The mission of the Department of Public Safety Standards and Training (DPSST) is to promote excellence in public safety through the development of professional standards and the delivery of quality training.

2015 Alarm Monitor Training and Refresher Course

Revision 12/07/15

This page intentionally left blank

Table of Contents

Table of Contents

ACKNOWLEDGEMENTS

We are grateful for the Subject Matter Expert (SME) Panel members' contribution and support in this very important process. Their dedication and hard work contributes to the training of alarm monitors who serve Oregon.

1. Jimmie Edmonds, Chair of Alarm Subcommittee, US Bank
2. James R. Essam, Alarm Central Station, Inc.
3. Amanda E. Hayden, Rapid Response Monitoring Services, Inc.
4. Roberta L. Smiley, Multnomah County Sheriff's Office

We also wish to recognize the Electronic Security Association (ESA), (formerly known as National Burglar and Fire Alarm Association (NBFAA) for the curriculum fundamentals.

In addition, we would like to thank following who provided their expertise:

1. Kathleen Schraufnagel, Monitronics Security
2. Lissa Laboda, Vector Security
3. Anna Roderick, Wayne Alarm
4. Theresa M. King, State of Oregon, DPSST JTA and Training Compliance Coordinator

.

INTRODUCTION

Welcome to the Alarm Monitor Training!

This manual has been designed with the building block approach. The first four modules, **Ethics and Professionalism**, the **Alarm Industry Overview**, the **Alarm System Overview** and the **Central Station Overview** begin a foundation for all alarm monitors.

With this foundation laid, additional topics build upon this core training. The unique components of **Computers, Signals, Panels and Detectors** are addressed. These components build the foundation allowing **Security and Safety In-depth** to focus on its application to the components.

When all of the preceding building blocks are in place, your training will culminate in two final modules; **Customer Service** which allows you to effectively interact with the customer and responders, and **False Alarm Prevention** in which we focus on a "collective solution."

This manual contains both the initial training and an abbreviated refresher course which is located in the back of the manual.

DEPARTMENT OF PUBLIC SAFETY STANDARDS AND TRAINING

Mission

The mission of DPSST is to promote excellence in public safety by delivering quality training and upholding professional standards for police, fire, corrections, parole and probation and telecommunications personnel, in addition to private security providers and private investigators in Oregon.

DPSST Overview

DPSST is committed to the very highest ideals of professionalism and public safety. DPSST operates as an agent of the 24-member, multi-disciplined Board. Five discipline-specific policy committees, including the PSIPC, serve as recommending bodies to the Board for the purposes of developing minimum standards for their respective industries. The Board and policy committees meet quarterly. Board and Committee membership is dictated by Oregon Revised Statute. [ORS 181.620 & ORS 181.637]

Website link: http://www.oregon.gov/DPSST/PS/pages/index.aspx

The legislature directed the Department of Public Safety Standards and Training (DPSST), with the approval of the Board on Public Safety Standards and Training (Board) and the Private Security and Investigator Policy Committee (PSIPC), to develop minimum standards for certification as a Private Security Professional. These include reasonable minimum physical, emotional, intellectual and moral fitness standards. [ORS 181.878]

PRIVATE SECURITY INVESTIGATOR POLICY COMMITTEE (PSIPC)

The PSIPC is a 13-member committee consisting of representatives from private security and private investigator industries. Policy committee members are accountable and accessible to all members of the private security industry. The group is committed to its vision and operates in an environment of integrity, fairness, flexibility, cooperation, collaboration, open communication, and respect for the individual. The committee believes in education, training, and continuous quality improvement that will promote personal and professional development throughout the industry.

PSIPC member contact information is available on the DPSST web site at www.oregon.gov/DPSST. To express an interest in joining the Policy Committee complete and submit the Policy Committee Interest Form located on the website.

Vision Statement

The PSIPC recognizes that as traditional law enforcement roles continue to change, there will be an increased demand for private security services. The constant fluidity of potential risks will ignite major growth in the complexity, liability and technology throughout the industry. Through training, technology, career development, and collaboration and integration with other public safety disciplines, the overall quality and performance of private security professionals and investigators in Oregon will continue to increase their professionalism.

To do this the PSIPC aims to:

1. Improve the industry's image with law enforcement and the public;
2. Increase the number of qualified, high caliber people who choose private security or investigation as a career, increasing the levels of employee retention industry-wide;
3. Increase the number of elective courses and training options available to all levels of private security and private investigator personnel; and
4. Educate the public regarding the importance and dollar-value of well trained, certified security professionals and licensed investigators.

ETHICS AND PROFESSIONALISM

Learning Goal: **To develop an understanding of the necessity for standards of ethical conduct, and the relationship between private security, law enforcement and the community.**

In this section we will consider the role of a private security professional, how they interact with the community and with law enforcement. By considering our interaction with the community, we will take a closer look at our core values and how they relate to cultural diversity issues.

Learning Outcome 1-A-1 Understand how the duties of a private security professional and a law enforcement officer differ.

Your job duties and responsibilities are not the same as that of law enforcement officers. Law enforcement is generally used as a reactionary force (responding to issues that have already occurred). You will generally be used proactively (stopping issues from occurring). It is your job to act as a deterrent to crime, de-escalate situations, enforce policies on company or client property, communicate effectively, document incidents in clear and concise reports and as a last resort, make a citizen 's arrests.

Although services vary, they have one common factor – Private Security Professionals protect persons and property.

Private security professional means an individual who performs, as the individuals primary responsibility, private security services for consideration, regardless of whether the individual, while performing the private security services, is armed or unarmed or wears a uniform or plain clothes, and regardless of whether the individual is employed part-time or full-time to perform private security services. [1]

"Private Security Services" perform at least one of the following activities:

(a) Observing and reporting unlawful activity.
(b) Preventing or detecting theft or misappropriation of goods, money or other items of value.
(c) Protecting individuals or property, including but not limited to proprietary information, from harm or misappropriation.
(d) Controlling access to premises being protected or, with respect to a licensee of the Oregon Liquor Control Commission, controlling access to premises at an entry to the premises or any portion of the premises where minors are prohibited.

[1] ORS 181.870

(e) Securely moving prisoners.
(f) Taking enforcement action by detaining persons or placing persons under arrest under ORS 133.225 (Arrest by private person).
(g) Providing canine services for guarding premises or for detecting unlawful devices or substances.

The primary function of a private security professional is to observe, report and coordinate assistance.

Learning Outcome 1-A-2 Understand how a private security professional can change public perception of the security industry.

Historically, a portion of the public has perceived the private security industry in a negative light. Public perception can be improved by the conduct of the security professional on-site with direct interactions with the public. It is important to understand that the actions of a security professional, whether good or bad, will affect a multitude of people. These actions reflect not just on the security professional, but on their fellow security professionals, their employer, and the industry as a whole.

Security professionals must demonstrate exemplary conduct, attitude, and demeanor both on and off the job. The community expects the private security industry and its professionals to demonstrate and maintain a high set of values.

Learning Outcome 1-A-3 Understand the importance of developing relationships in the community.

While the police continue to handle crime fighting and law enforcement responsibilities, private security industry and the community can work together with the police to modify conditions to discourage criminal behavior. Establishing and maintaining mutual trust is the central goal of this partnership. Building this trust requires an ongoing effort.

Learning Outcome 1-A-4 Understand the importance of following the client or employer's standard operating policies and procedures

Highlighted throughout this manual is the importance of knowing and following the client or employer's standard operating policies and procedures. When acting on behalf of the client, the private security professional must ensure they are operating within established parameters, as there are potentially serious civil and legal ramifications if they are found to be operating outside of these policies and procedures. A private security professional should ask for or request a standard operating procedures manual, (SOP) to gain information about specific sites.

Learning Outcome 1-A-5 Know the three characteristic goals common to all private security professionals.

1. In our society, citizens have an expected standard of behavior for persons who protect them and their property. These minimum standards include training and criminal background checks. By ensuring these minimum standards, the community in which we serve will have greater trust in us individually, in the services we provide, and in our industry as a profession.

2. As private security professionals, our primary goal is to provide a service. Because our industry is so diverse, these services vary. They could include monitoring intrusion alarms from a controlled environment to interacting with hundreds of citizens in an airport or shopping mall. The service we provide has basic common factors, which include the protection of persons and property.

3. Historically, a portion of the public has perceived our profession in a negative light. To improve the perception by the public, we must maintain exemplary and ethical business practices. While a great deal of the responsibility lies with the security manager or security contractor, from the bidding process to carrying out services or contracts in an ethical manner, much of the public perception can be improved by the conduct of the private security professional on a site, who interacts with the public. An important question we must all ask ourselves: "*How would I conduct myself if I were being monitored by a television camera"*

Learning Outcome 1-A-6 Understand how on and off the job conduct can affect the public's perception of the security industry.

Because the community expects us to act in a professional manner, their perception is formed by the actions of one officer, and altered by the actions of another. We must provide a consistently high standard for conduct, demeanor and attitude, on and off the job. Our conduct is reflected in how we perform our assignments. Our demeanor is the manner in which we stand, walk and interact with others. It is how we conduct ourselves.

Our attitude reflects our feelings toward people. It is an indication of our purpose or intention. It is important to remember who we are and what we represent when we are off-duty.

Learning Outcome 1-A-7 Understand what unethical conduct includes.

While there are numerous types of unethical conduct, some are more destructive to public trust than others.

1. **Untruthfulness** causes public distrust; it causes them to question our integrity and may affect their compliance with directions.

2. **Theft** is the taking of property that is not yours. This applies to the envelope we take from work to mail a bill, the office pen we left in a shirt pocket at the end of a shift and now use at home, or even the personal, long-distance telephone call we make during our shift.

3. **Substance abuse** (which includes alcohol abuse) crosses all professional, ethnic, gender and age barriers. Those affected by substance or alcohol abuse compromise their reputations and that of the industry they represent.

4. **Criminal conduct** is that conduct which is contrary to law, statute or ordinance, for which you may be imprisoned.

5. **Brutality** is behavior which is neither professional nor an expression of real strength. Brutality is a cowardly action which temporarily builds a weak self-esteem by imposing physical or emotional trauma on another person. When a private security professional's behavior moves beyond that action which is necessary to stop another person's illegal actions, the private security professional becomes guilty of brutality. This demonstrates lack of good judgment and common sense, both of which are necessary characteristics of a private security professional.

6. **Prejudice** is a preconceived judgment or opinion. An adverse opinion formed without just grounds or before sufficient knowledge (*Merriam-Webster Dictionary*)

7. **Bribery** involves a thing of value being given to a person to influence him or her to act dishonestly. By receiving money other than your employer's compensation, there may be an expectation to provide biased or special service or protection to that individual in an inequitable manner.

Learning Outcome 1-A-8 Understand the importance of core values as it relates to the Private Security Code of Ethics.

To maintain high standards in the private security industry, we have established a system of principles, or core values: the Private Security Professional's Code of Ethics.

Core Values

Core values form the foundation on which the private security industry performs work and conducts itself. These values should underlie the work of security professionals, how they interact with each other, and which strategies they employ to fulfill their mission.

The core values for the private security industry are:

1. **Honesty** - includes integrity; credibility, acting honorably and maintaining confidences;
2. **Good Character** - includes being respectful and courteous, being faithful, diligent and loyal to the employer's charge, using discretion, demonstrating compassion and exhibiting courage;
3. **Fair Treatment of Others** - includes treating others equitably, demonstrating good judgment and not being discriminatory;
4. **Public Trust** - includes maintaining public confidences, being law-abiding and adhering to recognized industry standards; and
5. **Respect for the Laws of this State and Nation**.

[OAR 259-060-0020]

Code of Ethics

I swear or affirm that as a Private Security Provider, my fundamental duty is to protect the interest of my employer, client and/or industry. As a private security provider I recognize that I am bound to the core values specific to my discipline.

I acknowledge that Honesty is a core value that includes integrity, credibility, acting honorably and maintaining confidences. I acknowledge that a lack of honesty includes untruthfulness, dishonesty by admission or omission, deception, misrepresentation or falsification, and from these I will abstain.

I acknowledge that Good Character is a core value that includes being respectful and courteous, being faithful, diligent and loyal to the employer's charge, and using discretion, demonstrating compassion, and exhibiting courage.

I acknowledge that Fair Treatment of Others is a core value that includes treating others equitably, exercising good judgment and not being discriminatory against others.

I acknowledge that Public Trust is a core value which includes maintaining the public confidence by being law abiding and adhering to recognized private security industry standards.

I acknowledge that Respect for the Laws of this State and Nation is a core value.

I will constantly strive to maintain these core values, dedicating myself to my chosen profession.

CULTURAL DIVERSITY

Learning Goal: To develop an increased deportment and awareness of cultural and interpersonal issues which dictate the predominant values, attitudes, beliefs and outlook among multi-cultural environments.

Learning Outcome 1-B-1 Understand the advantages of learning about cultural diversity.

The private security industry honors the humanity that we are part of, and celebrates the differences that distinguish us. DPSST and the private security industry have an expectation that all security professionals will value all people without regard to race, color, sex, disability, national origin, age, religion, marital status, veteran status, sexual orientation, gender identity, gender expression or occupation.

Maintaining a culturally diverse workplace demands high standards of ethical and moral values and requires that personal biases be controlled. Private security professionals must recognize any personal biases and ensure those biases do not to enter into ethical decision making. We recognize that embracing diversity in the workplace and living the core values significantly enhances customer and colleague satisfaction.

Learning about cultural diversity leads to positive outcomes when dealing with members of different cultures. During this process we learn about our own biases. It is through this learning process that our efforts will enhance public perceptions of the private security professional, and promote good public relations.

Learning Outcome 1-B-2 Understand why all persons have biases.

Biases are always with us. While we are not born with biases, we begin to learn biases from our families and those closest to us at an early age. We also develop biases from our experiences in life. As we grow and mature into adulthood we bring these biases along with us.

Cultural biases may develop out of fear and/or ignorance. Fear is a strong and unpleasant emotion caused by the anticipation of danger, and ignorance is simply a lack of knowledge. Together, fear and ignorance give rise to our preconceived judgments and opinions of persons who are different from us. We can develop cultural biases from the community we grew up in by accepting the "cultural norm" of the community, or we can develop cultural

biases based on personal experiences. Cultural biases generally are the result of a combination of these factors.

Learning Outcome 1-B-3 Understand how we can become aware of and control biases on the job.

Our biases are always with us. Even when we identify our personal biases they will not disappear. Biases will tend to dictate our actions. For this reason it is important to realize that we have biases we may or may not be aware of. The private security professional must strive to recognize his or her own biases and control them when communicating with others.

Learning Outcome 1-B-4 Understand the need to comply with company policy and federal guidelines.

When working at the job site, the security professional should be aware of all company policies and procedures, as well as any applicable federal regulations regarding cultural diversity. The officer must be prepared to follow, and if necessary, enforce them. This may include policies on racism, verbal harassment and menacing, among others.

Learning Outcome 1-B-5 Understand the need to understand Stereotyping vs. Core Values.

People tend to think of others in stereotypes. Stereotypes are an oversimplification of a particular group or person and are usually negative beliefs and opinions. Thinking in stereotypes is easy to fall into but you should not make assumptions about any group or individual. Because often times we do not exercise a core value perspective of others it is more difficult to think of others in terms of their core values.

Learning Outcome 1-B-6 Understand the need to know ADA requirements.

Despite the legal requirement of fair treatment for people with disabilities, all too often they are still viewed as lesser individuals to be pitied, feared or ignored. These attitudes may be based on fear of a person who is different or simply from a lack of information about disabilities. As much as the disability itself may affect an individual's life, being treated as a lesser person hinders that their ability to lead a productive life and prevents enjoyment of the same opportunities as others.

1. ADA General Rule: The ADA prohibits discrimination against a qualified individual with a disability who can perform the essentials of the job.

2. All security professionals must have an understanding of disability etiquette.

    a. Use **common sense** -- People with disabilities want to be treated the same way as everyone else.
    b. Be **polite** -- Show the person the same respect you expect to receive. Treat adults as adults. Call a person by first name only when invited to do so.
    c. Be **considerate** -- Be patient, take the time to try to understand the problem or need of the individual. Be considerate of the extra time it might take for a person with a disability to get things done or said.
    d. **Relax** -- Don't be embarrassed if you happen to use accepted, common expressions, such as "See you later" or "Gotta run" that seem to relate to the person's disability.
    e. Offer **assistance** -- Do not hesitate to offer assistance. However, do not automatically give help unless the person clearly needs help or asks for it. Ask the person if assistance is needed and how. Do not insist on helping.
    f. **Communicate** -- Talk directly to the person, not their companion.
    g. Respect **privacy** -- If you don't generally ask people about their personal lives, then don't ask people with disabilities about theirs.
    h. Emergency action -- Know the location of individuals who have disabilities at your job site so you can help with **evacuation** during an emergency.

Learning Outcome 1-B-7 Understand the need to have a zero tolerance of sexual harassment.

Most employers have a policy of maintaining a working environment that is free from any form of sexual harassment. The Equal Employment Opportunity Commission defines sexual harassment as unwelcome sexual advances, requests for sexual favors, and other verbal and physical conduct of a sexual nature when:

1. Submission to such conduct is made either explicitly or implicitly as a term or condition of employment;

2. Submission to or rejection of such conduct by an individual is used as a basis of employment decisions affecting such an individual; or

3. Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Learning Outcome 1-B-8 Understand the need to have zero tolerance of all discriminatory behavior.

Under ORS 659A.403 all persons are entitled to full and equal accommodations of any place of public accommodation without discrimination or restriction based on race, color, religion, sex, sexual orientation, national origin, marital status or age.[2]

Learning Outcome 1-B-9 Understand the rewards of cultural diversity

Embracing cultural diversity brings new and different points of view to company operations and problem-solving situations. Maintaining a culturally diverse work place demands high standards of ethical and moral values and requires that your personal biases be controlled. It requires the security professional to recognize his or her personal biases and not allow them to enter into ethical decision making. Recognizing diversity and thinking in core values enhances customer satisfaction and makes good business sense.

[2] This includes prevailing laws governing places of public accommodations where alcoholic beverages are served.

ALARM INDUSTRY OVERVIEW

Learning Goal: To provide an overview of the electronic alarm industry

The electronic alarm and security industry includes businesses that manufacture alarm system components, install and service alarm systems, and provide security services such as central station monitoring and staffed protection

Learning Outcome 2-A-1 Know the types of alarm systems available

1. **Intrusion** - An intrusion system is designed to detect unauthorized intrusion into a building or area of a building. A wide range of control equipment and detection devices may be selected to meet customer needs for detection of an attempted or actual burglary. Most intrusion systems will sound an alarm at the site and report to a central station. When a system is monitored, the monitoring center accepts the responsibility to monitor agreed upon signals from the system and notifies the appropriate respondents.

2. **Fire** - Manual or automatic fire systems and sprinkler supervisory systems use a combination of devices to sense a fire emergency at the earliest point to alert all occupants of a building and to notify the central station so the fire department can be dispatched.

3. **Hold-up, Panic or Personal Emergency** Response Systems- These systems allow a customer to report an emergency, such as an armed robbery or ambush or medical or health emergency. Emergency Notification Systems are designed to protect the life of the person and at the same time provide a means of notifying authorities through the central station. Some systems will also cause film or video cameras to take pictures and or open two way voice devices to allow communication with a central station.

4. **Process Supervision and Environmental Monitoring** - Industrial process supervision involves monitoring specific environmental or equipment conditions in all or part of the facility. This allows the appropriate person or agency to be notified if there's an abnormality. Low temperature, machine failure, or high-water levels are examples of conditions that might activate a sensor to generate a signal.

Learning Outcome 2-A-2 Know the services within the Electronic Alarm "Team"

While there may not be a "typical" company, most electronic security companies sell, install, service, and monitor the systems and services they provide. The functions listed below may be accomplished by one or more employees of the alarm company.

1. **Sales** - Together, the customer and the sales person determine which areas of the home or business are to be covered and what type of system is to be installed. The professional sales person should work carefully to design a system to meet the needs of the customer at the same time insuring compliance with all applicable codes and regulations. A Salesperson may need to consult with the installation department for specific device locations but will ensure that areas of coverage are agreed to by the customer.

2. **Installation** - The Installation crew will review the areas of coverage and specific device locations in an initial walkthrough with the customer. The installer must take into consideration the elements of construction and the aesthetics of the facility when suggesting specific locations. Upon completion of the installation of the alarm system hardware and programming of software functions the installation crew will again walk through the entire facility with the customer and ensure that the customer has approved the installation and can operate the system completely and accurately. If the system is monitored by a central station a full set of test signals should be transmitted and documented for the record.

3. **Maintenance** - It is the ultimate responsibility of the owner or customer to ensure that the system remains in proper working order. It is the job of the maintenance or service department to maintain and repair the system in a timely manner when requested by the owner. Every service visit by the technicians should include a complete inspection and test of the system for proper working condition while on site.

4. **Customer Service** - Customer record keeping, service request scheduling, resolution and documentation and other general system questions are functions handled by the customer service department.

5. **Administration** – Usually includes the Management, payroll, billing, collections, and clerical duties to ensure that the alarm company functions in an efficient and effective manner.

6. **Alarm Monitor** - The Alarm Monitor or Central Station Operator is the person that acknowledges the alarm or supervisory signals follows the appropriate instructions and notifies all responsible parties of the alarm or supervisory conditions. A permanent record of all events are documented and retained by the central station and the alarm company.

