



III. F ACCESS CONTROL 2 HOURS





CALSAGA Security Officer Training Program

Module III.F - Access Control

Table of Contents	1
Notes	2
Course Outline and Syllabus	3
Introduction to Access Control	5
Introduction to Electronic Alarm Systems	6
Electronic Alarm Systems	7
Receipt of Alarms	11
The False Alarm Problem	13
Closed Circuit Television Systems (CCTV)	14
Access Control Systems	15



Notes

Security officers are required to receive 40 hours of training in the initial year of having their Guard Card and 8 hours annually in year two and beyond.

Schedule for Training – First Year Guard Card

- Prior to applying for the Guard Card – 8 hours
 - Power to Arrest/Appropriate Use of Force
- Within 30 Days of Issuance of Guard Card – 16 hours
 - 8 hours of mandatory courses (Pick two from: II. A, II. B, II. C, II. D)
 - 8 hours of elective courses (these are the ones that start with III.)
- Within 6 months of Issuance of Guard Card – 16 hours
 - 8 hours of mandatory courses (the remaining mandatory courses that were not done within the 30-day window – II. A, II. B, II. C, II. D)
 - 8 hours of elective courses (these are the ones that start with III.)

The 8 hours of Annual Continuing Education must include 2 hours of review of the Appropriate Use of Force topics as set forth in section I.B. of the Appendix of the Powers to Arrest manual. You can choose which sections to offer for the two hours but be mindful that the law specifies some sections as being required to be conducted in person. Mandatory and/or Elective courses shall be used to meet the remaining 6 hours.

This course module is part of the CALSAGA Security Officer Training Program. This course module complies with Bureau of Security & Investigative Services (BSIS) training directives and in compliance with Business and Professions Code Sections 7583.6 and 7583.7 and Title 16, Division 7, Article 9, Section 643 of the California Code of Regulations. The course(s) comply with the Department of Consumer Affairs Skills Training Course for Security Guards and Proprietary Private Security Guards.

Use of this module is subject to all of the restrictions and copyrights specified by the Terms of Use, End User License Agreement, Disclaimer, and Release of Liability for CALSAGA Training. Failure to comply with any part of the Terms of Use, End User License Agreement, Disclaimer, and Release of Liability for CALSAGA Training may result in legal action.



III.F Access Control – 2 hours Course Outline & Syllabus

Learning Goals

- The officer will be provided with an understanding of the electronic security systems that protect a facility.
 - The officer will be provided with an understanding and working knowledge of various personal identification systems.
 - The officer will be provided a basic understanding of CCTV systems and the manner in which they enhance security at a protected facility.
-
- A. Electronic Alarm Systems
 - 1. Used to detect fire
 - 2. Used to detect an unauthorized entry
 - 3. Notify authorities during an emergency
 - 4. Used to monitor equipment and report malfunctions

 - B. Equipment
 - 1. Sensory Device
 - 2. Control Unit
 - 3. Annunciator
 - 4. Power Source
 - 5. Alarm Circuit

 - C. Types of Alarm Sensors
 - 1. Perimeter or point of entry
 - 2. Area Protection, Motion and heat sensors
 - 3. Object Protection
 - 4. Electro-mechanical
 - 5. Intrusion
 - 6. Magnetic
 - 7. Wire/Screen
 - 8. Pressure Mats
 - 9. Soundwave and Microwave
 - 10. Capacitance
 - 11. Vibration
 - 12. Audio
 - 13. Light



- D. Receipt of Alarms
 - 1. Advantages of using a system
 - 2. Disadvantages
 - 3. Direct line to police or fire department (Outlawed in most California cities and counties)
 - 4. Proprietary

- E. False Alarm Problem
 - 1. Error/Negligence
 - 2. Environmental
 - 3. Design flaw
 - 4. Solution to the problem

- F. Closed Circuit Television Systems (CCTV)
 - 1. Uses of CCTV Cameras
 - 2. Types
 - a. Pan, Tilt & Zoom
 - b. Fixed
 - 3. Switchers/Multiplexers
 - 4. VHS Time-Lapse Recorders
 - 5. Digital Recorders
 - 6. Remote Viewing Capabilities

- G. Access Control Systems
 - 1. Manual/Use of Personal Identification
 - a. California Drivers' License
 - b. Review of Employee Data Base
 - c. Visitor Sign-in Registration
 - d. Computerized Systems
 - 2. Types of Systems
 - a. Bar-code
 - b. Magnetic Stripe
 - c. Weigand
 - d. Proximity
 - e. Biometrics
 - f. Access Control Devices
 - 3. Procedures to Implement During System Malfunction



INTRODUCTION TO ACCESS CONTROL

Access control is one of the core functions of private security officers. Quite simply, access control means being in charge over who is allowed, and who is not allowed, into a facility or into parts of a facility.

