CONSTRUCTION ELECTRICIAN APPRENTICESHIP PROGRAM

Level 4 Line J: Install Signal and Communication Systems

LEARNING GUIDE J-8

INSTALL SECURITY ALARM SYSTEMS

ita
industry training authority

THE RIGHT SKILLS ▶ A PROVEN ADVANTAGE

BRITISH COLUMBIA

Foreword

The Industry Training Authority (ITA) is pleased to release this major update of learning resources to support the delivery of the BC Electrician Apprenticeship Program. It was made possible by the dedicated efforts of the Electrical Articulation Committee of BC (EAC).

The EAC is a working group of electrical instructors from institutions across the province and is one of the key stakeholder groups that supports and strengthens industry training in BC. It was the driving force behind the update of the Electrician Apprenticeship Program Learning Guides, supplying the specialized expertise required to incorporate technological, procedural and industry-driven changes. The EAC plays an important role in the province's post-secondary public institutions. As discipline specialists the committee's members share information and engage in discussions of curriculum matters, particularly those affecting student mobility.

ITA would also like to acknowledge the Construction Industry Training Organization (CITO) which provides direction for improving industry training in the construction sector. CITO is responsible for organizing industry and instructor representatives within BC to consult and provide changes related to the BC Construction Electrician Training Program.

We are grateful to EAC for their contributions to the ongoing development of BC Construction Electrician Training Program Learning Guides (materials whose ownership and copyright are maintained by the Province of British Columbia through ITA).

Industry Training Authority
January 2011

Disclaimer

The materials in these Learning Guides are for use by students and instructional staff and have been compiled from sources believed to be reliable and to represent best current opinions on these subjects. These manuals are intended to serve as a starting point for good practices and may not specify all minimum legal standards. No warranty, guarantee or representation is made by the British Columbia Electrical Articulation Committee, the British Columbia Industry Training Authority or the Queen's Printer of British Columbia as to the accuracy or sufficiency of the information contained in these publications. These manuals are intended to provide basic guidelines for electrical trade practices. Do not assume, therefore, that all necessary warnings and safety precautionary measures are contained in this module and that other or additional measures may not be required.

Acknowledgements and Copyright

The issuing/publishing body is: Crown Publications, Queen's Printer, Ministry of Citizens' Services

The Industry Training Authority of British Columbia would like to acknowledge the Electrical Articulation Committee and Open School BC, the Ministry of Education, as well as the following individuals and organizations for their contributions in updating the Electrician Apprenticeship Program Learning Guides:

Electrical Articulation Committee (EAC) Curriculum Subcommittee

Peter Poeschek (Thompson Rivers University)
Ken Holland (Camosun College)
Alain Lavoie (College of New Caledonia)
Don Gillingham (North Island University)
Jim Gamble (Okanagan College)
John Todrick (University of the Fraser Valley)
Ted Simmons (British Columbia Institute of Technology)

Members of the Curriculum Subcommittee have assumed roles as writers, reviewers, and subject matter experts throughout the development and revision of materials for the Electrician Apprenticeship Program.

Open School BC

Open School BC provided project management and design expertise in updating the Electrician Apprenticeship Program print materials:

Adrian Hill, Project Manager
Eleanor Liddy, Director/Supervisor
Beverly Carstensen, Dennis Evans, Laurie Lozoway, Production Technician (print layout, graphics)
Christine Ramkeesoon, Graphics Media Coordinator
Keith Learmonth, Editor
Margaret Kernaghan, Graphic Artist

Publishing Services, Queen's Printer

Sherry Brown, Director of QP Publishing Services

Intellectual Property Program

Ilona Ugro, Copyright Officer, Ministry of Citizens' Services, Province of British Columbia

To order copies of any of the Electrician Apprenticeship Program Learning Guide, please contact us:

Crown Publications, Queen's Printer
PO Box 9452 Stn Prov Govt
563 Superior Street 2nd Flr
Victoria, BC V8W 9V7
Phone: 250-387-6409
Toll Free: 1-800-663-6105
Fax: 250-387-1120
Email: crownpub@gov.bc.ca
Website: www.crownpub.bc.ca

Version 1
Revised, April 2014
New, October 2012

LEVEL 4, LEARNING GUIDE J-8:

INSTALL SECURITY ALARM SYSTEMS

Learning Objectives

- The learner will be able to describe the operating principles of security alarm systems.
- The learner will be able to describe the procedures to install and test security systems.

Activities

- Read and study the topics of Learning Guide J-8: Install Security Alarm Systems.
- Complete Self-Test 1. Check your answers with the Answer Key provided at the end of this Learning Guide.

R Resources

You are encouraged to obtain the following text to supplement your information for learning:

- *Canadian Electrical Code – Part 1* (latest edition), published by the Canadian Standards Association

BC Trades Modules
www.bctradesmodules.ca

We want your feedback! Please go the BC Trades Modules website to enter comments about specific section(s) that require correction or modification. All submissions will be reviewed and considered for inclusion in the next revision.

SAFETY ADVISORY

Be advised that references to the Workers' Compensation Board of British Columbia safety regulations contained within these materials do not/may not reflect the most recent Occupational Health and Safety Regulation. The current Standards and Regulation in BC can be obtained at the following website: http://www.worksafebc.com.

Please note that it is always the responsibility of any person using these materials to inform him/herself about the Occupational Health and Safety Regulation pertaining to his/her area of work.

Industry Training Authority
January 2011

Learning Task 1:

Describe the basic features of security systems

To build an effective security system, the security system planner must consider the purposes of the system. There is no single system that is suitable for all applications, because every installation will have different requirements.

Purposes of security systems

A security system is designed to protect property and people and to provide a feeling of security to its users. Common security systems include alarm systems, door locks and hardware, outdoor lighting and guard dogs. Most security systems are designed to meet one or more of the following purposes.

Deterrence

The deterrence value of a system lies in its ability to stop prospective criminals from committing the acts they are considering. The presence of a system must be prominently displayed (using warning decals, for example) for deterrence to be effective.

Prevention

Prevention physically limits the criminal. Items such as fences and locks are designed to stop persons from entering an area or opening a door.

Detection

If the perpetrator has ignored the deterrence and bypassed the prevention methods, the next step is to detect the presence of the intruder. An alarm system has one or more methods of detection, such as motion detectors and door contacts.

Response

Once the intruder has been detected, some form of response is needed. This may come in the form of police or private guards. Most alarms have some form of audible warning, such as a siren, and many are monitored offsite by a monitoring station.

Apprehension

The responding authorities apprehend the intruder. Electronic equipment may be used to aid in the identification of the criminal or to serve as evidence to obtain a conviction.

Each element of a security system provides protection in different forms and in different ways. A total security system uses more than one approach and serves all of the purposes described above.

Which type of security system is most appropriate depends on what you want it to do. Most security consultants use the "onion-skin" approach to security: successive layers of protection throughout a building or installation. The layers may be separate security systems or parts of a larger system providing various forms of protection.