Learning Outcome 2-A-3 Understand the importance of the Central Station and the Monitor

The central or monitoring station is–the primary point of contact for most alarm system owners after the system is installed. The central station is a 24-hour, 7 day a week operation, where signals from the customers system are received and processed. The Central Station operators process signals from the customers system and alert appropriate responding agencies (police, fire, medical, service, etc.) The Central Station is usually regulated by the state and complies with standards and regulations designed to ensure reliability and integrity. Minimum staffing levels are regulated and operators must pass background checks. Operators must be trained to meet state requirements and pass a state mandated exam. The operator is a vital link in the company's success in protecting the lives and property of customers.

ALARM SYSTEM OVERVIEW

Learning Goal: To identify what an alarm system consists of and it's purposes

Learning Outcome 3-A-1 Understand what an alarm system is designed to do

An alarm system is an assembly of equipment and devices designed and arranged to:

1. Provide quick detection of a change of status
    a. From Normal to Alarm
    b. From Open to Close
    c. From Alarm to Restore
2. Provide notification of occupants
3. Verify scope of event (life or asset threat, equipment maintenance requirement, expected and routine action)
4. Report the event change to the central station

Learning Outcome 3-A-2 Know the difference between Detection vs. Protection

While these terms are often used interchangeably, they have different meanings. Detection senses events or unauthorized status changes and reports them to a monitoring center, it does not prevent them. Protection implies that the undesired events will be prevented. While alarm systems have a deterrent effect, alarm systems cannot prevent threats from happening, they can only sense what has happened.

Learning Outcome 3-A-3 Know the difference between Local vs. Monitored systems

A local alarm system is a sounding device that makes noise to alert the occupants or frighten away the intruder. Monitored systems send electronic signals to a central station for analysis and relay to the proper responding agency. Occasionally and in some jurisdictions signals are sent directly to the police or fire departments.

Learning Outcome 3-A-4 Know the basic parts of an alarm system

1. **User Control Interface**- Keypad, key switch, computer or telephone device that provides the ability to control the alarm system. The User Control Interface provides the means to check system status, arm, disarm or reset the system.

2. **Detection** – Devices designed to monitor a condition, detect inappropriate changes and send notice of status change to the control panel.

3. **Control** - The control is the management center for all components of any alarm system. This panel provides power to devices, monitors the status of detection devices, processes information from user interfaces and devices and then makes appropriate notifications and annunciations when activated.

4. **Annunciation**- Bells, horns, sirens, strobes and graphic displays are devices designed to notify occupants of an emergency condition and initiate appropriate actions including evacuation if warranted.

5. **Transmission**- Control panels may communicate electronically in a variety of methods including traditional telephone, cellular telephone, internet, short or long range radio, to notify off site personnel that an event has occurred.

6. **Power Supply and back-up Battery**- provides the primary power and back up battery power to operate the system. The power supply and battery are usually included in the same box with the control panel.

Learning Outcome 3-A-5 Understand the purpose of "Zones"

Alarm systems are installed in facilities of all sizes, shapes and configurations. A common method of system design is to divide the system into separate areas or "Zones" to define particular areas or functions for ease of installation and service. Zone information is particularly critical when attempting to dispatch authorities to an alarm situation. Passing details of impacted zoned areas is important to responders discerning level of response. If the Fire Department knows that the fire is on the third floor they can save critical time responding.

Learning Outcome 3-A-6 Know the types and purpose of alarm devices

1. **Perimeter Sensors** – The perimeter is defined as the outer boundary of a system separating the area of coverage and the area outside of coverage. For a building system, it is the walls with doors and windows, floors and ceilings. For an outdoor system, it is a fence or the outer edge of the sensor pattern. Perimeter Sensors include magnetic door contacts, Infrared beams, seismic shock sensors, glass break detectors, and intrusion system screens.

2. **Interior Sensors** – Interior detectors usually detect motion or infrared body heat in the interior of the protected area. These include combination motion sensors, ultrasonic, microwave, passive infrared and photoelectric type detectors, and audio processors.

3. **Other Sensors** - Other sensors include environmental sensors, industrial process sensors, equipment performance sensors and temperature sensors.

4. **Fire Alarm Sensors** – Fire alarm sensors include smoke and heat detectors, rate of rise detectors, duct detectors, and water flow valve detectors to name a few.

5. **Manual Initiating Devices –** Manual pull stations for fire alarms, panic or hold-up buttons, and medical emergency pendants are types of manual initiating devices.

Learning Outcome 3-A-7 Know the difference between Armed, Disarmed and In - Alarm

Alarm systems as a whole can be turned on or off or "armed" and "disarmed" by the user. Parts of the alarm system may be controlled separately to be armed or disarmed and other parts may be "armed at all times" and not controlled by the user. By looking at a few types of alarm systems we can better understand the Armed, Disarmed and In Alarm functions.

1. **Intrusion system** – in this type of system you are only trying to detect the unauthorized entry into the location that the alarm is installed
   a. In the case of a business during business hours the entire system may be off or "disarmed" to allow full movement and free entrance into and throughout the facility for business purposes. When closing up at the end of the day you will turn on or "Arm" the system to detect any unauthorized entrance or interior movement while the building is closed and locked. In the "Armed" state any violation will set off the system annunciators and communicators indicating that the system is "In

Alarm". Usually a siren will sound inside and outside if equipped and the communicator will be sending electronic signals to the central station.

b. In a residential system example you may arm the system different ways while you are home or while you are away. While you are away you would "Arm" the entire system. While you are home you may only want to "Arm" the perimeter zone leaving you free to move around inside the house" (this is another example of how zones can be useful)

2. **Combination System**. –Combinations systems are usually intrusion and fire alarm systems combined and controlled in a common control panel. In this type of system you may have Zones that you are not able to "arm or disarm". These are usually fire and life safety type zones that are always "Armed" and if a device on these zones is ever activated the control panel will immediately go into the "in alarm" state and sound annunciators and send signals to a central station. The intrusion system portion of the system is controlled by the user and "armed and disarmed" by the user.

Learning Outcome 3-A-8 Understand Monitoring Options

All monitored alarm systems have in common the fact that signals are transmitted to a central location where trained personnel acknowledge those signals received on specialized equipment and perform the specified instructions designated by the installing company and end user. This facility is called a Central Station. There are several types of central stations and they are defined by ownership, certification and location. These central stations may or may not be certified and inspected by agencies that develop and enforce adopted standards such as Underwriters Laboratories, Inc., (UL) Factory Mutual (FM) or other nationally recognized organizations.

1. **Full Service Alarm Company with Central Station** – a for profit company that sells, installs, services and monitors the alarm systems is called Full Service Alarm Company. They are typically corporate or privately owned and operated by the same business entity.
2. **Proprietary Alarm Company and Central Station** – A proprietary company typically installs, services and monitors alarm systems that are privately owned by the same entity. They may be at the same location or at several locations and may be monitored on site or at a common location.
3. **Independent or Third Party Central Station** – These central stations are typically owned and operated by independent companies and provide monitoring services for independent alarm companies on a contract basis. These monitoring companies are usually certified and inspected by UL and others on an annual basis.

CENTRAL STATION OVERVIEW

Learning Goal: To provide an understanding of the central station functions

Learning Outcome 4-A-1 Understand the general functions of a central station

A central station is a facility where trained monitoring personnel process signals sent from alarm panels through electronic receivers and automation systems. Monitoring Operators acknowledge those signals follow displayed instructions to notify appropriate responding agencies and other required personnel. These facilities must be operational and staffed 24 hours per day and 365 days per year to respond to the emergency situations alerted by the various alarm systems.

Learning Outcome 4-A-2 Know general security features of a central station.

1. **Secured Facility.** A central station is a secure facility designed to house specific electronic equipment and personnel for the processing of alarm signals. Central Stations usually include back up monitoring equipment, electrical systems, and telephone communications systems in addition to at least two monitoring operators on duty at all times.

2. **Central Station Design.** Central station buildings are designed with floors walls and roofs that resist entry from unauthorized intruders. If the Central Station is part of a larger building it is usually designed and built with additional secured entrances, reinforced interior walls and an access control system. The central station should be a restricted area where observation and entrance from the outside is not permitted. Windows should be secure, opaque and resistant to force unless well above ground level.

3. **Central Station Fire Resistant Construction** Fire resistant construction should be employed in the construction and outfitting of the central station. Fire alarm systems, fire suppression systems, automatic sprinklers and portable fire extinguishers are installed to protect the central station from fire and smoke damage.

4. **Central Station Communications.** The most critical elements of the central station are the communication systems. These systems are integral to the operation of the station, the employees inside, and most importantly the subscribers whose alarms are monitored by the central station. Very often these systems are life safety systems and lives are dependent on the proper operation of people and equipment.

5. **Staff Identification.** Only authorized personnel are allowed inside a central station. Employees should display valid company identification and access should be restricted by locked doors, an access control system, or a positive identification and electronic door lock. Visitors should only be allowed if escorted by authorized employees, or allowed entry after a verification process using closed circuit television, a bulletproof glass window in the door or a secure mantrap to verify proper authorization.

6. **Challenges.** There are many challenges to the operation of central stations that come from both natural and man-made causes. Weather and other forces of nature, in addition to man-made disasters can all interfere with the normal operation of a central station. Employees and subscribers alike must allow for contingencies to ensure continued operations under all but the most serious of life threatening occurrences to keep the station running properly to monitor and respond to alarm signals properly.

Learning Outcome 4-A-3 Understand options to protect critical functions of central stations

Multiple methods. Central stations will provide several types of redundancies to ensure that they can perform critical functions. They may incorporate different technologies to perform the same function and have one technology back up the other.

1. **Electrical Power Service** The main source of electrical power is usually provided by the Public Utility Company or Municipal Power Company. A secondary power supply is always required for redundancy and several methods are available. Independent gasoline or natural gas powered generators are one method. Banks of stand by batteries are another method.

2. **Back-up Generator** may be fueled by natural gas or gasoline and is usually designed to automatically turn on whenever the main power fails and continues to run until the power comes back on.

3. **UPS and Surge Protectors** or suppressers are devices that maintain consistent power and reduce the effect of a high voltage transient or “spike”. An Uninterruptible Power Supply or UPS is a device designed to provide consistent power for a limited time to allow for an orderly shut-down of systems and preservation of programming and data. Surge suppressors will block transient spikes of voltage from lightning or other type of power surges.

4. **Central Station Batteries** may be used as an alternative or as a supplement to a generator. Batteries may be used to provide a few hours' worth of power to critical equipment while a generator starts or larger capacity batteries may be used for longer time periods. Automatic emergency lighting systems commonly use batteries.

Learning Outcome 4-A-4 Understand the purpose and scope of signals.

Alarm systems send a variety of electronic signals indicating the status of the protected facility and equipment to central stations. These signals will describe different types of information including alarm conditions, supervisory conditions, trouble conditions and tamper conditions.

1. **Alarm Signals** - These signals indicate that an emergency condition has just been created and requires immediate action including notification of police, fire, medical or other emergency response personnel. Alarm signals might also include a tamper signal indicating that an unauthorized attempt at disabling the system has occurred.

2. **Supervisory Signals** – these signals indicate that a system or device may not work properly. An example would be a low pressure alert on a sprinkler system, low fuel on a generator system, a smoke detector needs to be reset or other type system attention need.

3. **Trouble Signals** – These signals indicate a malfunction of the alarm system or devices attached to the system. It may also indicate grounded or shorted wires and cables, AC power failure, or low battery. These signals indicate the immediate need for system repair.

4. **Transmission methods.** There are a variety of methods for transmitting signals from the protected facility to the central station or monitoring facility. These methods range from regular voice telephone lines, often called POTS lines or Plain Old Telephone Lines, to cellular phone systems, to internet or IP communications, to short or long range radio systems or combinations of the above. Today's modern technology continues to evolve and we see new methods every few years. Professional salespeople should pick the most reliable and appropriate method for each application and location.

5. **Alarm Receiving Equipment.** This specialized equipment is designed to receive and understand the electronic signals sent by alarm systems, translate those electronic signals and print the information. Usually the receiver will send all the signals to an

automation system but it can directly present the information to a monitoring operator for action. The receivers will document the time and information that is received. The information will be printed and/or sent to an automation system where it will be merged with all the appropriate information including the name, address, phone numbers of contacts and instructions for each type of alarm. The automation system will also log all of the activity. Some types of signals are only logged for the record. If the signals received require action by an operator the automation system will create an incident, display the instructions to the monitoring operator and record all of the operator's activities until the incident is closed.

Learning Outcome 4-A-5 Know general types of central station recording systems

Given the critical nature of central station activity, it is imperative that the activity of a central station is recorded and stored for an unlimited period of time. Communication is the heart of any central station. Voice and Data Communication are the two critical types that must be recorded to maintain the integrity and function of the central station.

1. **Automated or Computerized Systems.** The computer system maintains and stores all subscriber information, alarm history and service records. Most alarm receivers today are connected to a computer and the signals from those signals are automatically recorded. The information consists of the account number along with an event code. The computer identifies the account, retrieves the customer information, merges it with the instructions for that event and displays the information and instructions to an operator for immediate action. The operator can properly notify the appropriate parties and take whatever action is required. . The operator logs all information and activity about the event into history in the computer for future retrieval.

2. **Phone Recording System**. Central stations generally use a multi-channel recorder to record the telephone conversations on select or on all of the phones located in the central station. This device is a tool primarily used to confirm that proper information and prompt dispatch is made.

CENTRAL STATION PROCEDURES

Learning Goal: To identify safe, accurate, and efficient methods to respond to alarms

The primary responsibility of the Central Station to its customers is to pass along all signals to the proper authorities and/or customer representatives. Central stations maintain information in computers on written files or both. The central station is responsible to relay signals as quickly as possible, not holding or delaying them.

Learning Outcome 5-A-1 Know the basic steps to signal processing

Based on the alarm type and specific company instruction, the order may be different but will usually consist of:

1. Read and respond to interpret the signal
2. Notify the customer
3. Dispatch authorities
4. Record/document your actions

Learning Outcome 5-A-2 Understand the central station functions

1. **Reading and interpreting signals**- Central station operators deal with hundreds of signals each day. Most central stations now use computers to help sort these signals out. Each signal must be correctly interpreted.

2. **Identify the customer** whose system sent the signal.

3. **Determine the type of signal.** Doing this accurately forms a basis for the appropriate response.

4. **Notify Authorities.** If the signal requires emergency action, react quickly to notify police, fire, or appropriate authorities to the alarm site.

5. **Customer notification.** After notifying the authorities, notify the customer. If the first customer representative cannot be contacted, additional persons may need to be attempted. In addition to written instructions, the alarm monitor may get additional instruction from the customer about how to handle the current situation.

6. **Document and keep records.** Maintaining accurate records is a critical part of the job. Accurate documentation of each activity and telephone call completed is vital to every signal handled.

7. **False alarm prevention.** Police and firefighters frequently take risks enroute to a report of a fire or intrusion and each year it cost authorities more to respond to alarms. It is critical to avoid dispatching the authorities unless it is absolutely necessary.

8. **Customer Satisfaction.** Satisfying the customer means being ready to answer a question, or provide service, at any time of the day or night. The customer's impression of the alarm company will largely depend on how he or she is treated by the alarm monitor. How the system operates is important, but a customer remembers they are treated. It is not enough to be technically competent. The alarm monitor must also have, and show, the desire to solve each customer's problem quickly, pleasantly, and efficiently.

Learning Outcome 5-A-3 Demonstrate application of the type of "Time" central stations use

Central stations use 24 hour or military time. This system starts at midnight (2400 hr.) and counts up as usual until noon (1200 hr.). Here things change: 1 PM is 1300 hours, 2 PM is 1400 hr., etc. until 11 PM, which is 2300. This system enables one to determine the difference between 1 PM and 1 AM.

Standard Time	Military Time	Standard Time	Military Time	Standard Time	Military Time	Standard Time	Military Time
1 am	0100	7 am	0700	1 pm	1300	7 pm	1900
2 am	0200	8 am	0800	2 pm	1400	8 pm	2000
3 am	0300	9 am	0900	3 pm	1500	9 pm	2100
4 am	0400	10 am	1000	4 pm	1600	10 pm	2200
5 am	0500	11 am	1100	5 pm	1700	11 pm	2300
6 am	0600	12 noon	1200	6 pm	1800	12 pm	2400

The new day starts at 0001

Learning Outcome 5-A-4 Demonstrate application of the time zones around the world

1. **Standard time and time zones.** The local mean solar time at any location depends on where that place is on the globe. To avoid confusion, most nations keep what is called "standard time" in established zones known as "*time zones*". The world is divided into 24 time zones.

2. **Daylight savings time.** An adjustment of regional standard time, called "*daylight saving time*", was adopted by some countries to conserve fuel by reducing the need for artificial light in the evening hours. Clocks are advanced one hour in the spring and set back one hour in the fall (in most locations).

3. **Recording signals with proper time.** With today's technology it is possible to monitor a signal from another time zone. While it may be one time at the central station, it may be another at the alarm site. Some automation systems will compensate for this and show the time for the alarm site. In the United States, there are four time zones: Pacific, Mountain, Central and Eastern.

Learning Outcome 5-A-5 Know sources which have created industry standards

1. **Underlying Authorities**. National regulations establish some industry standards. The Bank Protection Act's objective is to discourage and deter crimes through regulations on installation, maintenance and operations of security devices and procedures. Locally, the authorities having jurisdiction (AHJ) is the person or agency that decides which standards will be applied to a particular job. The AHJ can be one or all of the following: a federal, state, local, regional authority, a designated insurance company representative or the property owner.

2. **Organizations.** Over the years, several groups have developed standards that form the foundation of how most companies deal with the complexities of alarm equipment installation, functioning and monitoring. These organizations fill one or more of the following roles relating to the standards:

    a. Establish Standards for items and services in specific applications
    b. Testing items or services to assure they meet the intended standards
    c. Determine applicable Standards
    d. Evaluate compliance to Standards

These organizations include:

a. **ANSI** – American National Standards Institute promotes and facilitates voluntary consensus standards and conformity assessment systems.
b. **CSAA** – Central Station Alarm Association is an ANSI-accredited standards writing organization; they work on standards to benefit consumers, regulators and the security industry.
c. **SIA** – Security Industry Association; ANSI accredited standards-developing organization that participates in standards promoting openness and inter-operability of electronic security systems and components.
d. **NFPA** – National Fire Protection Association; information source for fire and life safety information to eliminate fire deaths and injuries.
e. **ESA** – Electronic Security Association; formerly National Burglar and Fire Alarm Association (NBFAA). Issues certifications attained by meeting a higher standard of training; requires continuing education and work experience requirements.
f. **NICET** – National Institution for Certification Engineering Technology; creates the certification of engineering technicians and technologists among many field including fire protection.
g. **IQ** – Installation Quality; certification for alarm installation and alarm monitoring companies that identifies them as a company who follows specific standards to reduce false alarms.
h. **ASTM** – American Society for Testing and Materials; creates industry standards through consensus of stakeholders for the development and use of materials, products, systems and services.
i. **IEEE** – Institute of Electrical Electronics Engineers; the world's largest professional association for the advancement of electrical technology.
j. **UL** – Underwriters Laboratory; independent safety science company and leader in testing, inspection, certification, auditing and validation.
k. **FM** – Factory Mutual; offers product certification and testing services; identifies and addresses inherent business risks.

UL and FM not only have established standards but list the companies that comply with their standards.

3. **Shall vs. Should.** The standards set by standard establishing organizations often include recommendations as well as standards. In any standard, the word "*shall*" indicates a mandatory requirement while the word "*should*" indicates a recommendation of something that is advised but not required.

Learning Outcome 5-A-6 Know the purpose of company standards

Most companies have developed specific procedures for handling central station documentation and alarm processing. These procedures are usually based upon the concepts in this training. When faced with justifying an action in a court proceeding, a company should cite recognized standards instead of a common company or industry practice.

Learning Outcome 5-A-7 Know the components of data entry

1. **Alarm system sold** - Once the alarm system in sold, paperwork should be completed and forwarded to the central station. In most companies it is preferred, if not required, the account information is recorded in the central station computer before the job is tested. This allows complete and accurate testing of the system before it is placed in full operation.

2. **Activate after installation and demonstration** - After the installer has completed the installation, including a test and demonstration of the system, the account is activated or placed in service.

3. **Accurate data entry** - One of the key concerns in entering account data is properly describing the locations of various devices.

Learning Outcome 5-A-8 Demonstrate understanding of the basic signal processing procedures

In a specific situation, the alarm monitor should follow the procedures as indicated on the actual alarm screen or documentation. If for any reason the alarm monitor is unsure of the proper action, the following is a general guide. The objective of the central station is to monitor and dispatch on any signal received.

1. **Responses Vary.** Some signals received at the central station are sent merely to be recorded for later action or reporting (opening and closing), others need immediate action by the alarm monitor. Signals that indicate an intrusion, fire, holdup, or medical emergency require immediate follow-up by the alarm monitor. Most automated or computerized monitoring systems will allow a set of selected signals that do not require monitor action to be “auto-logged” into the account history. Auto logging allows the central station to generate a printout (chronological order) of all signal activity for a specific period of time.

2. **Alarm Priority.** Many computer automation systems will prioritize the signals automatically and route them to the operators automatically. With some computerized systems, and all manual systems, the monitor will need to decide which signal is next. Generally the following priorities are assigned to signal types. Priority is assigned first according to the degree to threat to life and then property involved. Consult with your trainer to determine if your company has established different priorities.

