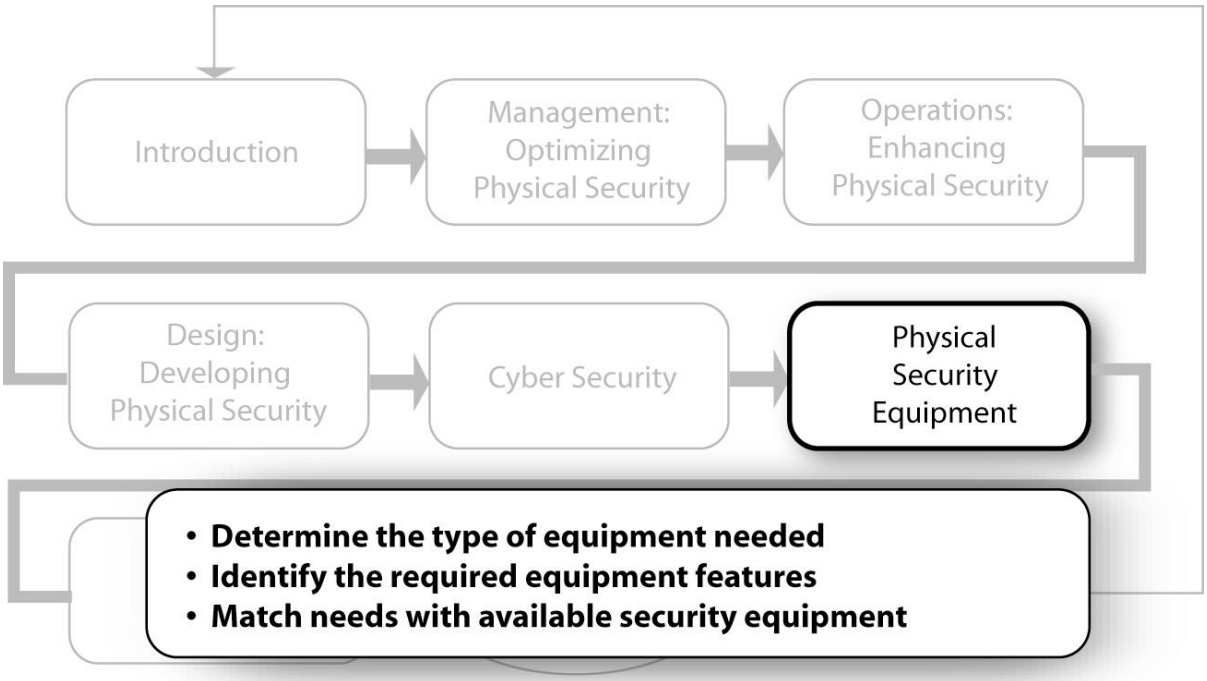
SECTION 6

Choosing the Optimal Physical Security Equipment



6.1 Overview

The previous sections of this document identified applications for which utilities may want to purchase and install electric and electronic security devices. Utilities should base their decisions on their DBTs, as well as other operational and design considerations.

A variety of security systems and components are commercially available. Before implementing a security system, it is important to understand the characteristics and requirements of the area and facility to be protected. With this understanding in hand, detailed criteria can be developed to specify exactly how the security system should be implemented.

This section provides an overview of issues and situations that should be considered, as well as basic information, when determining the type of electric or electronic security system to install once the decision has been made that such a system will be employed. Included are descriptions of three major categories of security equipment: intrusion detection systems (both interior and exterior), access control (card reader) systems, and closed-circuit surveillance camera systems. Each of these sections provides information on recommended security devices, including interior and exterior intrusion detection systems, card readers, biometric readers, camera lens and equipment requirements, digital

video recording and CCTV compression. Lighting, power, and security wiring standards are also discussed.

6.2 Questions to Ask

To determine the type of security system to install, it is important to understand the characteristics of the area to be protected, as well as the security expectations and requirements. This section describes the information that should be obtained and questions that should be asked to help utilities plan and implement a security system.

6.2.1 Threat

The types of security equipment employed will be dependent on the utility's DBT. Questions to consider include:

- Is the anticipated adversary an outsider, an insider, or an outsider collaborating with an insider?
- What tactics, motivation, skills, knowledge, tools, or weapons might the adversary use? Protecting a facility from a skilled, trained adversary with knowledge of the facility requires a different tactic than protecting against a teen-aged vandal.

6.2.2 Known Vulnerabilities and Key Assets

A utility's vulnerability assessment identifies the assets that are most critical to meeting its mission. The types of assets to be protected influence the types of equipment recommended to protect them.

6.2.3 Areas of Coverage

The characteristics of the area that the equipment will be expected to cover are critical factors that need to be taken into account. Questions to consider include:

- What is the area or region to be protected?
- Does the area occupy a level surface?
- Is the area enclosed? Is the area indoors or outdoors? Indoor areas typically have lower nuisance alarm rates and are easier to protect.
- If indoors, what ambient noise levels, thermal conditions, or vibrations may exist?
- If outdoors, what humidity, temperature conditions, and wind conditions exist?
- Are small animals or children living near the protected space?
- How large is the area?
- What is the configuration and physical layout of the area to be protected?
- What are the existing lighting conditions within the area?
- Are there any restrictions that limit placement or levels of site lighting, such as neighborhood zoning requirements?