Alarm systems

An alarm system is just one part of a total security system, yet it serves three purposes:

- Deterrence using warning decals.
- Detection of intruders using motion detectors and door contacts. For this reason, alarm systems are frequently called *intruder alarms*, to distinguish them from other types of alarms.
- Response facilitated by audible warnings, such as sirens, or offsite monitoring.

The layers of protection of an effective onion-skin approach fall into three categories: perimeter protection, space protection and spot protection.

Perimeter protection

Perimeter protection, also called *point-of-entry* protection, refers to the devices designed to protect the outer perimeter of a building or installation. An example is a door contact that reacts when the door is opened.

Perimeter protection provides early warning by sounding an alarm when the intruder is attempting to enter the premises but is not yet inside. The earlier the intrusion is detected, the more effective the system. Systems employing perimeter detection also allow users to stay inside the protected area.

Space protection

Space protection, also called *volumetric protection*, is designed to detect the presence of a person within a volumetric area. An example is a motion detector that is set up to detect the movement of a person anywhere in the room. Space protection has two advantages over perimeter protection:

- It is very cost effective, in that one detector is able to provide coverage for a large space. Typical motion detectors provide over 45 m^2 of coverage within a room or area.
- When planning an installation, it is less important to anticipate the spots at which entry will likely occur. With perimeter protection, intrusion will be detected only at the spots that have been protected, while space detection will cover the whole room.

However, space protection has its limitations. First, it does not provide early warning. Intruders are detected only when they are already inside the premises. Response to the alarm will often be initiated too late.

Space protection usually does not allow customers to stay inside the protected area. Any movement by the customers themselves will trigger the alarm.

For these two reasons, space protection is best if used as a layer within an alarm system: perimeter devices provide early warning; space protection is a backup if the perimeter is penetrated.

Spot protection

Spot protection is also called *object* or *trap protection*. Spot protection is designed to protect a specific object or area. If an intruder manages to avoid detection by the perimeter and space protection systems, then protection at a strategic spot makes up the next layer in the security system.

Spot protection is usually installed around an item of value, such as a cash box or an expensive painting. It may also be used when the space within the protected area is too large to protect effectively with conventional space protection. In this case, it is common to provide space protection only in areas through which an intruder will likely pass, such as a hall or stairway.

Basic alarm system circuitry

An alarm system can be divided into three main circuits (Figure 1):

- Detection circuit
- Control circuit
- Output circuit

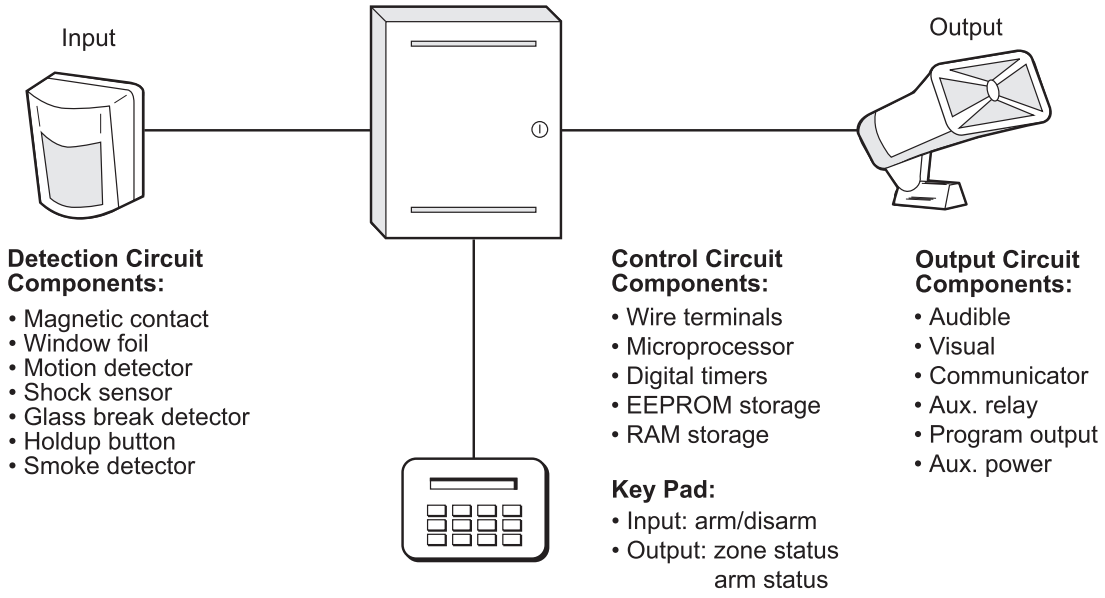

Figure 1—Components of an alarm system

A detection circuit consists of the detection devices, the set of conductors that connect the devices to the alarm control panel, and the electronic circuitry within the panel that monitors changes in the circuit.

The conductors of the detection circuit are sometimes referred to as the loop. The *loop* is connected to a set of contacts, such as a switch or relay on the devices. Detection circuits will generally operate in only one of two states:

- Secure—when the detection devices are not detecting an intrusion
- Insecure (alarm)—when an intrusion is detected

In the secure condition, current flows from the panel, through the loop conductors and the detection device contacts, and back to the control panel. When an intrusion occurs, the loop current is interrupted and the control panel responds to the change in current. The control then supplies power to one or more outputs, which may be bells, sirens, strobe lights or electronic communicators. (The control panel has other specialized functions that will be covered later in this Learning Task.)

Of the output devices, the most commonly used is the siren. An electronic circuit converts the supplied 12 V DC to an AC signal, which is passed through a horn speaker. The result is a loud, police-type siren that is readily identified as an intrusion alarm.

Usually, alarm sirens are installed in protected areas. In residential alarms, the siren is installed in the attic, with the horn pointing out of a vent or soffit. In this way the siren can be heard but not seen.

Detection circuit operation

Detection circuits and the devices that are meant to connect to them come in two basic types: closed-loop and open-loop. The following describes only the closed-loop circuits.

Closed-loop circuits

The closed-loop is the most common type of circuit used in intrusion alarm equipment. The term *closed-loop* derives from the fact that when the loop is in the secure condition it is a continuous, closed loop. All devices in a closed-loop circuit are connected in series, so that current flow through the loop is the same through all devices. The contacts on the devices are in the closed position. Figure 2 shows a closed-loop circuit with switches used to represent the detection devices. In an actual circuit, the switches may be door contacts or the contacts on a relay inside a motion detector.

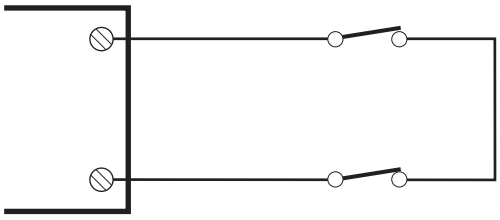

Figure 2—Closed-loop circuit with switches representing detection devices

When the device detects an intrusion, it goes into the alarm condition. The contacts will open, causing the current in the loop to stop flowing. The current-sensor notices the change and provides a voltage signal to a logic circuit, which activates the appropriate alarm outputs.

Figure 3 shows a closed-loop circuit in an alarm condition.