SIGNAL TYPE	USUAL PRIORITY	COMPANY'S PRIORITY
Fire	1	
Medical	2	
Panic, Hold-up, Ambush	3	
Intrusion	4	
Unauthorized Opening	5	
Communications Failure	6	
Supervisory, Low or Temperature, Flood	7	
Equipment or Sprinkler Supervision	8	
Late to Close	9	
Late to Open	10	
AC Power Failure	11	
Low Battery	12	
Late to Test	13	

3. **Alarm Verification Procedures.** Verification will significantly reduce false alarm dispatches to the authorities. Many central stations will automatically attempt to verify, unless the alarm user information is marked otherwise. All central stations should have a standard policy.

   a. **Verification involves the monitor calling the premises** and allowing the phone to ring an appropriate number of times. If there is no response, the dispatch is usually made.

   b. **If an invalid pass code, word, or number is give**, the dispatch is usually made and the police advised that an unauthorized person is at the site. Use of an invalid pass code, word or number could indicate the presence of an unauthorized person, an error, or a duress situation.

c. **If verification of a false or accidental alarm** is received after a dispatch, the authorities should be re-contacted and advised.

d. **When verifying a passcode** and no passcode is given or the wrong code is given, never give the customer a second chance. You do not know if the person is under duress or if someone is listening to your conversation. Thank the person, hang-up the phone and dispatch the police explaining the situation.

e. **Customers desiring to convey duress message** to the operator should be instructed to give a totally incorrect number, preferably with extra digits and/or alphabetic characters. Most alarm dealers encourage the customer to immediately call the central station if they accidentally trip an alarm, regardless of any verification procedure established, and cancel the alarm with their passcode. Quite often monitors calling to verify are met with busy signals due to the communicator still having the line seized. The customer calling to cancel will help assure prompt contact in the event of a miss-dial or phone delays encountered by the monitor.

f. **Alarm Notification Procedures.** In addition to police and fire departments, the central station may be asked to notify several other parties after an alarm. Normal procedure is to notify the first person on the notification list. If the first party cannot be reached, the monitor should go down the list, in order, until someone is contacted. If no one answers at any number, the efforts should be recorded on the alarm computer or manual records. Customers are encouraged to have several names listed in the notification section of each account.

g. **Steps to be taken prior to dispatching an Alarm Signal.** Some companies view previous subscriber activity. If there is a comment (within the last 5 minutes) indicating the alarm was canceled, verify with the operator who handled the cancellation. If an alarm on the same zone has already been dispatched three times within the last 30 minutes, notify the emergency list and dealer only. If the alarm has not been dispatched previously, only dispatched once within 30 minutes or has not been dispatched for over 30 minutes, then follow no alarm dispatch procedures. Check with company on times and procedure/policy.

4. **Alarm Notification**. As a general guideline, the following information should be available to refer to authorities:

a. Identify yourself and company.
b. State the reason for the call.
c. Give address of alarm activation, not LEARNING OUTCOME Box. Include apartment number and customer name.
d. Give directions to the premises if applicable.
e. Give permit number if applicable.
f. Give location of violated sensor, if applicable.
g. Advise if alarm system is audible or silent.
h. Advise if key holders are reporting.
i. Give callback numbers (Central station telephone number).
j. Ask for the dispatcher's name or number.

Learning Outcome 5-A-9 Demonstrate understanding of general trouble signal processing

The following are the recommended steps, however your company may have another variation of escalation; check with your management prior to a response.

1. **Equipment/sprinkler supervision** dispatch procedures include calling the premises. If no answer, notify emergency list and/or alarm dealer. The basic goal for the monitoring of these type of signals is to notify the customer, their emergency list, and/or the alarm company that a potential problem exists with the alarm equipment which, if not acted upon, could result in loss of life and/or property.

2. **Radio Communication/Radio Trouble/Telco Court System Fail/Cut Wires dispatch procedures**:

   a. **Communications failure - 1-way**
      i. Call premises
      ii. If no answer, notify emergency list or alarm company

b. **Communication failure - 2-way (Supervised or Active Communication)**
   i. Call premises
   ii. Dispatch police or security if a response account, or
   iii. Notify emergency list and/or dealer
   iv. This is most appropriate for high risk targets such as jewelry, museums and financial institutions.

c. **Telco Failure, system fail, cut wires**
   i. View activity to see if signal has restored. If restored, advise senior operator of disposition
   ii. If signal has not restored, follow dispatch procedures
   iii. Call premise
   iv. Dispatch police or security professional if response account, or
   v. Notify emergency list and/or dealer.

a. **Restore/No Restore/L-T-T dispatch procedures**
   i. Restore/no restore signal
   ii. View previous activity. If previous signal for the day received and acted upon, no action is required. If there has been no previous signal received that day, some companies follow normal intrusion dispatch procedures.

b. **L-T-T- (Late to test)**
   i. Call premises and advise
   i. During normal business hours, notify alarm dealer or call list

c. **24-Hour test**
   If no "test signal" is received when expected, call alarm company or customer.

g. **Low Battery**
   i. Call the alarm site during normal business hours
   ii. Contact the alarm company or customer

h. **A/C Power Failure**
   i. Call the alarm site
   ii. If no answer at the premises, notify emergency list
   iii. If security professional response, dispatch security professional
   iv. If no answer at premises or list, notify alarm dealer

i. **Environmental Supervision - Low Temperature, High Temperature, Flood/Water Detector AC Power/Phase Monitor**
   i. Call premises
   ii. Notify emergency list
   iii. If no answer at premises or list, continue to try until someone is notified
   iv. Any type of problem inform shift supervisor and/or manager
   v. If no answer on emergency list and if a response account, dispatch security professional

Learning Outcome 5-A-10 Know opening and closing processes

Openings and Closings. For monitored closings, each unarmed system is periodically checked against its closing schedule. The customer may be working late or may have left without setting the system. The customer may be under duress and the alarm monitor should get a passcode to ensure it is the customer that has been contacted, not an intruder.

1. **Basic Opening and Closing Service** - This service is provided to customers whose systems are capable of sending distinct open and close signals as the panel is disarmed or armed. If requested by the customer, the basic service may provide a weekly printout of dates and times the open and close signals were received. The central station does not supervise these items.

2. **Supervised Openings and Closings** - Similar to the basic service however the central station will monitor the times to assure the account is opened and closed according to the designated schedule. There may be a grace period or "*window*" for monitor time errors by the customer. Generally, the customer may open any time as long as it is not earlier than the "*window*" before the scheduled opening time, or may close at any time after opening as long as it is no later than the "window" after the scheduled closing time.

   a. **Late to Open signals** should be forwarded to a representative on the notification list.
   b. **Late to Close** signals should cause the monitor to call the premises, asked for a passcode, and ask when they intend on closing.
   c. **Unscheduled Opening** signals indicating a subscriber has opened early or late requires calling the site and verifying the subscriber's identity.
   d. **Unscheduled Closing** indicates the subscriber has closed early or late. Unless specified in this signal, it is logged with an alarm monitor comment.

Learning Outcome 5-A-11 Understand customer interaction processes

Use of Passcard, Codes, and Passwords. Most companies utilize a password, pass code, ID number or secret code to identify who is authorized to cancel alarms, conduct tests, be present on the customer's premises, and arm or disarm the system. Only a person designated by the alarm owner may change Passcard numbers and codes. Most companies require changes be made in writing. In an emergency, such as a fired employee, divorce, etc., some allow a temporary change to be made over the phone if it is verified later by mail.

1. **Cancellation.** Recommended procedure to handle an alarm cancellation:
   a. Direct the call to the operator responsible for alarm dispatch cancellations
   b. Ask the field personnel and/or customer for the following information:
      i. Name
      ii. Account number
      iii. Name on the account
      iv. Address of the account
      v. Pass code or password
      vi. What signal or type of signal are they canceling
      vii. Verify the above
   c. View subscriber activity to confirm the alarm is being handled by another monitor. If it is:
      i. Inform the operator handling the alarm you have a cancellation, retrieve the alarm and verify with the customer the type of signal received if the alarm is to be canceled.
      ii. Upon verification, finish the alarm and log the cancellation with the pass code or word received from the customer.
   d. If another operator is not currently handling the alarm, perform the following:
      i. Cancel the signal in your records or computer
      ii. If a dispatch has been made, call the authorities to cancel the alarm.

2. **Customer Requests for Service.** Depending on your company policy, you may advise the customer to call the alarm company directly. If you monitor for another company, or in the case of extenuating circumstances, call the alarm company personnel directly.

3. **Complaint and Error Procedures.** Most companies have a written procedure for use when questions or complaints arise. They allow an accurate and prompt response to questions and concerns. Accurate documentation of the "who, what, when, where, and why" of these situations is critical to the satisfactory resolution of claims and problems.

COMPUTERS

Learning Goal: To identify the purpose and scope of computers in the central station

Learning Outcome 6-A-1 Understand the purpose of computers in the central station

Computer servers are typically more robust and powerful than simple desktop computers. They provide the necessary hardware platform for the processing of alarm events and the storage of data.

Learning Outcome 6-A-2 Understand the purpose of a computer network in the central station

The computer network is a series of cable connections ("*CAT 5 or CAT 6*") wiring that connect all of the workstation computers, computer servers, and often alarm receiving equipment, together into a data network. This enables the computers, servers and alarm receivers to communicate with each other. The network also provides for communication with the Internet and for alarms system to communicate directly with the automation system computers using the Internet. The central station network will also utilize data protection devices such as firewalls, routers and specialized software designed to prevent intrusion into the network from outside the central station.

Learning Outcome 6-A-3 Know the difference between hardware vs. software

For purposes of this section, the hardware in the central station would include the computers and servers along with related peripherals such as a keyboard, mouse, monitor and printers. The software typically refers to the operation system, network operation system, the alarm monitoring automation system and other programs that are written and designed to function together over the computer network.

SIGNALS

Learning Goal: Identify the types of signals received in central stations and their purpose

Learning Outcome 7-A-1 Know the types of signals received in central stations

1. Fire
2. Hold-up
3. Duress
4. Panic
5. Intrusion
6. Medical emergency
7. Process or condition
8. Environmental condition

Note: Each general category may have several specific signals that can be sent.

Learning Outcome 7-A-2 Demonstrate understanding of signals that are common to all categories

Any system (fire, intrusion etc.), generates signals designed to monitor the status or operation of the alarm system itself.

1. **Trouble Signals -** A signal indicating trouble of any nature, such as a circuit break or ground, occurring in the devices or wiring associated with an alarm system. Indicates a condition that will impair the satisfactory performance of the intrusion system. Many systems provide separate indicators for each specific problem (e.g.: low battery, a/c power loss, etc.).

2. **Zone Trouble**- signals and similar maintenance codes are often reported to the alarm company personnel rather than the customer. This procedure allows service personnel to contact the customer to coordinate a request for repair service. Various types of trouble signals can be sent.

3. **Test Signals -** Some alarm systems can be set up to periodically send a test signal to verify operation to the monitoring company. Others allow the alarm user to press a button or code to send a test signal.

4. **No Test Received -** A signal generated by the automation system indicating that a test report has not been received at the appropriate time.

5. **Communications Failure -** If a communications device such as a digital communicator, or radio transmitter, or internet (IP) communicator fails to report in, at, or within its scheduled time a communications failure signal may be received from the central station equipment expecting that signal. A communications failure may be due to tampering or equipment failure. Some companies choose to treat this as an alarm and dispatch the police or a security professional. Others consider this an equipment failure and send a technician or alert the alarm user.

6. **AC Fail -** The purpose of this signal is to notify both the alarm user and the alarm company a potential problem may exist if the alarm control equipment is without power for a sustained period. This may indicate an area wide power outage or simply an unplugged alarm transformer. The signal reduces the response of the alarm user or the service technician. It does not require the dispatch of police, fire or medical authorities.

7. **Low Battery -** Many systems are capable of sending automatic "*low battery*" signals when the battery powering the system reaches a certain voltage level. A low battery signal indicates that the battery to a control, radio, etc. is low and/or defective and could result in an inoperative alarm system during a power failure. Prompt attention to low battery conditions is encouraged. Erratic communicator performance, or total failure, can result from deteriorated or discharged batteries. Certain brands of digital communicators use the same low battery code to indicate a "fault in the fire loop," a problem requiring immediate attention.

8. **Restore Signal -** A signal indicating that a device or system has returned to its normal condition. Restore or restorable signals are generated by many systems when the customer has reset the system after an alarm, or when an automatic "*time-out*" feature has shut down the system after operating for a specific period. Restorers do not necessarily indicate that an authorized individual returned the device or system to normal. It could indicate that the intruder closed the door or window behind themselves.

Learning Outcome 7-A-3 Demonstrate understanding of various types of signals and their purpose

1. **Fire -** Manual or automatic fire systems and sprinkler supervisory systems use a combination of devices to sense a fire emergency at the earliest point to alert all the occupants of a building and notify the central station for the fire department to be dispatched.

2. **"Initiating devices"**- such as sprinkler water-flow switches, pull stations, or smoke, heat or flame detectors are designed to indicate when a fire occurs. A fire alarm is a condition that presumes that a fire condition exists and is being reported by the fire alarm system. Fire alarm signals usually require a response by the fire department. All fire alarm systems are active 24 hours a day even when the intrusion system is disarmed (turned off). Fire alarms usually activate audible and visual "notification appliances" (e.g.: horns & strobes) throughout the protected premises.

3. **Supervisory Signal -** Indicates that a device is out of its normal condition. Switches or valves are monitored to indicate when they are turned or changed. Supervisory signals are intended to draw the attention and response of service personnel. One of the most common uses of supervisory signals is for monitoring when water to all or part of a sprinkler system is turned off. Another common use is to monitor when power is turned off to a critical device.

4. **Hold-up or Panic -** These systems allow an alarm user to report an emergency such as an armed robbery or an ambush. Most systems allow the customer to follow a robber's instructions and allow a button to be pressed or trip a switch to generate an alarm to the central station. Some systems will also cause film or video cameras to take pictures of the robber(s). Hold-up, panic and emergency systems are active 24 hours a day even when the intrusion system is disarmed (turned off). They can be manually operated from a fixed location or use - to allow an alarm user to activate the alarm from multiple locations.

    a. **Hold-up -** A holdup alarm is generally intended to signal any action to obtain or attempt to obtain valuables by threat or force that directly threatens the user. Signals can be manually activated by the direct action of the person attacked or of an observer of the attack, such as pressing a button or removing a bill from a money clip in a cash drawer.

b. **Emergency- Panic -** A device such as a push button switch may be manually activated to indicate an emergency has occurred.

c. **Duress- Ambush -** (sometimes referred to as a silent panic) A covert device producing a silent alarm designed to allow a person in a life-threatening situation such as holdup to call for help without arousing suspicion. To reduce the chance of false alarms, the device may require two separate simultaneous acts to activate. Entering a special code, different from the normal arm/disarm code, at a keypad normally activates duress alarms. As an example, an alarm user might use the special duress code if forced to turn off his or her intrusion system against his or her will. Generally, this code does not activate sounding devices at the alarm site.

5. **Medical Alert Signal -** A type of alarm system, often referred to as personal emergency response systems (PERS), allowing notification that medical assistance is needed, usually by pushing a button.

6. **Intrusion –** An intrusion system detects unauthorized intrusion into a building or area of a building. A wide range of control equipment and detection devices can be selected to meet the customers need for detection of an attempted or actual burglary. Most intrusion systems will sound an alarm at the site and report to a central station.

7. **Abort or Cancel Signal -** An abort or cancel signal means a request by an authorized alarm user to the alarm site to cancel a response by the police. If the alarm user turns off or disarms the system while it is communicating, many systems will change the signal to an abort or cancel signal.

8. **Forced Arming Shunted Zone -** Bypass signals indicate the customer has bypassed a portion of the system (a zone) on closing. A zone will not report an alarm while in the bypassed state.

9. **Exit Alarm -** In an effort to give more information to avoid or correct false alarms, newer panels may generate an exit alarm. An exit alarm can be generated when an alarm is activated (usually accidentally) within a short time from exiting a premise. Exit Alarms are sometimes referred to as a Break on Exit

10. **Opening & Closing Signals -** Opening signals are generated whenever the alarm system is turned off by a valid user. Closing signals are generated by the alarm system whenever a valid user turns on the system. Some systems providing opening signals will send a general signal. Others send a number or letter to indicate the person disarming the system. Opening or closing signals occurring at a scheduled time are referred to as scheduled openings or closings. Opening or closings at other times are called unscheduled openings or closings.

    Scheduled openings and closings are manually or automatically logged and generally require no further action. If the signal is received outside of the schedule (unscheduled) operator action is usually required.

11. **Process Supervision and Condition Monitoring** - Process Supervision involves monitoring specific environmental or equipment conditions, in all or part of the customer's building that may result in severe damage to their premises or property if not acted upon promptly. This allows notification to the customer if there is an abnormality. Low or High temperature, machine failure, or high water levels are examples of conditions that might activate a sensor to generate a signal.

12. **Carbon Monoxide Gas Alarms.** - A signal from a carbon monoxide detector is designed to indicate that an unacceptable level of carbon monoxide gas is present. This may indicate a failure in a furnace or improper ventilation in a room housing a fireplace or wood stove.

ALARM COMMUNICATIONS

Learning Goal: To understand the communication of alarms for effective alarm monitoring.

Learning Outcome 8-A-1 Know the sources for monitoring

1. **Central Stations**: The term central station has become a generic term referring to all types of privately operated monitoring locations. Technically, the term "*central station*" refers to monitoring facilities constructed and operated according to a standard.

2. **Monitoring Stations**: Monitoring stations are facilities that may or may not meet the standards but have not been inspected by a listing agency to verify compliance.

3. **Proprietary Stations**: The same company they provide monitoring for owns proprietary monitoring facilities.

4. **Public Agencies**: In some areas, police departments and fire departments monitor alarm systems.

Learning Outcome 8-A-2 Know the basic communication standards

1. **Passive/ Non Supervised Communications**: regardless of the communication mode or path used, the communication path is initiated only when the communication device needs to communicate a signal. The path is opened, connection to the receiver is established, message is passed, the receiver confirms receipt and the path is closed (a phone call is Passive).

2. **Active/ Supervised Communication**: regardless of the communication mode or path use, the path is initiated upon installation of the communication device and remains open. A continual acknowledgement between receiver and the alarm is passed. If the path is broken both the receiver and the alarm alert locally indicating the failure. The devices attempt to reopen the path. This is the most secure means of communication (phone calls are not supervised)

Learning Outcome 8-A-3 Understand how phone lines work

1. Public Switched Telephone Network (PSTN):
   A local phone company provides line power, dial tone and ringing tone to a local telephone line for a call to pass. The following types of switches are utilized:
   a. An electronic switching system
   b. An electromechanical switching system
   c. A computerized switching system.

2. Central Office Feeder Cables: Feeder cables run from the local central office to the cross connect terminal cabinets in the phone company's outside infrastructure.

3. Cross-connect cables are mounted on poles, on the ground on cement pads, or in underground chambers called Controlled Environmental Vaults (CEVs).

4. Distribution Cables: At the cross connect locations, Feeder cables are divided into smaller bundles known as distribution cables. Residential and commercial phone customers are connected to these distribution cables.

5. Cross connect cabinet: Each pair of wires in the feeder cable is attached to terminals mounted on a plastic base called a terminal block.

6. Network Interface Device: At the subscribers premise a drop cable runs from the distribution cable to a network interface device (NID). The NID contains a station protector to guard the subscriber's phone equipment from damage from lightning and high power lines.

7. Older phone network: Older Telco infrastructures use Analogue Technology. Currently this is the predominant communication technology utilized by the Alarm Industry

Learning Outcome 8-A-4 Understand how phone lines are used for Alarm Communication

Digital Communicators: [The term "*Digital*" in this context should not be confused with the competing communication Technologies of analogue and digital. Digital Communicators use Analogue Technology]

Digital communicators use regular dial tone telephone line, Plain Old Telephone Service (POTS)to make a phone call and send its information to the central station. Since the customer has already paid for the phone line, the cost of this method is limited to the cost of the call. There are some disadvantages to digital communicators; they signal only when in alarm condition and the lines are not constantly supervised at the remote location.

Types of Communicators. There are two types of digital communicators; standalone and integrated.

a. Standalone communicators usually have to be connected to a control panel.
b. Integrated communicators are combined with the control in one single unit.

Learning Outcome 8-A-5 Understand potential problems with phone communicators

Digital communicators use the customer's regular phone line. To use the regular phone lines effectively, there are concerns.

1. If a customer is using the phone at the same time an alarm condition need to be communicated.

   When the customer and the alarm use the phone at the same time a technique known as "*line seizure*" gives the alarm system priority. If the customer is using the phone when the alarm system sends a signal, the digital communicator will disconnect the customer until the alarm signal has been sent. Once the signal is sent the customers phones are reconnected. Line seizure is accomplished with connection to the regular phone lines through a phone jack, called a RJ31-X.

2. If there is a problem with the customer's phone.

   Line fault detectors can be installed to notify the customer when the line is down. This will let the customer know through a small sounder or a display on the keypad however it will not let the central station know. Line fault monitors can be set up to activate a secondary communications link (radio, direct line, etc.).

3. If there is noise on phone circuit.

   Digital Communicators communicate using analog technology. An analog signal must have its shape preserved accurately if it is to sound like the original. Extraneous noise introduced on a phone circuit can warp the message sent making it uninterruptable by the alarm receiver. Failure by the receiver to interpret an incoming Digital Communicator message results in a Hang Up. The Communicator redials with the probability of a reliable circuit being established within Telco infrastructure.