- Are the assets visible from the perimeter fence or property line?

6.2.4 Levels of Resolution

To accurately specify the required security hardware, it is important to define the required level of resolution that the security system must achieve: detection, classification, or identification.

- **Detection.** The capability to determine the presence of an intruder (but not necessarily classify as a human, animal, or object).
- **Classification.** The capability to determine the classification of an intruder as human.
- **Identification.** The capability to determine the identity of a human intruder.

6.2.5 System Size and Device Quantity

Before selecting equipment, it is also important for a utility to think about the size of the area that it wants to cover and the number of devices it will need. Understanding the potential growth of the water system also allows the designer to provide a security system that scales with a minimum of cost and effort as the system size and requirements expand.

6.2.6 Electrical Power, Wiring, and Transmission Methods

Availability of electrical power will also influence selection of security devices. Questions to consider include:

- What electrical power is available for the security hardware, if any?
- What backup power is provided for security?
- Are lightning strikes a consideration? Is a lightning protection system advisable for new electronic equipment?
- Will all wiring be protected within conduit?
- How are alarm signals transmitted back to a monitoring system?
- Will hardwired systems be used or are wireless communication methods being considered?
- What bandwidth is available for transmitting security alarms and video images? For example, dial-up telephone modems or radio telemetry systems provide limited bandwidth for transmitting video images, whereas high bandwidth broadband connections allow higher rates of transmission and smoother video image playback.

6.2.7 Viewing and Assessment

Utilities also need to consider how information transmitted by security devices will be used. Approaches to viewing and assessing camera images and responding to alarms should be part of the criteria when making decisions on equipment selection. Questions for consideration include:

- What areas need surveillance? What camera surveillance systems may be required? Is there a need to have CCTV camera coverage at the entire site perimeter?

- What monitoring system is in place to receive the alarms: a SCADA system or a separate intrusion detection system? For example, it is advisable to separate SCADA from security alarms whenever possible so that an adversary cannot disable both simultaneously.
- Who will monitor the alarms? Will the system be monitored on a continuous basis, or as alarms come in?
- Who will view the security alarms and assess them?
- Where is the monitoring system located?
- What is the security response once an alarm occurs?
- Is the response onsite or offsite?
- What is the response time?

6.3 Basic Information About Physical Security Equipment

Before determining the type of physical security system that would be the best for a utility, it is important to understand the basic components, features, and requirements on which a utility will have to decide.

6.3.1 Power and Wiring

Without a reliable power source and intact wiring, a security system cannot function. Indeed, cutting the power to a security device may be an adversary's first course of action. Recommendations for reliable power and security wiring are presented here.

6.3.1.1 Power Supplies

Typically a security system includes items that require 120 Vac (volts alternating current) power and low-voltage (12 Vac, 24 Vdc [volts direct current]) power. If an auxiliary power supply is included for supplying low-voltage power, be sure that calculations are performed on the load and voltage drop of the system. Load and voltage drop should meet the following criteria:

- The power supply should be loaded to no greater than 75 percent of capacity to allow for future expansion.
- Worst-case voltage drop should be no greater than 10 percent for the longest length low-voltage circuit from power supply to device.

6.3.1.2 Lightning Protection

In many parts of the country, a lighting protection system is essential for the protection of electronic devices. The goal of a lighting protection system is to:

- Limit step or contact voltage and induced voltage.
- Limit fire propagation.
- Reduce the effect of surges on sensitive equipment.

Typically, a lightning protection system utilizes a separate grounding system that is tied to the facility ground system. Consider the following when planning for a lightning protection system:

- Coordination is required with roofing, parapet, and interior building design to allow for installation of air terminal or riser cables.
- Criteria for lightning protection may involve the utility's insurance company.

For more specific information, refer to NFPA 780, Standard for the Installation of Lightning Protection Systems.

6.3.1.3 Power Backup

For all electronic components of the security system, some method of power backup is recommended. With automatic generator-backed systems, if normal alternating current (AC) power fails, there is a 5- to 10-second lag before the generator backup engages. With manual systems this time period can be much longer.

Some basic backup power considerations are as follows:

- UPS systems are recommended for security devices requiring 120 Vac power, such as computers and video monitors.
- Batteries are cost-effective and reliable for low-voltage devices, such as cameras and card reader systems. Provide automatic charging means to automatically maintain battery charge under normal power conditions.
- Battery recharge circuits should automatically recharge batteries within 24 hours after the batteries have been discharged.
- Modular battery backup systems provide an advantage because they may be expanded by simply adding more components and batteries. As backup power requirements increase, the battery system capacity can be adjusted to meet current needs.
- When considering UPS systems, compare the cost and flexibility of using smaller point-of-use UPS units against a large system-wide UPS. In some cases, greater flexibility and cost-effectiveness may be achieved using point-of-use UPS units. Additionally, the cost of maintaining a spare point-of-use UPS unit is much lower then providing a redundant system-wide standby UPS unit.

Tips for Small Utilities

Consider using battery backup and a small self-charging UPS for backup power to smaller security installations.

