is also important because it lets keep track of system users.

Equally important is a report of the configuration, or description of the system's operating characteristics. These operating characteristics are determined when the system is installed. The number of reports and the way in which they can be organized is limited only by imagination. The important factor in selecting an EAC system, then, is whether the system provides, or can provide, the reports needs.

2.4.8.6 OPERATOR SECURITY LEVELS

Not alt operators are created equal. It is common to have a group of operators who are required to monitor alarms and perform some manual control of the system, but are not allowed to change the system configuration or add new credential holders. When checking new software, determine whether the system allows restricting operator access to various parts of me system in the manner that suits needs.

3.1.7.7 EMERGENCY

The determination of what constitutes an emergency and what steps are required to respond must be determined prior to selecting an EAC system. EAC system should allow to anticipate a broad range of emergencies and provide a means to instruct operators what to do when they happen. To help evaluate this capability consider the following questions:

Can EAC system tell who is in threatened areas when an emergency occurs?
When an alarm occurs, are the appropriate steps for response clear to the operator?
Emergencies are unusual events and, because of this, the responses are not well practiced. The software must be clear and easy to understand so that mistakes are not made in the excitement of the moment.

2.4.8.8 DATA BASE

EAC systems have a lot of information that is appropriate for databases. A database is simply a table of information that can be accessed and sorted in multiple ways. Data base software packages for PCs are available at any store selling software. These products are like toolkits; by themselves they can be used for EAC, but have to figure out the data needed to store and create the tables and interface yourself.

EAC systems make use of the data base engine from these products to create an application that has this work already done. The database engine is the core program of the commercial product without the user interface. Data base software is fairly mature and most EAC systems use a commercially available data base engine. The EAC system benefits from the data base product's experience with handling data quickly and reliably.

Use of a commercially available data base engine might also make it easier to import or export data from the EAC system which is useful if data is to be shared with Human Resources or other data-intensive systems.

EAC-related data includes:

- Programming configurations for devices in the EAC system.

- Time zones and access level definitions.
- Access area definitions where the credential readers are assigned to specific areas to be controlled and tracked.
- Detailed information on the credential holders. Since the large majority of credentials are cards, this is typically referred to as the "card database." This will include personal information, the credential issued, the credential's standing (i.e., active, expired, or lost), and sometimes the photograph, signature, or other biometric information.
- Event logs that gather information on access transactions, device activity, and other system events.
- Communications interfaces such as the addresses of the control panels, the port they are connected to, and for temporary interfaces such as a modem the connection information (telephone number).
- System logs that track computer use, operator logins, and changes in configurations.
- If the EAC system integrates a CCTV system, it must keep track of camera locations, available monitors, and actions to be taken when specific, events occur.

The data base portion of the EAC system determines how fast information can be accessed and the reliability of that data during operation and especially when the computer is unexpectedly turned off or loses power.

Databases are especially susceptible to damage on power loss. It is a good practice to understand the likely effect a power loss will have on data base and what steps should be taken if the data base is corrupted (damaged). Any reasonable database will have automatic or manual methods of analyzing, isolating, and perhaps even correcting the damaged data.

Extremely important

It is important to check and repair a database as quickly as possible when suspect corruption. Continuing to operate a damaged database has the distinct possibility of further corrupting good data.

2.4.8.9 COMMUNICATIONS

The communications portion of the software is the least visible but most crucial to the correct operation of the system. This is the traffic cop that determines which information flows first, where it goes, and even insures that the information was delivered correctly.

Earlier discussions about connections indicated that the software dictated the devices and communication standards that are supported. This is the part of the software that determines those options. The product specification will indicate the number and types of devices supported and the standards that are followed. Data is typically transmitted serially. This means that the bits of information that are transferred between devices flows one after the other down the transmission cable. Even local area networks transfer information serially, although at very high speeds.

Usually there can only be one message at a time on any one cable. To get a better picture of what is happening in the communication system let's use an analogy. Example: The communication cables are like train tracks. The messages being conveyed are the trains. The longer the message, the more cars on the train. The various devices in the communication system, such as the central panel or the repeater, are the terminals where trains cither unload their cargo (message) or are transferred to another track (cable) to continue the journey to another terminal (device).

Some of the tracks are relatively stow (thousands of bits per second) while others are faster (tens or hundreds of thousands bits per second). Some tracks like those used in local area networks, are very high speed (tens or hundreds of million bits per second).

Each of the devices must track which train, or message, is allowed to travel which track (cable) The devices must insure that the high priority trams are allowed to travel first and that there are no collisions due to multiple trains being allowed on the track at the same time. A long train uses the track for a longer time making it unavailable to other trains. Hopefully this makes it easier to understand that determining the overall speed of data transmission is a combination of:

- The transmission speed of the systems components.

- The length of the messages,
- The routing ability of the devices that control the communications. The speed of data transfer is crucial in EAC systems.

An EAC system is monitoring real-time events. This means that when an alarm occurs, the operator must be notified at that time, not some minutes or hours later.

> "Peat-time" in an EAC system is determined in terms of human response time or essentially tenths of a second.

Obviously as alarm pile up rapidly on the display, the operator's response time for each event will slow down as time is spent analyzing and responding to each alarm. The software must continue to receive the events as they occur and not delay or lose event transactions.

A properly sized EAC system must be able to handle the worst-case scenario of every alarm occurring at the same time. Of course, this event is highly unlikely. Check with the supplier for the response-time analysis of the EAC system are evaluating. We are looking for the time it takes to receive an alarm in a busy system. Pay close attention to the definition of "busy" and make sure that if you are comparing systems, the manufacturers are using the same assumptions about loading and what is being measured.

2.4.8.10 BOTTLENECKS

Every system has a communications bottleneck. The bottleneck may be large enough that it does not impact the speed required by system, but it is always a good idea to know where the bottlenecks are in system so that as the system grows know the areas that need to be addressed first.

To locate the bottleneck in system, took for the device that has a combination of the largest number of connected devices and slowest data transmission rate. Sometimes locating the bottleneck is obvious and sometimes will need a communications professional to help you.

The communications portion of the software is also responsible for monitoring the communications links and the data being transferred to insure that the communication link is secure and the data is correctly delivered. An alarm should be reported if the supervisory computer unexpectedly loses communication with any of the control panels or other devices it is monitoring. The system should then continue to monitor that node to detect when communications is reestablished.

The communications protocol determines the proper delivery of messages. This includes verification that the message was received, and that the message had not been corrupted by electrical noise or other problems. If the message is not correctly received the transmitting node will reattempt to send the message. Retransmissions can be typical because of the many ways in which communications can be interrupted or corrupted.

The communications software will attempt multiple retransmissions before reporting the error to the operator. Sometimes the level of sensitivity for retransmission rates can be adjusted.

This is helpful when troubleshooting a system, or when simply wants to reduce the number of alarms in a system that is known to have poor communications connections.

2.5 Communication (Wired And Wireless)

2.5.1 CONNECTIONS

Security professionals are spending more and more time peering into monitors and less time "on the beat." This is because an electronic access control (EAC) system is a large computer network. Consequently, understanding hardware, especially the connections that make computers work, is becoming increasingly important.

The maze of connections associated with computer networks is confusing. Full-time technicians are familiar with connection principles. They earned this knowledge through special courses and on-the-job experience. Most other people are not.

2.5.2 CONNECTION INVENTORY

The following list pinpoints the type of information that should be kept on individual devices:

2.5.2.1 TECHNICAL INVENTORY OF EQUIPMENT:

Type of device, Manufacturer, Installer, if any Physical requirements, including plug types, wires and/or cables, Voltage requirements, Locations Wiring paths and/or junctions (connection points), Software name. If any, most recent version installed, and Cautions and warnings.

Every change in the system requires documentation. This can be an easy task that does not require reams of paper and hours of typing when know how to use technology.

A **database** kept oh a computer can provide an efficient way to manage this type of information. It can, however, be maintained on handwritten index cards.

Take **photos** of the installation sites and wiring connections. Enlarge them to 5" by 7" so that their details are clear. File these photos, along with product literature and instruction sheets. If a graphical database can be use on the computer, scan this information so that the pictures and illustrations are present whenever information is seen on monitor.

Video recorders with sound are inexpensive (as low as $400) and produce tapes that are good enough for inventory purposes. If lighting is dim, use a high-powered flashlight during filming. Make tapes of devices and systems, describing them as go.

Use *Snappy*, a $200 video frame grabber that attaches to computer's printer port, to capture pictures from video recorder. Once "snapped," these images can store in computer files and/or print them on paper to be stored with standard files.

Digital cameras are also inexpensive, however, **video recorder does a better job** of capturing the system and maintenance procedures. Video cameras "see" more information than single shots and often include detail that might have forgotten about.

Another plus to using video recorders is being able to **verbally describe situations** while record them. This method often provokes deeper reflection on the subject than might have when writing a report.

2.5.2.2 FACILITY MAPS

The placement of security devices and connection points throughout a facility can be easily seen on facility maps. These maps show the placement of devices and wiring paths through the use of symbols and can be as detailed or simple as wish.

Excellent examples of color-coded facility maps can be seen in the SDM Field Guide. The symbols they use are available on a poster that costs $5, including shipping.

2.5.2.3 INFORMATION UPDATES AND TRAINING TAPES

Update the information about site on a regular basis. If a video recorder use to do this, you'll find yourself making training tapes for new staff at the same time extremely cost efficient! Videotapes make a wonderful way for senior staff (possibly people who are about to retire) to pass their knowledge to the rest of the security team.

2.5.2.4 KEEP ALL INFORMATION SECURE

Obviously, good record keeping procedures simplify the maintenance of an EAC system. All records must be kept secure, however, so that they do not fall into the wrong

hands. Establish good procedures so that can always identify who is using materials. Regularly check files to make sure that everything is in place.

2.5.3 WIRING AUDITS

Security managers are usually responsible for all connections related to their area of command. Regularly scheduled wiring audits let them check whether the:

- Wiring is healthy (not corroded),
- Connections are solid.
- Connections meet code and
- System has been exposed to tampering.

Normally, security personnel do not have the expertise to install systems. This fact should not, however, make them overly dependent on outside installers and constants, or limit the amount that they can learn about their own installation.

To make sure that connections are made to specification, check the credentials of every member of the installation team. Next, audit the installers' work, both in progress and when complete. Take nothing for granted. Hire a third-party expert and accompany this person during the audit process. Learn as go.

Take photos or videotapes during the audit. Use these to train staff as well as to serve as a reference as to how connections should look, so you can tell when they are broken.

2.5.4 CABLE JACKETS

Everyone knows what a very simple electrical extension cord looks like. Not everyone knows, however, that the two prongs on the plug-end indicate that there are two wires inside the cable, each serving a different function.

In general, every prong, pin or pinhole on a plug is attached to a wire housed inside a cable. Even tiny connectors, such as telephone jacks, are attached to several wires. These unseen wires hide the means of connectivity from us, making the connection process seem mysterious.

If a cable split open. You will often notice that individual strands of wire are wrapped in colorful coatings (called "jackets"). Manufacturers use colors to code the wire for easy reference. The figure 2.5.1 page 93 shows cable jackets & types.

Table 2.5.1 Color Code

Wiring Practices National Fire Protection association NPFA 79 – Electrical Standard for Industrial Machinery	
Wire color	**Description**
Black	Line, load and control circuit at line voltage
Red	Ac control circuits, at less than line voltage
Blue	DC control circuit
Yellow	Interlock control circuit supplied from an external power source. (International standard =orange)
Green	Equipment grounding, conductor where insolated or covered May have yellow stripes. (International standard yellow and green)
White	Grounded circuit equipment. May also be natural gray? (International standard = light blue)

Both cable and individual wires are wrapped with a variety of materials, including those final jackets. These wrappings include insulation and shielding materials, as needed, and sometimes strengthening materials that protect the wire assembly against stretching during installation. The materials used are selected for specific applications, such as for exterior and interior installations, Protecting against dampness, cold and heat and shielding from electromagnetic interference, Cable assemblies must be flexible enough to let all included materials expand or contract at different rates. Consequently, the thickness of a cable assembly is determined by the material needs of all its parts. The table above shows the cable jackets color code.