Learning Outcome 8-A-6 Know solutions for phone communicator problems

1. **Multiple phone lines**
   Multiple phone lines can be used to monitor one another. With this arrangement, both lines are constantly monitored for faults. If a fault occurs on one line the other line is used to notify the central station. This will work unless both lines are cut or fail. There are three basic ways to use multiple phone lines: split, backup and double reporting.

   a. Split Reporting: Some zones or types of alarms, such as fire, intrusion, etc. are sent to one line, other zones are sent to one or more additional lines.

b. Backup: All signals are sent to one line and transfer to another line if they fail to get through on the first.

c. Double: All signals go to two lines. The duplicate line can be, in the same receiver, in a different receiver in the same location or in a different receiver in a different location.

2. **Test Signals:**
   Most digital communicators can be programmed to send test signals to the central station at regular intervals. If the expected signal from the communicator is not received, within a certain time, then the central station can take action.

3. **Redundant communications**:
   Digital communicators can be backed up by other technologies including, long range radio or cellular.

Learning Outcome 8-A-7 Understand how enhancing digital communicators can reduce False Alarms

Several features have been added to enhance the service performed by digital communicators.

1. **Listen In**
   a. This option allows the operator to hear what is going on in rooms at the alarm site that have been equipped with a microphone. This enables the operator to pass on valuable information to the responding authorities. If intruders are heard in the premises, this information can be used to give added priority to the dispatch.

2. **Two-Way Voice**
   a. This system feature allows the operator to listen in to the alarm site and also talk through speakers placed at the alarm site. This can make communication between the alarm site and the central station considerably easier.

3. **Video Verification**
   a. Improvements in video technology allow the operator to see several snap shots of activity (Slow Scan) before and after the alarm or to monitor real time activity from the alarm site. Video systems can be separate from the rest of the security system or integrated into the control and communicator. Video may be viewed on standard computer monitors or through a separate monitor. Video received at the central station can be recorded on a video cassette or disk recorder for future reference.

4. **Caller ID**
   a. This feature can identify a system's phone number. This can be useful in dealing with signals sent in error by an installer before the central station has been notified, or in tracing down a malfunctioning system.

Learning Outcome 8-A-8 Understand how technology changes have impacted on alarm communication over plain old telephone systems (P.O.T.S.)

In the mid 2000s the Nation's major Telecommunications firms approached the Federal Communication Commission (FCC) to transition the telecommunication infrastructure technology from analogue to digital. The purpose for the request was to permit significant broadening of communication potential over the telecommunication media; this would allow a transition to Voice Over Internet Protocol (VOIP).

1. **Analog vs. Digital**
   An analog signal must have its shape preserved accurately if it is to sound like the original. With a digital system, the signal is either on or off so noise does not alter the message.

2. **Multiplex / Multiplexing**
   When alarms first communicated to a monitoring center, each alarm system had a single wire circuit dedicated for its communication to a receiving device exclusive for the account. The cost of a dedicated circuit for communication for each alarm system made signal transport expensive.

   Technology developed the concept of "Plex" which is to stream several applications simultaneously along a single circuit. Alarms were frequently installed in close proximity to other alarm systems.

   Multiplexing messages down a single circuit addressing unique conversations with each alarms systems became a means to share the cost of the single circuit by multiple alarm systems.

   To support multiple conversations on a single circuit and avoid confusion these conversations must be separated from each other. There are two concepts of separations, Time and Frequency.

   a. One technology separates messages to multiple units by timing messages sequentially (not simultaneously). This is Time Division Multiplexing (TDM).
   b. The other technology separates messages sent to multiple units by communicating to each on different defined frequencies simultaneously. This is Frequency Division Multiplexing (FDM).

      Multiplexing is sometimes referred to as "Muxing." Some multiplexing systems are passive (Non Supervised) receiving, alerts from alarm systems on the circuit one at a time with the receiving device acknowledging receipt to the sending unit. Other multiplexing systems are active (Supervised) in which there are polling and responding messages to and from each alarm system on the circuit. Multiplexing is

no longer a concept applied only to wire circuits. Multiplexing can be applied to wireless circuits and may be applied to the various communication media below.

3. **Telcos in transition**
   The Telco infrastructure transitioning to a Digital Technology has the potential of warping the shape/structure of an analogue signal initiated by a Digital Communicator making the message unintelligible for the receiving unit to correctly interpret. This fact is forcing Digital Alarm Communicator Transmitter (DACT) based alarm systems on to other communication modes or paths other than phone lines (POTS). These modes are Voice Over Internet Protocol (VOIP), Cellular, Internet and Long Range Radio. The transition of an existing Digital Communicator system is accomplished with dialer capture modules that convert the units' analogue protocol output into the same protocol in a digital technology scheme.

4. **Cellular system (GSM)**
   A cellular system is a mobile telephone system that divides large service areas into small cells, each with its own low power transceiver. Computers switch a telephone call from one transceiver to the next without interrupting its signal as the cellular phone moves from one cell to another.

   Until the mid 1990's cellular networks used analogue technology when they transitioned to digital technology known as Global System for Mobile (GSM). Communication in this mode can be expensive depending upon the requirements of the communication. This technology is itself undergoing technology change requiring upgrading of transmission units to accommodate the changes (2g, 3g, 4g and EST.) Passive Communication

5. **VOIP**
   Digital Phone Systems utilize calling units that function like a Digital Communicator that communicates using digital technology as opposed to analogue. Passive Communication

6. **Internet**
   Communication is over the Internet with alarm signals sent to an established IP address of a receiver that acknowledges receipt of the message. Communication can be Passive or Active (Supervised) assuring the availability of the communication path.

7. **Long Range Radio**
   Radio Frequency (RF) transmission is usually accomplished with Frequency Modulation (FM). Some networks utilize a poling scheme initiated by the receive polling all transceivers within the network. Other networks utilize a Mesh Radio scheme in which all transceivers will function as initiators of messages or repeaters for the initiated message passing it to the receiving antennas.

CONTROL PANELS

Learning Goal: To understand the basic components of control panels and their function

Learning Outcome 9-A-1 Understand the purpose of control devices

Initially, control panels were simple electronic devices. With the development of computerization, control panels have become computers with sophisticated advanced features. There are many different companies manufacturing hundreds of different control panels. Many control panels have unique features, however all control panels perform some common functions They detect problems through the sensors connected to them, and they report these problems to someone.

Controls also provide the user a method of turning the intrusion system on and off, and allow the customer to enter or leave the monitored area without setting off the system. Controls allow some portions (fire, holdup, etc.) of the system to remain "armed" 24-hours a day, 365-days a year. Controls provide the alarm user, a responding authority or an inspector with a method of silencing bells, or control other system features.

Learning Outcome 9-A-2 Know the function of the control panel

The control panel coordinates actions the system takes in response to messages received from sensors connected to it. The control panel converts power it received from a wall socket, battery, or both, to be utilized by the system.

Learning Outcome 9-A-3 Know three general methods used to connect parts of the alarm system to the control panel.

1. **Hardwire**
   Hardwired systems use concealed or exposed wiring to connect the components. When wireless techniques are used for some of the system, sounding devices are usually connected to the control with wiring. The time and cost of installing the wire can be more expensive, a hardwired system is not generally subject to "radio interference". Since all devices can be powered from a central power source in the control, individual batteries at each device are not required.

2. **Wireless**

   Wireless systems use radio frequencies to connect to the controls. In wireless systems, hardwired or wireless methods may be used to connect the user controls to the control panel. Small battery powered radio transmitters are used to signal alarms to a radio receiver in the control panel. When the battery wears out, it must be replaced or the transmitter's signal cannot reach the control. Some use "household" batteries that last for about 10 months, while others use special batteries that last for several years.

   a. **Premise Wireless (RF) System**

      Each wireless system has its own general radio frequency or house code. Some systems assign each receiver and transmitter a specific sub-frequency or path. In others, multiple transmitters can be connected to a single receiver. If all transmitters use the same signal - supervision is decreased or omitted. Many systems supervise signal strength and verify operation by monitoring each sensor at preset intervals. If the transmitter fails to "check in" a specified number of times over a preset period of time, an indication is made locally and/or remotely that a sensor has failed to send a signal. This is distinctive from the alarm signal. Batteries can also be supervised by reporting when they fall to a predetermined voltage. This is also a distinctive signal.

   b. **Hardwired vs. Wireless**

      Hardwired and wireless systems have an equal number of devoted fans. While there are applications that can only be installed with hardwire and others that can only be done with wireless, most applications can be installed either way. The choice is left to the installer and the alarm user. Hardwired systems are preferable in areas with high levels of radio frequency interference and in systems where maintenance of batteries in the transmitters would present a problem. Wireless systems are preferable in areas where concealing wires is difficult or when portability of the system is desired.

3. **Line Carrier**

   Line carrier systems use existing electrical wiring at the alarm site to transmit messages between the alarm system components. Signals are sometimes multiplexed on the alarm sites power lines between the sensors and the control. A more common use of line carrier technology is to transmits signals to light or sounding devices in a home when the alarm is activated. Challenges of line carriers are outages in power lines. May prevent a signal from successfully transmitting and many alarm sites have more than one phase or set of power lines, so special equipment may be needed for communication between them.

Learning Outcome 9-A-4 Understand the purpose of partitions

The computerization of controls has permitted grouping of multiple alarm zones and alarm points into separately functioning alarm groups. A group is referred to as a partition. A partition is a separate section of an alarm system that can operate independently and is controlled from the master keypad or by separate user keypads, each related to a specific partition. Some controls support multiple partitions. Partitions are used to allow for different hours of operation or because of a desire to restrict particular individual or groups of users. Each partition has a unique ID in alarm signal reports from the control panel. Prior to the introduction of partitions, multiple control panels were required at a single location (each with a unique account number).

Learning Outcome 9-A-5 Understand the purpose of keypad control points

Keypad controls allow the alarm user to turn the intrusion system on and off or enter and leave the monitored area without setting off the system. User controls also allow the alarm user to see which sensors are active and what doors are open, etc. User controls indicate "system events" such as alarms or trouble with phone lines, equipment or circuits. In short, user controls allow the user to control the system and get information.

Learning Outcome 9-A-6 Know the types of Keypads in use today

The general types of keypads are alphanumeric and LED. Either type can be mounted at the control or separate from it. Both allow the entry of a numerical code to arm and disarm the alarm system and may be used to perform various other functions such as shunting or programming system functions.

1. **Alpha-numeric keypads** combine keypads similar to a push-button telephone dial with an alphanumeric display showing letters and numbers.
2. **Digital keypad** also uses a keypad but display information by lighting small lights known as LED's (Light Emitting Diodes).
3. **Touch screens** - Touch screens allow the user to get multiple customized displays of graphic and textual information for easier interaction with the system

Learning Outcome 9-A-7 Understand an appropriate application of key switches

Although, most systems use some other control method, there are times when key switches are the most appropriate way to control the system. Because they are simple to use, understand, and no codes or combinations need to be remembered they are ideally suited for some alarm users who might view another system as too complicated. There are two types of key switches; momentary and maintained.

1. **Momentary Key switches**. To arm or disarm the system:
   a. Turn the Key.
   b. Spring loading returns key to its original position.
   c. Insert and remove the key from the same position.

2. **Maintained Key switches**
   a. To arm the system, turn the key to one position
   b. To disarm, turn the key to the other position.
   c. The key can be removed from either position.

Learning Outcome 9-A-8 Know other components of keypads

1. **Telephone control** - Since most alarm systems are connected to the telephones and phones are often in locations where user control devices have traditionally been located, many control panel manufacturers have incorporated ways for the phone to be used as a user control. When phones are used to control the system, feedback on system status and events is given audibly over the phone. Because the system is connected to the telephone network, systems with this feature can be controlled from anywhere a phone call can be made.

2. **Computer control** - Some systems are connected to a computer and allow control of events and receipt of information.

3. **Smartphone Apps** – many controls permit enhancement options permitting access to the control panel remotely via a Smartphone.

Learning Outcome 9-A-9 Know what a detection circuit (loop, zone) is

A Detection Circuit (loop, zone) is a portion of the detection or monitoring system that responds in a specific manner to sensed conditions. It is usually separately annunciated at the premises and/or remotely at a central station.

Learning Outcome 9-A-10 Understand what a zone is, and its purpose

A zone is another name for a detection circuit. It enables central station operators to tell precisely where in a premise an emergency is occurring. Zoning is dividing a system into a series of subsystems. Each zone or subsystem can consist of a single device or a group of devices in a given area. Dividing a system into zones allow individual zones to be setup or programmed to react to the same type of input in a different way. A door contact on one door might give an immediate alarm while another might be delayed. Identifying an area or type of signal to the user makes the system more "*user friendly*". Most alarm companies have made zoning a standard practice because of the troubleshooting advantages. Zoning reduces service time by enabling the customer and service technician to pinpoint the area needing corrective action. Some controls allow the user to bypass a particular zone or zones while turning on the remainder of the system. Some controls allow defective zones to be bypassed while the remainder stays on.

1. **Point annunciation**

Point annunciation goes one step further than zoning consisting of a single sensor. As the cost of additional zones is reduced, it has become more common to see systems that use point annunciation. Controls and sensors that can be individually identified are often known as addressable devices.

2. **Cross zoning**

Cross zoning is the practice of suppressing an alarm signal until two or more detectors in separate zones register alarm conditions. If the feature is available, it will be performed by the control when the control is programmed for cross zoning.

3. **Labeling can be critical**

Effective design will label zones in a way that is clear to all that use or respond to the system. This may require two sets of labels, one from the alarm user and another for the police and fire authorities. As a central station operator be aware of both sets of labels

since the information will go to two separate sources, the subscriber and the police. Labeling for the alarm user is done using names familiar to the user (Johnny's Room, Kitchen, Etc.). Labeling for the police and fire authorities is done from the perspective of looking at the building from the outside (1st Floor East, Basement Rear, Etc.).

Learning Outcome 9-A -11 Know the purpose of intrusion circuits

The alarm user will use some type of user control to turn the intrusion system on and off. Circuits turned on and off by the user control are known as "*controlled zones*". Circuits or zones that remain on 24 hours a day are known as "*24 hour zones*":

Entry-exit delays allow a user a preset amount of time to access the control panel or exit without setting the alarm off.

1. **Entry delay**

When the alarm user opens a door to enter the detection area a timer in the control panel begins counting down. A buzzer or sounder is sounded (pre-alarm) to remind the user to turn off the system. If the user turns off the system in time, the pre-alarm sound turns off, along with the intrusion portion of the alarm system and no alarm is generated. If the user or an intruder fails to turn the system off in time, an intrusion alarm is generated.

2. **Exit Delay**

When the alarm user is ready to leave, after having closed all monitored doors and windows, the system is turned on (arm) at the user control point. The system begins counting down the exit delay (a predetermined amount of time the user is allowed to leave). If the user leaves the detection area within the time frame, the system arms and no alarm is activated. If the user takes longer than allowed, the alarm is generated.

3. **Delayed vs. Instant**

Use of the entry-exit delay can delay the response to a particular sensor. Rather than place the delay on all intrusion alarm sensors by programming, the delay is placed only where needed. Zones that use the entry-exit delay feature are known as delay zones. Instant zones generate an alarm immediately when activated.

4. **Perimeter vs. Interior**

Sensors are often placed on perimeter or interior circuits or zones for two reasons. These designations are used to identify locations more easily. Perimeter and interior are also often used to determine which sensors will be active when the alarm user is at the alarm site (home) and which will only be active when the user is away from the site (away).

5. **Home vs. Away**

The home vs. away feature is used to allow a user to turn on (arm) a system that includes interior sensors and still move around the house. When a user turns the "home" system on, only the perimeter sensors are active. When the user turns on the "*away*", all of the sensors are active such as a motion detector. This allows the user flexibility to have a portion of the system active while home yet still includes additional detection capability.

6. **Interior Follower**

Interior follower zones offer greater security by adjusting how the entry delay is applied. Sensors connected to these are delayed only after an entry/exit delay zone is activated. This enables the sensor on an interior follower zone to activate an alarm immediately in most situations and still accommodate someone crossing its path, such as a motion sensor covering the area between the user control and the door. In a system with normal entry-exit delay, the motion sensor would need to be delayed in all instances. In a system with the interior follower feature, the motion sensor will be delayed when the user exits or when the user or an intruder opens the door first. But if the user or an intruder crosses the path of the motion first the alarm will be instantly activated.

7. **Fire Circuits**

Fire circuits are on or active at all times even if the control is disarmed "off". Some codes prohibit using combination intrusion and fire controls in commercial applications.

Learning Outcome 9-A-12 Understand alarm conditions which are active even when an alarm system is disarmed

Examples of these alarms are panic, emergency, ambush, duress and holdup alarms. These alarms are active 24 hours a day, regardless of whether the alarm is armed, and can be silent or audible. Additional ongoing monitoring may include temperature controls, the failure of equipment, or the operation of equipment (generators, sump pumps, etc.) or medical emergencies.

Learning Outcome 9-A-13 Know the various circuit options

To customize how circuits or zones operate, the following options are used:

1. **Automatic Reset**: A feature that automatically silences the annunciator, returning the system to a non-alarm condition after a length of time.
2. **Auto-restore:** A feature to automatically reset alarm system circuitry and sensors to prepare for an additional alarm, if necessary, after a preset period of time.
3. **Automatic Zone Shunting**: A feature faulting zones when arming is automatically bypassed. Not to be used with 24 hour zones or fire zones.
4. **Chime Zone**: When disarmed, a chime will sound when a zone is violated. When armed, an alarm will sound.
5. **Cross zoning**- The practice of suppressing an alarm signal until two or more detectors in separate zones register alarm conditions.
6. **Day Zone**: A feature of an intrusion detection system that uninterruptedly monitors an area even when the system is disarmed and produces trouble when disarmed.
7. **Priority Zones**: A trouble or fault prevents the system from arming.
8. **Priority with Bypass**: A trouble prevents the system from arming, but bypassing can be done using a special code.
9. **Swinger Shutdown**: A method to prevent more than a set or programmable number of alarms from a particular zone.
10. **Twenty-four hour circuit**: A circuit that initiates an alarm regardless of the systems arming status.

Learning Outcome 9-A-14 Understand the purposes of visual annunciators

1. **Strobes:** Strobes are lights that flash when activated. They can be separate devices or mounted on or near the audible device. Strobe lights are more effective in areas where they don't compete with other lit objects.

2. **Other Types of Annunciators:** Annunciators are used to communicate information to the alarm user. Common types of information are whether a system is armed or which zones are active. Annunciators can use LED displays, alphanumeric displays and graphic displays.

Learning Outcome 9-A-15 Know the types of audible alarm devices

Audible alarm devices are noise making devices such as a siren, bells or horn used to indicate an alarm condition. Bells are devices that use an electrically vibrated clapper to repeatedly strike a gong. Buzzers continuously vibrate a membrane while the power is applied. Chimes are audible signals with a soft tone, ordinarily used in systems to advise selected personnel of a condition. Sirens are combinations of speakers and sound equipment which may produce noises, relay voice announcements, or a combination of both.

1. **Audible Time-outs** - Some local ordinances require that audible devices stop sounding after a 10, 15 or 30 minute period. Underwriters Labs (UL) has set the following minimums: for household intrusions - four minutes, commercial or household fire - until manually reset, commercial intrusions- 15 minutes if control automatically resets; 30 minutes if not. A bell or siren cut-off is a timing circuit which turns off the bell or siren device after a pre-set time.

2. **Voice Evacuation system** - With a voice evacuation system building occupants can be given instructions in the event of an emergency.

Learning Outcome 9-A-16 Understand the purpose of secondary power

Because an alarm system will not operate without power, a secondary power source is usually connected to the alarm system. Common sources of secondary power are batteries and generators. A battery housed with the control panel is normally connected to automatically takeover in the event of normal AC power failure. Generators are electricity producing devices powered by standard gasoline, natural gas or diesel. NFPA has set standards for how long a system should operate on secondary power.

Learning Outcome 9-A-17 Understand the purpose of audio systems

Control panels may incorporate an audio detection system designed to detect the sound or vibrations caused by attempted forceful entry into a protected structure. The system consists of microphones and a control unit containing an amplifier, accumulator, and power supply. The unit's sensitivity is adjustable so ambient noises or normal sounds do not initiate an alarm signal. 'When an alarm is initiated, a connection to a central station is normally established and operators may listen in to what is happening at the alarm site. The operator then determines what action is appropriate.

FIRE, SMOKE AND GAS SENSORS AND DETECTORS

Learning Goal: To understand usage of sensors and detectors for fire, smoke and gas detection.

Learning Outcome 10-A-1 Understand the purpose of a fire and smoke sensors and detector

An alarm system needs detection devices to report "off normal" conditions. The type of detector used depends on what the system detects.

1. Fire Alarm Sensors

Fire alarms use detectors that sense smoke, heat, and flame. While most fires go through "stages" or processes, not all fires do, and the proportionate amount of time for each stage may vary greatly.

2. Types of Detectors

Fire detection devices are often referred to as "*initiating devices*". Some are designed to sense the signs of fire automatically while others rely on people to see the signs of fire and manually activate a device.

Learning Outcome 10-A-2 Know two types of Heat Detectors

There are two types of heat detectors, fixed temperature which activates if the room or area exceeds the rating of the sensor, and rate-of-rise, which sense a 15 degree per minute increase in room/area temperature.

1. **Fixed Temperature Heat Detector -** Fixed temperature heat detectors activate when the temperature exceeds a present level. Detectors are designed to activate at different levels. The fusible link detector and quick metal heat detectors use heat collectors to collect the heat. These collectors must be replaced after they are activated.

2. **Rate Of Rise Operation -** A bimetallic diaphragm assembly bends when heated to meet a contact point that signals the alarm. Heat detectors are generally used in areas where property protection is the only concern or where smoke detectors would be inappropriate.