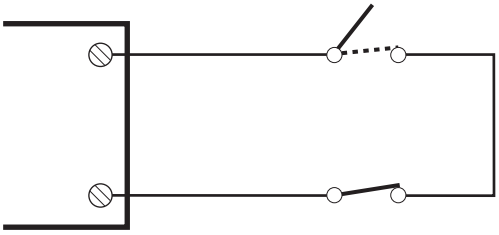

Figure 3—Closed-loop circuit in an alarm condition

Inside the alarm control panel, the circuit is connected to the power supply. Resistors are connected in series to limit the current through the loop. A current-sensing circuit monitors the flow of current. The amount of current flowing through the loop depends on the limiting resistors, as well as on any resistance in the circuit external to the alarm panel. Usually the current sensor will allow for 100 Ω or more in the external circuit.

The circuits described above have a serious drawback, however. A control panel using these circuits would be unable to provide supervision of the circuit.

Supervision is the ability of a control panel to monitor the electrical characteristics of the circuit. In the closed-loop circuit shown in Figures 2 and 3, current flows when the loop is secure. If current flow stops, the panel considers that an alarm has occurred. The loop is said to provide *open-circuit supervision*, as the panel monitors when the loop becomes open.

However, if the loop is shorted, as shown in Figure 4, the panel will not react, since the current has not changed. If an intrusion is detected by one of the devices, the loop will not open and the panel will not register a change in current. Such a short may be caused by a staple driven through the cable or may be the result of deliberate tampering.

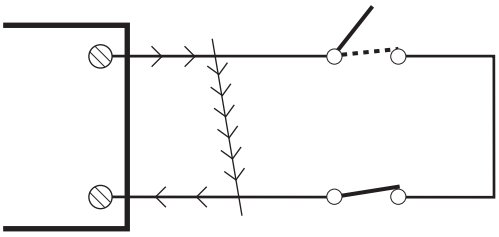

Figure 4—Loop circuit shorted

A loop that cannot provide adequate supervision could easily be defeated by a burglar with a little knowledge of alarm systems. Therefore, other types of loops were developed to provide better supervision against tampering.

There are four basic types of closed-loop circuits:

- Two-wire
- Two-wire with end-of-line resistor
- Four-wire
- Four-wire ULC

Two-wire

Two-wire loops provide only partial supervision and are easily defeated. Two-wire closed-loop circuits are commonly used in low-security applications such as residential alarms.

Caution! If two-wire loops are used, the conductors and device contacts should be concealed to prevent tampering with the loop.

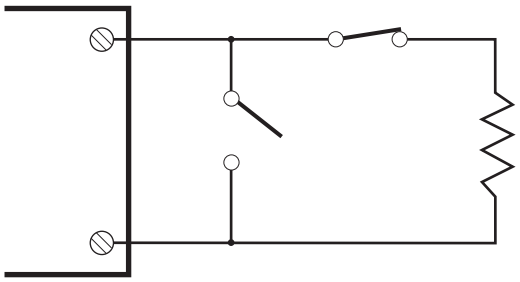

Figure 5—End-of-line resistor (ELR) circuit

Two-wire with end-of-line resistor

The two-wire with end-of-line resistor loop is very popular, especially in higher-security applications such as those in commercial buildings. An end-of-line resistor (ELR) is connected in series with the loop external to the control panel (Figure 5). The ELR provides further limiting of the loop current along with the internal resistance of the circuit. A typical value for the ELR is 1 kΩ or 2.2 kΩ.

When the loop is secure, current flows through the devices and through the resistor. The loop current is dependent upon the ELR, and the current sensor in the control panel monitors the amount of current. If the current changes by a significant amount, the control panel responds by sounding an alarm. If the loop is opened, the current will drop to 0 A and the current sensor will respond to the change in current. If the loop is shorted, the ELR will be bypassed and the loop current will rise. The short-circuit current will now be limited only by the internal resistance of the loop. In either case, an alarm will sound.

As this type of loop will respond to both short-circuit and open-circuit conditions, both closed-loop and open-loop devices may be connected to a two-wire ELR loop.

Keep in mind that the ELR must be connected *at the end of the loop* for it to provide full supervision. Many installers overlook the importance of this and install it inside the control panel. While the ELR is still in series with the loop, it provides protection against opens but will not supervise against shorts in the loop.

Four-wire

The four-wire loop is also called a *double-circuit* or *HI/LO* loop. Two separate loops are used to provide full supervision of the detection circuit (Figure 6). One of the loops is a positive (HI) loop and the other is a negative (LO) loop. In the secure condition there is no current flow between the two loops. Figure 6 shows a four-wire loop in the secure condition.

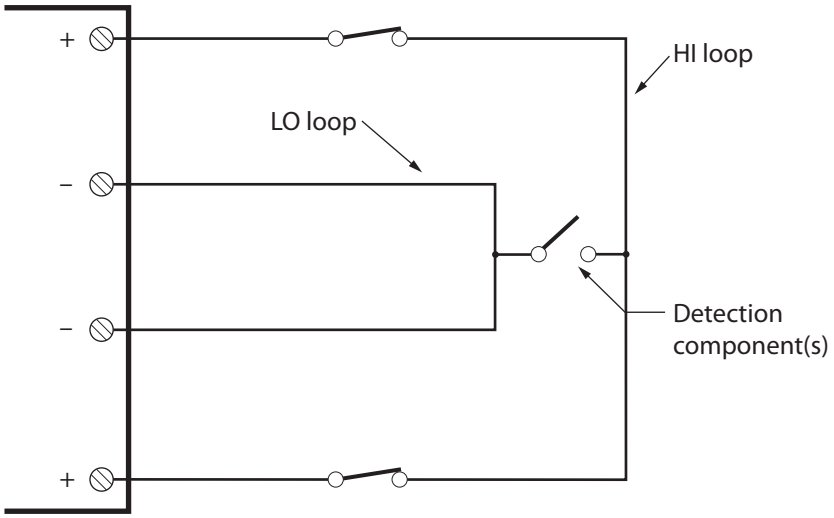

Figure 6—Four-wire loop in the secure condition

Notice that there are both closed-loop and open-loop circuit devices connected to the four-wire loop. This type of circuit is able to accommodate detection devices that have both closed-loop and open-loop contacts. It is also able to supervise both shorts and opens on the loop. Normally, the closed-loop devices are only connected to the HI loop. In some cases, the LO loop is called a *24-hour loop*, because it is capable of sounding an alarm if it is interrupted at any time of day. This provides protection against tampering even though the alarm system may be turned off.

Although the four-wire loop is less common than the two-wire ELR, it is often found in installations using window foil. The double circuits provide a high-security measure against tampering with the foil.

Four-wire ULC

The four-wire ULC is a variation of the four-wire loop described above. It is so-named because it is recognized as a high level of security by the Underwriter's Laboratories of Canada (ULC). (ULC is an organization that sets standards for, among other things, the installation and testing of alarm systems.) For an alarm system to gain ULC approval, it must employ this type of loop as its detection circuit.

Like the four-wire loop type, the four-wire ULC loop has both a HI and a LO loop. The contacts on the detection devices must be SPDT, with C, NO and NC terminals. Figure 7 shows a four-wire ULC loop.