Security officers will maintain access control over a facility through a variety of means, but they can be roughly divided into two categories: manual procedures and electronic procedures.

This module will outline the methods by which security officers in charge of access control can perform these duties.

As with all security post assignments and contract security employers, the policies and procedures of your employer and the specific post orders for your work site, will supersede any information in these modules.



INTRODUCTION TO ELECTRONIC ALARM SYSTEMS

Electronic alarm systems provide another element of defending a company's assets from loss. An intrusion alarm system, which will detect unauthorized entries into a building, must be evaluated as to the cost of the alarm system versus the value of the items that are to be protected. To ensure overall security, there must be a balance amongst services, equipment and alarms. A security system must:

- Be planned to operate without major problems.
- Be economically feasible for the property or building which is being protected.

Alarms can function in a variety of ways and serve a variety of needs. Alarms can be used to:

1. Detect fire
2. Detect an unauthorized entry
3. Notify authorities during an emergency
4. Monitor equipment and report malfunctions



ELECTRONIC ALARM SYSTEMS EQUIPMENT

The need for an alarm system and the type must be evaluated according to the needs of the owners of the facility. Some facilities will be more prone to burglary or robbery while another may be more likely to be damaged because of fire.

There are five basic components to any alarm system:

1. A sensory device
2. A control unit
3. An annunciator
4. A power source
5. An alarm circuit

These will be explained in greater detail on the following pages.

Sensory Device: Initiates the alarm signal because of sensing a stimulus or condition to which the system has been designed to react. Heat and smoke detectors and door contacts are examples of sensory devices.

Control Unit: The final point for all sensors and switches in the alarm system; the control unit is usually housed in heavy metal, tamper resistant cabinets; the elements within the control unit are arranged to receive signals from the sensors and to relay these signals to the appropriate final point within the control unit.

Annunciator: A visual and/or audible signaling device which indicates activation of the alarm system. An annunciator is selected depending upon the circumstances and location of the alarm system and the desired or required response. For example: a bank would utilize a “silent” annunciator alarm to report a robbery while a school would use horns, sirens and lights to announce a fire.

Power Source: A 110-volt power system which is generally filtered to provide the proper current and voltage normally used. An emergency power source or battery backup system should also be included.

Alarm Circuits: Used to transmit signals from the sensors to the control unit, which in turn transmits the signals to the local or remote annunciator alarm unit. Alarm systems include open, closed circuit, or increasingly, wireless systems:

- Open circuit: An electrical line which does not have a flow of current present until switch or relay is closed completing the circuit.
- Closed circuit: An electrical line with current flowing through it. Any change in this electrical current flow will initiate an alarm.
- Wireless Systems: A wireless transmitter transmits a signal from the sensor to the control unit. It is becoming increasingly popular as wireless technology expands.



In addition, systems can be arranged with modern “supervised” sensors, which give greater accuracy of exactly where an alarm is triggered and allow service ease when a problem occurs with an alarm system.

As discussed earlier, alarm sensors can take a variety of forms. Basically, there are three types of alarm sensors:

1. Perimeter or point of entry
2. Area protection
3. Object protection

In a thorough security system, all three types of alarm sensors may be utilized in an effort to provide a high level of security.

Sensors are designed to initiate alarms under several different conditions:

1. When a surface or area being protected is penetrated.
2. When the sensor is opened, grounded or shorted out.
3. When the sensor fails due to age or wear.
4. When the container which houses the sensor is opened. This is known as a “tamper” alarm.

SENSORS CAN BE OF VARIOUS TYPES:

ELECTRO-MECHANICAL

Electromechanical sensors are reliable but can be costly. They are designed to place a current carrying conductor between an intruder and the area to be protected. The conductor carries the current, which keeps a holding relay in an open position. If the current flow stops for any reason the device releases the relay and allows the contacts to close so that an alarm circuit is activated.