6.3.1.4 Security Wiring

Basic

- All interconnecting wiring between security system components should be monitored for integrity so that an abnormal condition (e.g., wire-to-wire short, wire break, or wire ground-fault condition) is automatically indicated when arming the system.
- Coaxial cable RG-59U, the most common coaxial cable style is rated for up to 750 feet. Use fiber-optic cable for CCTV runs farther than 750 feet.

Advanced

- Fiber optic cable offers several advantages over coaxial cable; it is impervious to electromagnetic interference, radio frequency interference and offers good security against eavesdropping. For new CCTV installations, fiber is recommended over coaxial cable, except for very short runs (under 50 feet).

6.3.1.5 Sample System Performance Criteria

Utilities may want to consider including performance standards such as these when determining the type of basic physical security system to purchase and install:

- Four-hour battery backup, at a minimum, should be provided for security equipment.
- All exposed security wiring should be installed in conduit.
- No splices or wire nuts should be used within wiring circuits. All wiring terminations should be made via mechanical termination blocks.
- All wiring shall comply with the NFPA 70, National Electrical Code, specifically Articles 725 and 800, as appropriate.
- Security panels shall be UL listed as meeting standard UL804.

6.3.2 Visibility and Lighting Recommendations

Visibility and lighting are critical elements of a successful security system.

6.3.2.1 Visibility

Within a parking lot, trees and shrubs should not obstruct viewing. Tree branches and leaves should not be lower than 10 feet above the lot surface. Interior shrubs and bushes should not be higher than 18 inches so as not to obstruct vision or conceal an adversary.

6.3.2.2 Lighting

A significant part of visibility is lighting. Lighting should enable people parking to note individuals at night at a distance of 75 feet or more and to identify a human face at about 33 feet. These are distances that will allow them, if necessary, to avoid the individuals or take defensive action while still at a safe distance.

Security lighting increases the effectiveness of guard forces and closed circuit television by increasing the visual range of the guards or CCTV during periods of darkness. It also provides increased illumination of an area where natural light does not reach or is insufficient. Lighting also has value as a deterrent to individuals looking for an opportunity to commit crime. Normally, security lighting requires less intensity than lighting in working areas. An exception is at normal doorways.

Exterior lighting for areas such as parking lots should provide a minimum level of visibility when guards perform inspection of the protected area. Guards and CCTV surveillance systems must be able to:

- see badges, people, and other guards at gates
- observe activity
- inspect vehicles
- observe illegal entry attempts
- detect intruders in the protected area
- observe unusual or suspicious circumstances

Each parking lot presents its own particular security challenges based on physical layout, terrain, atmospheric conditions, and security requirements. The goals of direct illumination are to provide a specified intensity throughout the area for support of guard forces or CCTV, provide good visibility for customers or employees, and have a minimum of glare.

The most severe problem is illuminating the small narrow "corridors" formed by adjacent parked cars. To get light into these areas, it is recommended that any point in the entire parking lot be provided with illumination from at least two and preferably four lighting (pole) locations. The lights should be mounted at a minimum height of 20 feet.

6.3.2.3 Example System Performance Criteria

- Provide lighting that is a minimum of 0.2 foot-candles around key assets for observation by unaided eye.
- Provide minimum of 1 foot-candle (the average maintained horizontal to the surface) for self-parking areas.
- Lighting at entry and exit points should be at least 1.5 to 2.0 foot-candles for safety and for adequate observation by employees or CCTV.
- Two foot-candles of lighting should be provided for attendant parking areas because of liability and potential damage to automobiles.
- Where additional lighting for business attractions or customer convenience is a consideration, lighting of 5.0 foot-candles and higher is often used.
- The light-to-dark ratio should be designed such that the lowest value of illumination on the pavement is not less than one-fourth of the recommended average (a 4:1 light-to-dark ratio). The lighting should be maintained at no worse than 6:1.
- RP-20-98, Lighting for Parking Facilities, published by the Illumination Engineering Society of North America (IESNA), provides recommended illumination levels for parking facilities.

Tips for Small Utilities

Low-pressure sodium lights are reasonably efficient and provide a uniform lighting ratio.

6.4 Types of Physical Security Equipment

Once the utility understands the characteristics of the area to be protected and the security expectations and requirements (as described in the previous section), the utility can determine the type of security equipment to use. There are many different types of security equipment. These types include:

- Access control systems (card readers, PIN access, and biometrics)
- Intrusion detection (interior and exterior)
- CCTV surveillance

Each of these types of security equipment is described in this section.

6.4.1 Access Control

An access control system allows the movement of authorized personnel and material into and out of facilities while detecting and possibly delaying movement of unauthorized personnel or contraband. Entry control elements may be found at a facility boundary or perimeter, such as at vehicle gates, building entry points, or doors into rooms or other special areas within a building.

Access control systems make a verification decision and then determine whether to grant or deny access to a person. This verification decision is usually based on determining whether the person:

- carries a valid credential, such as an access card.
- knows a valid PIN.
- possesses the proper unique physical characteristic that matches the person's characteristic recorded at enrollment. This is called biometrics and includes characteristics such as a fingerprint or hand geometry.

These three concepts, from basic to advanced, can be thought of as "what you have," "what you know," and "what you are."