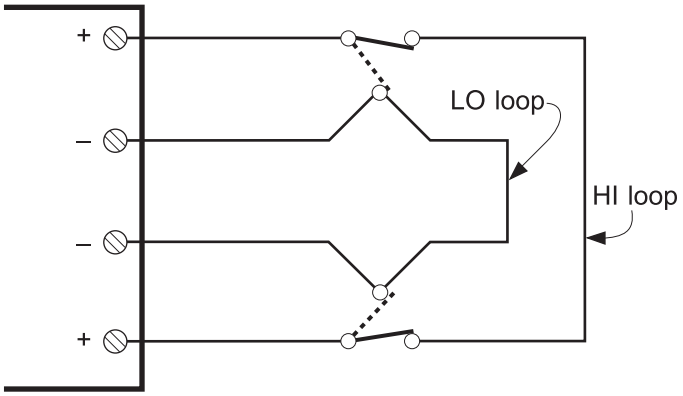

Figure 7—Four-wire ULC loop

When a device goes into the alarm condition, two simultaneous events occur. The HI loop is opened, and it is also shorted to the LO loop. Figure 8 shows a four-wire ULC loop in the alarm condition.

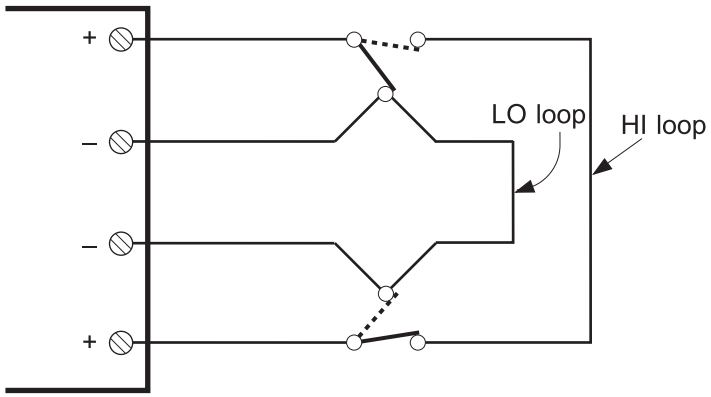

Figure 8—Four-wire ULC loop in the alarm condition

This type of loop provides an even greater level of security against tampering. The two-wire ELR and the four-wire loops are supervised against shorts in the loop, but if an intruder deliberately places a short across the terminals of the device, that device will be defeated. (Many devices, such as door contacts, have the terminals exposed.) However, the four-wire ULC loop not only opens the HI loop but also provides a current path between the two loops, so the system is less easily defeated by tampering.

It would be possible to tamper with the four-wire ULC loop by shorting the HI loop and then removing the LO loop from the single terminal. For this reason it is imperative that the two conductors of the LO loop not be twisted together before connecting them to the terminal. Any attempt to remove them must generate a tamper alarm condition by opening the LO loop.

Common detection and alarm devices

Installing alarm detectors properly means allowing them to work as intended without causing false alarms (which are becoming an epidemic problem). To install alarm detectors properly, you must understand how each type operates and be aware of the factors that can cause problems.

Commonly used detection and alarm devices include the following:

- Magnetic contacts
- Passive infrared (PIR) detectors
- Microwave and ultrasonic motion detectors
- Dual-technology detectors
- Photoelectric beam detectors
- Glassbreak detectors
- Audio detectors
- Shock sensors

Magnetic contacts

A magnetic contact consists of two parts: a magnetically activated switch and a magnet. The switch is usually mounted on the frame of a door or window and the magnet is mounted on the door itself. When the magnet is adjacent to the switch, the switch is held in the desired open or closed state.

An installer can choose from an immense variety of magnetic contacts of different shapes, sizes and colours to meet the requirements of any installation. Magnetic contacts come in two basic mounting types.

Surface-mount contacts

As the name implies, surface-mount contacts are meant to be attached directly to the surface of the door and frame. They are usually used where appearance is not critical and cable can be run on the surface of the walls. Surface-mount contacts are available in screw-on and self-stick models. The loop conductors are connected to the contact at the screw terminals on the top (Figure 9).

Since the terminals on surface-mount contacts are exposed, they can be vulnerable to tampering. Some contacts are sold with plastic terminal covers that hide the screw terminals from view.

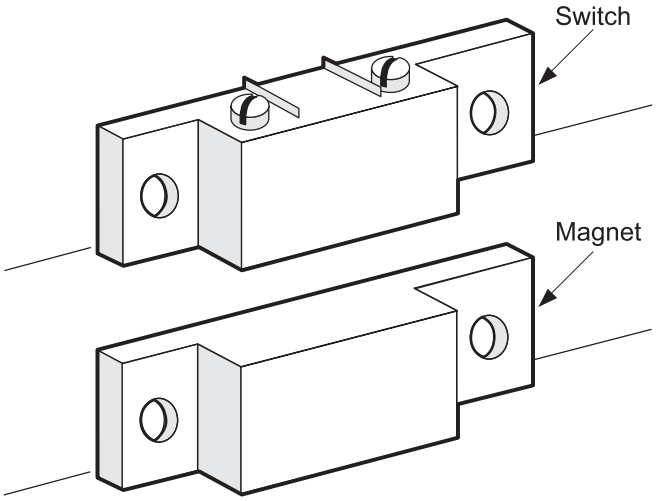

Figure 9—Typical surface-mount contact

Flush-mount contacts

Flush-mount or recessed contacts (Figure 10) are intended to be inserted into holes drilled into both the door and frame. When installed, the switch and magnet are not easily seen and the conductors are hidden from view.

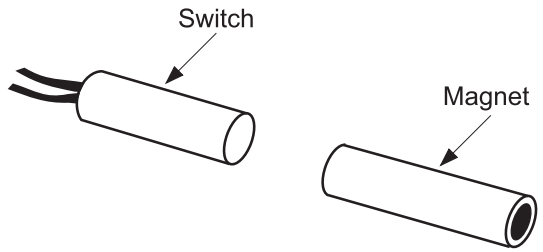

Figure 10—Typical flush-mount contact

The earliest magnetic contacts were mechanical switches, but virtually every magnetic contact manufactured today is of the type called a *reed switch*. A reed switch is made of two slivers of metal enclosed in a hermetically sealed glass tube. When the switch is in the presence of a magnetic field, the slivers are attracted to each other and make contact for as long as the magnetic field is present. The slivers are made with a small amount of spring tension to keep them apart when the magnet is pulled away.

Note the following precautions when installing reed switches:

- Reed switches are very fragile and will not withstand much shock or pressure. If the glass tube becomes cracked, oxygen and water vapour will enter. In most cases the switch will perform normally, but over time corrosion will build up on the metal slivers, ultimately resulting in failure. If the switch shows signs of damage or if you suspect that the reed inside has cracked, discard it.
- Reed switches have low current-handling capabilities. Most reeds are able to conduct currents of only 250 mA or less. At higher currents the contact points will either melt off or weld together.
- The switch and magnet must be aligned correctly, to allow the switch to remain closed during slight movements of the door.
- Reed switches must be kept away from steel in the vicinity, such as steel doors or frames. Since steel has a lower reluctance than air, the magnetic flux of force will tend to travel through the steel and not through the air. This reduces the force available to operate the contact and will reduce the gap.