FOIL

Foil is usually installed on glass in the form of a thin metallic tape which carries an electrical current. Once the foil is broken, cut or torn, the electrical current is interrupted, thereby causing an alarm. Foil serves as a psychological deterrent. The cost of foil is small, but its installation requires considerable time. Because they are prone to false alarms, foil sensors are not part of modern alarm systems and will likely only be encountered in antiquated systems.

INTRUSION SWITCHES

Intrusion switches are used on windows, doors and skylights. The switches are made of two electrical contacts. One is installed on the opening surface (door or window) while the other is installed on the fixed surface. When the surface (door or window) is closed, the two contacts provide a closed circuit so there is a continuity of current flow. When the surface is opened, the contacts separate, and the electrical circuit is broken, and the alarm is signaled. These switches are always installed on the inside or the side of the material to be protected.



MAGNETIC SWITCH

Magnetic switches consist of a magnet and a switch connected to an actuator. The switch is usually mounted on the fixed surface with the magnet fastened to the opening surface. When the surface is closed, electrical current flows. When the surface is opened, the magnetic field is broken, and an electrical circuit is activated, and the alarm is signaled. Protection of Assets authors Walsh and Healy state that the most efficient magnetic switch is a balanced magnetic type that will activate an alarm upon the increase, decrease or attempted substitution of an external magnetic field.

WIRE AND SCREEN DETECTORS

Wire and screen detectors are used to enhance security for windows and can provide a valuable service to the home security system owner. Wire is woven into the window screen. If the screen and/or the alarm wire are cut, the electrical current flowing through the wire will be interrupted, which will activate the alarm. Screen detectors, while providing a good level of security, are not inexpensive.

PRESSURE MATS

Pressure mats are another antiquated sensor system not commonly used today because they are prone to false alarms. They are designed to initiate an alarm when a weight of 5-20 pounds per square foot is applied to the surface. Pressure Mats utilize electrical wiring placed within a rubber or plastic coating which is normally hidden underneath carpeting. Pressure mats are suited for carpeted office areas but are most widely used in home security systems.

SOUNDWAVE AND MICROWAVE SENSORS

Soundwave and microwave sensors are based on the "Doppler" principle according to authors Walsh and Healy. Doppler was an Austrian scientist who discovered that "microwaves or soundwaves are disturbed by movement."

Sensors which utilize this principle have a transmitter that sends a wave pattern and then receives it. If the pattern being received is the same as the one being transmitted, a stable condition exists. Once a distortion of a wave-pattern caused by movement is detected, an alarm will be initiated. Soundwave, or ultrasonic, employs soundwaves of a higher frequency than the human ear. Sensors of this type are usable only inside a building. Audio noise does not affect the sensors, nor does air currents. However, if heating/air conditioning air currents move displays suspended from a ceiling, the display movement may activate an alarm. Radar detectors work in the same manner as ultrasonic, but the radar wave is different. Radar can be used outside, and their waves do not permeate construction such as plaster walls.



CAPACITANCE SENSORS

Capacitance sensors are large electronic sensors that radiate energy and detect change in the capacitive coupling between an antenna and ground. These are normally low in cost and are suitable for outside use.

VIBRATION SENSORS

Vibration sensors use a sensitive contact microphone which is installed indoors on the surface to be protected. Vibrations caused by someone attempting to penetrate the surface are picked up and transmitted to an amplifier that initiates an alarm. These are not considered useful outside.

AUDIO SENSORS

Audio sensors are microphones that are activated when sound initiates the alarm. Audio sensors are used for vaults.

LIGHT SENSORS

Light sensors operate on the principle of a change of light or if a beam of light is interrupted. The use of a photoelectric cell is the simplest means of changing the transmitted light beam through a propeller-like baffle. The receiver must be tuned to a frequency which matches the RPM of the motor and vibrations in speed caused by temperature change.

Each of these types of sensors has its own advantages and disadvantages in terms of their cost, effectiveness, and suitability for different security needs.