2.5.5 CABLE TYPES

The term "conductor" refers to metallic material that carries electrical current. Nonconductive material, such as the glass used in fiber optics, does not carry current. The illustration below shows a sample of conductor cables. Conductor cables contain copper wires and require a ground wire or grounding material within the jacket, in

addition to the wires that carry current. Nonconductive material (fiber optics) does not require a ground.

Protecting against dampness, cold and heat and shielding from electromagnetic interference. Cable assemblies must be flexible enough to let all included materials expand or contract at different rates. Consequently, the thickness of a cable assembly is determined by the material needs of all its parts.

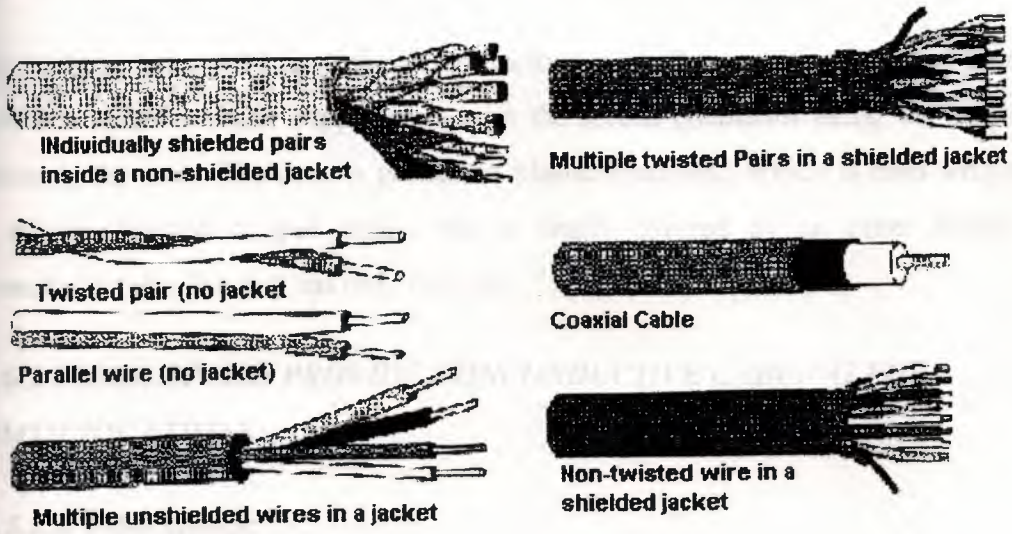


Figure 2.5.1 Cable Types

2.5.6 NETWORK CABLES

2.5.6.1 THE THREE TYPES OF CONDUCTOR CABLES COMMONLY USED IN COMMUNICATIONS ARE:

2.5.6.1.A Unshielded Twisted Pair (UTP):

A circuit requires two wires: one for sending and the other for receiving. Each wire is covered by a jacket. Typically, the cable used in communications holds four pairs of twisted wire. Each pair is twisted differently, with the number of twists per inch being the defining factor.

Twisting each pair of wires helps cancel noise (electrical signal interference) from the adjacent wires within the cable as well as from other devices in the building, such as motors, relays and transformers.

2.5.5.1.B Shielded Twisted Pair (STP):

This cable holds two sets of twisted wires. Each set is wrapped in a foil Jacket. Both foil jackets are wrapped together inside a braided copper mesh and then the whole assembly is wrapped by an outer jacket. This cable is used for some computer networks, such as a Token-Ring LAN

2.5.6.1.C Coaxial Cable:

This cable is commonly used for video hookups as well as various types of computer networks. It has a single copper core, with the second conductor being the shield that surrounds the core. The core is packed in plastic insulation, which is then wrapped in the shield (braided copper mesh) and is finally covered by an outer jacket. The connector is tube like and has only one pin.

2.5.6.2 FIBER OPTICS PROVIDE NONCONDUCTIVE CABLING FOR COMMUNICATIONS:

2.5.5.2.B Fiber Optics:

Fiber optic cable is made up of glass or plastic filaments (slim threads) that allow the transmission of light. Light transmission over each filament creates a stream of bright and dark spots, which, when measured over time, result in an ON/OFF code that can be interpreted.

There are three primary advantages for using fiber optic cable:

- First is that fiber optics are totally free from electrical interference.
- Second is that they can carry data further without signal degradation. Fiber optics covers more than 11 times the maximum distance for coaxial and 15 times the distance for twisted pair cable before signal boosters are required.
- Third is that light transfer can be precisely controlled, almost eliminating the possibility of tapping. Conductive cabling can be tapped, allowing the eavesdropper to read all passing data, including unencrypted passwords. In a precisely adjusted fiber optic situation,

however, tapping alters light transmission patterns, causing the entire system to fail before information is illegally captured. From figure below we can see the construction of fiber optic cable, which makes fiber optics highly tamper resistant.

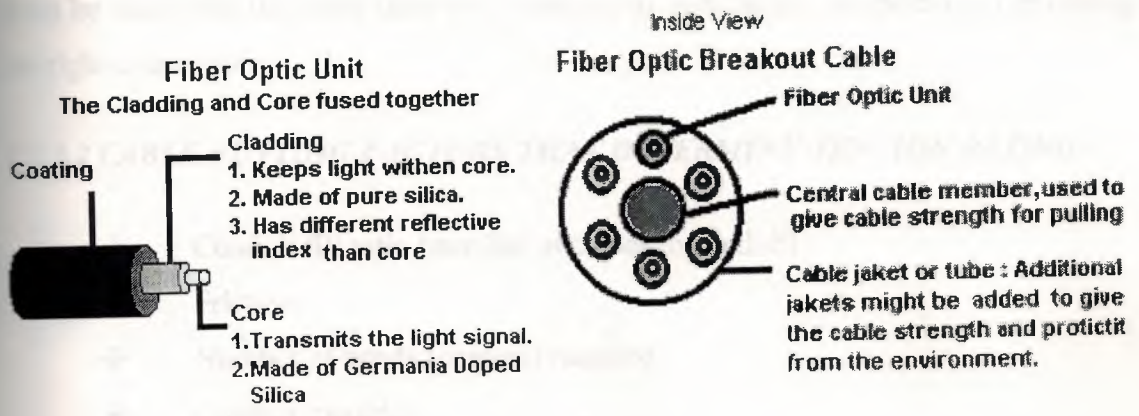


Figure 2.5.2 Fiber Optic Cable

2.5.7 CONDUIT PIPING

As everyone knows from looking at the back of a PC, the profusion of individual cables can be messy. To avoid tangles, cables are threaded inside a conduit pipe, which is a hollow metal or plastic tube that is run between walls. Security Recommendation: To prevent tampering, alt security wiring should run in unmarked conduit and not in loose raceways. This includes all wiring from the devices to EAC control panels and from the control panels to the main computer. Conduit categories are based on various smoke and flame characteristics. The best grade, which is also the most expensive, is General Purpose. It can be used in any of the four conduit categories.

2.5.7.1 CONDUIT CATEGORIES:

1. Residential (CM-X) — lowest grade
2. General Purpose (CM or CM-G)—commercial grade
3. Riser-rated (CM-R) — runs up or down walls between floor levels
4. Plenum (CM-P) — runs in ducts used for environmental air as well as air spaces in the ceiling

Older facilities may not have enough spaces available to hide conduit. In this case, wires can be run though a square channel raceway attached to the exposed walls. This is

not, however, a recommended method as it greatly heightens exposure to tampering. Cable is pulled through conduit, which puts a tremendous strain on the cable assembly. Consequently, the sturdiness of cable is rated by its maximum pulling tension and care must be taken mat the cable used will stand up to installation, in addition to providing the right connections.

2.5.7.2 CABLE PUTTING FACTORS THAT DETERMINE TENSION RATING:

- Conduit fill ratio (number of cables to conduit)
- Friction
- Number of bends (comers) required
- Conduit material
- Cable jacket material
- Maximum cable tension before snapping
- Amount and type of lubricants used to ease friction

Some cable jackets, like those used in fiber optics, contain materials that are specifically designed to take the entire force of the pull without stretching or cracking the contents. Special tools are required to make use of this jacket-type.

Care must be taken to not yank a cable through a tight conduit packed with other cables, or around a sharp comer, as this can break wires. Once the cable is instated, breaks are difficult to pinpoint and are expensive to fix. Needless to say, it is important that cable be repeatedly tested for wholeness throughout the installation process, or nasty surprises can result at the end.

2.5.8 CABLE SPECIFICATIONS AND SPLICING

Most installation guides specify cable and connector types. They also tell the purposes for which individual wires within the cable are used and how those wires attach to specific prongs, pins, or pinholes on connectors, if all this information is not packaged with the device.

The wires bundled within one cable can be transferred to several different cables through the process of splitting. To split a cable, you must first remove that cable's

jacket far enough to expose the enclosed wires, and then fan (separate) the wires for easy handling. Fanned wires are joined to different wires through splicing. This requires that the jackets be removed from the wires so that the physical wiring material is exposed. This material is connected to the same material in a second wire through a number of methods, the most common of which employs a connector cap that clamps the two together.

Connections might be made device-to-device or made in special junction boxes (which are also known as "breakout boxes"). These boxes protect spliced connections and usually serve as rerouting centers for joined cable.

Conduit is rated as to whether it can hold:

- Conductive wire (contains metallic properties)
- Nonconductive wire (contains no metallic properties)
- Composite wire (contains metafile and nonmetallic properties)

They are also rated for maximum voltage circuits. Grounding is required for all conductive and composite wires in conduit and injunction boxes.

The flow of information deteriorates, over long wiring paths. To boost the information signals, repeaters are installed at intervals. These devices, rebroadcast information, giving the flow a fresh start from that point.

2.5.9 WIRELESS CONNECTIONS

As of the mid-1990s, the development of wireless applications has been fueling a technological revolution. Here's why:

- **Portability:** Wireless devices can be set up in temporary sites. Visitor traffic, for example, might create the need to increase security in a given area for only a short period of time. Wireless access control, motion sensors, CCTV and other devices can be installed m such a case and then dismantled without extensive carpentry or damage to the environment.

- **Accessibility:** Wireless devices can be put where wired devices can't easily go. EAC in elevators, for example, requires long stretches of cable. Wireless EAC, however, can be installed with a minimum of fuss.
- **Creativity:** New wireless transmission techniques are being perfected that provides greater ranges, more jam-proof signals and no need for licensing. Among these is the increased use of frequency hopping technology, better known as spread spectrum that was developed by the military with high security in mind.

In 1993, revenues for in building, wireless hardware exceeded $ 100-million. By the year 2000, that figure could easily reach $1.9 billion worldwide.

In 1994, six million portable notebook computers were sold, most of which required a link to desktop computers and over 50 million cordless phones were in use throughout the world.

Experts believe that the above figures mark only the beginning of a movement that may surpass the computer revolution. One reason for this is that as the technology emerges, new applications will be developed that cannot be predicted today.

Portability of communications is important, especially to users of wireless phones and cellular services. The security industry, however, has more specialized demands. It must move data (such as held by electronic access control) quickly and with few physical constraints.

Cabled data-moving systems require massive investments in cabling and switching equipment. Wireless systems, however, can bypass these hardware investments even though throughput speed might sometimes be sacrificed.

The Personal Computer Memory Card International Association (PCMCIA) developed circuits the size of a credit card that plugs into the back of a computer. One PCMCIA device lets anyone create his or her own wireless computer network, or else instantly link with existing networks. Best, it uses highly secure spread spectrum technology, mentioned above.

In the right environments, radio waves can penetrate objects and walls without any signal disruption. Infrared technology, which depends on line-of-sight transmission, is struggling to compete. Tried and true infrared components include LEDs, laser diodes and photodiodes.