PIR detectors

Although several types of motion detectors are commonly used today, over the last decade the passive infrared (PIR) detector has clearly emerged as the leader in motion detection. Since the early 1980s, the cost of an average PIR has decreased dramatically, yet the reliability has increased to the point where false alarms should *never* occur in a properly installed system.

A PIR is called *passive* because, unlike other detectors, it does not radiate a signal. Instead, it passively detects changes in infrared (IR) radiation. IR radiation is a form of electromagnetic energy very much like light, radio waves and X-ray radiation. The only difference between these forms of energy is the wavelength, or frequency of the wave.

The term *infrared* means "below red." This refers to the fact that, on the entire electromagnetic spectrum, infrared radiation is found immediately below what human eyes perceive as red light. However, IR is not a single frequency of radiation but an entire range of frequencies.

Infrared radiation is emitted by all objects in the universe. As the temperature of an object decreases, the amount of IR radiation it emits decreases proportionately. At zero kelvin, or absolute zero (about –273°C), all molecular motion stops and infrared radiation is not emitted. As the object's temperature increases, the quantity of IR it emits will increase.

The heart of a passive infrared detector is the *pyroelectric element* (PE). A PE is a semiconductor device that undergoes a change in resistance when exposed to infrared energy. The amount of change is very minute and is proportional to the amount of IR received. A microprocessor analyzes the electric signal and triggers an output if the amount of IR received increases or decreases. A PIR installed in any room will initially react to the ambient IR energy level of the room and the objects within. After several seconds, the PIR will stabilize as it becomes used to the ambient IR energy. Any further changes in the IR levels will cause the detector to signal an output again.

Figure 11 shows a PIR with the cover removed, revealing the printed circuit board with the pyroelectric element. Also shown is a *walk-test* LED that allows the installer to test the coverage area. The walk-test LED illuminates when a person enters the protected area.

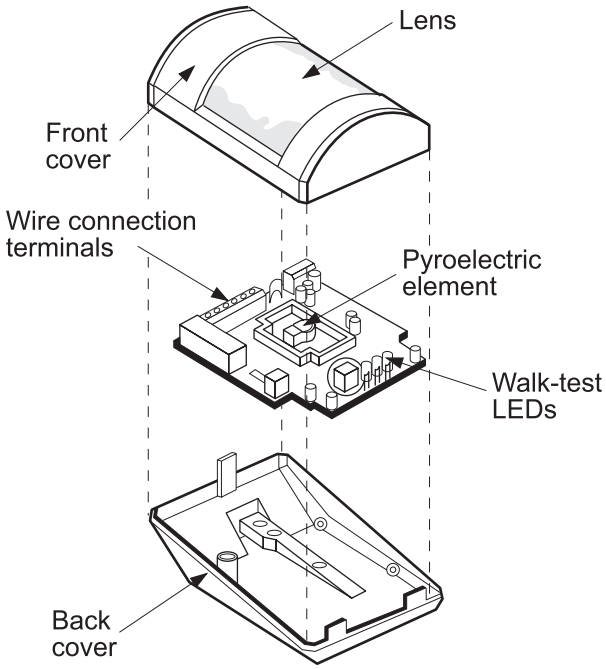

Figure 11—Passive infrared (PIR) detector showing printed circuit board and pyroelectric element

A PE by itself is unable to focus on specific objects. Lenses and mirrors are used to focus the IR energy from select portions of the room onto the PE. In this way, the PE monitors the IR energy levels only in certain spots throughout the room. The resulting pattern produced is called the *detection pattern*. On many detectors, the lens or mirror may be changed to provide different detection patterns.

The detection pattern is composed of several individual zones of detection called *fingers*. Each segment of the mirror or lens represents one finger of the detection pattern. The fingers on most detectors are arranged in a three-dimensional pattern to provide detection for a large space. PIRs commonly have standard patterns with three layers of detection, each of which has six or eight fingers. Figure 12 shows a top and side view of a popular PIR detection pattern.

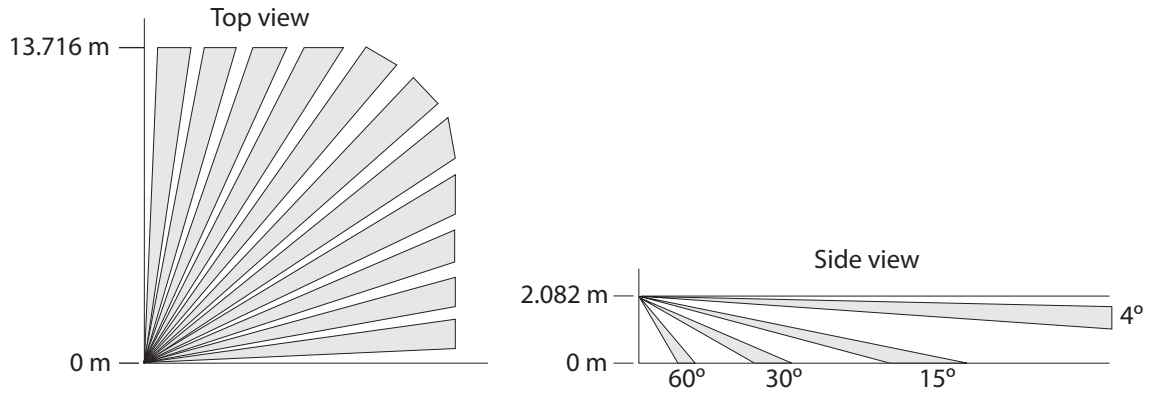

Figure 12—Two views of a PIR detection pattern

PIR detectors are by far the most common detectors used in the industry today. Some of the reasons for their popularity are:

- They are self-adjusting. Normal daily and seasonal changes in ambient temperature are compensated for by the processing circuits. Only rapid changes in temperature will cause an alarm.
- They are relatively foolproof to install.
- PIRs are passive devices; they do not emit harmful radiation.
- They are extremely versatile. Detection patterns are changed by simply changing the lens or mirror. A company may stock one model of PIR, yet have a hundred detection patterns at its disposal.
- Locations of detection fingers are easily located in a protected area and may be masked if they pose a potential problem.

PIRs do have certain disadvantages and limitations on their use.

- They may be tripped by objects that change temperature rapidly. Avoid allowing PIR fingers to terminate on:
  - blowers, heaters or heating ducts
  - glass or other highly reflective surfaces
  - dangling objects, including Christmas ornaments
  - areas exposed to direct sunlight
  - sources of white light
- The detection is unsupervised. If a detector is totally blocked, there is no indication to the control panel, because the PIR simply adjusts to the IR energy of the blocking item.
- The range and sensitivity of PIRs depend, to a certain extent, on the ambient temperature. Some detectors may fail to recognize a warm intruder moving into a warm room.

Microwave and ultrasonic motion detectors

Ultrasonic detectors were the first true motion detector and were once extremely popular. Microwave detectors operate in a manner similar to ultrasonics and share many of the same characteristics. Ultrasonics and microwaves are rarely installed in new alarm systems, but many can be found still in service in schools, museums and other large institutional buildings.