6.4.1.1 Credentials (Access Card Types)—What You Have

There are a number of different types of credentials (or access cards) used in personnel access control, including photo identification, exchange, stored-image badges, and coded credentials. There are many techniques available for coding a badge or card. The most common techniques include magnetic stripe, bar codes, proximity, and smart cards. The most commonly used card readers are magnetic stripe or proximity technology.

Card reader access control systems provide the most reliable, flexible method of controlling access to a

Tips for Small Utilities

Single door card reader systems are available that include everything necessary to control a single door. These may be cost-effective for a small utility having few doors or staff. Also available are single-door access control systems that use a PIN for door entry but can be integrated into a networked card reader system in the future.

facility. Card reader systems come in many configurations, from stand-alone systems that control only one door to scaleable systems that can provide enterprise-wide control for an entire corporation spanning multiple continents. Newer card reader systems offer sophisticated database intelligence that allows integration with payroll, information technology, and human resources databases. If an employee is terminated, his or her access privileges can be revoked within the access control system instantaneously. Some access control systems offer seamless integration with video surveillance systems, where access control alarms and video surveillance images are displayed on common PC workstations.

As shown in Figure 6-1, the card reader system typically consists of:

- a computer server or workstation that displays alarm conditions and allows programming of the system
- a badge station, allowing creation and programming of badges
- local control panels that control the doors, card reader units, and access cards
- a printer unit that prints each event and alarm condition

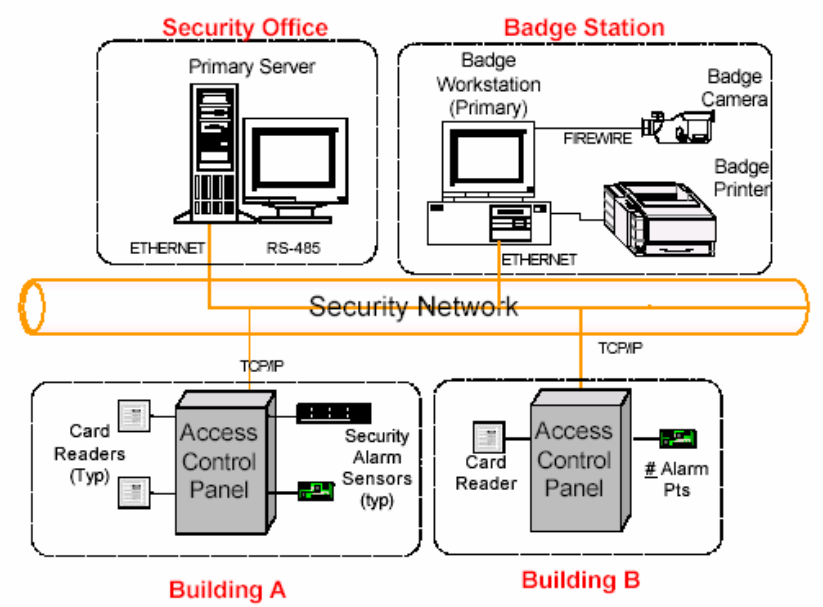


FIGURE 6-1
Typical Card Reader System

Under normal operation, the system grants access at doors with card readers by comparing the time and location of any attempted entry with information stored in memory. Access is granted only when the security card used has a valid entry code at the card reader for a designated time frame.

Significant advantages of the card reader system include the capability for event tracking and programmable software functions, such as these:

- Event tracking/event logs are lists of security events recorded by the access control system that indicate the actions performed. Each event log entry contains the time, date, and other information specific to the event.
- Two-man rule software is software programming that is optional on many card reader systems. It prevents an individual cardholder from entering a selected empty security area unless accompanied by at least one other person or exiting if only one person will remain in the area.

Once two cardholders are logged into the area, other cardholders can come and go individually as long as at least two people are in the area. Conversely, when exiting, the last two occupants of the security area must exit together.

- Anti-passback software prevents users from giving their cards to someone else to use. This feature is sometimes available with keypads. To prevent the same PIN from being used by many people, a time element can be programmed in—the PIN will not work again until that time expires. Some anti-passback systems require that if a card is used to enter an area that card must be used to exit that area before it can be used to gain access to a different or unrelated area. This feature also helps eliminate "piggy-backing" or tailgating by unauthorized persons.

6.4.1.2 PIN—What You Know

There are two primary considerations for selecting a secure PIN. First, the PIN should be long enough and have enough digits to prevent easy guessing. Second, the PIN should not be a number that is too meaningful to the individual to whom it is assigned (e.g., birthday or nickname). If a person is allowed to choose his or her own PIN, he or she should be discouraged from choosing a PIN that is too meaningful and could be easily guessed.

Some systems provide a maximum number of PIN entry attempts before disallowing the credential or generating an alarm to the central control system.

6.4.1.3 Biometrics—Who You Are

Commercial equipment is available that uses hand or finger geometry, handwriting, eye pattern, fingerprints, speech, face, and various other physical characteristics to identify an individual. When selecting or deploying biometric devices, consideration of the security objectives is required so that the optimal device is selected and that it will operate as desired.

Hand readers and fingerprint readers are the most common biometric access control applications. Fingerprint reader stations are physically smaller in size and have a lower cost than hand geometry readers. Fingerprint readers are best suited for installations with smaller user populations (such as a lab area accessed by approximately 20 people), whereas larger user populations are better served by hand geometry readers.