New infrared Transceivers (transmitters/receivers) are being developed that can bounce and reflect signals off walls and ceilings. Given the height of signal travel, these are not prone to random interruption such as may be caused by pedestrian traffic. The result is an infrared wireless network that can transmit at 100 Mbps throughout a 25 by 25 tool area. A new line of signal repeaters (power boosters) is increasing the distances of infrared transmission. Best, light technology is not subject to regulations, it is free from restrictions worldwide and it ensures data access across international boundaries.

Spread spectrum radio frequency technology, however, has captured everyone's imagination. Its secure signals, low power and general freedom from licensing makes it perfect for small and large computer networks, alike. It can be used for building-to-building transmissions and even as the backbone of new public communication services.

Currently, the technology behind wireless voice service is shifting away from analog and is moving to digital signals. Unlike voice, however, wireless data transmissions are extremely sensitive to errors caused by signal fading. Fortunately, emerging technology is boosting data signals, making it feasible to transmit data through cellular services. It is believed that the next generation of mobile radio communications terminals will be used more for data transmission than they will for voice.

Tied to these changes is the need for power conservation. This is forcing battery technology to provide longer life. If is also affecting transceiver design.

To lighten power requirements, components of transmitters are being eliminated. According to a representative at Hitachi, for example, their MOSFET modules do not need a negative supply voltage, nor do they require a drive circuit or power-supply switch and have zero current drain when the phone is not transmitting.

2.5.10 RADIO FREQUENCIES

Most, but not all, wireless transmissions are based on radio frequencies (RF). RF signals can be plotted on an analog chart, which measures amplitude and wave cycles over time. Understanding the chart, however, requires knowledge about amplitude, sinusoidal waveforms, harmonic content, carrier waves and phasing, to name just a few things.

The general public is most familiar with RF signals as described in Hertz Hz. This indicates the number of wave cycles (vibrations) per second that are present in the signal. These can be expressed as follows:

- Numbers 1 to 999: 50 Hz. 250 Hz, 875 Hz, etc.
- Thousands: 1000 Hz or 1 KHz
- Millions: 1000000 Hz or t MHz
- Billions: 1.000.000.000 Hz or 1 GHz

Signals are not limited to RF, however. In nature as well as man-made environments, many frequencies from differing origins compete with one another for airspace. Those that win disrupt or jam the losers. The RF signals that control a car burglar alarm, for example, are often within the range of signals generated by an electrical storm. This results in false alarms. Unwanted signals are a serious problem in security as well as in broadcasting. Consequently, governments have tried to control the problem by restricting users to specific frequencies within the frequency spectrum (range of all frequencies possible). This control is in the form of broadcast licensing and regulatory restrictions.

The range of frequencies in which a signal operates is called frequencies or just plain bandwidth. The following chart indicates the regulated bandwidth allocations in the communications industry. All RF transmissions require antennas. At the simplest level, an RF transmission requires a transmitter, a transmitting antenna, a receiving antenna and a receiver. When a transmitter is combined with a receiver, such as in a cordless phone, it is often called a transceiver.

The transmitter contains the power to broadcast the signal, if the transmitter is underpowered, the signal will not reach its destination. Transmitter ranges are enhanced by devices called repeater. These receive the broadcast signals before they become weak and retransmit them at full strength. A cellular phone system, for example, is made up of a series of repeaters placed throughout a community. The messages they control hop from repeater to repeater until they get to their final destinations.

Users of radio frequencies and other electromagnetic signals (such as the flow of information between computers) need to understand what it takes to make a clear, uninterrupted signal and, conversely, how that signal can be jammed. The following list describes some considerations:

2.5.11 WIRELESS TRANSMISSION CONSIDERATIONS:

- Government Regulation and Licensing: All RF and/or high voltage devices must meet government regulations, whether or not they require licenses. If they do not meet regulations, their potential for being jammed or jamming other devices is high. Do not rely on product labeling to establish regulation conformity. When buying security equipment, double check manufacturer specifications directly with the FCC.
- Surrounding Building Material: Metal substructures to buildings can block and/or distort signals some metals (like brass) more than others, if the RF device is portable, check for metals in all of the areas in which it will be used.
- Surrounding Natural Environment: metallic particles found in surrounding stone and/or earth can block and/or distort signals. RF transmission of any kind is difficult, for example, in communities that are rich in iron ore.
- Weather Changes: Check the weather change patterns in community. Periods of heightened electromagnetic activity found in lightning storms can block and/or distort signals, whether transmitted through RF or cable.
- Surrounding Equipment: Equipment that uses high, powerful frequencies can block and/or distort signals. Hospital imaging rooms, for example, can cause problems for other devices, especially the computer controlled devices found in security systems. Machine noise as well as the proximity of high voltage lines also disrupts RF.

- Line-of-Considerations: Infrared wireless transmission is not bothered by electromagnetic interference, but does require line-of-sight transmission. Determine what could unintentionally block the transmission area.
- Public Safety: Check whether RF devices interfere with Pacemakers or other health-related devices.
- Distance: Determine whether the RF device can cover the territory required and whether repeaters are necessary. Make sure transmission area is well within the limits, with room to spare. "Just fits" usually don't.
- Antennas: Determine the size and types of antennas required and whether premises can accommodate them. If antennas must be outside, determine whether local laws control their placement. If the antennas are outside property line, check whether other property owners will allow erecting them. An unwilling neighbor can destroy the best wireless system design.
- Power Requirement: All signals require power and power requires cabling or batteries. Make sure that enough power is available for the time during which the device will be used. RF frequencies that require more than one Watt also require licensing and other regulations. This may restrict the freedom of use for which the device was intended.

2.5.12 ANALOG-TO-DIGITAL

When a computer receives information from an analog signal, such as a standard telephone signal, it must translate that information into binary code. (See the MM for further information.) Each point on an analog chart corresponds to a number and a moment in time. These unique numbers exist on a table (a chart of numbers) that the computer uses to translate analog numbers into binary numbers (or vice versa).

Analog-to-digital translations are made by a special computer chip that is embedded in a data acquisition circuit board. A similar chip is found in a modem (an acronym meaning "modulate - demodulate") that connects computers through analog telephone lines.

Although the telephone system trunk lines are controlled digitally, line card circuit, which are the links between the general-use lines and specific customers, are mostly analog. Modems are only needed when computers communication through analog

data, video, fax and/or speech — to be sent in one transmission over old-fashioned phone wire. It does not, however, necessarily speed things up.

Multiplexing can be used to transmit a variety of digital video signals in one data stream by patching these signals together. Transmission of one image, unfortunately, must be stopped before another can be sent. Needless to say, images are lost in the process.

Another solution is to eliminate modems.

In the early 1980s, a group of telephone carriers banded together to develop the Integrated Service Digital Network (ISDN) to speed the flow of data over standard phone lines. The objective was to bring the greatest improvement for the least possible cost. ISDN technology improves the data transmission properties of standard copper wire telephone cable by making use of multiplexing technology, in addition to providing pure digital connections.

ISDN splits the services of common two-wire phone cable into three channels. Two channels provide 64 Kbps (64,000 bits per second) data transmission each and can be combined to provide 128 Kbps (128,000 bits per second). The third channel (D-channel) is used for call setup and signaling. It can also be used for voice through the use of a codec, mentioned earlier.

Higher speeds can be achieved when fiber optic cable is used: the actual transmission speed, however, is only as fast as the transmission, switching and receiving equipment will allow. As of 1995, the highest transmission speed a modem could achieve using analog telephone lines was 28-8 Kbps (28,800 bits per second). Unfortunately, this speed cannot be consistently maintained because of data compression problems. Data compression works by reducing stretches of repeated information, such as "white space" through more efficient codes. The problem faced by ISDN is that although the vast majority of trunk lines are digitized, the lines leading to individual residences and businesses are not. Converting these connections requires abandoning all existing telephones, installing new line cards at every point and investing in new digital receivers for everyone at a cost of trillions.

The implication of Metricom's success, then, is that wireless technology is challenging wired systems. Wireless transmission, of course, requires antennas and some communities do not want antennas erected. Consequently, in 1995, the United States Government began debates on antenna placement and licensing to safeguard that interstate data transmission would continue to improve especially important to national security! Dedicated computer networks, however, transmit data at far higher rates than is done over public carriers. These rates can range from 1 Mbps to 100+Mbps. depending on me networking system. Like transmission over public carriers, however, speed degrades when many people are using the network at the same time. Like telephones, if a receiving computer is busy, data cannot be transmitted at all.

- **Data Transmission Carriers:** Data networks, such as between security substations, currently make use of a number of wired and wireless transmission carriers, depending on need and budget. These include:
- **Computer-to-Computer:** (networking) - dedicated systems, which include cable and wireless modes of communications, these transmit data at the fastest rates. Acronyms include LAN (local area network), WAN (wide area network or building-to-building), and MAN (metropolitan area network or communicating throughout a geographic area).
- **Public Switched Telephone Network (PSTN):** standard phone lines with a maximum bandwidth of 28.8 Kbps based on V.34 protocol.
- **Integrated Services Digital Network (ISDN):** standard phone lines controlled exclusively by digital switching equipment which provides two 64 Kbps digital channel plus one channel connections and voice transmission. A bandwidth of up to 128 Kbps can be achieved by combining the first two channels. Note: A codec is required on this digital network in order to send voice.
- **Digital Data Service (DDS):** a special leased line (dedicated line) that offers either 56 Kbps or 64 Kbps bandwidths.
- **Switched 56 Network (SW56):** a dial-up service that offers a 56 Kbps bandwidth. A special code number must be dialed to connect into the network before the destination number can be entered. This lets users pay only for the time they use without requiring a full-time teased line.

- **Digital Cellular Service:** wireless data transmitting service with a t9.2 Kbps bandwidth.
- **Digital Spread Spectrum Service:** wireless voice and data transmitting service based on spread spectrum technology with a bandwidth up to 77 Kbps and guaranteed throughput of 38.4 Kbps.
- **Satellite:** wireless transmission that carries data long distances at speeds comparable to those of DDS or ISDN lines. This is not, however, the best way to transmit data as pauses in transmission can significantly increase transmission time, thereby reducing transmission speeds or destroying it altogether. Improvements in transmission speeds and switching technologies are being made daily. The race is on.
- **Estimated Data Transmission:** *Importance of Communication Speeds.* The chart on the next page will allow calculating rule-of-thumb values to determine potential bottlenecks and delays in communication system.

Monitoring the actual transmission speeds in system will allow spotting problems and fixing them before the system completely fails.

2.5.14 TRANSMISSION CONSIDERATIONS

Wireless systems are used when the cost of wiring is prohibitive or too complex to maintain. Whether the need is present or not, however, today almost any device that sends information can be designed to do so wirelessly. Unlike their cabled cousins, however, radio signals can be more easily contaminated by noise (lightning, nearby power cables, machinery) and consequently, cannot provide fail-safe performance. In addition, because frequencies are generally available "in the air." many receivers can capture them keeping spies well employed. This is a particular problem with cordless room monitors, phones and cellular services, to name a few.

The military has the highest need for confidentiality and so has developed many jam-proof RF systems, which are not available to the general public. As they develop better systems, however, their older technology is released to the general market.

Spread spectrum, for example, was developed during World War II (1940s) and was declassified in the mid-1980s. It provides jam-proof security by broadcasting a single

message over multiple wavelengths. Each part, then, is sent over different frequencies, making it impossible for a spy to patch together the broadcast without a one-of-a-kind receiver. Access control devices using spread spectrum operate in the 902-928 MHz range and can transmit to distances of 3,500 feet or more with special antennas. The FCC does not require licensing as long as its maximum transmission power is restricted to 1 Watt. Computer networks and digital services using this technology broadcast at higher bandwidths.

Spread spectrum is now playing an important part in the communications industry because of its high level of security. Its technology is used in data transmission services such as Metrocom, mentioned earlier in this chapter, wireless computer networks, wireless phones and. of course, wireless access control.