Unlike PIRs, ultrasonics and microwaves are active devices. An ultrasonic detector operates by emitting high-frequency sound waves. Microwave detectors emit microwave radiation in the 10–12 GHz range. Both detectors operate by reacting to doppler shift. A *doppler shift* is the change in frequency of a wave that occurs when there is relative movement between the sound source and the observer. If you have ever listened to the whistle of a train as it passed, you may have noticed that the whistle sounded higher in pitch as the train approached, then became lower as the train moved away. This happens because the sound wave is compressed as the wave moves toward you (who are in the direction of its travel), and is stretched as the train (and the sound wave) moves away from you. The relative movement between the train and you is what causes the apparent doppler shift; passengers on the train do not notice any change in sound.

In both ultrasonics and microwaves, the transmitted signal bounces off objects within the protected area. Stationary objects, such as walls and floors, will reflect the signal without causing a change in frequency. Any object moving within range will cause the frequency to shift, either higher or lower. Another transducer receives the signal and converts it back to an electrical impulse. The processor circuit compares the two signals and activates an output if they differ in frequency.

The much higher operating frequency of the microwave detector gives this device two distinct characteristics:

- Microwave radiation easily passes through most materials. Metal objects reflect microwaves, and dense materials like concrete absorb some of the energy of the radiation. Wood and glass objects allow microwaves to pass through them as though they

were invisible. A microwave detector mounted inside a wood-frame building can easily detect the motions of a large metal object outside the building.

- Microwaves are unaffected by the ambient conditions that can cause false alarms in PIRs and ultrasonics. Humidity, high-pitched noises, rapid changes in temperature, and air turbulence have no effect on microwave detectors. Microwaves are capable of covering much larger areas than either PIR or ultrasonic detectors.

There are several fundamental differences between PIRs and both ultrasonics and microwaves. Each type of detector reacts to different ambient conditions and has its own advantages and disadvantages.

Compared with PIRs, ultrasonics and microwaves have the following advantages:

- *Sensitivity to motion toward the detector*

  Ultrasonics and microwaves are more likely to detect intruders if the movement is toward or away from the detector.

- *Sensitivity to a different set of ambient conditions*

  Ultrasonics and microwaves are unaffected by sources of heat in the way that PIRs are, but they are sensitive to other conditions. Moving or rotating objects and sources of high-pitched noises can cause false alarms with ultrasonics.

- *Sensitivity to variations in ambient humidity*

  Passive infrared detectors will adjust automatically to normal atmospheric changes, but ultrasonics are unable to do so. The sensitivity of ultrasonics increases dramatically under low-humidity conditions.

- *Sensitivity to the room acoustics*

  The size and acoustic qualities of the protected area affect the detector's ability to operate. Large, open areas and soft surfaces (carpets, drapes, upholstery) will absorb the sound waves and decrease sensitivity. Confined areas and harsh surfaces (linoleum or tile flooring, reflective surfaces) will allow sound waves to reflect more easily, and sensitivity will increase.

- *Subject to interference between two detectors*

  The signal emitted from one detector will cause interference in any others mounted within range. If more than one detector is to be mounted in the same area, they must be tuned to completely different frequencies. Some systems designed for large installations have a single, central frequency generator and processing unit with multiple slave transmitters and receivers. Since the signal comes from one source, the transmitters and receivers do not cause interference with each other.

In addition to the differences described above, microwave detectors have other characteristics that can cause problems with their operation.

- Sensitivity to fluorescent and neon lights: the frequency of the energy pulses in both types of lighting will cause interference with microwave detectors and may cause false alarms. Detectors should be kept at least 2 m away from these lights.
- Inability to contain the detection pattern: Since microwaves pass through most walls, it is possible for the detector to react to large metal objects outside of the protected area.
- Reflective properties of water: Water flowing through plastic pipes may reflect the waves, causing a doppler shift and resulting in a false alarm.

Dual-technology detectors

Dual-technology detectors, also known as *dualtechs*, rely on two different sensing methods to achieve greater reliability. The underlying principle is that both sensors must detect motion. Since the weaknesses of one technology will not be the same as that of another, a dualtech will be less likely to experience false alarms from changes in ambient conditions. Dualtechs have become extremely popular in recent years due to their reliability and resistance to false alarms.

For a dualtech to be effective, the technologies must be inherently different in their operating principles. Ultrasonic and microwave detectors, for example, would not give good results working together as a dualtech, since they both operate by detecting doppler shifts. PIR/ultrasonic combinations are available, but the majority of dualtechs sold today are PIR/microwave.

Table 1 shows a comparison of the conditions affecting PIRs, microwaves and dualtechs. "OK" means that the ambient condition given will cause little problem to the detector. "Caution" means that, the condition stated will cause problems, and precautions should be taken to avoid false alarms. "X" means that the detector is not suitable to operate under the conditions specified and should not be used.

Table 1: Comparison of conditions affecting PIRs, microwaves and dualtechs

Ambient conditions	PIR	Microwave	Dualtech
Vibrations	OK	X	OK
Changes in temperature affecting range	Caution	OK	OK
Metal objects within view of detector	OK	X	OK
Movement of large, steel garage doors	Caution	X	OK
Sensitivity to small animals	Caution	Caution	OK
Water movement in plastic drain pipes	OK	X	OK
Movement on other side of glass	OK	X	OK
Sunlight or sources of white light	X	OK	OK
Heaters	X	OK	OK
Moving machinery, fan blades	OK	Caution	OK
Radio interference or induction from high-voltage wires	Caution	Caution	OK

Photoelectric beam detectors

Photoelectric beam (photobeam) detectors are the oldest type of space protection in use. They are suitable for use both indoors and out, and unlike other detectors described here, the detection pattern of photobeams is consistent and easy to keep away from hazards. Compared to PIRs, they are more expensive and time-consuming to install; nevertheless, photobeams are still widely used today in outdoor and long-range installations.

Photobeams have two parts: the transmitter and the receiver. The basic operating principle is that a beam of light emitted by the transmitter is directed toward the receiver. As long as the receiver sees the beam from the transmitter, the system will be secure. If the path between the transmitter and receiver is blocked, the beam will be interrupted and the receiver will activate an output. Figure 13 shows a photobeam system at work.