Learning Outcome 10-A-3 Know two types of Smoke Detectors

There generally two basic types of smoke detectors, photoelectric which senses the presents of smoke, and ionization which senses the presence of combustible gases.

1. **Photoelectric Smoke Detectors**. There are two basic types of photoelectric smoke detectors; Light scattering detectors use the reflective properties of smoke to detect smoke. Beam detectors rely upon smoke to block enough light to cause an alarm. The light scattering principle is used for the most common single housing detectors.

2. **Ionization Detector** - An ionization detector uses the change in how air conducts electricity when smoke is present to detect smoke. An alarm is indicated when the amount of smoke in the detector rises above a certain level.

Learning Outcome 10-A-4 Know other types of fire safety detectors

1. **Duct detectors** control the spread of smoke within a building by turning off the HVAC system, operating exhaust fans, closing doors or pressurizing smoke compartments in the event of a fire. This prevents smoke, fumes and fire by-products from circulating through the ductwork.

2. A **rate compensation detector** is a tube shaped device that responds when the temperature of the surrounding air reaches a predetermined level, regardless of the rate of temperature rise.

3. A **restorable semi-conductor line type heat detector** uses a semiconductor material and a stainless steel capillary tube. The capillary tube contains a coaxial center conductor separated from the tube wall by a temperature sensitive semi-conductor material. Under normal conditions small current (below the alarm threshold) flows. As the temperature rises, the resistance of the semiconductor thermistor decreases, it allows more current to flow and initiates the alarm.

4. **Non restorable fusible line type heat detectors** use a pair of steel wires in a normally open circuit. The conductors are held apart by heat sensitive insulation. When the temperature limit is reached the insulation melts, the two wires contact and an alarm is initiated. The fused section of the cable must be replaced following an alarm to restore the system.

5. **Cloud chamber smoke detectors** use sampling tubes to draw air from several areas. The air is passed through several chambers where humidity is added to allow sub-micron particles to become visible. Photoelectric detectors then react to any smoke particles and initiate an alarm

6. **Ultraviolet (UV) and Infrared (IR) flame detectors** react to radiant energy that is either visible to the human eye or outside the range of normal human vision.

7. **Pull Stations.** Manual pull stations are required by consumer safety code to be distributed throughout a commercial monitored area so they are unobstructed, readily accessible, and in the normal path of exit from the area. Examples are single or double action pull stations or glass break pull stations.

8. **Key Operated Station**. Applications are restricted. Key operated stations are permitted in certain occupancies where facility staff members may be in the immediate area and use by other occupants of the area is not desirable. Typical conditions include detention and correctional buildings and where mental health treatment is provided.

9. **Wet Sprinkler System**. A permanently piped water system under pressure, using heat-activated sprinklers. When a fire occurs, the sprinkler heads exposed to high heat open and discharge water individually to control or extinguish the fire. When activated, a sprinkler system may cause water damage. Wet systems should not be used in spaces subject to freezing.

10. **Dry Sprinkler System.** Heat operated sprinklers are attached to a piping system containing air under pressure. Air pressure in the pipes holds a valve closed keeping water back. When heat activates a sprinkler head, air pressure is released. This allows a valve to open and water flows through the pipes to the activated sprinkler head.

11. **Waterflow Alarms**. When a building sprinkler head is activated from heat, the sprinkler head allows water to flow. A flow device which detects movement of water is installed in the sprinkler system.

12. **Fire Pump.** Many fire systems include a sprinkler system that is dependent on the availability of an immediate supply of water. A fire pump is used to force water from the community water reservoir to the building's sprinkler system.

    The main purpose of a fire pump is to supply the sprinkler system with a sufficient amount of water. The pump is automatically triggered when a change in air or water

pressure is detected in the sprinkler system. Once the fire pump is activated, it sends an alarm signal identified by the words "*Pump Running*" to the Central Station indicating that the pump is sending water to the sprinkler system.

13. **Risers**
    A riser alarm is another specialty fire alarm detector which focuses on the detection of water availability to sprinkler systems. Similar to the fire pump system, a riser alarm may be used with either wet or dry sprinklers. However, unlike the fire pump that is attached to the customer's building, this type of alarm is actually part of the community water system.

14. **PIV Detector** (Post Indicator Valve)
    This type of alarm monitor produces a tamper signal that is used to detect when someone or something has tampered with the main water control valve which brings the water into the building from the community water source.

15. **Gas Detectors**:

    a. **Carbon Monoxide (CO)**
       Carbon monoxide is a colorless, odorless and highly poisonous gas that is produced when fuels containing carbon are burned. It is dangerous when it is inhaled as it prevents the oxygen carrying substance in blood cells from absorbing needed oxygen. This leaves the victim disoriented and unaware that they have been exposed.

    b. **Natural Gas**
       Natural gas includes a group of gases that are colorless and odorless compounds not only poisonous but combustible and extremely explosive. (Methane, Propane, Butane).

       The main role of the natural gas detector is to warn individuals of dangerous levels of natural gas in the air. Even though most homeowners know when natural gas is present, very few understand the volatile nature of gas or how their actions could make the difference between a life threatening scenario and the loss of life and property. Even low levels of natural gas can prove explosive and fatal. Exposure to low concentrations of natural gas can be both asphyxiating and explosive.

Types of Gas Detectors:

Biometric units – Also called gel cell or litmus, these detectors utilize a semi-permeable gel that changes color when exposed to CO and or natural gas. This gel absorbs CO or natural gas at the same rate as human hemoglobin, and its color is directly related to the amount of CO/natural gas absorbed. The detector has a light beam which shines through the gel and senses the change in color, activating the device.

Taguchi units – Also called tin oxide or figaro, these detectors utilize a specially doped semiconductor that changes its resistance when exposed to CO or natural gas. The detector senses this change and activates the unit.

16. **Supervisory Signals.** The position of a control valve may be monitored so a supervisory signal is sent whenever the control valve is turned to shut off the water to the sprinkler system. If this valve is turned off, no water flows through the sprinkler system. In some systems, water pressure from the municipal water supply may not be strong enough to push enough water to all parts of a building. In these cases a fire pump is usually required. When the fire pump runs, a supervisory signal is sent. If the pump runs and does not shut down within a few hours, action such as a visit to the site may be required. When water is scarce or unavailable, an onsite water tank may be required. Supervisory signals may be generated when the temperature of the water drops to a level low enough to freeze or if the water level or Pressure drops below a safe level. In a dry system a supervisory signal is generated if air pressure drops below a usable level.

17. **Trouble signals.** The power to the pump is monitored to make ensure the pump will operate if needed. Fire pump power is a trouble signal. Water tank level is a supervisory signal.

SECURITY AND SAFETY IN-DEPTH

Learning Goal: To identify the types and purposes of detectors and sensors

This section will acquaint you with a basic security concept called "security and safety in-depth" which identifies what sensors should be applied, and where they should be for the greatest deterrent while identifying the degree in which a threat penetrates the protected location. This is accomplished by defining lines of defense, or layers of protection. Multiple lines of defense are established in stages from the exterior to the interior and then to specifically protected asset points. Specific detectors or sensors are applied to the line of defense level being addressed. Additional sensors can be applied to additional lines of defense as needed. In the order of application the lines of defense are the perimeter, interior and points. We will also consider other devices that are used as an alert for various conditions or identify safety issues.

Learning Outcome 11-A-1 Know the types of sensors or detectors generally used to secure a perimeter

Perimeter Detection

The perimeter is the outer bounds of an area to be protected. It may be defined by fences or walls defining the property. This includes exterior walls, windows, doors, the roof and the flooring. Perimeter sensors are used to detect penetration of the perimeter.

1. **Magnetic Contacts -** Magnetic contacts are used to sense when a door or window is opened. Magnetic switches are composed of two parts; a magnet mounted on the moveable door or window and a magnetically operated switch called a "reed" which is mounted to frame of the door or window. The standard reed switch is designed to be either a normally open or closed circuit. For example, when the door or window is closed, the magnet is adjacent to the reed, and the switch is in its "normal" non-alarmed position. When the door or window is opened, the magnet moves; this releases the switch and breaks the contact which activates the alarm. Contacts can be surface mounted on a door or window or flush mounted so that they are concealed when the door or window is closed.

2. **Mechanical Switches** Mechanical switches are used to detect the opening of a protected door or window. These sensors are contact switches that resemble a push button; a mechanical switch with a spring-loaded plunger. When the door or window is closed, the plunger is depressed. When the door or window is opened the plunger protrudes and the alarm is triggered.

3. **Audio Discriminators**. Audio discriminators are audio sensing devices that are tuned to specific audio frequencies. They are tuned to the frequencies generated when a variety of building materials (Wood, Metal, Glass, Brick or Concrete, est.) are subject to assault or impact (glass breakage, splintering of wood, etc.). The most predominant are glass break detectors.

   When glass breaks it generates frequencies much higher than normal background noises. When these higher frequencies occur they are detected and the alarm is activated. Most sound discriminators can detect these various types of glass breaking up to 35 feet away when installed at a right angle to the windows.

4. **Seismic Sensor -** Devices that detect changes in seismic pressure as an intruder approaches. Most commonly they are tubes filled with a fluid buried as a single tube or a pairs the length of the perimeter. The tubes are connected to a sensing device registering an alarm when an approach changes the pressure in the tubes

5. **Projected beam sensor -** a narrow beam of energy projected over a defined distance emitting from a transmitter device to a receiving device. An object passing thru the beam interrupts, or blocks it momentarily, thereby generating an alarm. The energy transmitted falls into a light sources and RF emitters. Beams are normally installed at a height above the ground or floor surface to increase the likely hood the interruptions is the result of a human. The beam may be a single beam or beams stacked and separated by defined distances. Stacked beams are less subject to false alarms' a single beam break does not cause a trigger but multiple simultaneous breaks indicate a mass more likely to be that of a human being. Beams are also installed with reflective devices that create a web pattern over the path of access. Beam are used in conjunction with fence and exterior walls to detect attempts to go over these barriers

6. **Light Beams** – These beams can be within the entire light spectrum (visible light, ultraviolet light and infrared lights). Those that are not visible are less likely to be detected by an intruder.

7. **RF beams** – these are radio frequencies that are not visible to the human eye

Learning Outcome 11-A-2 **Know the types of sensors or detectors generally used to secure an interior**

Interior sensors allow further detection if the perimeter is penetrated or bypassed by an intruder. Although the perimeter is a well-defined line, the interior may be multiple rooms, halls and doorways. Alarms generated in the interior lines confirm that the intruder has either penetrated the perimeter or is inside their target area. Detection is now covering

space as well as necessary areas of passage to an intruder's goal. The sensors employed are space covering detectors and contacts for doors and windows.

1. **Passive Infrared (PIR)**.
   All animate and inanimate objects have inherent temperature that varies from the ambient room temperature. The heat of objects emits infrared energy at a level consistent with its temperature. The heat of a human body is considerably higher than that of most inanimate objects. Infrared energy is a spectrum of light not visible to the human eye. The color of the light spectrum emitted varies base on the heat of the object. Heat varies and the color of the infrared varies in relation to the heat emission. PIRs are passive because they do not emit anything into the protected area but read the levels within their field of view. It sees each object separately in the field of view. If an object within the field moves while the device is active, an alarm is triggered. PIRs are optical devices and their field of view can be modified by an optical lens (like a camera lens). By applying lenses the field of view can be modified to how low the view is in relation to the floor. This can overlook the areas a pet might pass and minimize the probability of a false alarm

2. **Active Infrared Motion Detector (IR)**
   Active infrared motion detectors use an IR sensor, as well as a source of radiation. The sensor is a transmitter of infrared and a separate receiver. The receiver is able to detect interruptions in the radiation it receives from the radiation source. The detector is able to detect the heat energy of an intruder as the intruder passes through its detection range.

3. **Continuous Wave Radar Motion Detector (CW)**
   Continuous Wave (CW) motion detectors use microwave signals to emit frequencies to bounce off of the surrounding area (which is why they are sometimes referred to as "microwave motion detectors"). The sensor detects when there are subtle changes in these frequencies which signals a disruption. When an intruder passes the field of a CW microwave sensor, he disrupts the frequency which sets off the sensor's alarm.

4. **Ultrasonic Motion Detector**
   An ultrasonic motion detector is able to use sound energy in order to detect movement in a specific region. This ultrasonic sound energy is emitted in waves. When the sensor detects movement, the sound waves are disrupted, triggering the sensor.

5. **Vibration Motion Detector**
   A motion detector detects simple vibration caused by the changes in mass and its movement within the protected area

6. **Video Motion Detection (VMD)**
   VMD sensors operate through almost any good quality CCTV camera providing both a detection of activity and observation of the events progress. The VMD sensor system monitors changes in the camera's field of view and if a change occurs through an intruder entering the scene an alarm condition is generated. More sophisticated systems also include an image tracking feature which can monitor a number of separate intruders simultaneously by drawing a different colored line around each of them and leaving a trail line of where they have been.

7. **Volumetric Detection**.
   Sensors are located and adjusted so that a human is detected moving at a rate of one step per second in a wide or broad detection area.

   a. Some audio discriminators include a "listen-in feature". The digital communicators stay on line after the alarm is transmitted to allow the operator to hear what is happening at the premises.
   b. Some are combined with vibration sensors. Detector monitors sound of forced entry and monitors for vibrations. An alarm is sent only when both occur.

8. **Infrasonic**.
   Infrasonic senses the change in air pressure when doors or windows are opened. Infrasonic commonly found in combination with audio sensors as a means to verify alarms. Motion of people or animals within the area should not affect the system.

9. **Pressure Mats**.
   These sensors are located under carpet or rugs in areas likely to be walked upon. These sensors must be left out of the system when people are routinely in the area.

10. **Combined technology sensors**.
    These sensors use two technologies to verify human motion in order to prevent false alarms in hostile environment.

Learning Outcome 11-A-3 Know the types of sensors or detectors generally used to secure a location point

1. **Trap Detection**. Detection areas of expected travel paths of an intruder

2. **Spot Detection**. Point detection on a particular object such as a safe, vault, storage areas, money rooms.

3. **Detection of "stay behinds"**- This detection is for an intruder who enters the facility during the business day and stows away in an area undetected. Upon closing the intruder comes out of hiding. The goal is to determine the areas likely to attract and conceal the intruder and detect at the earliest opportunity.

4. **Holdup Devices –** Manually activated
   a. **Button**- A mechanical switch used to initiate a holdup alarm signal usually constructed to minimize accidental activation.

   b. **Money clip**- A sensor device which activates a signaling device when money is removed from between the contacts.

   c. **Portable duress sensor**- A device which can be installed quickly and which does not require the installation of dedicated wiring for the transmission of an alarm signal.

   d. **Foot rail -** A duress alarm, often used at cashiers' windows, in which a foot is placed under the rail, lifting it, to initiate an alarm signal.

Learning Outcome 11-A-4 Understand how sensors can be disguised

Various types of sensors can be concealed or disguised. Alarm sensors that are obviously by their appearance detection devices are subject to being compromised by an intruder. For that reason some applications may use disguised sensors. Some of them may appears as the devices below

1. Duplex electrical outlets
2. Thermostats
3. Speaker grills
4. Smoke detectors
5. Light fixtures

Learning Outcome 11-A-5 Understand how alarms are processed

An operator receives alarm signals that alert them to the progress of the attempt to intrude. The following critical information must be reported to the responding authority.

1. The alarm must be reported to the responding authority.
2. Subsequent alarms must also be reported to the responding authority; these reports may raise the priority of response since additional sensors or detectors increase the probability that the report is not false and may be indicative of more than one intruder.
3. Repeated reports of alarms provide information about the intruder's path within the protected facility and may identify additional intruders.
4. Reporting of points of exit after intrusion may indicate the perpetrator(s) departure
5. Reporting detail makes you a valuable member of the response team.

Learning Outcome 11-A-6 Understand the roles non security systems play in the protection of life and property

Almost all of these sensors send signals when the problem occurs and when things return to normal. Often the sensitivity of these sensors is set so that signals are sent in time to notify someone before damage occurs; timely response is usually very important.

1. **Miscellaneous Sensors**. Since anything that can close or open a switch or produce an electrical change can be monitored, the possibilities for sensors are almost endless. These include:

    a. Water or moisture sensors which might indicate flooding,
    b. Temperature or humidity sensors that would indicate levels of humidity or high or low temperatures that might cause problems for equipment,
    c. Process monitoring sensors might indicate that machine has stopped running, or
    d. Power failure monitoring

2. **Medical Devices**
    Medical Emergency Alarm Devices are designed to produce an audible or visual signal indicating a need for medical assistance. Similar to the Personal Emergency Devices, each Medical Emergency Device may be manually triggered when there is a medical emergency requiring an ambulance or paramedic care or may include an automatic fall detection feature. Upon activating the device, an alarm signal is transmitted to the Central Station. There are three Medical Emergency Alarm Devices.

a. **Panel Activated -** medical emergency by pressing the Medical Alert on the panel.

b. **Wireless (Pendants/Key Fobs) -** This type of Medical Emergency Device is available as a keyfob or can be worn as a pendent. This device may include a global positioning system (GPS) which will allow medical response to locate the patient.

c. **Inactivity Alarms -** An Inactivity Alarm differs from all other Personal Emergency Alarm devices because it is manually triggered by the user. This device is not equipped with buttons, but uses a small wireless detector. This is accomplished in a variety of ways. It may be an audible device which sounds after a programmed period of time. When it sounds, the button must be pressed to silence it. Failure to respond generates an inactivity alarm. It may also be triggered by a motion sensor which fails to detect movement after a programed period of time.

CUSTOMER SERVICE

Learning Goal: **To recognize the importance of the customer and to properly work with customers**

Learning Outcome 12-A-1 **Understand why customer service is important**

Many customers stop doing business with a company because of the way they were treated on the first contact. A vast majority of customers never complain – they just stop doing business with the company. Customer service comes down to the golden rule of treating others as you want to be treated.

Learning Outcome 12-A-2 **Demonstrate effective communications as an alarm monitor.**

1. Customers cannot see you. Always smile and sit up straight, good posture keeps you alert and attentive. Your priority is to focus on what the customer is telling you, so minimize background noise, express common courtesy and refrain from eating or chewing gum while talking to customers. People want to hear a smile. Customers will be able to determine the mood you are in and the message you are trying to convey by your tone. Pace, volume, intensity, inflection and attitude all contribute to the tone of your voice. Be enthusiastic. Avoid negative tones.

2. Customer service equals customer response. Customers respond to people who respond to their needs. Your customer's opinions of your company will depend on the service you provide, the needs that are met, and the options provided them.

3. Customer feelings are important. Greetings should always be pleasant; get and use their name when whenever possible in the conversation. When saying good-bye, restate any action items to be followed up on and the time frames necessary. If they are to receive a call back let them know when they can expect it and thank them for their time.

4. Let the customer feel unique. Personalize the service to their needs

5. Record their information accurately and ensure timely follow-up

6. Listen to the customer. There is always the possibility that the customer on the other end of the line is facing a dangerous or highly emotional situation. Listening effectively could very possibly save a life. Since we have no visual clues from the customer, we only have our listening skills to assist us in understanding their emotions and needs. Repeat key points, and get them immediate help when possible.

7. Avoid placing a customer on "*hold*". The time will seem longer to the customer than to you. If you must place the customer on hold, be sure to ask them if they can hold and let them know why. For example: "*I need to check with the supervisor on this can you hold or would you prefer a call back?"* If they agree to hold be sure to check back in 30-60 seconds with updates on your progress reports.

Learning Outcome 12-A-3 Demonstrate methods of working with irate customers

When dealing with irate customers it is important to remember that this is not personal, you should know you are not responsible for the customer's problem or the pain associated with it but you are the one who answered the phone so you are the one that must handle the problem. As long as the customer has a problem you have a problem. Take responsibility to resolve the issue to the customer's satisfaction.

1. **Concede** instead of convince. Show through empathy that you understand the customer's situation. Apologize for the situation and remain committed to resolving the problem.

2. **Hear them out and don't interrupt**. Validate the customer's feelings by listening without interruption. When they are finished they will be better able to hear possible solutions.

3. **Use patience**. Avoid the urge to jump in with a solution before the customer has finished talking. Listening to their words as well as their emotions will help you answer their concerns more effectively. Remember this is not personal.

4. **Use tact**. Make the customer feel confident that you care about getting their problem resolved. When possible involve the customer in the solution; identify their expectations and focus on the facts not the emotions as you attempt to provide acceptable solutions.

5. **Empathize** with their concerns. Identify with the customers situation recognize their emotion with understanding and concern.

6. **Acknowledge their concerns**. Remember to acknowledge the situation and the emotion, and then focus on taking action and moving toward a solution.

7. **Remain calm**. Remember this is not personal. You are not responsible for the customer's problem or the pain associated with it.

8. **Do not argue with them**. In a friendly way vocalize your expectations and needs of the caller to help resolve the problem.

9. **Use positive statements** such as *"I agree," "I understand," "I know," "I see," "You have a right to feel that way," ""We can…"* (Emphasize what you can do instead of what you cannot do. Always attempt to provide the caller with acceptable alternatives. Customer complaints may intensify if no resolution is offered.)

10. **Take notes** (Jot down key points that will help you remember but avoid writing down every word that is said; avoid concentrating too much on what you are writing instead of what you are hearing; let the customer know you are documenting their concerns and review them to reinforce understanding.