2.5.14.1 PROBLEMS WITH SIGNAL CARRIERS AND RECEIVERS:

As stated earner, connections (wired or wireless) require a transmitter, an information carrier and a receiver. General broadcasting sends its signals as a one-to-many. This means that one broadcast will be received by anyone who is tuned on an appropriate receiver. Private communications, however, are usually transmitted as one-to-one, or one-to-a-select-few. This means that when all the carrier lines are used, no new transmissions can be made Likewise, if the target receiver is in use, no transmissions can be made, no matter how many lines are available.

Phone lines and cellular services in large communities jam during peak hours. This even happens in small communities where the trunk lines haven't kept up with the growing population, or there is a sudden surge of visitors, as happens during the summer with tourists. In addition, computers are being called upon to monitor more and more areas. If the system isn't distributed, or too many remote computers are trying to send alarms to the same host computer, jams occur. Security professionals need to calculate the effect of receiver availability and the potential of line-jams when designing their EAC communications network. The fastest data transmission system in the world is only as good as its ability to make a connection.

essage over multiple wavelengths. Each part, then, is sent over different frequencies, making it impossible for a spy to patch together the broadcast without a one-of-a-kind eceiver. Access control devices using spread spectrum operate in the 902-928 MHz ange and can transmit to distances of 3,500 feet or more with special antennas. The CC does not require licensing as long as its maximum transmission power is restricted o 1 Watt. Computer networks and digital services using this technology broadcast at igher bandwidths.

Spread spectrum is now playing an important part in the communications industry because of its high level of security. Its technology is used in data transmission services such as Metrocom, mentioned earlier in this chapter, wireless computer networks, wireless phones and. of course, wireless access control.

2.5.14.1 PROBLEMS WITH SIGNAL CARRIERS AND RECEIVERS:

As stated earner, connections (wired or wireless) require a transmitter, an information carrier and a receiver. General broadcasting sends its signals as a one-to-many. This means that one broadcast will be received by anyone who is tuned on an appropriate receiver. Private communications, however, are usually transmitted as one-to-one, or one-to-a-select-few. This means that when all the carrier lines are used, no new transmissions can be made Likewise, if the target receiver is in use, no transmissions can be made, no matter how many lines are available.

Phone lines and cellular services in large communities jam during peak hours. This even happens in small communities where the trunk lines haven't kept up with the growing population, or there is a sudden surge of visitors, as happens during the summer with tourists. In addition, computers are being called upon to monitor more and more areas. If the system isn't distributed, or too many remote computers are trying to send alarms to the same host computer, jams occur. Security professionals need to calculate the effect of receiver availability and the potential of line-jams when designing their EAC communications network. The fastest data transmission system in the world is only as good as its ability to make a connection.

CHAPTER THREE: SYSTEM DESIGN AND INTEGRATION

3.1 System Design

3.1.1 A TECHNICAL DESIGN PERSPECTIVE

Up to this point, this project discussed many of the components used to create an Electronic Access Control (EAC) system. This describes the issues involved in combining these elements into a system. A system is a collection of components that functions together for a single purpose. Obviously, the single purpose of an EAC system is to control physical access to a building or other facility.

3.1.2 SYSTEM DESIGN GOALS

From a technical standpoint, all properly designed EAC systems have at feast two things in common:

- Systems are sized to meet the needs of the intended function, and
- Systems have safeguards against failure.

3.1.2.1 SYSTEM SIZE

A property sized system meets the needs of the intended function. It allows for future growth, but does not saddle the system with unneeded equipment. Sizing choices are made for now and in the future. They include the number of:

- Doors to be controlled (In this project 18doors)
- People who will use those doors (In this project around 50 employees)
- Sensors to be monitored (In this project around 22 sensors)

3.1.2.2 SYSTEM SAFEGUARDS

Systems are designed to work, not fall. Unfortunately, in the real world, failure occurs too often and at times and places that can be highly inconvenient. Therefore every system must be designed to fail gracefully. This means that as components fail, the system should continue to provide as much functionality as possible. Planning for graceful failure means that the designer must review each component of the system and

determine the resulting operation of the system should that component fail. If the remitting operation is unacceptable, redundant or alternate methods must be added. The good news is that today's distributed intelligent systems are designed to be redundant. They generally allow to" multiple component failures before facility security is compromised.

3.1.2.3 REDUNDANCY

The EAC has true redundancy. The system can be configured with dual LANs between computers and can also have dual databases or LANs to the field processors. Triple redundancy can be achieved by backing up each field processor with an adjacent processor in case of failure.

Both the embedded PC technology and the distributed database architecture have made this redundancy capability possible. Because manufacturers do not offer this capacity, many large commercial and government installations do not have redundancy.

3.1.2.4 REPORT GENERATION

Numerous reports can be created using the EAC's vast database and tailored to the specific needs of the site and operator. A list of lost or stolen badges can be created as can a list of cardholders who were denied access into an unauthorized area.

3.1.3 EAC SOFTWARE OVERVIEW

The software is written in C and utilizes the SCO UNIX Operating System. It is compatible with the latest PC chip technology having been designed to run on 486 and Pentium processors.

The EAC software employs a Graphical User Interface (GUI) utilizing X-Windows to equip an operator with the full power and flexibility of the system in an easy-to-use format. Graphical maps are created to both provide notification of alarms and events and serve as platforms from which an operator can control the field devices in real time. Coupled with a collection of simple data forms, the system permits a user to configure the site to gather data regardless of his or her skill level.

The software gives EAC the ability to function in the role of a complete card access system capable of monitoring site security and controlling access throughout a location. Card Control Systems has taken advantage of the UNIX operating systems flexibility and developed a product that can address the needs of the largest sites with complex card access requirement. Coupled with the Video Badging Component, the EAC can create the very access cards it will later monitor and track making for a seamless connection of the two functions.

In addition to monitoring a site, the software is designed to assess itself continually by updating the status of software processes at the heart of the system. Processors in the field and communication links between them (utilizing a LAN) are monitored and the results are depicted graphically through the GUI's on-screen maps. The System utilizes a powerful database to permit users to build and generate a variety of reports - many tailored to specific site usage by the system operator.

3.1.3.1 DATA ENTRY USING FORMS

In addition to enrolling personnel into the database, forms provide a simple way to shape the parameters of the system by adding or modifying devices telling the system what time to perform various functions and creating relationships between, inputs and outputs (such as turning on the lights in a building when the first employee at work that day presents his or her badge). The operator is prompted to enter the correct information in spaces provided directly on the screen and when the form is completed satisfactorily, the information is automatically added to the database.

These higher-level programming techniques have begun to appear in the security industry base computer software programs. However, the field processors continue to use micro-controller technology.

Use of embedded PC technology projects these software technologies beyond the base system and into the field, in addition to shortening development cycles. The modular packaging design allows for configuring hardware simply and quickly with minimum technical risk.