Not everyone can use biometric devices. Fingerprint readers have a higher false-rejection rate than do hand geometry readers. For example, a portion of the population cannot use fingerprint readers because of dry skin. Manual labor staff who routinely use their hands may have worn fingerprints or scars on their fingertips, making it difficult for effective fingerprint reading. In addition, physical changes occur with age or injury that can impact biometric reader effectiveness. In these cases, a hand geometry reader might be a more effective technology.

Training on the capabilities and limitations of the selected biometric device is essential. The procedures need to provide for the periodic update of biometric data for each person tracked by the device; enrollment of staff into a biometric reader is not a one-time action.

6.4.2 Interior Intrusion Detection

Many types of interior intrusion detection systems are in use today, including volumetric sensors and boundary penetration sensors.

6.4.2.1 Interior Volumetric Sensors

Volumetric sensors monitor an internal area to detect the presence of an intruder. There are several types of volumetric sensors, including microwave, ultrasonic, passive infrared (PIR), and dual-technology (microwave and PIR). The most commonly used are dual-technology sensors.

Dual-technology sensors use both microwave and PIR sensor circuitry within one housing. An alarm condition is generated if either the microwave or PIR sensor generates an alarm condition. In some dual-technology sensors, alarm settings may be adjusted to require that both the microwave and the PIR unit detect an intruder presence before an alarm condition is generated.

Tip for Small Utilities

Designs for smaller utilities might consider an exterior door contact(s) and interior dual-technology sensor connected to a SCADA alarm point.

Dual-technology sensors have some drawbacks; for example, the PIR channel is relatively vulnerable. An elusive burglar may use an infrared emission-blocking cloak or screen to camouflage his infrared radiation. In addition, in hot climates when air-conditioning is off, there is a serious problem of misdetection with high ambient temperatures. Some dual-technology sensors attempt to overcome this limitation by having installer-selectable logic, where detectors from either channel are enough to trigger an event. However, this mode is not very popular because it suffers from the false alarm weaknesses of both technologies.

6.4.2.2 Interior Boundary Penetration Sensors

Boundary penetration sensors detect the presence of an intruder across an interior boundary, such as a door, window, or hatch. The most typical boundary penetration sensors are door switches, glass-break sensors, and linear-beam sensors.

- **Door switches.** The workhorse of the security intrusion detection field, door switches include contact switches, magnetic switches, and balanced magnetic switches. These switches may be used in a variety of applications, from monitoring doors to monitoring hatches, vaults, and panel enclosures. By far, the most effective is the balanced magnetic switch. This switch has internal circuitry that resists tampering or defeat from strong magnetic fields. By comparison, standard magnetic switches have been defeated by applying a strong magnet to the exterior of the door to bypass an alarm and force the door open.
- **Glass-break sensors.** There are three basic types of glass-break sensors: acoustic sensors (listens for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feels the shock wave when glass is broken), and dual-technology sensors (senses acoustic and shock vibrations). Because glass-break sensors do not sense motion or intrusion from entering a door or hatch, the sensors should be used in conjunction with other methods (such as volumetric sensors). It is recommended that glass-break sensors not be placed directly on a glass surface.

- **Linear-beam sensors.** Also referred to as a photoelectric beam or photoelectric eye, linear-beam sensors consist of a transmitter that emits a beam of light that is invisible to the human eye and a receiver that receives the beam of light. If the beam of light is interrupted or broken by motion from an intruder, an alarm is triggered. Linear beam detectors can be surface mounted or recessed. These sensors require a straight line of sight between the transmitter and the receiver.

6.4.3 Exterior Intrusion Detection

Several types of exterior intrusion detection sensors exist and may be classified according to type, method of use, style, and mode of application. The following exterior systems are most applicable to water system applications and are listed in order from basic to advanced in the following paragraphs: freestanding sensors, buried-line sensors, and fence-mounted sensors.

6.4.3.1 Freestanding Sensors

Freestanding sensors are the most common style of exterior sensor available. Types include active infrared, PIR, microwave, and dual-technology sensors. Microwave and dual-technology detectors are frequently used as freestanding sensors.

Tips for Small Utilities

Monostatic microwave sensors work well for monitoring reservoir ladders or other small areas. The device can be aimed down a reservoir ladder toward the ground, for example. Make sure the device is rated for outdoor use before installing.

- Microwave sensors come in two styles: bistatic and monostatic. Bistatic microwave sensors use a transmitter and receiver pair. Monostatic microwave sensors use a single sensing unit that incorporates both transmitting and receiving functions. With both bistatic and monostatic sensors, the sensors operate by radiating a controlled pattern of microwave energy into the protected area. The transmitted microwave signal is received, and a base level "no intrusion" signal level is established. Motion by an intruder causes the received signal to be altered, setting off an alarm. Microwave signals pass through concrete and steel and need to be applied with care if roadways or adjacent buildings are near the area of coverage, otherwise nuisance alarms may occur. Many monostatic microwave sensors feature a cut-off circuit, which allows the sensor to be tuned to cover only a selected region to reduce nuisance alarms.
- Dual-technology sensors use a combination of PIR and microwave technology, as discussed previously.

