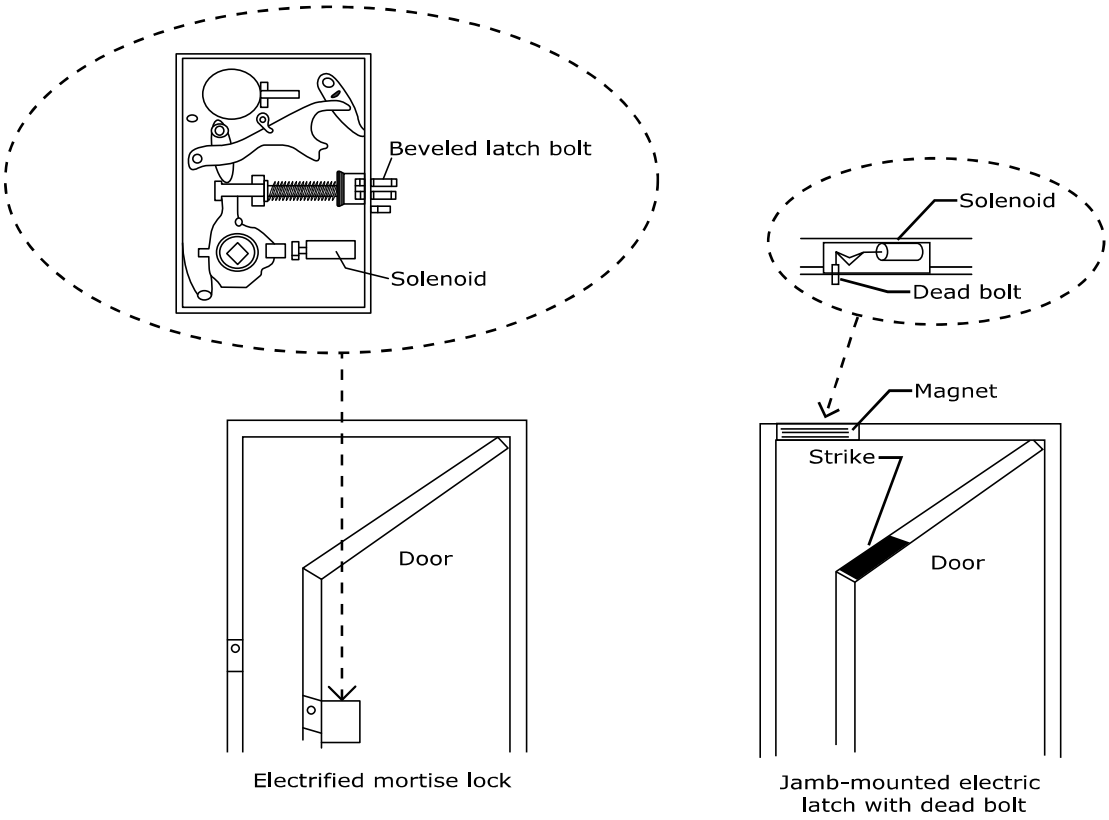
Door Release Hardware Types , continued

Figure 17.8
Electric latch and mechanical operation



Electrified Exit Hardware

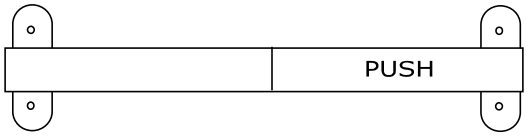
Electrified exit hardware (see Figure 17.9) is often called panic hardware. The use of panic hardware is often required in the path of egress and is common in double-door applications. Common considerations are:

- Electrified exit hardware normally requires special power supplies because of the initial power (e.g., inrush) necessary to unlock devices. The power drop concern for these devices often leads to placing the power supply near the controlled doors.
- The actuating solenoid is on the door (e.g., inside the hardware case). A power transfer from the doorframe is necessary.
- In retrofit applications, many existing models of panic devices can be electrified without purchasing new hardware. This capability eliminates altering the original hardware design. If the door is in the means of egress, then the modifications shall be listed for the intended purpose.

Door Release Hardware Types , continued

Figure 17.9
Electrified exit hardware

Powered panic egress push bar



Non-powered egress push bar

Video Surveillance

Overview

Video surveillance is the extension of human vision to areas requiring surveillance. Some primary applications of this technology include:

- Investigation.
- Prosecution.
- Deterrence.
- Observation.
- Intrusion detection.

Traditional uses of surveillance systems include:

- Operational.
- Safety.
- Security.

Privacy and Liability Considerations

ESS systems receive noticeable attention with regard to privacy rights, particularly with the increasing usage of VSS. The legalities of surveillance and privacy are rooted in case law, which varies from state to state.

A good rule of thumb in the use of video surveillance is to not apply its use in areas where a right to privacy is expected. There are variances to this rule (e.g., when the appropriate signage is posted), but if there is any doubt about privacy expectations, seek and document an informed legal opinion.

An area of concern is the inherent liability of providing video surveillance. The use of this technology implies that monitoring and response would be provided in the areas under surveillance. This information shall be kept in the forefront of the ESS system design throughout the project's life cycle.