Plan 1

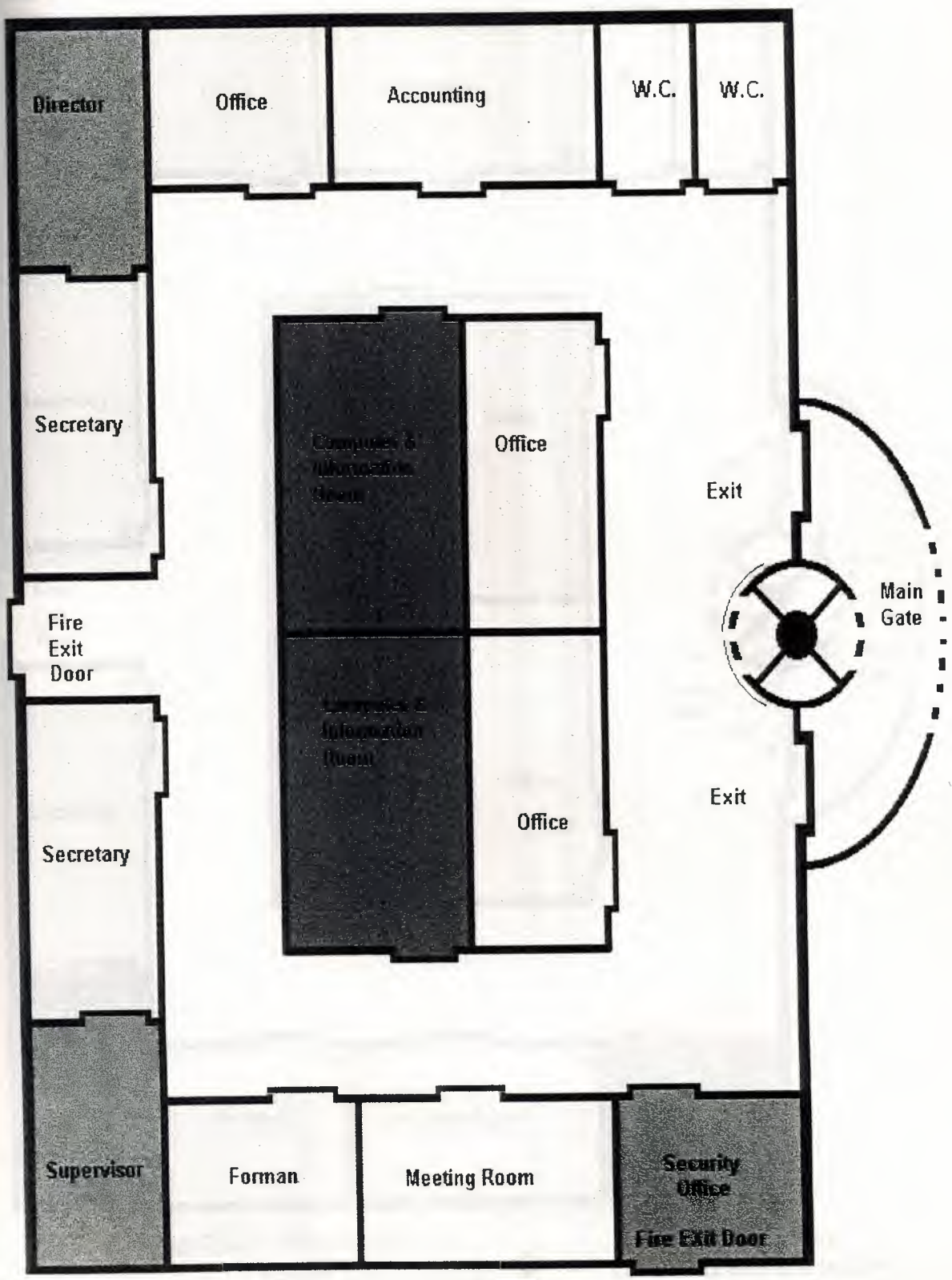


Figure 3.2.1 PLAN 1 The distributions of rooms and security zones

Plan 2

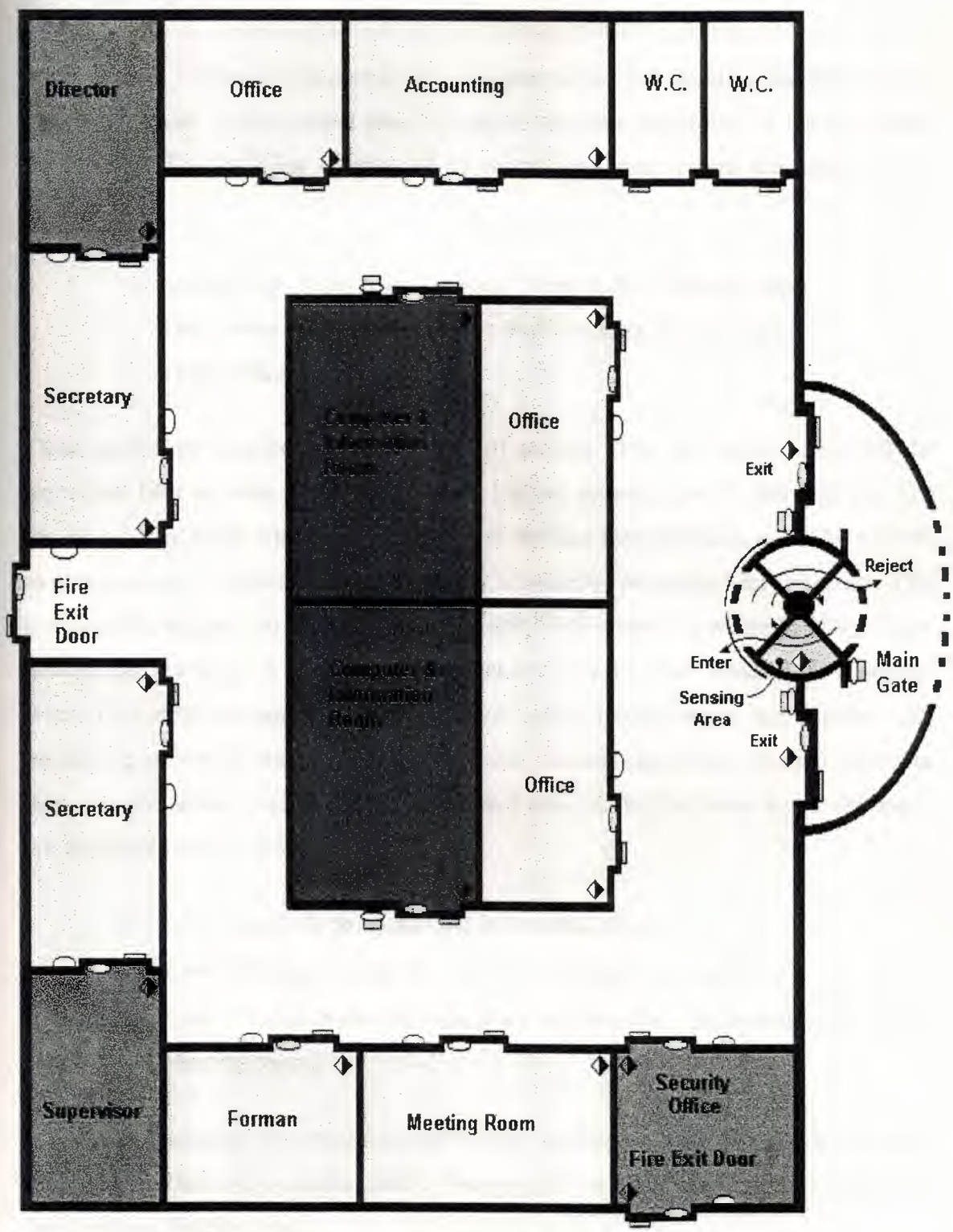


Figure 3.2.2 PLAN 2 Electronic access control system EAC applied to the building

3.2 Plan 2 & 1

In these plans, I illustrate the distributing of rooms within this building and distributions of security zones. In the second plan, I illustrate the same plan (plan 1), but with doors components. This building consists of 13 rooms, and these rooms are distributed as follows:

1. Accounting, Supervisor, Director, Meeting and Foreman room.
2. Two rooms for each of secretary and computer & information.
3. Three offices.

These rooms are distributed into 3 levels of security. The first level, which will be mentioned later as zone A. This level is the highest security level in this building. The second security level, which is also high level, but less than previous, it will be referred as zone B. Zone C, which is the lowest level of security, we applied for the rooms. This level we can accept it as middle level of security with respect to whole building. These three levels, we apply it in our rooms but not between. In other words there is another level of security, we apply it at the corridor, which monitoring is just applied. This monitoring is done by the use of cameras. These cameras can contain its own sensors or they toke the sensed signals from independent sensors. Within these levels the rooms are distributed as follows:

- Zone A include computer and information rooms.
- Zone B includes supervisor, Director and security rooms.
- Zone C includes the rest, which are the Secretary, Accounting, Offices and Meeting rooms.

These three zones are in normal days and within working time in other words in holiday and nights (if there is no another shift). These rooms are distributed into two zones. And here are their distributions:

- Accounting, Secretary, Supervisor, Director, Foreman And Computer & Information room.
- Offices and Meeting room.

First group of rooms are obeyed under the fourth security level. The rest obey under the fifth security level (also corridor), in case of second shift or overtime work. The offices, which are still working, are obeyed under its normal security level. Forth and fifth security level will be mentioned later

In case of emergency all rooms are not allowed to go in but only to go out. In the case we need to go inside one of the rooms, the only way to open the door is done by taking permission from security office.

Our building has three gates and two fire exits and the system is also controlling 13 doors. Each of the thirteen doors has its own door closer, lock and credential reader. These doors are controlled by three ways:

- Through supervisory computer in the security office.
- By control panel, when stand-alone.
- By the hand reader in some cases.

How To Open The Door?

- By applying the credential into the credential reader in the three cases mentioned above.
- By opening the door from supervisory computer, here the security man is responsible for the entrance and this operation is done as follows:
    - Entering the name and password of security man
    - Filling the forms, which includes mainly the reasons for this operation, Date, Time and door(s).

➢ In case of emergency only name and password are enough and then individual can open the door.

3.2.1 MAIN GATES

In this building we have one revolving door, which is used only for entering and another two doors for exiting. These doors got hand readers. These hand readers are used not only for opening the door but also, it works to register the attendance time. Each door of these doors has an automatic door closer, which is fast and strong. The locks of the

revolving door and exiting doors are electrical, but the lock in the revolving door is fail-secure while in the exiting doors are fail-safe.

3.2.2 NORMAL DOORS

The thirteen doors got two types of credential reader.

- Card reader (smart card reader)
- Hand reader with smart card reader

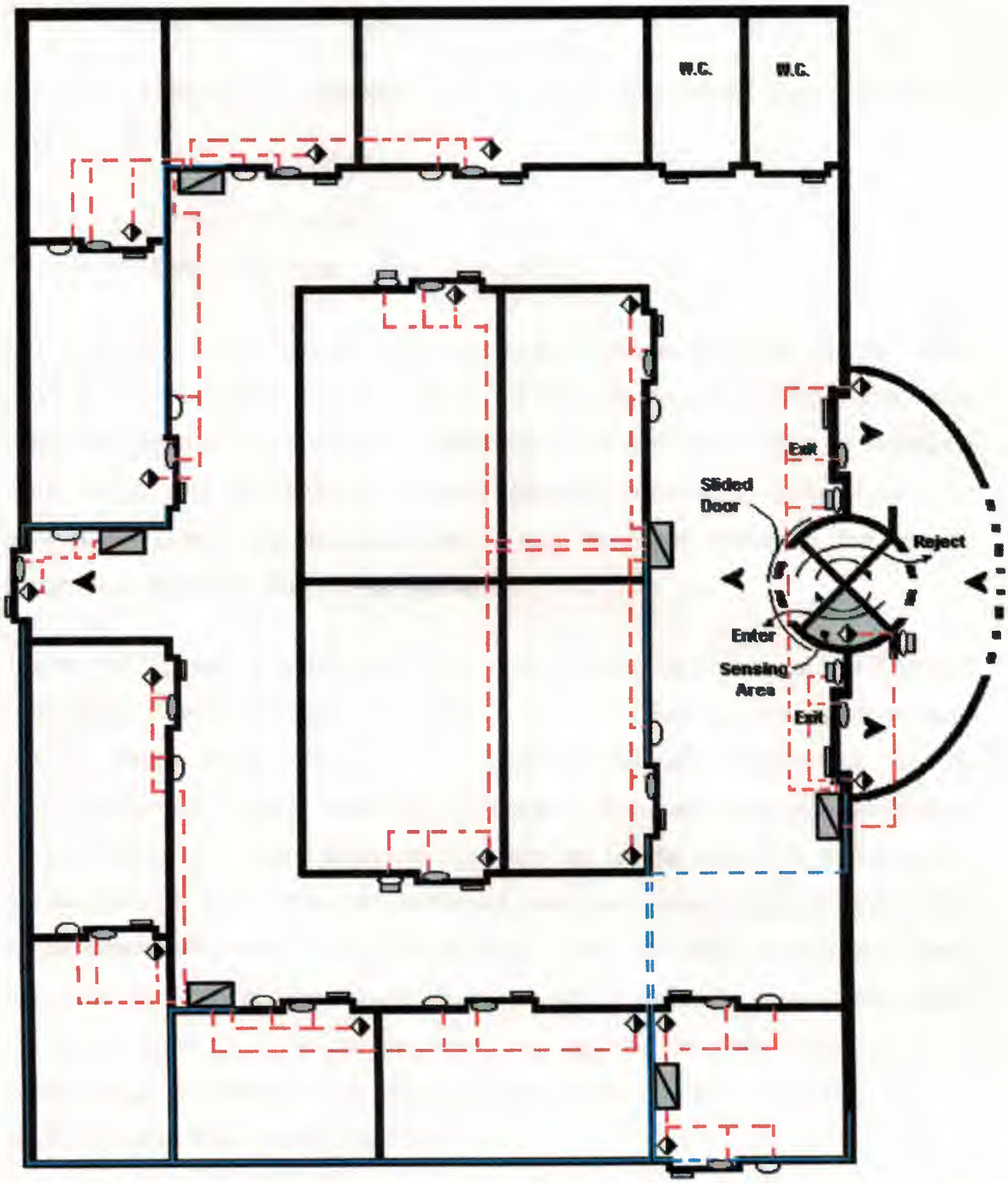
These doors, which have card reader, got normal door closer and magnetic or electromagnetic lock. The one that got hand reader has automatic door closer and electric lock.

Figure 3.2.3 Hand Reader With Smart Reader & Smart Card Reader (contact/contact less)

3.2.3 FIRE EXIT GATES

These gates have an automatic and high speed closer. This door closer is different from the normal closer, and we can also see it in the main gates. Fire exit door has its own specialist. It has special door hands, which is called Exit or Panic Bar. When this bar is pushing by any one in case of emergency, the lock automatically opens this operation is mentioned early in the previous chapter. This bar has wide area to open and to make it easier and faster to run out from the building. These doors are fail-safe and their locks are electrical one.

Plan 3



Control Panel usually inside the wall contains back up battery and power supply unit

LAN (TCP/IP) Network Communication Lines, RS 485 standard is used.

Control Connections lines (power lines, communication lines using RS 422 or RS 232 standards and other). Not in its same locations and it from different line types

Figure 3.3.1 PLAN 3 EAC System Connection Lines

3.3 Plan 3

In this plan I showed the connection of the system in our building. These connections have two types

- Network connections
- Door connections (control connections)