RECEIPT OF ALARMS

When any of the sensors described in the prior section are triggered, the alarm signal is then “received” somewhere. Alarms can be received at several different locations. There are four main types of systems by which alarm signals are received:

1. Local Alarm Systems
2. Central Station Systems
3. Direct Line to Police/Fire (Note: Outlawed in most California jurisdictions)
4. Proprietary Systems

Each of these alarm systems has its own advantages and disadvantages.

Local alarm systems activate a sound generating device, often on the outside of the building, to call attention to the alarm.

Advantages of using a local alarm system include:

- Psychological deterrent (intruder knows he has been detected)
- Damage should be minimized since the intruder hears the alarm.
- The alarm is inexpensive to install and easy to maintain.

Many sprinkler systems have local annunciating systems which consist of a bell which rings as water flows through the sprinkler riser.

There are some disadvantages in using only a local alarm system which include:

- Easy to defeat because of their simplicity.
- The intruder will probably not be apprehended.
- The alarm may be disregarded if no one is nearby to hear the alarm.

Central station systems are a type of alarm system that is not heard by the intruder and is called a “silent” alarm. Police are normally notified immediately of the alarm by staff in the central station, which aids in apprehension since the intruder is not aware of the alarm. Many alarm companies provide a monitoring service for the central station systems. This will require the company who desires the coverage to test the system on a regular basis to ensure effectiveness. This type of system uses telephone lines to carry the alarms. Direct lines or use of a loop system may be employed to provide the service.

The direct police or fire department termination system is the third type of alarm system. The advantage of this type of system is obvious: a quick response should be given to the alarm. However, in many cities the police and/ or fire department are not permitted to receive the alarms directly unless the facility is a school, church or other public building. The high number of false alarms has required police and fire agencies to demand this change.



Proprietary termination is the final type of alarm receipt system. With this type of system, a facility monitors its own alarms by using either security officers, maintenance or other employees to respond to alarms. Advantages of the proprietary system include:

- System can be designed to meet the needs of the owner.
- The system is operated and controlled by the owner.
- Functions can be virtually unlimited if designed properly.
- Line security is enhanced since the alarm line begins and ends on the owner's property.
- System can be cost effective if designed properly

Disadvantages of the proprietary system include:

- Incurred costs of providing personnel to monitor the alarms
- Additional incurred costs if the system has not been designed properly.
- Even by using a proprietary system, security guard patrols will often still be needed.



THE FALSE ALARM PROBLEM

If police officers were asked what they believe is the single greatest problem with alarm systems, most would probably answer that false alarms are the greatest problem. Between 90 - 98% of all alarms are false. False alarms are a result of:

1. User error or negligence
2. Poor installation or servicing
3. Faulty equipment

More than 50% of all false alarms are due to user error or negligence. Because of poor installation and service, many states and local governments have developed standards for installing and servicing alarm systems. As with contract private security operators and officers, the Bureau of Security and Investigative Services in California licenses and regulates the alarm company industry.

False alarms affect police in three ways:

1. Encourage poor police searching of protected premises - "It's probably just another false alarm."
2. Poor attitude toward the alarm user and alarm industry.
3. Belief that intrusion alarms are more trouble than they are worth.

Solutions to the false alarm problem include:

1. Sell the system correctly; consider the environment, habits and routines of subscribers, and don't overprotect.
2. Don't use space protection excessively.
3. Instruct the subscriber on the proper use of the system.
4. Reinstruct the subscriber at frequent intervals.
5. Train and retrain alarm company employees on procedures and troubleshooting techniques.
6. Maintain system in proper working order.



CLOSED CIRCUIT TELEVISION SYSTEMS (CCTV)

Closed Circuit Television or CCTV systems play an important role in an overall security system. CCTV systems support the security officer in the observation and surveillance of the facility and areas that are to be protected.

While CCTV systems are not necessarily inexpensive, in recent years because of technological advancements, these systems cost much less than in previous years. CCTV systems are most effective when incorporated into a security program that uses security personnel. CCTV cameras can be utilized to minimize security officer coverage and related expenses. It should not be believed that cameras can completely replace security staffing.

CCTV cameras support security in several ways:

1. Allows for hidden surveillance of an area which is vulnerable to theft.
2. Allows for the positive identification of persons and/or material prior to granting entrance or exit privileges.
3. Provide a deterrent to crime when cameras are visible to employees and visitors.
4. Confirms theft or other incident(s), especially when used in conjunction with a video tape recorder
5. Provides better utilization and efficiencies of security personnel.