Learning Outcome 12-A-4 Understand methods of working with a customer who is out of control

If the customer is out of control, or swearing:

1. Use short periods of silence to allow the customer to think and calm down. "Please hold while I get a supervisor for you." May be all they need to hear to assure them that their issue is being given the priority and importance that they feel is needed and the customer is often much calmer when the call is resumed.
2. Remember it is usually not you, and it is nothing personal.
3. If the customer is so out of control that you cannot identify the facts surrounding their issue, use phrases like:

    a. *"I feel uncomfortable when you swear at me, please help me understand your problem without swearing."*
    b. *"When you yell and swear I cannot concentrate on the solutions to your problem. Please help me solve this for you."*

c. *"I can no longer help you if you continue to berate me I will not be able to offer effective solutions."*
d. *"If you don't stop, I'm going to have to report your call as abusive."*

You may need to repeat the same sentence a few times to get through to an angry customer, be sure to use the exact same wording each time as this will be more effective than repeating the same statement in a different way.

FALSE ALARM PREVENTION

Learning Goal: To reduce false alarms and maintain a common goal with public safety disciplines of protecting lives and property

Learning Outcome 13-A-1 Understand the impact of false alarms

1. The cost of police response to alarms that are false is increasing.
2. There are increasing numbers of alarm systems being installed across the nation.
3. The alarm factor, which is the number of false alarm dispatches compared to the number of alarm systems, must be reduced through a combined effort of private sector and public safety.
4. False alarms lower the public image of the alarm industry, reduce referrals, reduce sales leads, and harm the alarm industry image.

Learning Outcome 13-A-2 Know the purpose and scope of the Alarm Industry Action Plan

The Alarm Industry Plan

The Alarm Industry 1994-95 False Alarm Coordinated Action Plan was endorsed by the Alarm Industry Research and Educational Foundation (AIREF), the Canadian Alarm and Security Association (CANASA), the Central Station Alarm Association (CSAA), the National Burglar and Fire Alarm Association (NBFAA), and the Security Industry Association (SIA). The purpose is to reduce false alarms.

1. **Steps for alarm dealers and monitoring companies**

   a. Attempt to verify all intrusion alarm signals by telephonic or other electronic means before requesting police dispatch, along with any other signals that can be prudently verified.
   b. Pro-actively call customers who have experienced alarm activation to investigate and prescribe corrective action as needed.
   c. Use only dual-action holdup devices and eliminate using "1+" duress keypad coding.
   d. Implement procedures to prevent or cancel exit/entry false alarms (such as extend delay times).
   e. Educate alarm system owners and users about their responsibilities relating to alarm system use and false alarms.

f. Provide training for all company personnel on false alarm causes and solutions.
g. Communicate with local authorities about their particular problems, and work with them toward local false alarm reduction plan.

2. **Considerations for the Alarm Monitor and Installer**
   a. Many sounds are similar to the sound of breaking glass, such as jingling keys, a telephone ringing, clinking ice cubes, dishes or glasses being washed, breaking dishes or glasses, dogs barking, leaking or squeaky air compressors and fans.
   b. Certain applications are not recommended for either acoustic or shock glass break sensors. These include any place where there is loud music, clanging pots and pans, weights used at gyms or spas, ceiling fans.
   c. A sensitivity adjustment is available on most sound discriminators. This setting will help calibrate the detector to the size of the room as well as to a variety of room conditions. If every room were empty, the same size and we could ensure that no sources of noise would exist in the room the factory setting would always be acceptable. Drapes, furniture, carpet, desks, and other room objects may absorb or react the sounds in the room. To overcome this, adjustments are made to tailor the sound discriminator to the audio environment of each room.

3. **Steps for police and community officials**

   a. Implement a locally predetermined procedure to suspend police response to chronic abusers of alarm systems, and implement procedures, which allow resumption of police response after corrective action has been taken.
   b. Implement procedures to accept verified cancellation of dispatch requests from alarm companies.
   c. Require user training and annual inspections of alarm systems.
   d. Support the alarm industry in its efforts to establish or strengthen statewide licensing of alarm companies and employees.
   e. Use a model, such as the NBFAA Model Alarm Ordinance, as a framework to develop steps to combat this problem in concert with local representatives of the alarm industry.

4. **Alarm Company Action Plan**

   a. Review the Alarm Industry Plan
   b. Adopt new policies and procedures for new and existing systems

5. **Alarm Company Action Plan - Ongoing**

   a. Organize all new systems and procedures to meet the new standards.
   b. Concentrate efforts on accounts causing the most problems. It may be a system upgrade or training of the subscriber is needed. Always put in all new wiring for a system upgrade. Never sell or let a false alarm prone account go to a competitor. This will perpetuate the false alarm problem.
   c. Promote User Training. When asked, most dealers list customer education as the most effective way to reduce false alarms, yet few dealers have customer training programs.

      i. Develop a user-training program
      ii. Place all new customers on a test or no response for the first two weeks. This allows the customer to become familiar with the system and learn enough about it to ask intelligent questions.
      iii. Review the system on service calls.
      iv. Start a periodic re-training for all customers
      v. Periodically include false alarm reduction reminders in billings.
      vi. Determine what equipment has excessive false alarms or service calls and resolve it with the manufacturer. Good equipment should meet UL or ULC standards. The Security Industry Association (SIA) and Central Station Alarm Association (CSAA) have prepared guidelines useful in selecting alarm equipment.
      vii. Examine company procedures. All control panels have programmable features that require all intrusion zones to be normal or shunted before the alarm can be armed. Increase the entry and exit delay time. Alarm companies who have reprogrammed all their accounts so all perimeter doors have entry/exit delays report a noticeable reduction in false alarms.
      viii. Eliminate silent intrusion alarms. The audible not only scares the intruder, it warns the customer who has made a mistake.

STATE OF OREGON CERTIFICATION REQUIREMENTS

Learning Goal: To understand the State of Oregon Certification Requirements

Learning Outcome 14-A-1 Understand how to access State of Oregon current certification information

Alarm monitor private security professionals are welcome to become certified before seeking employment. *Note: they may not provide security services until all the certification requirements below are met.*

Information about DPSST, the Private Security Program, the Oregon Revised Statute (ORS), and the Oregon Administrative Rule (OAR), that provide regulatory authority and direction for the Alarm Monitor Private Security Professional program as well as all statutory requirements and processes for certification are outlined in: ORS 181.870-181-991 and ORS Chapter 259, Division 60. Links to the aforementioned information and documents can be obtained on the DPSST website via the following link:
http://www.oregon.gov/DPSST/PS/pages/index.aspx

Private security professionals with questions are advised to first check the DPSST website. If there are still questions, contact the Private Security Program staff by phone: 503-378-8531 or by e-mail: security.investigators@state.or.us.

Learning Outcome 14-A-2 Understand the minimum standards for becoming an Oregon private security professional

Minimum Standards

Individuals providing alarm monitor private security services are required to be certified by DPSST. To be certified, an individual must:

- Be at least 18 years of age
- Must have earned one of the following:
  - A high school diploma;
  - A General Education Development (GED) certificate; or
  - Hold a two-year or four-year, post-secondary degree issued by an accredited degree-granting college or university recognized by the Oregon Office of Degree Authorization under the provision of ORS 348.594(2) ;

- Be of good moral fitness as determined by a criminal background check, department investigation or other reliable sources
- Adhere to the core values that are an integral part of the private security profession:
    - Honesty;
    - Character;
    - Fair Treatment of Others;
    - Public Trust; and
    - Respect

  Note: Private security professionals are required to prescribe to the core values by signing the Private Security Professional's Code of Ethics (PS-27) prior to certification.
- Complete the alarm monitor basic training which consists of successful completion of basic classroom instruction, a written examination and an alarm monitor assessment.
  Note: If a test score is below 85 percent correct or an applicant fails to successfully complete any portion of the required training, the instructor must remediate or fail the applicant by requiring the applicant successfully repeat the deficient/missed section of the curriculum and retake the exam.

  Note: There is no waiting period, nor is there a limit on the number of times training and testing may be retaken.

  Note: All training and written exams must be completed by the applicant in English without assistance. [OAR 259-060-0020 & 259-060-0120 & 259-060-0135]

Learning Outcome 14-A-3 **Understand what steps a private security professional must take to receive the initial certification**

Initial Certification

Becoming a certified alarm monitor private security professional requires successful completion of:

1. Minimum of 12 hours of Alarm Monitor Private Security Professional training:

- The Instructor will enclose a copy of the PS-6 (training affidavit)
  Note: The PS-6 (training affidavit) form is only valid if submitted to DPSST within 180 days of the training completion date.

2. Submit required fingerprints.

- Fingerprints must be submitted to DPSST. There are three (3) options available for use:
    - Traditional Ink Fingerprinting;
    - LiveScan Fingerprinting; and
    - Electronic Fingerprinting via Fieldprint, Inc.

For additional details regarding the fingerprinting options refer to the following link: http://www.oregon.gov/dpsst/PS/Pages/fingerprintinginfo.aspx

3. Complete and submit the PS-1 (Application for certification or licensure form).
   Note: To avoid any delays in processing; the PS-1 application must be fully completed, signed, and submitted with all other required application materials and fees to DPSST. For the current fee schedule, refer to the informational pages attached to the PS-1 form or the DPSST website.

   Note: First-time applicants are required to enclose a fee for processing of fingerprints and cash or personal checks will not be accepted. Acceptable payment types are: cashier's check, business check, money order or credit card.

4. What is required for submission of a complete Initial Certification application to DPSST:

- PS-1 (application for certification or licensure)
- PS-6 (training affidavit)
- PS-20 (temporary work permit, if currently employed) - Which can only be issued by a Supervisory or Executive Manager.
- PS-27 (Code of Ethics)
- Fees
- Fingerprints - options & information:
- http://www.oregon.gov/dpsst/PS/Pages/fingerprintinginfo.aspx
  Note: If using Fieldprint, Inc. – You must include a copy of your "Confirmation Page" with your PS-1 upon submission to DPSST.

The documents must be mailed to DPSST prior to performing the duties of an Alarm Monitor Private Security Professional. Security Professional's must carry their copy of the PS-20 (temporary work permit) with them at all times when performing the duties of a Security Professional, until they receive their permanent certification card.

Learning Outcome 14-A-4 Understand how to renew a private security professional certification

Renewal Certification

Alarm Monitor Private Security Professionals must renew their certification every two years. The renewal process must be completed prior to the expiration date of the certification card. To mitigate last-minute issues, renewal may be initiated up to 180 days prior to expiration.

What is required for submission of a completed Renewal application to DPSST:

- PS-21 (application for renewal of certification)

- PS-6 (training affidavit) - Verifying completion of an Alarm Monitor Private Security Professional renewal course, within 180 days of making application for renewal.
- PS-20 (Temporary Work Permit) – If employed and submitting renewal application materials less than 30 days prior to expiration.
- PS-27 (Code of Ethics)
- All applicable fees

  Note: To avoid any delays in processing, the above must be completed, signed, and submitted with all other application materials and fees to DPSST within 180 days of the expiration date on the certification card.

Learning Outcome 14-A-5 Understand the impact of a "Deficiency" on the ability to perform the duties of a private security professional

Deficiencies

A "Notice of Deficiency" is an official notice sent to the Security Professional notifying them of the missing or incomplete application information. On issuance of the Notice of Deficiency, the applicant has 21 days to complete or submit the incomplete or missing portions of the required application materials.

If an applicant doesn't respond, with the appropriate information, within the Notice of Deficiency timeline (21 days) or if DPSST is unable to complete the certification/licensure renewal process due to non-compliance, upon the discovery of disqualifying criminal convictions or any violation of the temporary work permit provisions the application *may* be Administrative Terminated and all fees paid will be forfeited.

Learning Outcome 14-A-6 Understand the requirements to produce proof of certification

Proof of Certification

According to OAR 259-060-0030, a certification holder must present their temporary work permit to any DPSST staff member, Law Enforcement Officer or Oregon Liquor Control Commission agent upon demand or any other person upon reasonable request.

Learning Outcome 14-A-7 **Understand the notification requirement for a change of address**

Change of Address

An applicant or Private Security Professional must notify their employer and DPSST within 14 calendar days of any change of address by using the PS-23 (Private Security Professional - Change of Information) form.

I.R.I.S.

Information and Records for Investigators and Security (I.R.I.S.) allows Private Security Professionals, the public and employers to access information regarding the certification, licensing, employment and training status of Security Professionals. IRIS can be accessed via the following link: http://dpsstnet.state.or.us/IRIS_PublicInquiry/privatesecurity/smsgoperson.aspx

Learning Outcome 14-A-8 **Understand the notification requirements if charged with a crime**

Notification period if charged with a crime

The community expects Security Professionals to act in a professional manner and to provide a consistently high standard of attitude, conduct, and demeanor both on and off the job. Therefore, if a Security Professional is charged with a crime, according to the ORS 181.885, the effect of being charged with a crime may result in the termination or revocation of their Private Security license or certification.

1. If a Security Professional is charged with a crime, the Security Professional shall notify the Security Professional's employer, or, if the Security Professional is not employed, the Department of Public Safety Standards and Training, of that fact no later than 48 hours after the charge is filed.
2. If an Executive Manager knows that an employee has been charged with a crime, the Executive Manager shall notify the department of that fact no later than 48 hours after the Executive Manager acquired the knowledge.
3. The Department may suspend the certificate or license of a private security provider charged with a crime pending disposition of the charge.
4. If an applicant for certification or licensure as a private security provider is charged with a crime, the applicant shall notify DPSST of that fact no later than 48 hours after the charge is filed.

Learning Outcome 14-A-9 **Know the method of receiving relevant private security updates**

Private Security ListServ

To receive regular updates on relevant training opportunities, subscribe to the Private Security ListServ. The ListServ is an email distribution and notification system that allows DPSST to send information to constituents in a timely manner. We highly recommend that you join the ListServ; it is the fastest and most accurate method of insuring you have the most up to date information from DPSST. Use this link to join the ListServ:
http://listsmart.osl.state.or.us/mailman/listinfo/private_security_bulletin

REFRESHER COURSE

ETHICS AND PROFESSIONALISM

Learning Goal: **To develop an understanding of the necessity for standards of ethical conduct, and the relationship between private security, law enforcement and the community.**

To review this section in its entirety, refer to page 8

Learning Outcome 1-A-1 **Understand how the duties of a private security professional and law enforcement officer differ.**

The primary function of a private security professional is to observe, report and coordinate assistance.

Learning Outcome 1-A-2 **Understand how a private security professional can change public perception of the security industry.**

Public perception can be improved by the conduct of the security professional on- site with direct interactions with the public. Security professionals must demonstrate exemplary conduct, attitude, and demeanor both on and off the job.

Learning Outcome 1-A-3 **Understand the importance of developing relationships in the community.**

As the private security industry, the police and the community become partners, community policing places a greater emphasis on crime prevention. Establishing and maintaining mutual trust is the central goal of the community partnership. Trust gives private security professionals greater access to valuable information that can lead to preventing crimes.

Learning Outcome 1-A-4 **Understand the importance of following the client or employer's standard operating policies and procedures**

When acting on behalf of the client, the private security professional must ensure they are operating within established parameters, as there are potentially serious civil and legal ramifications if they are found to be operating outside of these policies and procedures.

Learning Outcome 1-A-5 **Know the three characteristic goals common to all private security professionals.**

1. Citizens have an expected standard of behavior for persons who protect them and their property; training and criminal background checks are the basis for the standard.
2. The primary goal of a private security professional is to provide a service which includes the common factors of the of protection of persons and property.
3. To improve the perception by the public, we must maintain exemplary and ethical business practices.

Learning Outcome 1-A-6 **Understand how on and off the job conduct can affect the public's perception of the security industry.**

Because the community expects us to act in a professional manner, their perception is formed by the actions of one officer, and altered by the actions of another. We must provide a consistently high standard for conduct, demeanor and attitude, on and off the job.

Learning Outcome 1-A-7 **Understand what unethical conduct includes.**

While there are numerous types of unethical conduct, some are more destructive to public trust than others. These include: Untruthfulness, Theft, Substance Abuse, Criminal conduct, Brutality, Prejudice, Gratuities, and Bribery.

Learning Outcome 1-A-8 **Understand the importance of core values as it relates to the Private Security Code of Ethics.**

To maintain high standards in the private security industry, we have established a system of principles, or core values: the Private Security Professional's Code of Ethics. The core values include Honesty, Good Character, Fair Treatment of Others, Public Trust and Respect for the Laws of this State and Nation.

CULTURAL DIVERSITY

Learning Goal: **To develop an increased deportment and awareness of cultural and interpersonal issues which dictate the predominant values, attitudes, beliefs and outlook among multi-cultural environments.**

To review this section in its entirety, refer to page 14

Learning Outcome 1-B-1 **Understand the advantages of learning about cultural diversity.**

All private security professionals must value all people without regard to race, color, sex, disability, national origin, age, religion, marital status, veteran status, sexual orientation, gender identity, gender expression or occupation. Embracing diversity in the workplace significantly enhances customer and colleague satisfaction.

Learning Outcome 1-B-2 **Understand why all persons have biases.**

We begin to learn biases from our families and those closest to us at an early age. We also develop biases from our experiences in life. As we grow and mature into adulthood we bring these biases along with us. All cultural biases develop out of fear and ignorance.

Learning Outcome 1-B-3 **Understand how we can become aware of and control biases on the job.**

Even when we identify our personal biases they will not disappear and they tend to dictate our actions. It is important to realize that we have biases we may or may not be aware of.

Learning Outcome 1-B-4 **Understand the need to comply with company policy and federal guidelines.**

The security professional must be aware of all company policies and procedures, as well as any applicable federal regulations regarding cultural diversity. The officer must follow, and enforce policies on racism, verbal harassment and menacing, among others.

Learning Outcome 1-B-5 **Understand the need to understand Stereotyping vs. Core Values.**

People tend to think of others in stereotypes. Stereotypes are an oversimplification of a particular group or person and are usually negative beliefs and opinions.

Learning Outcome 1-B-6 **Understand the need to know ADA requirements.**

ADA General Rule: The ADA prohibits discrimination against a qualified individual with a disability who can perform the essentials of the job.

Learning Outcome 1-B-7 **Understand the need to have a zero tolerance of sexual harassment.**

The Equal Employment Opportunity Commission defines sexual harassment as unwelcome sexual advances, requests for sexual favors, and other verbal and physical conduct of a sexual nature when:

1. Submission to such conduct is made either explicitly or implicitly as a term or condition of employment;
2. Submission to or rejection of such conduct by an individual is used as a basis of employment decisions affecting such an individual; or
3. Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Learning Outcome 1-B-8 **Understand the need to have zero tolerance of all discriminatory behavior.**

Under ORS 659A.403 all persons are entitled to full and equal accommodations of any place of public accommodation with discrimination or restriction based on race, color, religion, sex, sexual orientation, national origin, marital status or age.[3]

Learning Outcome 1-B-9 **Understand the rewards of cultural diversity**

Recognizing diversity and thinking in core values enhances customer satisfaction and makes good business sense.

[3] This does include prevailing laws governing places of public accommodations where alcoholic beverages are served.

ALARM INDUSTRY OVERVIEW

Learning Goal: To provide an overview of the electronic alarm industry

To review this section in its entirety, refer to page 18

Learning Outcome 2-A-1 Know the types of alarm systems available

These include: Intrusion, Fire , Hold-up, Panic or Personal Emergency Response Systems and Process Supervision and Environmental Monitoring

Learning Outcome 2-A-2 Know the services within the Electronic Alarm "Team"

While there may not be a "typical" company, most electronic security companies sell, install, service, and monitor the systems and services they provide. These include sales, installation, maintenance, customer service, administration and alarm monitoring.

Learning Outcome 2-A-3 Understand the importance of the Central Station and the Monitor

The central or monitoring station is–the primary point of contact for most alarm system owners after the system is installed. The Central Station operators process signals from the customers system and alert appropriate responding agencies (police, fire, medical, service, etc. The operator is a vital link in the company's success in protecting the lives and property of customers.

ALARM SYSTEM OVERVIEW

Learning Goal: To identify what an alarm system consists of and it's purposes

To review this section in its entirety, refer to page 21

Learning Outcome 3-A-1 Understand what an alarm system is designed to do

An alarm system is an assembly of equipment and devices designed and arranged provide quick detection of a change of status, provide notification of occupants, verify the scope of events and report the event change to the central station.

Learning Outcome 3-A-2 Know the difference between Detection vs. Protection.

Detection senses events or unauthorized status changes and reports them to a monitoring center, it does not prevent them. Protection implies that the undesired events will be prevented.

Learning Outcome 3-A-3 Know the difference between Local vs. Monitored systems.

A local alarm system is a sounding device that makes noise to alert the occupants or frighten away the intruder. Monitored systems send electronic signals to a central station for analysis and relay to the proper responding agency.

Learning Outcome 3-A-4 Know the basic parts of an alarm system

The basic parts of an alarm system include User Control Interface, detection, control panel, annunciation, transmission and power supply and back up batteries.

Learning Outcome 3-A-5 Understand the purpose of "Zones"

A common method of system design is to divide the system into separate areas or "Zones" to define particular areas or functions for ease of installation and service. Zone information is particularly critical when attempting to dispatch authorities to an alarm situation.

Learning Outcome 3-A-6 Know the types and purpose of alarm devices

1. **Perimeter Sensors** – The perimeter is the outer boundary of a system separating the area of coverage and the area outside of coverage. For a building system, it is the walls with doors and windows, floors and ceilings. For an outdoor system, it is a fence or the outer edge of the sensor pattern.

2. **Interior Sensors** – Interior detectors usually detect motion or infrared body heat in the interior of the protected area.