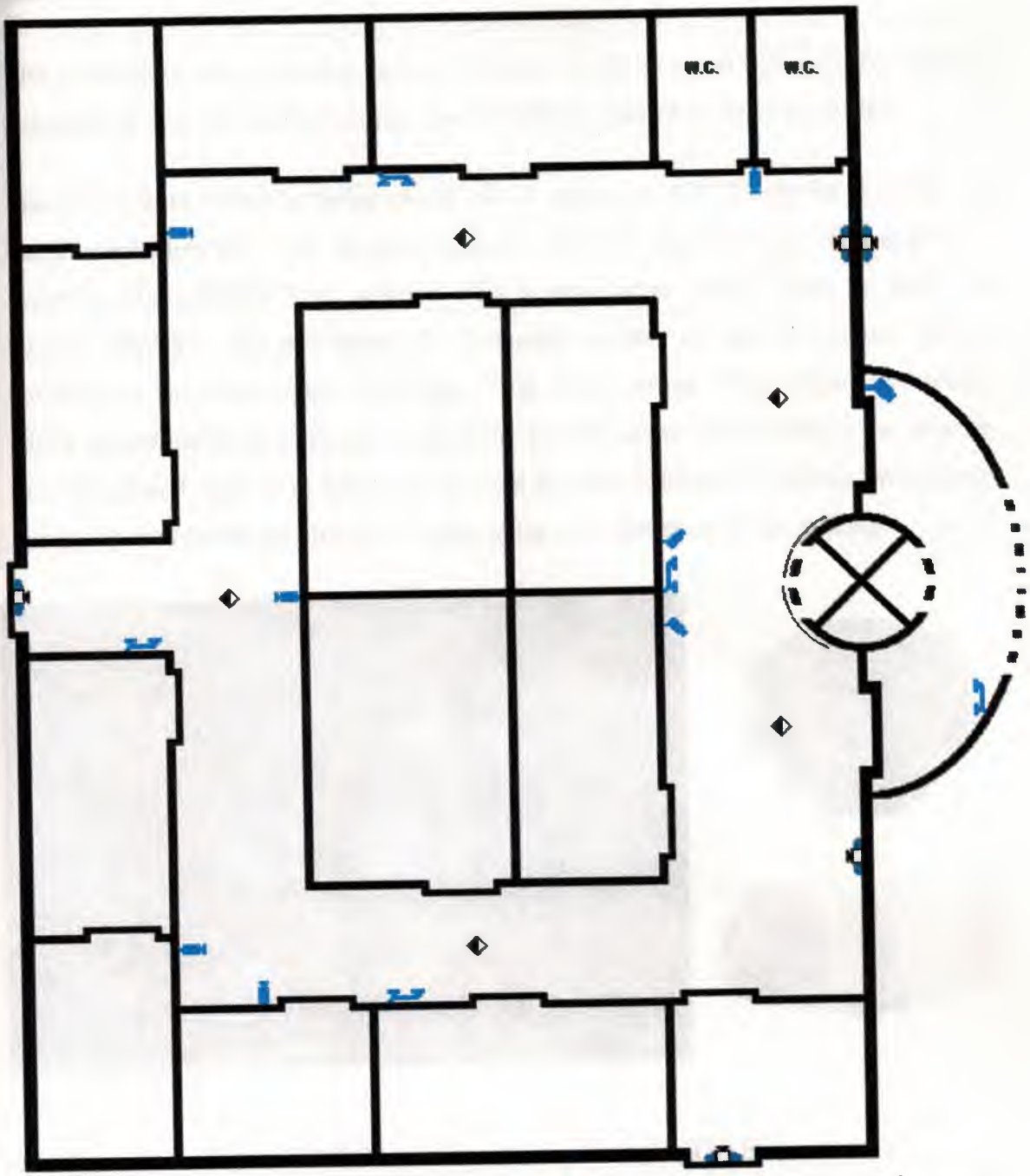
In the network connections the cables are mostly coaxial. Here we use multi-drop connection. This connection is shown in the previous chapter. This network connection starts with the supervisory computer and finishes with network terminating resistance while control panel is connected in parallel between. Now in my design I need my network line (bus) going into a long path to meet the future extending. The network connections lines work with RS-485 standard.

The second type of connection lines is the door connections or we can call it control connections. These connections connect the door lock (which includes also door status sensor), Motion sensor (which detects the entering and exiting operations from the room) and credential reader (what ever card reader or both hand reader and card reader) are connected to the control panel and these lines are not the same. It is different from one equipment to the other (e.g. in door lock it needs only power lines and another lines for the sensor, which includes in it, but for motion sensor we need only two lines. These lines hold the power and the changes the power, which makes the control panel detect the sensed signal from the motion sensor) and also the standard, which is used to communicate between the door parts is different from one to another (e.g. for card reader connection lines RS-232 standard is used).

Power line does not appear in our plan but they are mainly come from security office directly to each control panel. These panels contain inside power units, which contains transformer that changes the power, which are needed for each equipment. Most of the equipment works with low power. This power part contains also backup battery in case of power failure. It provides itself and the other equipment with power needed.

The network connection line is not only one line. It also contains another line for redundancy that increases our network efficiency towards bus cutting.

Plan 4



Motion Sensor

Colored Camera able to work with infrared technology.

Colored Camera usually this type of camera is too small & hidden

Communication device use to contact with security office and for announcing

Both visual and sound alarm use in case of fire or wrong entering

Figure 3.4.1 Plan 4 Auxiliary Systems

3.4 Plan 4

This plan shows two supporting systems. These two can be found within the building as independent systems, but this project deal with these systems as auxiliary systems.

The first system, which is called closed circuit television (CCTV) works to cover the building corridors and main entrance mainly, and doors as extra work. This system is important for effective EAC system. This system helps security man to sight the building situation; also it is helpful in decreasing number of security workers. In the building we have two types of cameras. First is the normal video camera (Colored), which is used inside the building to detect the building status. Second one is the same as first but it has the ability to work with no light by using infrared technology, which may result of power failure and this one founds in the main entrance of the building.

Figure 3.4.2 Closed Circuit Television (CCTV) System

The other system is communication system. This system is used already within the building to communicate between the offices, but in this project we deal with only that part, which is responsible for communicate between individuals in the corridor and main gate with security office. This system is used to increase the efficiency of the EAC system by helping the user to contact directly with security office when facing any problem with EAC system, such as failure in entering, failure in card, emergency etc.

Plan 5

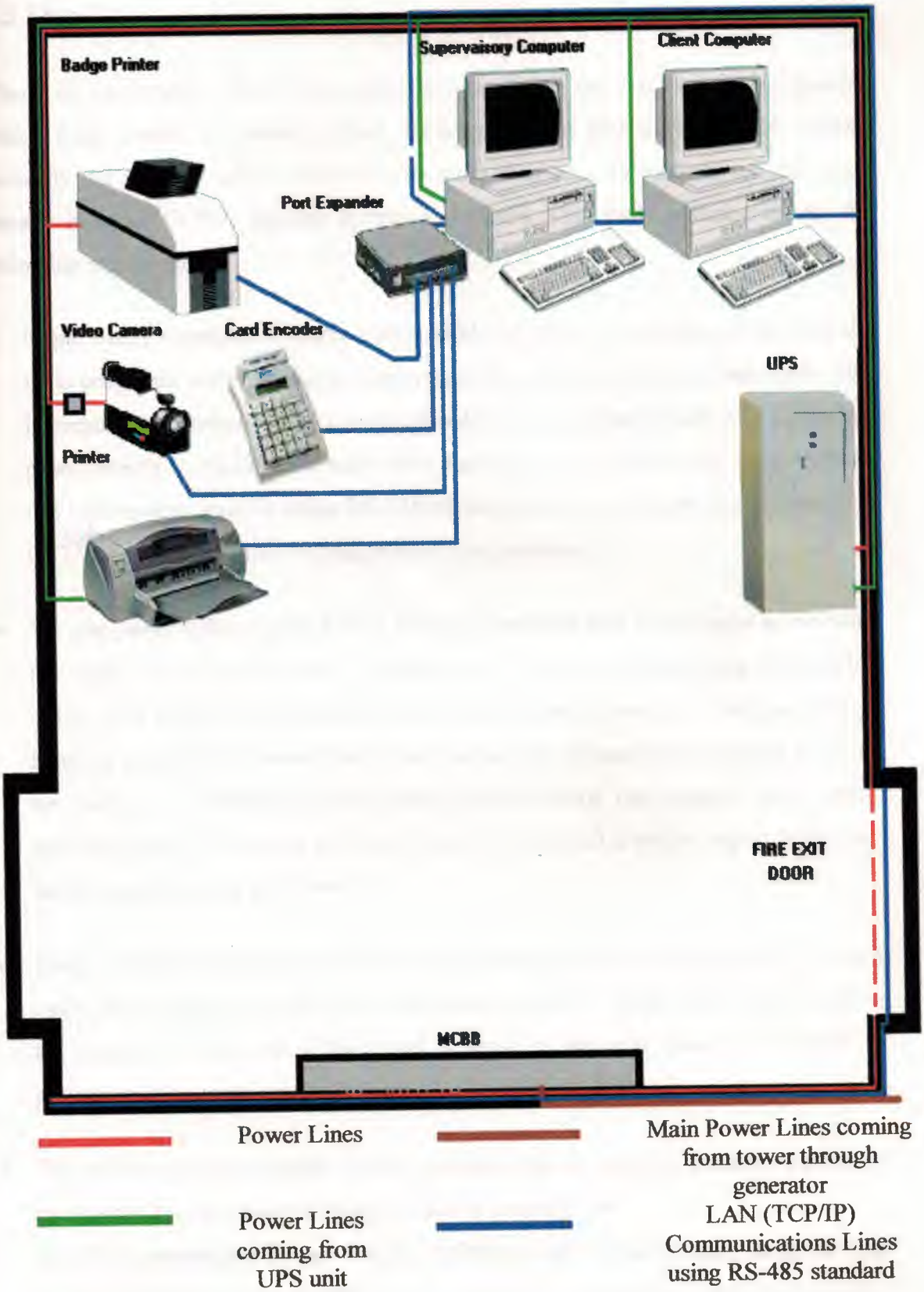


Figure 3.5.1 Plan 5 EAS Components, which found inside Security Room

3.5 Plan 5

Plan 5 shows security office from inside. In other words the EAC system equipments, which found inside the security office. I covered in this plan only the EAC system, normally the security office contains even more than security system, and this room usually includes CCTV, lighting system and others. This room contains mainly the following equipments:

- **Supervisory Computer,** which is responsible for all the EAS system, it contains the main programs, which is control the system through the software found inside, also it contain the database of all credential holder and it communicate with all control panel directly to make the system work fluently without bottleneck, the transfer of this information done by using RS-485 standard this computer can also connected to CCTV system for picture recognition and card encoder...

- We also have in the security office **Client Computer** that works same as previous, but when first computer fails. In normal case it is use for monitoring the building status in its screen but it mainly focus on the opened doors and main gate though focusing the cameras toward the opened doors, also we need printer in this room, so we can got an instance report, daily reports about our system status, error, attendance time for worker and many more, we can had a written report before last failure happen to our computer.

- **Badge Printer,** which can offer the cards needed in first export and later in such cases (lost, damage, stolen, temporary and new cards ...etc.), this is only found in the system, if and only if that card is apple to be print, some card unable to programmed or made out the industry.

- The office contains **Digital Video Camera** that is used to entering picture of cardholder into computer to badge printer or program use.
- The **Uninterruptible Power Supply (UPS)** provide the supervisory computer and the printer of EAC system with power in case of power failure, until the generator works or the power coming back, also it provides the other systems. UPS can work

- For loge time in case of failure of power generator to provide the necessary power (the control panel contains it own backup battery).
- **Main Circuit Breaker Board (MCBB)** This board is necessary to be found inside the security office to keep it away from any external destruction, actually this increase our system immunity.
- Also we have in this office **Telecommunications System** that enables us to contact with individuals outside the rooms within corridors.