CCTV cameras are used widely in retail operations, hospitals, office complexes, factories, and parking decks.

Monitors allow a person to view what the camera is scanning. If security personnel are required to monitor several cameras, care should be taken to ensure that observation of the monitors is designed in such a manner to allow for proper effectiveness.

A term seldom used in security is ergonomics, a science that focuses on human capabilities and limitations in the design of jobs, workstations, tools and equipment. Camera monitors which are placed in a security office or control center to be monitored by one person who is also required to answer the telephone, sign-in visitors, communicate with other personnel via two-way radio, page employees over a public address system, etc., will have great difficulty in effectively monitoring cameras. Security firms do not always have control over the design of workstations but must be aware that poor design can limit the ability to provide the best security possible.

Security consoles assist in providing security personnel with proper ergonomic design to ensure cameras are effectively monitored.

Digital recording systems are now replacing videocassette recorders in the security industry. With the advent of the Internet, the World Wide Web and digital recorders, persons with access can view CCTV cameras from anywhere in the world.

The operation, monitoring, and use of a CCTV system is very specific to the post at which you may be assigned. If CCTV is utilized at your post, you will receive additional instruction on the use of the system and the role it plays in your security function.



ACCESS CONTROL SYSTEMS

Access Control can mean many things to different people, but for purposes of this discussion, we will define access control as: “The means of controlling access and identifying users.”

Identifying individuals before allowing them access to a facility is a core responsibility of access control. Identifying individuals can be conducted by manual or electronics means.

MANUAL MEANS OF IDENTIFICATION

The most basic means of identification would include manual means such as asking for a government-issued photo ID. In California, this will typically mean a California Driver's License for visitors and/or an employee identification card or badge, combined with a list or log of individuals allowed access. For manual means, employees may be required to display their badge.

The procedures allowing for access by visitors will vary by security post, and you should refer to your post orders. Most facilities require visitors sign into a visitor log, identify who they are visiting, and their time in and out of the facility. Other facilities require visitors to be escorted.

If manual identification is being used at a facility, it is important that the security officer take this function seriously. If your post orders ask you to verify a photo ID, you should take the time to look at the ID and look at the person to see that they match. Check the visitor log to be sure the name they sign in with matches the name on the ID. If employees are not displaying their badges as required, you should politely but firmly ask them to do so. If post orders require visitors to be escorted up an elevator, it is not OK to let them go by themselves “just this once.”

ELECTRONIC MEANS OF IDENTIFICATION

More and more facilities are moving to electronic means of identification rather than manual. Basic access control systems employ the use of a card and are typically the one or two door variety. They simply identify a card as valid or invalid, and on that basis, allow or deny access. The system does not identify the valid card to a user, and there is no hard copy report or other record of entry. In short, it is no more than an electric key. The system does not identify who has what card, or even what card is used. If a card is coded for that door, then the system allows access. If it is not, then access is denied.

The more sophisticated systems can identify a card to an assigned user of the card. When the card is presented to the card reader, the system not only permits or denies access based on the validity of the card, but also can identify the user by name, employee I.D. number, and by access level. Beyond that, the system can also permit or restrict access by time, date, day of week, and as many as fifty access authorization levels, depending on the sophistication of the system.

What these systems record is as important as what they control. Every entry or “transaction” is recorded in the system. Larger access control systems can automatically log, display and print out upwards of 1.5 million transactions. For an average larger system, this could be as much as six months' worth of access information.

The ability to perform audit functions adds to the value of the access control system. Now you can answer these questions: Who went through what door? How often? What time of day or night? Did a person attempt access through a door that they shouldn't have? This information becomes very

CALSAGA Security Officer Training Materials - CALSAGA Security Officer
Training Program • Module III.F Access Control © 2025 CALSAGA •
Unauthorized use and reproduction prohibited. All rights reserved.



valuable when an incident occurs such as a theft or accident. The audit trail that can be retrieved from the access control system may eliminate or identify suspects. Who was in? What time? Why did Mr. Smith attempt to enter a restricted area? As the capacity of personal computers continues to increase, the ability to store and retrieve information will continue to increase as well. Already, the access control system is being utilized for such automation functions as Guard Tours, Time and Attendance, Telephone Call Accounting and Pricing, Doctor Registries in health care facilities, Copier Control and Pricing, and other automated functions that either save or generate revenue for the user organization.