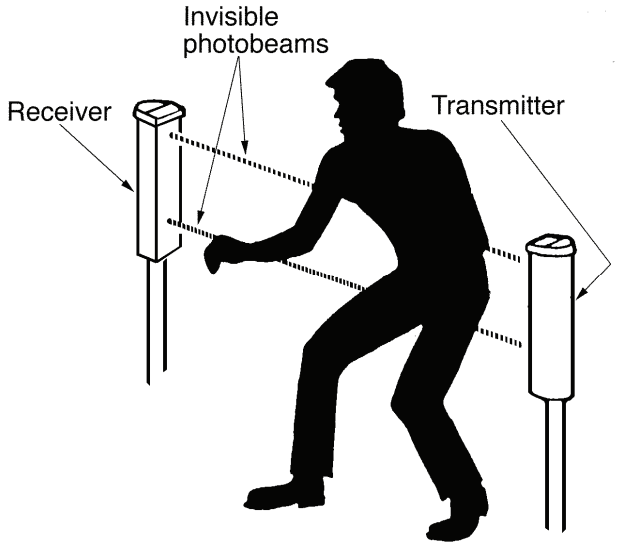

Figure 13—Photobeam system

Modern photobeam systems use infrared light as the beam. These IR beams are invisible to the human eye, which makes them easily hidden. An IR transmitter, similar to an ordinary LED except that it emits light in the infrared region, is directed toward the receiver. A pyroelectric element in the receiver reacts to the IR beam and produces a small amount of emf. The voltage signal is amplified and analyzed by electronic circuits, and an output relay is controlled by logic circuits.

To ensure that the IR receiver is not fooled by IR energy from other sources, the beam is pulsed in a coded pattern. The receiver ignores low levels of IR energy from normal sources. But if the receiver detects high levels of IR that do not carry the coded signature (such as deliberate attempts at tampering), an alarm will be generated.

Some photobeam systems have the transmitter and receiver incorporated into a single unit with a reflector used to bounce the beam back. Although this system eliminates the need to run conductors to two separate locations, the range of the beam is divided by half, and it is possible to defeat the system by introducing another reflector.

Photobeams are not affected by ambient conditions outside the beam and would be suitable to protect areas too hazardous for PIRs. In addition, photobeams are available with ranges of up to 2 km; few PIRs are capable of protecting more than 30 m. A further benefit of using photobeams is that the protection is supervised. If the beam becomes blocked during the day, it would stay in an alarm condition and would not allow the user to arm the system without correcting the fault.

For most installations, PIRs are superior to photobeams in many ways. Photobeams take longer to install than PIRs, because both the transmitter and receiver must be located, mounted and wired to the alarm system. Setting up a photobeam system usually takes more time and effort than simply walk-testing a PIR. Photobeams are less cost-effective if you remember that a PIR protects almost the entire volume of a room, while photobeams are strictly line-of-sight detectors.

Glassbreak detectors

A glassbreak detector is a device that reacts to the breakage of glass (such as a window in a protected premise) and causes an alarm condition on the protective circuit of an alarm system. Over the years, many methods of glassbreak detection have been tried. The earliest, window foil, is simply a lead conductor applied directly to the window. The conductor is part of the protective circuit; if the window breaks, it interrupts the flow of current and causes an alarm.

Glassbreak detectors are used on glass windows wherever perimeter protection (with its advantages of early warning) is desired. Both opening and fixed windows may use the same form of protection. In many cases, glassbreak detectors provide deterrence, since the detectors are usually visible from the outside of a building.

There are two main types of glassbreak detectors:

- Audio detectors
- Shock sensors

Audio detectors

Also called *audio discriminators* and *audio switches*, audio detectors operate by "listening" for the sound of breaking glass. A piezoelectric crystal transducer in the detector converts sound energy into an electrical signal. This signal is analyzed; if it matches the frequencies produced by broken glass, then an output is produced.

Newer microprocessor-based audio detectors have the ability to analyze not only the frequency of a sound but also its suddenness and duration. This feature dramatically increases the reliability of audio detectors, and they have become more popular in recent years as a result.

Audio detectors may be either frame-mount, which are meant to be mounted close to the glass, or ceiling-mount, which are designed to mount on the ceiling or wall away from the glass.

Probably the biggest advantage to using audio detectors is their ability to protect large areas. A typical ceiling-mount audio detector may have a range of 10 m, at angles of up to 90°. Several windows (either on the same wall or on perpendicular walls) or multiple-pane windows are all easily protected using a single detector.

As with any audio device, the acoustics of the room will affect the operation of audio detectors. Enclosed rooms or areas with hard reflective surfaces will cause the sound waves to echo and result in an increase in sensitivity. Large, open areas or soft surfaces such as carpets and drapes will absorb the sound waves and decrease sensitivity. As most audio detectors are not equipped with sensitivity adjustments, the detector should be mounted close to the window in order to detect a break.

Most detectors are limited in the size of window they will adequately protect. A frame-mount detector might not be close enough to a break on a large plate glass window. Small windows may not generate enough sound energy to trip a detector. Also note that audio detectors will not detect an intrusion through plexiglass, since it is a form of plastic and does not emit the characteristic sound frequencies when broken.

Although modern audio detectors have a greater ability to recognize the sound of glass breaking, many sources of noise can still cause false alarms. Sources of problems are:

- High-pitched squeaks
- Pet stores (animal noises are often a problem)
- Metal impacting or scraping on metal
- High-volume sounds (from stereo stores, factories, etc.)
- Kitchen noises (dropped plate, etc.)

Shock sensors

Shock sensors incorporating a variety of different technologies have been used for many years. Shock sensors are also used to detect forced intrusion through walls and ceilings; many models are designed specifically for such use. Although each model differs slightly, most early types consisted of metal contacts that vibrated or touched when a window was broken.

Modern shock sensors operate in a very similar way to audio detectors. A shock sensor is designed to detect shock waves generated by an intruder, that move through the glass or frame as a window is broken. A piezoelectric crystal acts as a microphone to convert mechanical energy into electrical energy.

A microprocessor in the unit analyzes the electrical signal to determine the nature of the shock wave. Like audio detectors, shock sensors look for waves with specific frequencies, duration and amplitude. It is the presence of these characteristics that distinguishes the wave as being caused by glass breaking and not by other sources.

Although modern shock sensors are reliable in operation, there are some environmental hazards that limit their use or may cause false alarms. Since the piezoelectric crystals react to movement, shock sensors should be used carefully in areas subject to excessive vibrations. Loose panes of glass should be secured before shock sensors are applied. Small glass panes (10 cm or less) may not generate strong enough shock waves to trigger many shock sensors, in which case other forms of protection should be considered.

Control panel functions

Perhaps the single most-difficult component to install in an alarm system is the control panel. This is because modern microprocessor technology allows for more power and flexibility than ever before, with a resulting increase in complexity of installation and programming.

Almost every alarm control panel on the market incorporates a computer into its circuits, meaning that the installer must also be a programmer. In order to successfully program an alarm control panel, installers must sort through a wide range of options and features, and they must understand the terminology.

The control panel reacts to changes in current on the detection circuit and provides outputs to various devices. Most modern alarm panels are able to monitor the status of many zones of detection, each of which consists of a loop and one or more detection devices. Panels with 4, 8 and 16 zones are common.

In order that the separate zone loops may be connected, the control panel must have terminals for the conductors. Screw terminals are usually mounted on the printed circuit board.

A microprocessor performs the complicated switching and logic functions required. Modern controls also contain the ability to store programmed instructions on a single integrated circuit (IC) chip. These instructions tell the processor how to operate as an alarm system, and are programmed by the manufacturer. The program may be customized by the installer, who selects options from a list found in the panel's programming manual.