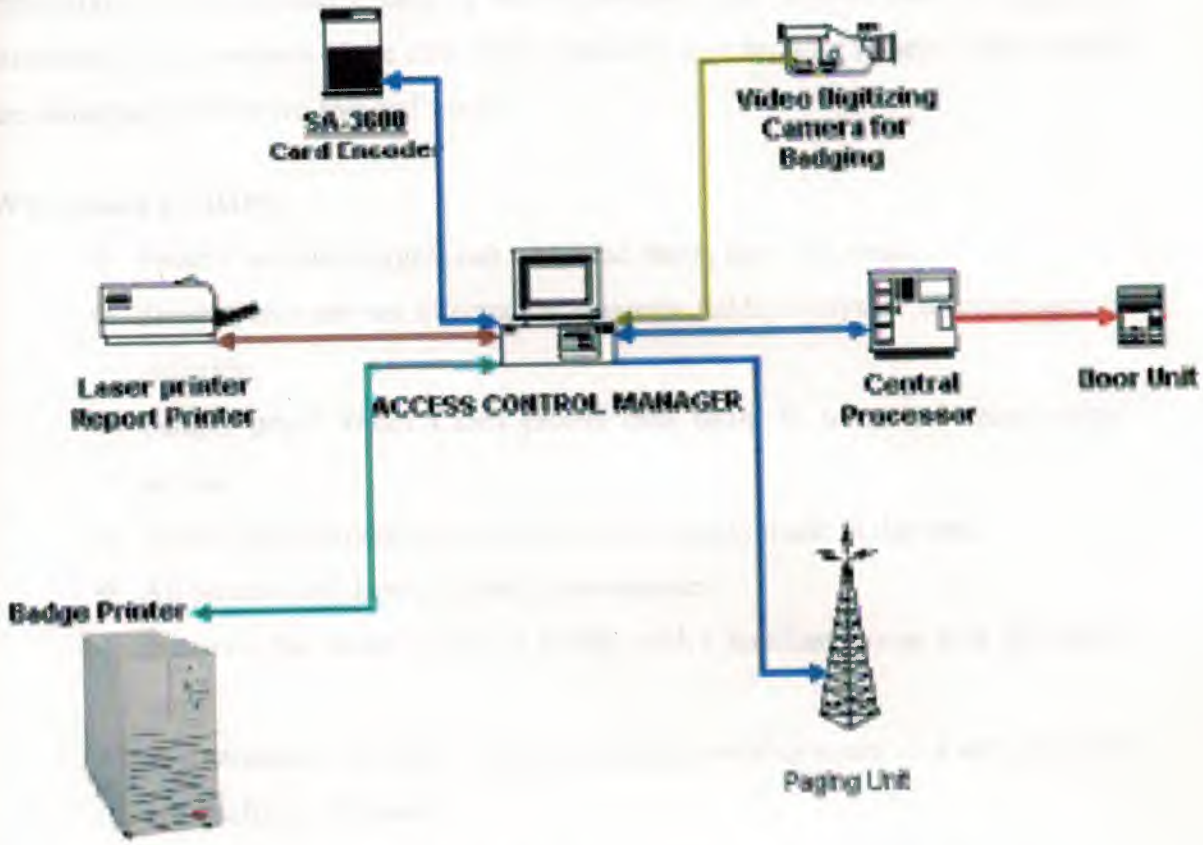


Figure 3.5.2 complete EAC system inside the security office.

3.6 System Components

3.6.1 CARD READER

A Smart Card, which has been chosen to be my system card, this card is a plastic card that has been embedded with a microchip that stores, manages and processes information. Where plastic cards are limited to little stored data, technological advances provide Smart Cards with the capability to contain not only more data but also multiple applications. The embedded chip is preprogrammed with several files or pages of information and contents of the chip can be protected by a security code(s). Smart cards are changing the way we live and work.

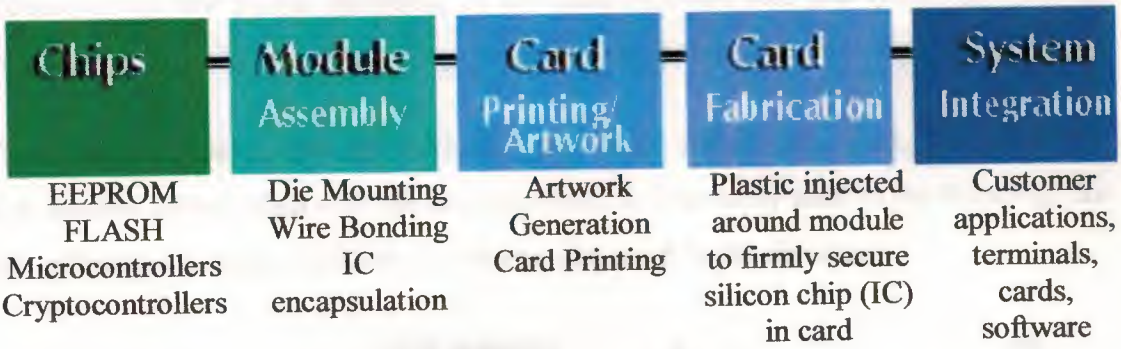
Why Smart CARDS?

- Smart Cards are rugged, can withstand shock, heat and torque.
- Smart Cards are not affected by magnetic fields, x-rays or electromagnetic radiation.
- Tamper-proof Smart Cards protect data better in terms of unauthorized access.
- Smart Cards provide an audit trail of all changes made to the card.
- All Smart Card data encoded is non erasable.
- Presently the Smart Card is a novelty with a familiar format that of a credit card.
- With enhanced artwork, it is a powerful advertising agent to a very practical and useful application.
- The ability to work as proximity card (contact less).

Smart Card Attributes:

- Smart Cards feature high reliability and robustness.
- Smart Cards can be integrated with magnetic stripe, signature panel, and/or embossing.
- Smart Cards can provide the most secure environment for transactions and records.
- Smart Cards can be configured and segmented as a credit/debit/electronic purse.

- The memory can be read and written in excess of 100,000 times.
- There are three categories of Smart Cards: contact, contact less and dual interface.
- High immunity (difficult to duplicate), that is because of the ability to store and to process the information.
- The AMMI Smart Card Chain:



Smart card as mentioned in previous chapter looks like the normal credit card in size, but it got a metal part inside, in some times it includes the photo of the holder and some other information, such as it might contain the name of holder and department and such information required, it can also work as mixed technology card, and for this kind of card the readers need to enter the card inside, not to slide it, also it works as proximity card (just passing). This type of cards helps the system when stand-alone because it is able to process and store some information, this type of card can easily be programmed, so it is possible to change the program inside the card at any time, which makes the card able to meet the improvement in programs.

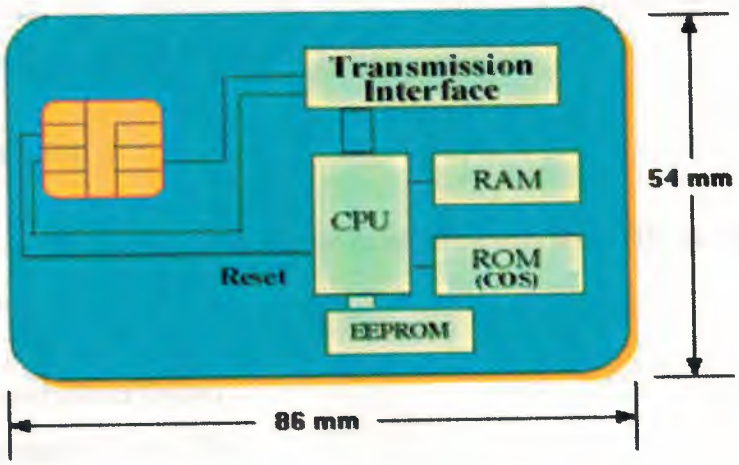


Figure 3.6.1 Smart Card Block Diagram & Size

3.5.2 THE LOCKS

The lock or strike of the door is the equipment that controls the door by keeping it close or enable it to be opened, those which are used in this building are divided into two types:

The Electromagnetic/Electric locks are the main locks used in this building that is because of the low power absorbing by this kind of locks, also this system provides us with very strong lock. And the energy absorb by the lock is just when locking the door.

The Magnetic Lock is that type of locks which have widely been used, but this kind of lock absorbs power when ever the door is closed so it is rarely used in our building, this type of locks is simple, this kind of locks we can see it in the elevators

Figure 3.6.2 Different types of magnetic & electromagnetic locks.

These lock include also the door sensor, which detect wither the door is open or not this sensor is used for two reasons: 1st for detect door status, 2nd to start timing for the door (the door must close after specific time, which is different for each door), this sensor directly connected to the control panel.

3.5.3 DOOR CLOSER

Here we care about the type of security we have when this door fail, as mention before we have two types:

- Normal closer (slow)
- Automatic closer (fast)

The 2nd type of closer I use it for high security level, which we applied in the main gates, fire exit door and computer & information rooms, while the 1st type we can see it at the others. The normal door closer with oil pressuring and the second may contains motor or by electromagnetic effect

Figure 3.6.3 Different Types Of Door Closer.

3.5.4 MOTION SENSORS

The motion sensor is not only sensor but it is a complete circuit that work to send ready signal to the control panel this sensor is used to detect both:

- Motion (whiter there is passing or not).
- Counting the number of persons whose pass the door.

And so this sensor has got an important role in the security and the efficiency of that security.

3.5.5 CREDENTIAL READERS

In this building I had use two types of reader, which are:

1. Hand reader and this also contains smart card reader
2. Smart card reader

The hand reader system is able two works alone without control panel in case of stand-alone.

WHY WE NEED SMART CARD READER WITH HAND READER:

- This smart contains some information that is necessary such when hand reader in case of stand alone
- In some cases we are able to use any of the readers such as when the employee hand got a problem
- We have two different types of smart card reader one we can see it out side the wall and the other inside the wall. Smart card reader has more immunity against environment and this is because of the fact that the reading head in smart card reader is inside the reader not on the face so smart card must insert inside the reader not to slide it.

3.7 How dose the system works

Here I shall speak about Enter & Exit operation and how system will work and how it will deal with different problems

3.7.1 ENTERING OPERATION

3.7.1.1 MAIN ENTRANCE

When any one come to enter the building and the system is not working, the camera in the main entrance give a signal to supervisory computer to turn the system on, this operation happens only when first employee come to the work at morning, the employee directly go toward the hand reader, insert his card into the card reader then entering the name & password -the name must be different from the original name- to the machine, then the reader test these information, usually, the card reader which is combined with the hand reader has this ability to that, but in case of the normal reader it must transfer these information to the control panel and from there to the supervisory computer and there it will be checked, then if these information is ok. The user will receive a message told him to enter his hand to the into the machine and then the machine will start scanning his hand to have three-dimensional picture, this picture will transfer toward the control panel and from there to supervisory computer and it will be compared with the information in the database files, the file will be chosen with respect to smart card information.

The image transfer through the network communication lines, these lines work with TCP/IP standard and this operation done in this way when we are working with normal conditions. This operation done by comparing the entry information with that in data file in the memory of the computer, when this operation done, the computer store specific information about this operation in the holder file, entry files, attendance time files and also it will send these some information to the print, each with needed data.

This information is:

- The cardholder data.
- The time of entering.
- The door number or name.
- The reason of that entering.
- Error in entering.
- And other special information for different software.

But in case of stand-alone the information in the hand reader test and store in the hand reader it self but in case of normal reader the information will transfer to the control panel and then the user will be able to enter the building but in case when error happen that user will not allowed to pass and in some cases there will be an alarm.

If the user got okay, he can pass, but that is not enough for entering the building, and that is because of the second barrier this barrier is the revolving door sensor the revolving door has inside it metal detector & motion detector, this metal detector is adjusted not to detect small metals that is usually found with worker, also most of the time there is a security man near the door and the sound signal can be heart by both the user and the security man, so security man can deal in some cases but this alarm is also shown in the supervisory computer screen.

The motion sensor in the revolving door is used for the same reasons that motion sensors in normal door are used, if both signal from metal detector and the motion sensor is correct the door slides open, if not it still closed, the revolving door is one way direction and some of the door rotate by hidden motor (so in this case there will be another sensor that detect the motion and then turn the motor). If there is any motor,

there is no need for the locks to be use in the revolving door, but if not, we need to have locks that unlock by another signal come from the control panel.

When the user pass to the building his card will record as inside the building and it will be not allowed to be used for any entering from outside, if that card used for any entering from outside, there will be an internal alarm, then the security man is responsible for the rest, and if any entering happen there will be an alarm in whole the building.

Also here I want to say that the time allowed for the user to enter the door is limited by 7 seconds and the user must leave the door within 5 seconds, else there will be an internal alarm.

This operation must done with allowed time, in other words this operation must not done in holiday or out of working time for specific card.

3.7.1.1.1 which error can happen within this operation:

3.7.1.1.1.1 Entering wrong card

IN THIS CASE THERE ARE THREE POSSIBILITIES:

- Different types of cards which are use in the system and if this happen there will be an internal alarm in the security room.
- Wrong entering for the card and this done by entering the card in the opposite direction or not full entering and these two the machine can easily chick this operation and inform the user in the screen of the hand reader this error widely happen
- Damage in the card and this damage can check by the machine or can be known because of this error.

3.7.1.1.1.2 Entering wrong name

In this case there are two possibilities:

- Different card with different correct name and password, in this case there will be an internal alarm in the security room.