3. **Other Sensors** - Other sensors include environmental sensors, industrial process sensors, equipment performance sensors and temperature sensors.

4. **Fire Alarm Sensors** – Fire alarm sensors include smoke and heat detectors, rate of rise detectors, duct detectors, and water flow valve detectors to name a few.

5. **Manual Initiating Devices –** Manual pull stations for fire alarms, panic or hold-up buttons, and medical emergency pendants are types of manual initiating devices.

Learning Outcome 3-A-7 Know the difference between Armed, Disarmed and In-Alarm

Alarm systems as a whole can be turned on or off or "armed" and "disarmed" by the user. Parts of the alarm system may be controlled separately to be armed or disarmed and other parts may be "armed at all times" and not controlled by the user.

1. **Intrusion system** – This system is for detection of unauthorized entry into the location that the alarm is installed.

2. **Combination System**. –This system includes intrusion and fire alarm systems combined and controlled in a common control panel.

Learning Outcome 3-A-8 Understand Monitoring Options.

1. Full Service Alarm Company with Central Station
2. Proprietary Alarm Company and Central Station
3. Independent or Third Party Central Station

CENTRAL STATION OVERVIEW

Learning Goal: To provide an understanding of the central station functions
To review this section in its entirety, refer to page 25

Learning Outcome 4-A-1 Understand the general functions of a central station

A central station is where trained monitoring personnel process signals sent from alarm panels through electronic receivers and automation systems. Operators acknowledge signals and follow instructions to notify appropriate responders.

Learning Outcome 4-A-2 Know general security features of a central station.

The security features of a central station include a secured facility, its design and construction and its communications and staff identification.

Learning Outcome 4-A-3 Understand options to protect critical functions of central stations

Central stations provide several types of redundancies to ensure that they can perform critical functions. These include electrical power service, back-up generators, UPS and surge protectors and central station batteries.

Learning Outcome 4-A-4 Understand the purpose and scope of signals.

Alarm systems send a variety of electronic signals indicating the status of the protected facility and equipment to central stations. These signals describe different types of information including alarm conditions, supervisory conditions, trouble conditions and tamper conditions. Alarm signals indicate an emergency condition. Supervisory signals indicate a system may not work properly. Trouble signals indicate a malfunction.

Learning Outcome 4-A-5 Know general types of central station recording systems

Automated or computerized systems maintain and store all subscriber information, alarm history and service records. Phone recording systems record conversations to confirm accurate information and prompt dispatch occurs.

CENTRAL STATION PROCEDURES

Learning Goal: **To identify safe, accurate, and efficient methods to respond to alarms**

The primary responsibility of the Central Station to its customers is to pass along all signals to the proper authorities and/or customer representatives.

To review this section in its entirety, refer to page 29

Learning Outcome 5-A-1 Know the basic steps to signal processing

In general the basic steps to signal processing include read and respond to interpret the signal, notify the customer, dispatch authorities and record/document your actions.

Learning Outcome 5-A-2 Understand the central station functions

The central station functions include:

1. Reading and interpreting signals
2. Identify the customer
3. Determine the type of signal.
4. Notify Authorities.
5. Customer notification.
6. Document and keep records.
7. False alarm prevention.
8. Customer Satisfaction.

Learning Outcome 5-A-3 Demonstrate application of the type of "Time" central stations use

Central stations use 24 hour or military time. This system starts at midnight (2400 hr.) and counts up as usual until noon (1200 hr.). Then, 1 PM is 1300 hours, 2 PM is 1400 hr., etc. until 11 PM, which is 2300.

Learning Outcome 5-A-4 Demonstrate application of the time zones around the world

1. **Standard time and time zones.** The local mean solar time at any location depends on where that place is on the globe. Time advances by four (4) minutes for each degree longitude to the east. The world is divided into 24 time zones.

2. **Daylight savings time.** An adjustment of regional standard time; clocks are advanced one hour in the spring and set back one hour in the fall.

3. **Recording signals with proper time.** With today's technology it is possible to monitor a signal from another time zone. Some automation systems will compensate for this and show the time for the alarm site.

Learning Outcome 5-A-5 Know sources which have created industry standards

National regulations establish some industry standards. Locally, the authorities having jurisdiction (AHJ) is the person or agency that decides which standards will be applied to a particular job. Several groups have developed standards that form the foundation of how most companies deal with the complexities of alarm equipment installation, functioning and monitoring.

Learning Outcome 5-A-6 Know the purpose of company standards

Most companies have developed specific procedures for handling central station documentation and alarm processing. These procedures are usually based upon the concepts in this training.

Learning Outcome 5-A-7 Know the components of data entry

Once an alarm system in sold, paperwork should be completed and forwarded to the central station. The account information is recorded in the central station computer and the alarm is tested. After the installation is complete, a demonstration of the system and a test is made. Accurate account data is important to describe the locations of devices.

Learning Outcome 5-A-8 Demonstrate understanding of the basic signal processing procedures

In a specific situation, the alarm monitor should follow the procedures as indicated on the actual alarm screen or documentation. The following is a general guide.

1. Most automated or computerized monitoring systems will allow a set of selected signals that do not require monitor action to be "auto-logged" into the account history. Auto logging allows the central station to generate a chronology printout of all signal activity for a specific period of time.

2. **Alarm Priority**. Many computer automation systems will prioritize the signals automatically and route them to the operators automatically. Priority is assigned first according to the degree to threat to life and then property involved.

3. **Alarm Verification Procedures.** Many central stations will automatically attempt to verify. Verification includes:

   a. C**alling the premises** and allowing the phone to ring an appropriate number of times. If there is no response, the dispatch is usually made.

   b. **If an invalid pass code, word, or number is give**, the dispatch is usually made and the police advised that an unauthorized person is at the site; this indicate the presence of an unauthorized person, an error, or a duress situation.

   c. **If verification of a false or accidental alarm** is received after a dispatch, the authorities should be re-contacted and advised.

   d. **When verifying a passcode** and no passcode is given or the wrong code is given, do not give the customer a second chance. Thank the person, hang-up the phone and dispatch the police explaining the situation.

   e. **Customers desiring to convey duress message** to the operator should be instructed to give a totally incorrect number, preferably with extra digits and/or alphabetic characters.

   h. **Alarm Notification Procedures.** In addition to police and fire departments, the central station may be asked to notify several other parties after an alarm.

   i. **Steps to be taken prior to dispatching an Alarm Signal.** Some companies view previous subscriber activity to determine a course of action.

4. **Alarm Notification**. As a general guideline, the following information should be available to refer to authorities:

a. Identify yourself and company.
b. State the reason for the call.
c. Give address of alarm activation including customer name.
d. Give directions to the premises
e. Give permit number.
f. Give location of violated sensor,
g. Advise if alarm is audible or silent.
h. Advise if key holders are reporting.
i. Give callback numbers
j. Ask for the dispatcher's name or number.

Learning Outcome 5-A-9 Demonstrate understanding of general trouble signal processing

The following are the recommended steps:

1. **Equipment/sprinkler supervision** - Call the premises. If no answer, notify emergency list and/or alarm dealer.

2. **Radio Communication/Radio Trouble/Telco Court System Fail/Cut Wires dispatch procedures**:

a. **Communications failure - 1-way**
   iii. Call premises
   iv. If no answer, notify emergency list or alarm company
b. **Communication failure - 2-way**
   v. Call premises
   vi. Dispatch police or security if a response account, or
   vii. Notify emergency list and/or dealer
c. **Telco Failure, system fail, cut wires**
   vi. View activity to see if signal has restored. If so, advise senior operator
   vii. If signal has not restored, follow dispatch procedures
   viii. Call premise
   ix. Dispatch police or security professional if response account, or
   x. Notify emergency list and/or dealer.
d. **Restore/No Restore/L-T-T dispatch procedures**
   iii. Restore/no restore signal
   View previous activity to determine course of action.

e. **L-T-T- (Late to test)**
   ii. Call premises and advise
   ii. During normal business hours, notify alarm dealer or call list

f. **24-Hour test**
   If no "test signal" is received when expected, call alarm company or customer.

g. **Low Battery**
   iii. Call the alarm site during normal business hours
   iv. Contact the alarm company or customer

h. **A/C Power Failure**
   v. Call the alarm site
   vi. If no answer at the premises, notify emergency list
   vii. If security professional response, dispatch security professional
   viii. If no answer at premises or list, notify alarm dealer

i. Environmental Supervision - Low Temperature, High Temperature, Flood/Water Detector AC Power/Phase Monitor
   i. Call premises
   ii. Notify emergency list
   iii. If no answer at premises or list, continue to try until someone is notified
   iv. Any type of problem inform shift supervisor and/or manager
   v. If no answer on emergency list and if a response account, dispatch security professional

Learning Outcome 5-A-10 Know opening and closing processes

1. **Basic Opening and Closing Service** - This service is provided to customers whose systems are capable of sending distinct open and close signals as the panel is disarmed or armed.

2. **Supervised Openings and Closings** - The central station will monitor the times to assure the account is opened and closed according to the designated schedule.

Learning Outcome 5-A-11 Understand customer interaction processes

1. **Use of Passcard, Codes, and Passwords.** Most companies utilize a password, pass code, ID number or secret code to identify who is authorized to cancel alarms, conduct tests, be present on the customer's premises, and arm or disarm the system.

2. **Cancellation.** Follow your company's procedure for handling cancellations.

3. **Customer Requests for Service.** Depending on your company policy, you may advise the customer to call the alarm company directly. .

4. **Complaint and Error Procedures.** Most companies have a written procedure for use when questions or complaints arise.

COMPUTERS

Learning Goal: To identify the purpose and scope of computers in the central station

To review this section in its entirety, refer to page 40

Learning Outcome 6-A-1-Understand the purpose of computers in the central station

Computer servers are typically more robust and powerful than simple desktop computers. They provide the necessary hardware platform for the processing of alarm events and the storage of data.

Learning Outcome 6-A-2 Understand the purpose of a computer network in the central station

The computer network is a series of cable connections wiring that connect all of the workstation computers, computer servers, and often alarm receiving equipment, together into a data network. This enables the computers, servers and alarm receivers to communicate with each other. The network also provides for communication with the Internet and for alarms system to communicate directly with the automation system computers using the Internet. The central station network will also utilize data protection devices such as firewalls, routers and specialized software designed to prevent intrusion into the network from outside the central station.

Learning Outcome 6-A-3 Know the difference between hardware vs. software

For purposes of this section, the hardware in the central station would include the computers and servers along with related peripherals such as a keyboard, mouse, monitor and printers. The software typically refers to the operation system, network operation system, the alarm monitoring automation system and other programs that are written and designed to function together over the computer network.

SIGNALS

Learning Goal: Identify the types of signals received in central stations and their purpose

To review this section in its entirety, refer to page 41

Learning Outcome 7-A-1 Know the types of signals received in central stations

1. Fire
2. Hold-up
3. Duress
4. Panic
5. Intrusion
6. Medical emergency
7. Process or condition
8. Environmental condition

Learning Outcome 7-A-2 Demonstrate understanding of signals common to all categories

1. **Trouble Signals -** A signal indicating trouble of any nature, such as a circuit break or ground, occurring in the devices or wiring associated with an alarm system.

2. **Zone Trouble**- Signals and similar maintenance codes are often reported to the alarm company personnel rather than the customer.

3. **Test Signals -** Some alarm systems can be set up to periodically send a test; others allow the alarm user to press a button or code to send a test signal.

4. **No Test Received -** A signal generated by a computer system indicating that a test report has not been received at the appropriate time.

5. **Communications Failure -** If a communications device fails to report in, at, or within its scheduled time

6. **AC Fail -** This signal notifies the alarm user and the alarm company a potential problem may exist if the alarm control equipment is without power for a sustained period.

7. **Low Battery -** Many systems are capable of sending automatic "*low battery*" signals when the battery powering the system reaches a certain voltage level.

8. **Restore Signal -** A signal indicating that a system has returned to its normal condition.

Learning Outcome 7-A-3 Demonstrate understanding of types of signals and their purpose

Signals

1. **Fire -** Manual or automatic fire systems and sprinkler supervisory systems use a combination of devices to sense a fire emergency at the earliest point.

2. **"Initiating devices"**- such as sprinkler water-flow switches, pull stations, or smoke, heat or flame detectors are designed to indicate when a fire occurs.

3. **Supervisory Signal -** Indicates that a device is out of its normal condition.

4. **Hold-up or Panic -** These systems allow an alarm user to report an emergency.
   a. **Hold-up -** Intended to signal a hold-up; signals can be manually activated.
   b. **Emergency- Panic -** A device that may be manually activated.
   c. **Duress- Ambush -** A covert device producing a silent alarm.

5. **Medical Alert Signal -** A type of system allowing notification that medical assistance is needed, usually by pushing a button.

6. **Intrusion –** Detects unauthorized intrusion into a building or area of a building.

7. **Abort or Cancel Signal -** An abort or cancel signal means a request by an authorized alarm user to the alarm site to cancel a response by the police.

8. **Forced Arming Shunted Zone -** Bypass signals indicate the customer has bypassed a portion of the system (a zone) on closing.

9. **Exit Alarm -** An exit alarm can be generated when an alarm is activated within a short time from exiting a premise.

10. **Opening & Closing Signals -** Opening signals are generated when the alarm system is turned off. Closing signals are generated when a valid user turns on the system.

11. **Process Supervision and Condition Monitoring** - Monitors specific environmental or equipment conditions,

12. **Carbon Monoxide Gas Alarms.** - Designed to indicate that an unacceptable level of carbon monoxide gas is present.

ALARM COMMUNICATIONS

Learning Goal: **To understand the communication of alarms for effective alarm monitoring.**

To review this section in its entirety, refer to page 46

Learning Outcome 8-A-1 Know the sources for monitoring

1. **Central Stations**: Refers to all types of privately operated monitoring locations.
2. **Monitoring Stations**: Facilities that may or may not meet the standards.
3. **Proprietary Stations**: The same company they provide monitoring for owns proprietary monitoring facilities.
4. **Public Agencies**: Police departments and fire departments who monitor alarm systems.

Learning Outcome 8-A-2 Know the basic communication standards

1. **Passive/ Non Supervised Communications**: regardless of the communication mode or path used, the communication path is initiated only when the communication device needs to communicate a signal.

2. **Active/ Supervised Communication**: regardless of the communication mode or path use, the path is initiated upon installation of the communication device and remains open.

Learning Outcome 8-A-3 Understand how phone lines work

1. Public Switched Telephone Network (PSTN): A local phone company provides line power, dial tone and ringing tone to a local telephone line for a call to pass.

2. Central Office Feeder Cables: Feeder cables run from the local central office to the cross connect terminal cabinets in the phone company's outside infrastructure.

3. Cross-connect cables are mounted on poles, on the ground on cement pads, or in underground chambers called Controlled Environmental Vaults (CEVs).

4. Distribution Cables: At the cross connect locations, Feeder cables are divided into smaller bundles known as distribution cables. Residential and commercial phone customers are connected to these distribution cables.

5. Cross connect cabinet: Each pair of wires in the feeder cable is attached to terminals mounted on a plastic base called a terminal block.

6. Network Interface Device: At the subscribers premise a drop cable runs from the distribution cable to a network interface device (NID). The NID contains a station

protector to guard the subscriber's phone equipment from damage from lightning and high power lines.

7. Older phone network: Older Telco infrastructures use Analogue Technology. Currently this is the predominant communication technology utilized by the Alarm Industry

Learning Outcome 8-A-4 Understand how phone lines are used for Alarm Communication

Digital Communicators use regular dial tone telephone lines to make a phone call and send its information to the central station. There are two types of digital communicators; standalone which usually has to be connected to a control panel and integrated which is combined with the control in a single unit.

Learning Outcome 8-A-5 Understand potential problems with phone communicators.

Digital communicators use the customer's regular phone line and there are concerns:

1. If a customer is using the phone at the same time an alarm condition need to be communicated, line seizure occurs giving the alarm system priority..

2. If there is a problem with the customer's phone a line fault detector can be installed to notify the customer when the line is down.

3. If there is noise on phone circuit this may cause an inaccurate signal.

Learning Outcome 8-A-6 Know solutions for phone communicator problems

1. **Multiple phone lines** can be used to monitor one another. With this arrangement, both lines are constantly monitored for faults. If a fault occurs on one line the other line is used to notify the central station. This will work unless both lines are cut or fail. There are three basic ways to use multiple phone lines, split, backup and double reporting.

2. **Test Signals; m**ost digital communicators can be programmed to send test signals to the central station at regular intervals. If the expected signal from the communicator is not received, within a certain time, then the central station can take action.

3. **Redundant communications**; digital communicators can be backed up by other technologies including, long range radio or cellular.

Learning Outcome 8-A-7 Understand how enhancing digital communicators can reduce False Alarms

1. **Listen In -** This allows the operator to hear what is going on at the alarm site

2. **Two-Way Voice -** This allows the operator to listen in to the site and talk through speakers placed at the alarm site.

3. **Video Verification -** This allows the operator to see several snap shots of activity before and after the alarm or to monitor real time activity from the alarm site.

4. **Caller ID -** This feature can identify a system's phone number.

Learning Outcome 8-A-8 Understand how technology changes have impacted on alarm communication over plain old telephone system (P.O.T.S.)

1. **Analog vs. Digital -** An analog signal must have its shape preserved accurately if it is to sound like the original. With a digital system, the signal is either on or off so noise does not alter the message.

2. **Multiplex / Multiplexing –** Passive systems (Non Supervised) receive, alerts from alarm systems on the circuit one at a time with the receiving device acknowledging receipt to the sending unit. Active systems (Supervised) are those in which there are polling and responding messages to and from each alarm system on the circuit.

3. **Telcos in transition -** The transition of an existing Digital Communicator system is accomplished with dialer capture modules that convert the units' analogue protocol output into the same protocol in a digital technology scheme.

4. **Cellular system -** A cellular system is a mobile telephone system that divides large service areas into small cells and the call is switched from one transceiver to the next without interrupting its signal as the cellular phone moves from one cell to another.

5. **VOIP -** Digital Phone Systems utilize calling units that function like a Digital Communicator that communicates using digital technology as opposed to analogue. Passive Communication

6. **Internet** - Communication is over the Internet with alarm signals sent to an established IP address of a receiver that acknowledges receipt of the message.

7. **Long Range Radio -** Radio Frequency (RF) transmission is usually accomplished with Frequency Modulation (FM). Some networks utilize a poling scheme initiated by the receive polling all transceivers within the network.

CONTROL PANELS

Learning Goal: **To understand the basic components of control panels and their function.**

To review this section in its entirety, refer to page 52

Learning Outcome 9-A-1 Understand the purpose of control devices

All control panels perform some common functions - They detect problems through the sensors connected to them, and report these to someone. They also provide the user a method of turning the intrusion system on and off, and allow the customer to enter or leave the monitored area without setting off the system, allow some portions (fire, holdup, etc.) of the system to remain "armed" 24-hours a day, 365-days a year and provide the alarm user, a responding authority or an inspector with a method of silencing bells, or control other system features.

Learning Outcome 9-A-2 Know the function of the control panel

The control panel coordinates actions the system takes in response to messages received from sensors connected to it. The control panel converts power it received from a wall socket, battery, or both, to be utilized by the system.

Learning Outcome 9-A-3 Know three general methods used to connect parts of the alarm system to the control panel.

1. **Hardwire -** Hardwired systems use concealed or exposed wiring to connect the components. When wireless techniques are used for some of the system, sounding devices are usually connected to the control with wiring.

2. **Wireless -** Wireless systems use radio frequencies to connect to the controls. In wireless systems, hardwired or wireless methods may be used to connect the user controls to the control panel. Small battery powered radio transmitters are used to signal alarms to a radio receiver in the control panel.

    a. **Premise Wireless (RF) System -** Each wireless system has its own general radio frequency or house code.

b. **Hardwired vs. Wireless -** While there are applications that can only be installed with hardwire and others that can only be done with wireless, most applications can be installed either way.

3. **Line Carrier -** Line carrier systems use existing electrical wiring at the alarm site to transmit messages between the alarm system components.

Learning Outcome 9-A-4 Understand the purpose of partitions

A partition is a separate section of an alarm system that can operate independently and is controlled from the master keypad or by separate user control points.

Learning Outcome 9-A-5 Understand the purpose of keypad control points

Keypad controls allow the alarm user to turn the intrusion system on and off or enter and leave the monitored area without setting off the system, allow the alarm user to see which sensors are active and what doors are open and indicate "system events" such as alarms or trouble with phone lines, equipment or circuits.

Learning Outcome 9-A-6 Know the types of Keypads in use today

The general types of keypads are alphanumeric and LED. Either type can be mounted at the control or separate from it. Both allow the entry of a numerical code to arm and disarm the alarm system and may be used to perform various other functions such as shunting or programming system functions.

Learning Outcome 9-A-7 Understand an appropriate application of key switches

1. **Momentary Key switches**. To arm or disarm the system, turn the key, the spring loading returns key to its original position and then insert and remove the key from the same position.

2. **Maintained Key switches.** To arm the system, turn the key to one position. To disarm, turn the key to the other position. The key can be removed from either position.

Learning Outcome 9-A-8 Know other components of keypads

1. **Telephone control.** Many control panel manufacturers have incorporated ways for the phone to be used as a user control. When phones are used to control the system, feedback on system status and events is given audibly over the phone. Because the system is connected to the telephone network, systems with this feature can be controlled from anywhere a phone call can be made.

2. **Computer control** - Some systems are connected to a computer and allow control of events and receipt of information.