6.4.3.2 Buried-line Sensors

Buried-line sensors include pressure/seismic sensors, magnetic field sensors, buried-ported coaxial cable, and buried fiber-optic cable sensor systems. Each of these systems relies on sensing the presence of an intruder by means of a buried cable system within the ground.

A factor that must be considered when using buried-line sensors are the presence of underground utilities. Underground utilities, such as gas, water, and sewer lines, must be sufficiently below the

detection zone, or false alarms may result. Typically, 3 feet is sufficient to prevent false and nuisance alarms. Underground electrical wires must also be considered.

Other factors also need to be considered when using a buried-line sensor. Rodents have been known to cause maintenance problems by gnawing on the sensor cables. Installations also should not be in areas where running water will either wash away the soil that buries the sensor, cause nuisance alarms during a heavy rain, or result in standing water or pooling issues.

A drawback to the buried-line sensor system is that it may have different sensitivities when buried below different surfaces. For example, if a continuous system is buried below a concrete surface as well as under a lawn, the sensitivities required for each surface may be different. A good sensitivity adjustment for concrete may be too sensitive for grass. In this case, it may be best to individually zone those areas so that the sensitivities may be adjusted for each.

6.4.3.3 Fence-mounted Cabling Sensors

With fence-mounted systems, it is critical that the fence construction be of high quality, with no loose fabric, flexing, or sagging material. The fence should also have solid foundations for posts and gates. Otherwise, nuisance alarms may occur.

Tips for Small Utilities

Fence-mounted sensor systems work well in areas without animals or passersby; otherwise nuisance alarms may result.

Several types of fence-mounted perimeter intrusion detection systems exist. These include electro-mechanical vibration sensing, coaxial strain-sensitive cable, fiber-optic strain-sensitive cable, and taut-wire systems. Two styles of fence-mounted sensors are most prevalent and are described below: coaxial and fiber-optic fence sensing.

- Coaxial strain-sensitive cable systems use a coaxial cable woven through the fabric of the fence. The coaxial cable transmits a dielectric field. As the cable moves due to strain on the fence fabric caused by climbing or cutting, the electric field changes are detected within the cable, and an alarm condition occurs.
- Coaxial strain-sensing systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. Some coaxial cable systems are susceptible to electromagnetic interference and radio frequency interference.
- Fiber-optic strain-sensitive cable systems are similar to the coaxial strain-sensitive cable systems. The fiber-optic system uses a fiber-optic cable, rather than a coaxial cable, woven through the fence fabric. Strain on the fence fabric causes micro-bending of the fiber cable, which is monitored by the control panel and generates an alarm condition.
- Fiber-optic strain-sensing systems are relatively new detection systems but have a strong following. The systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. The systems are impervious to lightning, electromagnetic interference, radio frequency interference, or other electronic signals and can be used over long distances.

Possible defeat measures include tunneling, jumping, or bridging across the fence system. Careful climbing at corner posts also may not generate sufficient vibration to generate an alarm condition.

6.4.4 CCTV Camera Systems

CCTV camera surveillance systems are integral to effective assessment of alarms. This section describes some of the requirements and components comprising a CCTV system.

As shown in Figure 6-2, a CCTV system typically consists of:

- one or more cameras
- transmission media (fiber cable, coaxial, or twisted-pair cabling)
- a monitor for viewing incoming camera images
- a matrix switcher or multiplexer that receives incoming video streams and directs them to monitors and recording equipment
- a means to record each event and alarm condition

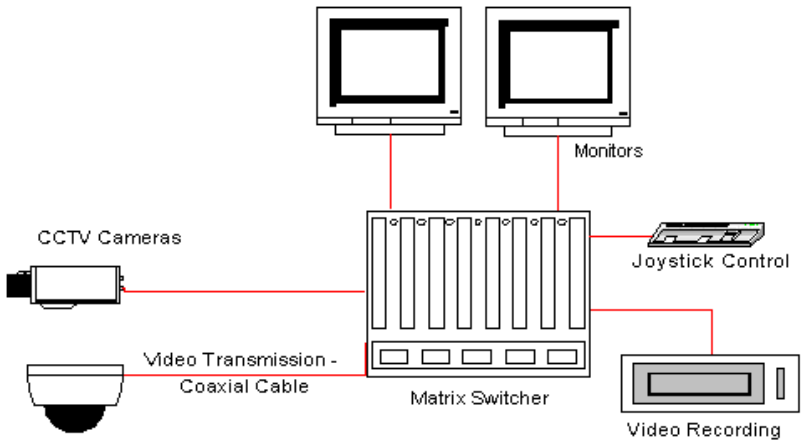


FIGURE 6-2
Typical CCTV System

6.4.4.1 Camera Characteristics

There are several key performance characteristics of a video surveillance camera. Among these are:

- Camera resolution. The amount of detail that the camera can distinguish and produce. The higher numbers indicate better resolution.
- Minimum illumination. The minimum amount of light needed for the camera to display images. For illumination, the lower the number, the better.
- Lenses. The lens size and type required for the camera.