- ❖ Wrong name and this operation the user will got another chance with and message will shown in the LCD of the reader, after the second chance there will be an internal alarm in the security room the security man is able to give the user another chance to enter his name, if the user fail in the third time the card will pause from the system and so, it can't use it again and the security man will do the rest.

- ✓ If the user passes after the third chance the card is still available but in both cases (passing or not) the error will be registered for the card user.

3.7.1.1.1.3 Entering wrong password

In these types of errors, we deal same as name's errors

3.7.1.1.1.4 Wrong hand picture

In this operation if any error happens the user can get only another chance and by the security man if that user fails in the second chance his card will be paused.

3.7.1.1.1.5 Unauthorized area

This error can be happen just inside the building and not outside and if that error happen there will be an internal alarm these types of errors are not allowed to be happen.

Authentication is the process through which the identity of a computer of network user is verified. A password is a form of authentication. Passwords allow users access to the network. A password consists of a string of characters that a user picks as an ID code.

There are a number of problems with passwords:

1. They must be regularly changed.
2. Users give their password to other co-workers to use.
3. Users create guessable passwords.
4. One user may have more than one password to do their daily work.
5. User put their passwords in an open area where others can see.

There are ways to prevent these security problems from happening:

1. Users should create long passwords.
2. Users should use uncommon or unfamiliar names.
3. Users should use letters with numbers and characters when creating their passwords.
4. Users should never give their passwords away.

To combat password problems and increase network security done by using smart cards, biometrics, and 2-factor authentication. Smart cards are cards about the size of a credit card that contains a small processing chip and a memory chip that can be read by a smart reader. They can be used to hold passwords, private encryption, decryption key and digital certificates. There are two types of smart cards. Contact cards, which the card must be passed through a smart card read, or Contact less cards that must be passed near an antenna in order to carry out a transaction. A biometrics authentication devise measures one or more of the users physical attributes to allow them access. It can scan the users fingerprint, the shape of their face, the pattern of their eye's iris, their signature or the sound of their voice. 2-factor authentication uses two of the three types of authentication to increase security

3.7.1.1.2 Notes

- In case of any internal alarm happen the cameras, which found in that area will be turn toward the error maker and it will be focused. This is in the case that the cameras is not, normally the camera directly focus toward any motion. The computer within this operation takes some picture for that user.
- Internal alarm means that:
  - Light & sound signal appear in the computer screen.
  - Just to increase the intention of security man toward that user.
  - To focus the camera toward the user.
  - To give the security man to do what necessary.
- If any paused card, old card, different card or any such errors happen there will be an internal alarm directly.

- ❖ If any mistakes happen and caused any kind of alarm, these errors will be recorded in specific files.
- ❖ In the main gate if any error happens the camera, which found there will take pictures for the user.

3.7.1.2 NORMAL DOORS

In the normal doors three types of security are applied to these doors, for the highest security level, same operation applied for main entrance applied here. But when the user exceed that door it is verified as inside that room and its card will be unable to use for the other doors, until that user leave the room.

In cases of security level 1 & 2, we have only card readers, and to pass inside, the user must satisfied these condition that related with each level, for level 2 we have these conditions:

- ➢ Correct card, name and PIN code.
- ➢ The power to use the card in this area, some card is not available for some cardholder and may be not available in this time.
- ➢ The employ must be one of the staff or there must be at least one of the staff inside that room.
- ➢ Time must be allowed.

In the level three the door must follow these conditions:

- ➢ Card, name and PIN code must be correct.
- ➢ Available card, the card must have the authority in this area.
- ➢ Time must be allowed.

If the area conditions satisfied, all the other operation (entering operation) are the same, the difference are that when the conditions satisfied, that the door lock will be temporary unlocked for *seven* seconds for the level 2, and *ten* seconds for the level 3, after that it will close again and it is need to open from the beginning, also *15* seconds will be given for both levels as waiting time until opening the door. If there is entering or not, if any error happened like no one enter or no one exit, the door doesn't opened, it

doesn't close, there is any wrong entering or exiting or the operation done from the different direction again there will be and *External Alarm.*

For the level 1 the door will be open for *five* seconds start when the door is open the start signal come from door status sensor and the lock will stay for *ten* seconds without opening the door, if this operation does not happen as mention before, there will be an external alarm, these errors have been mentioned before. If the time, which allowed to each cardholder, is finish and the user is still inside the building or room there will be an internal alarm.

3.7.1.3 MAIN EXIT

In the work time is finish the worker must leave the building within a specific time, (e.g. half an hour) after that, any worker stay in the building its card will be paused, there will be an alarm and security official will do the rest. In case over timework security office must be announced before so the cards will still available for the necessary time, also if there is another shift, there must be a record for those who includes in the shift.

Exit doors got the same level of security that for level one, but the hand reader in the main gates are used to register attendance time, while in the level one it is only used for time tracking. When the individual exit, they will be recorded as outside the building, so they have the ability to use it in the next day.

3.7.1.2.1 Emergency Cases

In Emergency cases both fire exit and exit doors are used for run away from the building, these doors have the ability to work when stand-alone with high speed, exit door can be open just by inserting the card into card reader of the hand reader, exiting in this way or from fire exit door is available only when the emergency case signal is sent from the supervisory computer, that allowed for stand-alone case also in both of the doors, both fire exit and exit door has exit or "panic" bar, instead of normal door hand, In emergency cases the door waiting and open times is available for only five seconds, if the door still open or opposite entering happen alarm will be announced.

Figure 3.6.1 Exit or Panic Bar

3.6.2 AUTHORIZATION CLASSES

While we have different security levels and many people can enter the building what ever they are worker, visitor or other. The security classes, which are available for those cardholder, must be different, and this must satisfy the different requirements

Class A

This class is allows the carrier to enter to any room and in any time, in this building the director and security major carries this class.

Class B

In this class it is allowed to the carrier to enter any room in the building at the normal days and level four in holidays and other than working time. This carrier is the supervisor; also it can pass to its room.

Class C

This class allows the carrier to enter any room in the building within normal days and working time and this carrier is the Forman.

Class D

This class allows to the carrier to enter any room but within specific time only such as from 7 o'clock to 8 o'clock morning for cleaning staff.

Class E

This allows to the holder to enter working office and the other related offices; in this class it is not necessary that is one of the staff is inside the room.

Class F

This class allows the carrier to enter only there working room this for normal worker, (e.g. secretary).

Class G

This class for temporarily card such as guest, maintenance team and some customers, in this class the card allowed to the carrier to pass the mean gate, number of rooms and it is allowed for specific time, usually, it is limited by four hours.

Class H

This class allows to carrier to enter any room but while one of the staff at least is inside and this is allowed for servant

Class I

This class allowed for security men, this allow to the security men to enter any room but it is limited by 2 min to leave the room.

All these level shortly explains in the following table:

Table 3.1.1 Security Classes

CLASS	Area	Time	Area	Time	OWNER	NOTES
	NORMAL		HOLIDAYS			
A	All	All	All	All	Director, Security Major	
B	All	All	L4	All	Supervisor	Also his room
C	All	All	Not	Not	Foreman	
D	All	Limited	Not	Not	Cleaning staff	From 7^{00} to8^{00}
E	W & R	WT	Not	Not	All	One of the staff in related
F	W	WT	Not	Not	Maintains staff	
G	Limited	Limited	Not	Not	Guest, Customer	Maximum 4h
H	All	All	Not	Not	Servant	One of the staff in related
I	All	All	All	Limited	Security men	Limited by 2 min

W: Working Office R: Related Office WT: Working Time L4: The 4^{th} Security Level

3.6.3 NOTES

When any card gets damage, theft, lost, temporary (expired) or discharge employee must immediately cancel and for such card holder, which in holiday it must be paused.

In some rooms such as director or supervisor room, there are two push button switch one near the door and the second is on the office of the director (or supervisor), these such button switches work and by inserting the card into card reader and entering both PIN and name the sound signal will inform the Director to push the switch so the door will open if the director does not push the switch the door can not be open

In all cases before I had talk about internal alarm this internal alarm can be sense in security office only this signal will appear in the computer screen but when any wrong entering happened or any problem happened in the building such as fire the external alarm will work

The secretary's card enables her to pass to the head office even if it is not there

CONCLUSION

In the present time, security is a prerequisite for the functioning of modern organizations. Access Control Systems are compulsory components of such intelligent safety precautions.

Access Control Systems provide:

- Overall item protection.
- Differentiated operational protection.
- Classified coded protection.
- Comprehensive protection of specific security zones and data areas.

The main targets of an Access Control System are the following:

- Controlling and defining access points.
- Grouping of identified persons as authorized or unauthorized.

Securing that access is restricted only to the authorized persons at the specific access points.

The Electronic Access Control System or Card Entry System has become more and more available in many countries and we can see it in many places around us due to the importance of this system and leniencies that is provided by the system as well as its ability to protect the buildings. The system is not only security system but also it can provide many services such as

- Time & Attendance Reporting
- Invalid Access Attempts
- Elevators
- Parking Gates
- Security Alarms
- Fire Alarm
- Lights
- Sprinklers

Over that the system can be use to control some equipment within the building, like a key. Such as the main server in any system, this equipment will never work until receiving signal from supervisory computer that both card and data are okay. Another use of security appear when working in some stations contains some dangerous operations, this operation can done only after nobody in the region, so if there is any one pass inside he must apply his card through the card reader, then he will be registered as inside so this equipments or operations will not done until all outside

However, the improvement of the system still need human interference which are in some cases very important, there is no system until now that works independently, such in monitoring and recognition, cannot be done away from the human eyes, even though the EAC goes much a head towards reducing human interference and effects.

Today computers have got high speed and so these systems can work with high capacity and high speeds and this is one of the factors standing behind the efficiency of the system, equipment quality and the completeness (well-design) of the system.

The software provided by the companies nowadays has become very easy to use and is supported by Windows operating system, these software are improving day by day and some times offered from the company site at the internet which gives this system more ability to satisfy consumer needs and hopes.

EAC had introduced in many applications in different types of buildings such as:

- Normal and Large companies
- Medical centers and hospitals
- Large low firms
- Got a large use in hotels
- Government buildings
- And universities

Today the EAC system works as a part of integrated system for buildings that include HVAC, lighting, elevating, CCTV, garage controlling, and other, all of them work together to save the power, to offer suitable services and surely offer the security of that building.

As systems get larger, the technical choices become less obvious. The system designer must also take into account the:

- Amount of data that is likely to be transferred between devices.
- Compatibility between devices made by different manufacturers.
- Installation issues, such as power and electrical grounding.

Also by integrated this system we can save in the following:

- Management time: Records make it easy. No fumbling for information is required.
- Employee training time: Employees have to learn one set of software and required operational response rules.
- Response time: procedures are well thought-out because they are related.
- Physical space: reduce the need of multiple monitors.
- Money: fewer workers can do more work.

We must care about the start and the end of the work, because in this time there are many employee want to entering or leaving at the same time, these cause difficulty in the system and we can not leave the employee waiting out jut because the system can not cover there number.

When building security system or any system we must care about companies offers and about the different manufacturing equipments, this is because of the different standard that might be used.

To increase the efficiency of the system, spare parts must be under the hands whenever it is needed this operation reduce number of failure, reduce the time that is needed to fix these equipments and keep the system controlling all operations automatically.

Both connection and network lines must be hidden, and control panel also must be locked, this lock must be both hardware and software, hardware using normal locks and software using password to access to the program inside the control panel.

Software must be able to test the equipment within the net and give any error had been detected on the supervisory computer monitor.

REFERENCES

[1] Konicek J., Little K., Security, ID system and lucks, Butterworth-Heinemann, Newton, MA, 1997.

[2] Frank J., Freed L., how computer work, Butterworth-Heinemann, Newton, MA, 1995.

[3] Neil Cumming, Security, a Guide to Security System Design and Equipment Selection and Installation, Butterworth-Heinemann, 1997.