The program is stored on a memory IC called an *EEPROM,* for Electrically Erasable Programmable Read-Only Memory. EEPROMs use MOSFET technology to store binary-coded instructions in memory cells. If changes to the program are required, the memory cell is simply overwritten. EEPROM chips have the advantage of being able to hold stored memory even when power is removed from the circuit.

The control panel is encased in a metal box that protects the printed circuit board and allows room for a rechargeable standby battery in case AC power is interrupted.

Although the installer may spend a lot of time wiring and programming at the panel, from the point of view of the end user, most of the action occurs at the keypad. This is a flat, usually plastic box that features light-emitting diodes (LEDs) and a telephone-like number pad (Figure 14). The keypad is usually mounted on a wall near the designated entry/exit door of a building. The keypads available vary in cost, appearance and features offered, but they all work in similar ways.

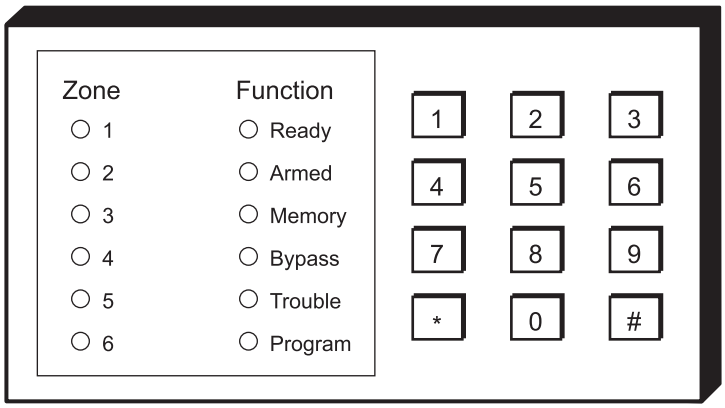

Figure 14—Typical LED keypad

LEDs on the keypad supply the user with information about the status of the system. Common LEDs are:

Loop status

A loop status LED indicates that a particular zone is in alarm. Usually a single LED is used for each zone of a multiple-zone system, allowing the user to see at a glance the state of all 8 or 16 zones.

Ready status

A ready status LED indicates when all zones are secure. Since most alarms may not be armed if a zone is insecure, the ready indicator is useful for the user to observe as a first step before attempting to arm the panel.

Armed status

An armed status LED indicates when the panel is armed or activated.

Arming the control panel is a matter of ensuring that the ready status LED is on (and all zone status LEDs are off), by punching in a valid numerical arm/disarm code. This is usually a four-digit or five-digit number that may be programmed by the installer and/or the user. Most control panels are capable of recognizing more than one arm/disarm code.

Upon arming the panel, the armed status LED will light, and the panel will begin counting a preprogrammed exit delay. During this period, no alarms can be generated and the user may exit the building. Most systems allow 30 to 45 seconds of exit delay time.

In addition to the basic arm/disarm function, most alarm panels offer more advanced features as follows

Zone bypass

Zone bypass enables the user to selectively bypass or disable one or more zones. This is useful when arming the system while people are still inside the building. Zones with motion detectors may be bypassed before arming the system, to allow free movement inside the building without setting off alarms. When the panel is disarmed again, any bypassed zones will return to normal operation.

System trouble

Most control panels perform diagnostic self-tests that display on the keypad and indicate the nature of a problem. Blown fuses, output circuit failures, loss of AC power and low standby battery are examples of common system trouble indications.

Alarm memory

With alarm memory, the user may display the zone or zones that initiated the most recent alarm activation. Some advanced systems are capable of remembering more than a single event; one popular control panel holds information relating to up to 150 separate events, including alarms and arm/disarm occurrences.

The most powerful feature of any alarm system is its ability to communicate alarm events to an offsite location known as a *monitoring station*. Most control panels have integrated into their circuitry a communicator, known as a *digital dialer*, that can transmit alarms to digital receivers using existing telephone lines. A digital dialer acts like an automatic telephone, calling a preprogrammed phone number and transmitting digital codes that are interpreted by a digital receiver in the monitoring station. The alarm codes are different for each zone or type of alarm reported, enabling human operators to dispatch the correct emergency response.

Installing an alarm dialer onto a telephone line requires the use of a special connection jack, called a *Jack 8*, that gives the dialer priority over other phones using the same line.

Many other monitoring technologies are used to allow alarm systems to communicate with monitoring stations. The most important factor to consider when deciding which monitoring technology to use is that of line security. Communicators range in line security from the digital dialer, which is inexpensive but has low security, to DVACS, a modem-like transmission medium that is virtually impossible to defeat by tampering with the line. Other alternatives for the alarm installer include cellular telephone and long-range radio transmission, both of which provide monitoring without hard-wired lines.

 Now do Self-Test 1 and check your answers.

Self-Test 1

1. List five purposes of total security systems.

2. What is the "onion-skin" principle?

3. What are the three layers of protection of an alarm system?

4. What are the three main circuits in a basic alarm system?

5. When a closed-loop detection circuit has current flowing through it, is it in the "alarm" or the "secure" condition?

6. What is circuit supervision?

7. What are the four loop types?

8. Why is it important to avoid even minor damage to magnetic reed switches?

9. What does a PIR detector detect?

10. List three advantages of PIR detectors.

11. How do ultrasonic and microwave detectors detect movement?

12. List three sources of false alarms for ultrasonic detectors.

13. What advantages do dual-technology detectors have over single-technology detectors?

14. Under what conditions would a photoelectric beam detector be suitable?

15. What indication LEDs are commonly found on alarm keypads?

16. What does it mean to "bypass" an alarm zone?

17. What part of the control panel allows direct communication with a monitoring station?

Go to the Answer Key at the end of the Learning Guide to check your answers.

Answer Key

Self-Test 1

1. • Deterrence
   • Prevention
   • Detection
   • Response
   • Apprehension

2. A concept in security planning that employs successive layers of protection.

3. • Perimeter protection
   • Space protection
   • Spot protection

4. • The detection circuit
   • The control circuit
   • The output circuit

5. the secure condition

6. the ability of the control panel to monitor if a loop is intact or not

7. • Two-wire
   • Two-wire ELR
   • Four-wire
   • Four-wire ULC

8. To prevent the introduction of oxygen and water vapour inside the glass tube.

9. changes in the levels of infrared energy within the protected area

10. Any three of the following:
    • They are self-adjusting.
    • They are relatively foolproof to install.

- They are passive detectors and do not emit radiation.
- The detection pattern may be changed by replacing the lens.
- The detection fingers may be easily masked to avoid problems.

11. They emit radiation, which is reflected off objects within the protected area. If an object is moving, it will cause a doppler shift in the reflected signal, and the detector will notice a change in frequency.

12.
- High-pitched noises
- Moving or rotating objects
- Changes in air humidity

13. Dual-technology detectors are more resistant to false alarms, since they are more stable in areas with harsh ambient conditions.

14. Photoelectric beam detectors are useful in areas where ambient conditions (such as temperature fluctuations, humidity, radio interference, sunlight or direct light sources etc.) render other detectors unsuitable.

15. loop status, ready status and armed status

16. Bypassing a zone means to deactivate it during the time the control panel is armed.

17. the digital dialer

ISBN 978-0-7726-6794-6