Other important considerations of CCTV camera systems are whether the cameras are fixed-position or pan, tilt, and zoom (PTZ) cameras:

- Fixed-position camera mounts. The camera is mounted in a fixed position and cannot rotate or pan. A good application for fixed cameras is detection surveillance, because video motion detection can be more readily applied to the static field of view.

Tips For Small Utilities

Because pan/tilt cameras are three to four times the cost of comparable fixed cameras, consider using multiple fixed cameras in place of one pan/tilt camera.

- PTZ camera mounts. These camera mounts allow the camera to rotate, pan, tilt, and zoom. Because of the drive motor and housing, PTZ cameras are often four times more expensive than fixed cameras. PTZ cameras are often used for surveillance applications to view and assess alarm conditions.

6.4.4.2 Other Camera System Elements

Matrix switchers are components that provide switching capability between cameras and viewing monitors. They typically offer functionality that allows programmable settings such as camera naming, guard-tour camera sequences, and salvo switching.

Digital video recording provides a great improvement in camera image storage. Benefits include eliminating consumable media (tapes), reducing physical storage space, ease of search-and-playback functions, and the capability to add watermarks for documenting evidentiary recordings.

Video motion detection systems permit detection of entry or intrusion using video images. This new technology is based on computer algorithms that analyze the received video image and compare it to stored images in the system memory. The incoming video is analyzed for the direction of the object's movement and changes in images and background "texture."

6.4.4.3 Low-light Cameras

Several technology solutions are available to permit viewing under low light conditions, including black/white switching cameras, infrared illuminators, or thermal imaging cameras. It is important to design illumination specifically for the CCTV camera being used. The range that the camera will see in the dark depends on the sensitivity and spectral response of the camera and lens combination.

Color – black/white switching cameras. Some cameras will automatically switch from color during daytime to black/white at night, which permits viewing under low light conditions. This can be an effective solution in situations where the existing illumination levels are too low during night conditions to permit color camera use, but color camera use is desired during daytime conditions. Numerous CCTV camera manufacturers offer auto-switching black/white cameras.

Infrared Illuminators. The human eye cannot see infrared light. Most mono-CCTV cameras, however, can. Thus, invisible infrared light can be used to illuminate a scene, which allows night surveillance without the need for additional artificial lighting. Infrared also provides many other benefits above conventional lighting, including:

- IR beam-shapes that can be designed to optimize CCTV camera performance
- Extended bulb-life
- Covert surveillance, no visible lighting to alert or annoy neighbors
- Lower running costs

A number of camera manufacturers produce a variety of beam patterns, such as 10° and 30° spot (precise) illuminators and 60° flood illuminators.

Thermal imaging cameras. Thermal imaging cameras use special technology that senses heat signatures rather than visual information. These cameras operate under complete darkness. Thermal imaging cameras are best used in long-range detection and surveillance applications. Because they register a heat signature, it is not possible to resolve the identification of the adversary; instead, these cameras are best used to indicate the presence of an adversary.

6.4.4.4 CCTV Assessment

Utilities need to consider how they will assess incoming security alarms. It is particularly important to assess alarms quickly, accurately, and without compromising the entire process. Visual observation or CCTV camera surveillance is imperative for assessment. If frame-grabber technology is used (recording pre-and-post alarm video images upon alarm conditions), then CCTV assessment is simplified and can be nearly automatic.

6.4.4.5 CCTV Compression Standards

Digital images and digital video are always compressed to save space on hard disks and make transmission faster. Typically, the compression ratio is 10 to 100. An uncompressed image with a resolution of 640 x 480 pixels is approximately 600K (kilobytes) (2 bytes per pixel). Compressed 25 times, the image is approximately 25K. There are a number of common compression standards:

- Joint Photographic Experts Group, more commonly known as JPEG, is a good and very popular standard for still images that modern programs support. This is the preferred standard for many network cameras. The JPEG compression ratio is approximately 10:1.
- Motion-JPEG is a variation of JPEG where still images are shown at a high frame rate. It results in very high-quality video, but unfortunately, consists of a lot of data, with a compression ratio of approximately 20:1.
- Moving Picture Experts Group (MPEG) 2 is a standard for video. Many variations are possible, but normally MPEG 2 performs at 720 x 480 pixels, 30 frames-per-second. Only modern computers (such as Pentium III with adequate random access memory [RAM]) can decode MPEG 2, as it requires larger computing capacity. The compression ratio is approximately 20:1 or better.
- MPEG 4 is a new standard for video. It provides better performance than MPEG 2, but it is not commonly used. Compression ratios for MPEG 4 can be 200:1 or better.

6.4.4.6 CCTV System Recommendations

Consider these recommendations when purchasing a CCTV system:

- Look for ease of use.
- Investigate the scalability of the system. If more cameras are needed locally or remotely, what is the effort required to add new cameras?

- Ask the dealer if the new system or device is compatible with existing devices such as cameras, matrix switches, and multiplexers. Rewiring for new cameras and devices is labor-intensive and can be expensive.
- Understand the service plan. Manufacturers provide service and maintenance programs, and some have premier service plans that provide feature upgrades and enhancements on computer-based video recorders.
- Consider how the images will be viewed, the number of monitors needed to support the system, and how multiple camera scenes will be multiplexed onto a common monitor (not every camera requires an individual monitor).