PERFORMANCE

What is the performance criteria that a company needs to look at in deciding whether to install or replace an access control system, a key system, or other means of access control?

1. Is the card valid? It needs to establish the identity of the card user.
2. Is the system reliable? Every time John Smith presents his card, it must validate his presence.
3. Is the system easy to use? It must not slow normal workflow or make ordinary tasks difficult.
4. Is the system secure? It must be resistant to counterfeiting or duplication of the card.
5. Is it durable? The system must be rugged and have a long-life expectancy.
6. Is the system hardened to its environment? The system must be physically adequate to protect against force or manipulation.
7. Is the system easy to maintain? It should offer some internal guidelines for troubleshooting the system.

SYSTEM TECHNOLOGY

There are many types of card access technology in use with various facilities and applications. Some of those that you will likely encounter include:

Hollerith Readers — Punched holes in card. When inserted in the reader, it provides a momentary contact closure to release a locked door. Sometimes seen in hotel rooms. Insert reader. It is inexpensive, but easy to duplicate.

Magnetic Stripe Readers — Reads the characters on magnetic tape affixed to card. Most popular because so much information can be stored on tape. Insert or swipe reader. It is relatively inexpensive, but easy to duplicate, and potential for vandalism, because it is a contact device.

Proximity Readers — Each card is individually tuned and can be read when near of reader. Non- contact and virtually never wears out. Can often be used without taking out of wallet or purse. Non-contact. It is expensive, can be duplicated, thick card.

Bar Code Readers —It is inexpensive, and good for low security areas. Can be easily duplicated, some errors or false reads. Good for dual technology cards, but not for high security.

Wiegand Readers — Embedded wire, almost impossible to duplicate. Offers higher level of security than others. Non-contact for low vandalism. Insert or swipe, non-contact.



BIOMETRIC SYSTEMS

These are expensive systems designed for high security applications, however as they gain acceptance, prices will move downward.

Retina Scanners: Identifies user's unique retinal blood vessel pattern, which are the patterns of blood vessels in the back of the eye. Like a fingerprint, each person's retina pattern is unique.

Hand Geometry: Measures the user's unique hand.

Fingerprints: Identifies user's unique fingerprints.

Voice Verification: Computer identifies user's voice pattern within previously established parameters.

VIDEO BADGING INTEGRATION

The video badging system incorporates a digital video ID system with the door access control system. It positively identifies the user by displaying the card holder's picture on the monitor at the security guard's desk the instant the card is passed through the reader. The value of the digital video image is that it allows the guard to see an image of the person passing through the door. Secondly, the video imaging system allows a quick and easy means of keeping, storing and upgrading the employee photo I.D. file, since it is stored on a digital disk rather than on hard film.

ACCESS CONTROL DEVICES

Doors, locks or barriers (commonly referred to as turnstiles) work in conjunction with card access systems. As a card reader scans and accepts a card, a signal is transmitted to a barrier to open, unlock or release a barrier for access to be granted. Most barriers or turnstiles are designed to prevent unauthorized access to an area and yet blend with the decor and aesthetics of the facility where they are installed.

Turnstiles are also used to direct and maintain crowd control at sports stadiums and arenas, amusement parks and offices and factories. Special attention must be given to the type and style of turnstile to make sure it will be acceptable at the facility.

USER FRIENDLY

The modern card access systems have become quite user-friendly, with one- and two-key stroke commands for the security officer operator. The manufacturers have learned over the years that not everyone is computer-literate and have built their systems based on that. Most new systems come with easy-to-understand user prompts and menu screens. The systems also provide basic troubleshooting commands to help identify problems and conditions that are not normal. Many even tell us what to do if certain conditions exist. The most important, and perhaps the simplest, feature of these modern systems is that they can tell us immediately who went through what door, or which door is propped open or ajar. If access control systems fail, security personnel will be required to ask for personal identification (i.e. California Drivers' License) from an individual prior to granting them access to a facility. Information should then be maintained in either the DAR or computerized reporting system.