Learning Outcome 9-A-9 Know what a detection circuit (loop, zone) is

A Detection Circuit (loop, zone) is a portion of the detection or monitoring system that responds in a specific manner to sensed conditions. It is usually separately annunciated at the premises and/or remotely at a central station.

Learning Outcome 9-A-10 Understand what a zone is, and its purpose

A zone is another name for a detection circuit. It enables central station operators to tell precisely where in a premise an emergency is occurring. Zoning is dividing a system into a series of subsystems. Each zone or subsystem can consist of a single device or a group of devices in a given area. Zoning reduces service time by enabling the customer and service technician to pinpoint the area needing corrective action.

1. **Point annunciation -** Point annunciation goes one step further than zoning consisting of a single sensor. Controls and sensors that can be individually identified are often known as addressable devices.

2. **Cross zoning -** The practice of suppressing an alarm signal until two or more detectors in separate zones register alarm conditions.

3. **Labeling can be critical -** Effective design will label zones in a way that is clear to all that use or respond to the system.

Learning Outcome 9-A -11 Know the purpose of intrusion circuits

The alarm user will use some type of user control to turn the intrusion system on and off. Circuits turned on and off by the user control are known as "*controlled zones*". Circuits or zones that remain on 24 hours a day are known as "*24 hour zones*":

Entry-exit delays allow a user a preset amount of time to access the control panel or exit without setting the alarm off.

Learning Outcome 9-A-12 Understand alarm conditions which are active even when an alarm system is disarmed.

Examples of these alarms are panic, emergency, ambush, duress and holdup alarms. These alarms are active 24 hours a day, regardless of whether the alarm is armed, and can be silent or audible. Additional ongoing monitoring may include temperature controls, the failure of equipment, or the operation of equipment (generators, sump pumps, etc.) or medical emergencies.

Learning Outcome 9-A-13 Know the various circuit options

The various circuit options include automatic reset, auto-restore, automatic zone shunting, chime zone, cross zoning, day zone, priority zones, priority with bypass, swinger shutdown and twenty-four hour circuit

Learning Outcome 9-A-14 Understand the purposes of visual annunciators

Strobes are lights that flash when activated. Annunciators are used to communicate information to the alarm user. Common types of information are whether a system is armed or which zones are active. Annunciators can use LED displays, alphanumeric displays and graphic displays.

Learning Outcome 9-A-15 Know the types of audible alarm devices

Audible alarm devices are noise making devices such as a siren, bells or horn used to indicate an alarm condition.

Learning Outcome 9-A-16 Understand the purpose of secondary power

Because an alarm system will not operate without power, a secondary power source is usually connected to the alarm system. Common sources of secondary power are batteries and generators

Learning Outcome 9-A-17 Understand the purpose of audio systems

The system consists of microphones and a control unit containing an amplifier, accumulator, and power supply. When an alarm is initiated, a connection to a central station is normally established and operators may listen in to what is happening at the alarm site. The operator then determines what action is appropriate.

FIRE, SMOKE AND GAS SENSORS AND DETECTORS

Learning Goal: **To understand usage of sensors and detectors for fire, smoke and gas detection.**

To review this section in its entirety, refer to page 61

Learning Outcome 10-A-1 Understand the purpose of a fire and smoke sensors and detector

An alarm system needs detection devices to report "off normal" conditions. The type of detector used depends on what the system detects.

1. **Fire Alarm Sensors -** Fire alarms use detectors that sense smoke, heat, and flame.

2. **Types of Detectors -** Fire detection devices are often referred to as "*initiating devices*". Some are designed to sense the signs of fire automatically while others rely on people to see the signs of fire and manually activate a device.

Learning Outcome 10-A-2 Know two types of Heat Detectors

There are two types of heat detectors, fixed temperature which activates if the room or area exceeds the rating of the sensor, and rate-of-rise, which sense a 15 degree per minute increase in room/area temperature.

Learning Outcome 10-A-3 Know two types of Smoke Detectors

There generally two basic types of smoke detectors, photoelectric which senses the presents of smoke, and ionization which senses the presence of combustible gases.

Learning Outcome 10-A-4 Know other types of fire safety detectors

1. **Duct detectors** control the spread of smoke within a building by turning off the HVAC system, operating exhaust fans, closing doors or pressurizing smoke compartments in the event of a fire.

2. A **rate compensation detector** is a tube shaped device that responds when the temperature of the surrounding air reaches a predetermined level, regardless of the rate of temperature rise.

3. A **restorable semi-conductor line type heat detector** uses a semiconductor material and a stainless steel capillary tube. The capillary tube contains a coaxial center conductor separated from the tube wall by a temperature sensitive semi-conductor material. Under normal conditions small current (below the alarm threshold) flows. As the temperature rises, the resistance of the semiconductor thermistor decreases, it allows more current to flow and initiates the alarm.

4. **Non restorable fusible line type heat detectors** use a pair of steel wires in a normally open circuit. The conductors are held apart by heat sensitive insulation. When the temperature limit is reached the insulation melts, the two wires contact and an alarm is initiated. The fused section of the cable must be replaced following an alarm to restore the system.

5. **Cloud chamber smoke detectors** use sampling tubes to draw air from several areas. The air is passed through several chambers where humidity is added to allow sub-micron particles to become visible. Photoelectric detectors then react to any smoke particles and initiate an alarm

6. **Ultraviolet (UV) and Infrared (IR) flame detectors** react to radiant energy that is either visible to the human eye or outside the range of normal human vision.

7. **Pull Stations.** Manual pull stations are required by consumer safety code to be distributed throughout a commercial monitored area so they are unobstructed, readily accessible, and in the normal path of exit from the area.

8. **Key Operated Station**. Key operated stations are permitted in certain occupancies where facility staff members may be in the immediate area and use by other occupants of the area is not desirable. Typical conditions include detention and correctional buildings and where mental health treatment is provided.

9. **Wet Sprinkler System**. A permanently piped water system under pressure, using heat-activated sprinklers. When a fire occurs, the sprinkler heads exposed to high heat open and discharge water individually to control or extinguish the fire. When activated, a sprinkler system may cause water damage.

10. **Dry Sprinkler System.** Heat operated sprinklers are attached to a piping system containing air under pressure. Air pressure in the pipes holds a valve closed keeping water back. When heat activates a sprinkler head, air pressure is released. This allows a valve to open and water flows through the pipes to the activated sprinkler head.

11. **Waterflow Alarms**. When a building sprinkler head is activated from heat, the sprinkler head allows water to flow. A flow device which detects movement of water is installed in the sprinkler system.

12. **Fire Pump.** Many fire systems include a sprinkler system that is dependent on the availability of an immediate supply of water. A fire pump is used to force water from the community water reservoir to the building's sprinkler system.

13. **Risers.** A riser alarm is another specialty fire alarm detector which focuses on the detection of water availability to sprinkler systems. Similar to the fire pump system, a riser alarm may be used with either wet or dry sprinklers.

14. **PIV Detector** (Post Indicator Valve) This type of alarm monitor produces a tamper signal that is used to detect when someone or something has tampered with the main water control valve which brings the water into the building from the community water source.

15. **Gas Detectors**:
    Carbon Monoxide (CO) Carbon monoxide is a colorless, odorless and highly poisonous gas that is produced when fuels containing carbon are burned.

    Natural Gas Natural gas includes a group of gases that are colorless and odorless compounds not only poisonous but combustible and extremely explosive.

    Types of Gas Detectors include **Biomimetic units** and **Taguchi units**

16. **Supervisory Signals.** The position of a control valve may be monitored so a supervisory signal is sent whenever the control valve is turned to shut off the water to the sprinkler system.

SECURITY AND SAFETY IN-DEPTH

Learning Goal: To identify the types and purposes of detectors and sensors.

To review this section in its entirety, refer to page 66

Learning Outcome 11-A-1 **Know the types of sensors or detectors generally used to secure a perimeter.**

Perimeter Detection. The perimeter is the outer bounds of an area to be protected.

a. **Magnetic contacts** are used to sense when a door or window is opened.

b. **Mechanical switches** are used to detect the opening of a protected door or window.

c. **Audio discriminators** are audio sensing devices that are tuned to specific audio frequencies. They are tuned to the frequencies generated when a variety of building materials (Wood, Metal, Glass, Brick or Concrete, est.) are subject to assault or impact (glass breakage, splintering of wood, etc.). The most predominant are glass break detectors.

d. **Seismic sensors** are devices that detect changes in seismic pressure as an intruder approaches. Most commonly they are tubes filled with a fluid buried as a single tube or a pairs the length of the perimeter. The tubes are connected to a sensing device registering an alarm when an approach changes the pressure in the tubes

e. **Projected beam sensor is a** narrow beam of energy projected over a defined distance emitting from a transmitter device to a receiving device. An object passing thru the beam interrupts, or blocks it momentarily, thereby generating an alarm.

Learning Outcome 11-A-2 **Know the types of sensors or detectors generally used to secure an interior.**

Interior sensors allow further detection if the perimeter is penetrated or bypassed by an intruder.

1. **Passive Infrared (PIR)**. are optical devices that measures the heat of an object.

2. **Active Infrared Motion Detector (IR)** use an IR sensor, as well as a source of radiation. The receiver is able to detect interruptions in the radiation it receives from the radiation source.

3. **Continuous Wave Radar Motion Detector (CW)** use microwave signals to emit frequencies to bounce off of the surrounding area. The sensor detects when there are subtle changes in these frequencies which signals a disruption.

4. **Ultrasonic Motion Detector** is able to use sound energy in order to detect movement in a specific region. This ultrasonic sound energy is emitted in waves.

5. **Vibration Motion Detector** detects simple vibration caused by the changes in mass and its movement within the protected area.

6. **Video Motion Detection (VMD)** sensors operate through almost any good quality CCTV camera providing both a detection of activity and observation of the events progress.

7. **Volumetric Detection** sensors are located and adjusted so that a human is detected moving at a rate of one step per second in a wide or broad detection area.

8. **Infrasonic** sensors sense the change in air pressure when doors or windows are opened.

9. **Pressure Mats** are located under carpet or rugs in areas likely to be walked upon.

10. **Combined technology sensors** use two technologies to verify human motion in order to prevent false alarms in hostile environment.

Learning Outcome 11-A-3 Know the types of sensors or detectors generally used to secure a location point.

1. **Trap Detection**. Detection areas of expected travel paths of an intruder

2. **Spot Detection**. Point detection on a particular object such as a safe or , vault.

3. **Detection of "stay behinds"**- This detection is for an intruder who enters the facility during the business day and stows away in an area undetected. The goal is to determine and detect the areas likely to attract and conceal the intruder.

4. **Holdup Devices –** Manually activated devices such as a button, money clip, or foot rail.

Learning Outcome 11-A-4 Understand how sensors can be disguised.

Various types of sensors can be concealed in electrical outlets, thermostats or speaker grills, They can be disguised as smoke detectors or outlets.

Learning Outcome 11-A-5 Understand how alarms are processed.

An operator receives alarm signals that alert them to the progress of the attempt to intrude. The following critical information must be reported to the responding authority.

1. The alarm must be reported to the responding authority.
2. Subsequent alarms must also be reported to the responding authority;
3. Repeated reports of alarms provide information about the intruder's path within the protected facility and may identify additional intruders.
4. Reporting of points of exit after intrusion may indicate the perpetrator(s) departure
5. Reporting detail makes you a valuable member of the response team.

Learning Outcome 11-A-6 Understand the roles non security systems play in the protection of life and property.

Almost all of these sensors send signals when the problem occurs and when things return to normal.

1. **Miscellaneous Sensors**. Since anything that can close or open a switch or produce an electrical change can be monitored, the possibilities for sensors are almost endless.

2. **Medical Devices**
   Medical Emergency Alarm Devices are designed to produce an audible or visual signal indicating a need for medical assistance.

CUSTOMER SERVICE

Learning Goal: **To recognize the importance of the customer and to properly work with customers**

To review this section in its entirety, refer to page 73

Learning Outcome 12-A-1 **Understand why customer service is important**

Customer service comes down to the golden rule of treating others as you want to be treated.

Learning Outcome 12-A-2 **Demonstrate effective communications as an alarm monitor.**

1. Customers will be able to determine the mood you are in and the message you are trying to convey by your tone. Pace, volume, intensity, inflection and attitude all contribute to the tone of your voice. Be enthusiastic. Avoid negative tones.

2. Customer service equals customer response.

3. Customer feelings are important. Greetings should always be pleasant; get and use their name when whenever possible in the conversation.

4. Let the customer feel unique. Personalize the service to their needs

5. Record their information accurately and ensure timely follow-up

6. Listen to the customer. There is always the possibility that the customer on the other end of the line is facing a dangerous or highly emotional situation. Repeat key points, and get them immediate help when possible.

7. Avoid placing a customer on "*hold*".

Learning Outcome 12-A-3 **Demonstrate methods of working with irate customers**

When dealing with irate customers it is important to remember that this is not personal. Take responsibility to resolve the issue to the customer's satisfaction. Use methods such as:

1. Concede instead of convince
2. Hear them out
3. Use patience
4. Use tact
5. Empathize with their concerns
6. Don't interrupt
7. Acknowledge their concerns
8. Remain calm
9. Do not argue with them
10. Use positive statements
11. Take notes

Learning Outcome 12-A-4 **Understand methods of working with a customer who is out of control**

If the customer is out of control, or swearing:

1. Use short periods of silence to allow the customer to think and calm down. "
2. Remember it is usually not you, and it is nothing personal.
3. If the customer is so out of control that you cannot identify the facts surrounding their issue, use phrases like *"I feel uncomfortable when you swear at me, please help me understand your problem without swearing."*
4. You may need to repeat the same sentence a few times to get thru to an angry customer, be sure to use the exact same wording each time as this will be more effective than repeating the same statement in a different way.

FALSE ALARM PREVENTION

Learning Goal: **To reduce false alarms and maintain a common goal with public safety disciplines of protecting lives and property.**

To review this section in its entirety, refer to page 77

Learning Outcome 13-A-1 **Understand the impact of false alarms**

1. The cost of police response to alarms that are false is increasing.
2. There are increasing numbers of alarms being installed across the nation.
3. The number of false alarm dispatches must be reduced through a combined effort of private sector and public safety.
4. False alarms lower the public image of the alarm industry.

Learning Outcome 13-A-2 **Know the purpose and scope of the Alarm Industry Action Plan**

The Alarm Industry 1994-95 False Alarm Coordinated Action Plan was created to reduce false alarms.

1. **Steps for alarm dealers and monitoring companies**
    a. Attempt to verify all intrusion alarm signals by telephonic or other electronic means before requesting police dispatch, along with any other signals that can be prudently verified.
    b. Pro-actively call customers who have experienced alarm activation to investigate and prescribe corrective action as needed.
    c. Use only dual-action holdup devices and eliminate using "1+" duress keypad coding.
    d. Implement procedures to prevent or cancel exit/entry false alarms (such as extend delay times).
    e. Educate alarm system owners and users about their responsibilities relating to alarm system use and false alarms.
    f. Provide training for all company personnel on false alarm causes and solutions.
    g. Communicate with local authorities about their particular problems, and work with them toward local false alarm reduction plan.

2. **Considerations for the Alarm Monitor and Installer**
    d. Many sounds are similar to the sound of breaking glass.
    e. Certain applications are not recommended for either acoustic or shock glass break sensors.
    f. A sensitivity adjustment is available on most sound discriminators.

3. **Steps for police and community officials**
    f. Implement a locally predetermined procedure to suspend police response to chronic abusers of alarm systems, and implement procedures, which allow resumption of police response after corrective action has been taken.
    g. Implement procedures to accept verified cancellation of dispatch requests from alarm companies.
    h. Require user training and annual inspections of alarm systems.
    i. Support the alarm industry in its efforts to establish or strengthen statewide licensing of alarm companies and employees.
    j. Use a model, such as the NBFAA Model Alarm Ordinance, as a framework to develop steps to combat this problem in concert with local representatives of the alarm industry.

4. **Alarm Company Action Plan**

    Review the Alarm Industry Plan and adopt new policies and procedures for new and existing systems.

5. **Alarm Company Action Plan - Ongoing**

    a. Organize all new systems and procedures to meet the new standards.
    b. Concentrate efforts on accounts causing the most problems.
    c. Promote User Training.

STATE OF OREGON CERTIFICATION REQUIREMENTS

Learning Goal: To understand the State of Oregon Certification Requirements

***To review this section in its entirety, refer to page* 80**

Learning Outcome 14-A-1 **Understand how to access State of Oregon current certification information**

Alarm monitor private security professionals are welcome to become certified before seeking employment. *Note: they may not provide security services until all the certification requirements below are met.*

Information about DPSST, the Private Security Program, the Oregon Revised Statute (ORS), and the Oregon Administrative Rule (OAR), that provide regulatory authority and direction for the Alarm Monitor Private Security Professional program as well as all statutory requirements and processes for certification are outlined in: ORS 181.870-181-991 and ORS Chapter 259, Division 60. Links to the aforementioned can be obtained on the DPSST website: http://www.oregon.gov/DPSST/PS/pages/index.aspx

Private security professionals with questions are advised to first check the DPSST website. If there are still questions, contact the Private Security Program staff by phone: 503-378-8531 or by e-mail: security.investigators@state.or.us.

Learning Outcome 14-A-2 **Understand the minimum standards for becoming an Oregon private security professional.**

The minimum standards for becoming certified or renewing a certification include being at being at least 18 years of age, possessing a high school diploma or GED and being of good moral fitness.

Learning Outcome 14-A-4 **Understand how to renew a private security professional certification.**

Alarm Monitor Private Security Professionals must renew their certification every two years. The renewal process must be completed prior to the expiration date of the certification card. To mitigate last-minute issues, renewal may be initiated up to 180 days prior to expiration.
What is required for submission of a completed Renewal application to DPSST:

- PS-21 (application for renewal of certification)
- PS-6 (training affidavit) - Verifying completion of an Alarm Monitor Private Security Professional renewal course, within 180 days of making application for renewal.
- PS-20 (Temporary Work Permit) – If employed and submitting renewal application materials less than 30 days prior to expiration.
- PS-27 (Code of Ethics)
- All applicable fees

Note: To avoid any delays in processing, the above must be completed, signed, and submitted with all other application materials and fees to DPSST within 180 days of the expiration date on the certification card.

Learning Outcome 14-A-5 **Understand the impact of a "Deficiency" on the ability to perform the duties of a private security professional.**

A "Notice of Deficiency" is an official notice sent to the Security Professional notifying them of the missing or incomplete application information. On issuance of the Notice of Deficiency, the applicant has 21 days to complete or submit the incomplete or missing portions of the required application materials.

If an applicant doesn't respond, with the appropriate information, within the Notice of Deficiency timeline (21 days) or if DPSST is unable to complete the certification/licensure renewal process due to non-compliance, upon the discovery of disqualifying criminal convictions or any violation of the temporary work permit provisions the application *may* be Administrative Terminated and all fees paid will be forfeited.

Learning Outcome 14-A-6 **Understand the requirements to produce proof of certification.**

A certification holder must present their temporary work permit to any DPSST staff member, Law Enforcement Officer or Oregon Liquor Control Commission agent upon demand or any other person upon reasonable request. OAR 259-060-0030

Learning Outcome 14-A-7 **Understand the notification requirement for a change of address.**

An applicant or Private Security Professional must notify their employer and DPSST within 14 calendar days of any change of address by using the PS-23 (Private Security Professional - Change of Information) form.

I.R.I.S. - Information and Records for Investigators and Security (I.R.I.S.) allows Private Security Professionals, the public and employers to access information regarding the certification, licensing, employment and training status of Security Professionals. IRIS can be accessed via the following link:
http://dpsstnet.state.or.us/IRIS_PublicInquiry/privatesecurity/smsgoperson.aspx

Learning Outcome 14-A-8 **Understand the notification requirements if charged with a crime.**

1. If a Security Professional is charged with a crime, the Security Professional shall notify the Security Professional's employer, or, if the Security Professional is not employed, the Department of Public Safety Standards and Training, of that fact no later than 48 hours after the charge is filed.
2. If an Executive Manager knows that an employee has been charged with a crime, the Executive Manager shall notify the department of that fact no later than 48 hours after the Executive Manager acquired the knowledge.
3. The Department may suspend the certificate or license of a private security provider charged with a crime pending disposition of the charge.
4. If an applicant for certification or licensure as a private security provider is charged with a crime, the applicant shall notify DPSST of that fact no later than 48 hours after the charge is filed.

Learning Outcome 14-A-9 **Know the method of receiving relevant private security updates.**

ListServ

To receive updates on training opportunities, subscribe to the Private Security ListServ.
http://listsmart.osl.state.or.us/mailman/listinfo/private_security_bulletin

Private Security Forms

The Department has adopted by reference the following forms:

PS-1 -- Application for Licensure or Certification of Private Security Services Provider.

PS-3 -- Private Security Order Forms Sheet.

PS-4 -- Affidavit of Person Rolling Fingerprints.

PS-6 -- (Affidavit of Instructor and Private Security Provider Testing Results)

PS-7 -- Private Security Instructor Evaluation.

PS-8 -- Private Security Instructor Proof of Skills Improvement.

PS-9 -- Private Security Waiver for Reciprocity.

PS-20 -- Private Security Services Provider Temporary Work Permit.

PS-21 -- Renewal of Private Security Services Licensure or Certification.

PS-23 -- Private Security Services Provider Change of Information.

PS-27 -- Private Security Code of Ethics.

NOTE: Most of these forms are available on the DPSST WEB site at www.dpsst.state.or.us. The only exception is the PS-6.

Index

Index

Index

Index

Index

Index