Considerations when implementing a CCTV system include these:

- Use ample light. The most common reason for poor quality images is that the light level is too low. Generally, the more light, the better the images. With lighting levels too low, images become noisy and blurry with dull colors.
- Avoid backlight. Try to avoid bright areas in the images. Bright images might become over-exposed (bright white) and objects might appear too dark. This problem typically occurs when trying to capture an object in front of a window.
- Reduce the contrast. A camera adjusts the exposure to obtain good average light level in the image. A person in front of a white wall tends to appear too dark. If a gray wall is used instead, this problem does not exist.
- Sensor size. The lens must make an image large enough for the sensor. The larger the sensor, the more expensive the lens. A lens made for a ½-inch sensor will work for 1/2-inch, 1/3-inch, and 1/4-inch sensors, but not for a 2/3-inch sensor. If a lens made for a smaller sensor is used on a bigger sensor, the image will have black corners.
- Lens and field of view. The lens selection and alignment should be established so that a reasonable width of the alarm sector (8 to 10 yards minimum) can be seen at the near field of view. The far field of view should be no more than 45 yards wide at the far end of the alarm sector to allow at least 4.5 pixels to cover a 1-foot square target. This minimum resolution is needed to classify the intrusion source as being a person versus an animal or debris, and requires that the camera be mounted several yards outside the zone being assessed.
- Focal length. Wide-angle lenses have a better depth of field than telephoto lenses. This means that you can focus both close to the camera as well as at a distance. Telephoto lenses require a more precise focus adjustment.
- Iris. Always use auto-iris lenses for outdoor applications. The iris automatically adjusts the amount of light reaching the camera and thereby optimizes its performance. The iris also protects the image sensor from being damaged by strong sunlight. With an auto-iris lens, always set the focus in low light. If the adjustment is made in sunlight, it is very easy to focus, but then at night the iris diameter increases and the image is no longer in focus. Special dark focus filters are available that reduce the light up to ten times.

6.4.4.7 Mounting a Camera Outdoors

When mounting a camera outdoors, remember that lighting changes depending on the time of day and the weather. Because of this, consider the following for outdoor cameras:

- As discussed previously, always use auto-iris lenses with outdoor cameras.
- Use caution when mounting a camera behind glass. If you mount a camera behind glass, such as in a housing, make sure that the lens is close to the glass. If the lens is too far away from the glass, reflections from the camera and the background will appear in the image.
- The mounting height for the camera should be high enough to angle the camera down to avoid sunglare, yet low enough so that no lamps are visible in the camera field-of-view.
- Avoid direct sunlight. Direct sunlight blinds the camera and may permanently bleach the small color filters on the sensor chip, causing stripes in the image. If possible, position the camera so that it is looking in the same direction as the sun.
- When using a camera outdoors, avoid viewing too much sky. Due to the large contrast, the camera will adjust to achieve a good light level for the sky, and the interesting landscape and objects might appear too dark. One way to avoid these problems is to mount the camera high aboveground. Use a pole if needed.
- Always use sturdy mounting equipment to avoid vibrations caused by strong wind. Wood poles should NOT be used for cameras, and the use of cantilevered-arm mounts or poles is discouraged because of stability concerns in wind. Metal triangular antenna tower sections are ideal for stability.

6.4.4.8 Sample System Performance Criteria

- For cameras used to detect an intruder (that is, the capability to determine the presence of an intruder but not necessarily classify as a human, animal, or object), the area of interest should occupy a minimum of 10 percent of the field of view, with a maximum field of view of 300 feet in length or less.
- For cameras used for classification of an intruder (that is, the capability to determine the classification of an intruder as human), the area of interest should occupy a minimum of 15 to 20 percent of the field of view, with a maximum field of view of 200 feet in length or less.
- For cameras used for identification of an intruder (that is, the capability to determine the identity of a human intruder), the area of interest should occupy a minimum of 25 percent of the field of view, with a maximum field of view of 75 feet in length or less.
- Exterior cameras should have minimum resolution of 470 horizontal lines.
- Exterior cameras should be rated for use at 0.05 foot-candles.
- CCTV cameras should be listed in accordance with UL 3044, Surveillance Closed Circuit Television Equipment.

- The camera should provide adequate onsite digital recording capacity for all cameras at 30 days of continuous storage at 1 frame per second.
- CCTV equipment should have integral digital video motion detection capabilities. The system should be programmable to degree of motion, range of motion, speed, number of pixels to cause motion, and area of motion detected.
- To conserve bandwidth and storage requirements, the CCTV equipment should be capable of providing a video compression ratio of 20:1 (or better).

6.5 Summary

A variety of different security systems and components are commercially available. Before implementing a security system, it is important to understand the characteristics and requirements of the area and facility to be protected. With this understanding, detailed and specific criteria can be developed to specify exactly how the security system should be implemented.

Technology and manufacturers of security devices are rapidly changing. Therefore, web resources are useful for getting the latest information on security products. EPA has published guidance for water and wastewater utilities on security devices and equipment in the form of its Security Product Guides. This guides are kept up-to-date on EPA's web site at http://www.epa.gov/safewater/security under the Primary Topic of "Security Enhancements, Research, and Technology." At the time of writing, guides are available for security products, cyber protection products, physical asset monitoring products, and water monitoring products.