Capture Devices

Camera Technology

In addition to traditional capture devices that operate within the visible band of the electromagnetic spectrum, other technologies provide unique viewing capabilities in other bands, including:

- IR cameras—Refers to specially designed imagers capable of seeing into the low IR bandwidth. They are sometimes referred to as starlight cameras because of their nighttime viewing capabilities.
- Thermal cameras—Captures heat or temperature values of a scene rather than light values, regardless of how bright or dark the scene appears to the human eye. Although the identification of colors and details are impossible with thermal cameras (e.g., because they only view temperature), these cameras are quite useful in viewing dark scenes for activities that have heat signatures.

Capture Devices, continued

Lenses

Video surveillance uses standard lens technologies to focus objects. Lens sizes are defined by their focal length represented in millimeters. Lens may range from ≈3 mm (0.12 in) to more than ≈101.6 mm (4 in). The larger the lens size, the more distant object the camera can focus. Lens sizes may be translated into the height and width of the viewed scene at a given distance.

Camera view is entirely dependent on the application. Camera placement should take advantage of ambient lighting and view the object at the preferred resolution and clarity. Camera placement and lens selection are based on security objectives identified through a needs assessment.

The three common types of camera lenses available are:

- Fixed lens—This lens is a specific focal length lens. Once installed, the view never changes unless the lens is replaced with a different size.
- Variable lens—This lens has an adjustable focal length (e.g., ≈3 mm [0.12 in] to ≈8 mm [0.31 in]) and is manually variable in the field. These lenses allow for post-installation adjustments of the field of view and are suitable where the view needs can change.
- Zoom lens—This lens has an integrated motor that drives an adjustable range focal length lens (e.g., ≈4.1 mm [0.16 in] to ≈41 mm [1.625 in], 12 mm [0.472 in] to ≈101.6 mm [4 in]) and may be automatically adjusted remotely from control and monitoring equipment.

Multiple lens options are also available, including:

- Iris control (e.g., manual versus automatic).
- Filters.

Mounting and Housings

Video surveillance applications include two typical types of camera mounts:

- Fixed—Refers to a camera dedicated to single view that does not change unless the camera is physically moved.
- Pan and tilt—Refers to a camera with a pan and tilt that allows for a 180 degree or 360 degree view, which is controlled electronically from a remote viewing station.

From a practical standpoint, the tradeoff between the two types is that a pan and tilt provides a more flexible area of coverage at a higher cost than a fixed camera. Pan and tilt technology allows for auto-panning where the camera moves in a predefined cycle.

Pan and tilt can be interfaced with other ESS systems so that the camera can automatically return to a preset position that is triggered by a secondary systems event.

Camera mounting locations are typically dictated by the available physical infrastructure and are balanced against the required field of views.

Capture Devices, continued

Camera mounting types include:

- Wall.
- Ceiling.
- Pole or mast.
- Parapet.
- Corner.

Mount interior cameras to clear ≈2.4 m (8 ft) AFF while exterior cameras should maintain a minimum of ≈4.6 m (15 ft). These heights are recommended to prevent intentional and accidental tampering with the camera.

Regardless of the mounting type, housings should always take into account environmental conditions and include heating and cooling measures where warranted. It is also best to ensure that mounting conceals all cable and electronics within a sealed unit.

Lighting

Camera technology has improved to an extent that minimal lighting supports image capture. Lighting designed from a safety and security standpoint should be sufficient to accommodate video surveillance needs.

If an IR illuminator is used, this device utilizes IR lamps to brighten scenes for both IR and visible band cameras.

Transmission

Wireless Transmission

Three primary types of wireless technologies are used for transmitting video signals:

- RF
- Free-space optics
- Microwave

Wireless transmission can aid in meeting the needs for rapid deployment of security surveillance devices (e.g., video surveillance cameras). These technologies may be limited to line of sight applications, requiring careful site surveys to determine potential signal obstructions.

Transmission, continued

Internet Protocol (IP) Transmission

IP-based video is accomplished by two possible methods:

- Digitization of video from an analog device and subsequent conversion to IP video
- Use of IP-based cameras

One of the advantages of IP video is its capability of integrating with existing ICT. IP video may be continuously transmitted to any point on the network, and video can be stored on network servers or storage facilities.

Digital video transported through IP can support almost any number of cameras at one time, limited only by the connection speed (e.g., bandwidth) available for the viewing device. The resolution limit may be scaled up or down, depending upon the monitor's size.

Image viewing is limited by the:

- System's features.
- User rights as determined by the administrator.
- Available network bandwidth.

Processing

Video processing switches the acquired video from the input to the selected output devices. The traditional system for the control and display of analog video surveillance is the cross-point matrix.

This system takes in a number of video surveillance camera signals and then switches these cameras to outputs for viewing and recording. Typically, the number of inputs is higher than the quantity of outputs.

Video Surveillance Matrix

The video surveillance matrix switches and distributes video signals from multiple inputs to multiple outputs. This is accomplished through a mesh architecture technology that allows an administrator or user to interface with the system to control the desired operations.

The ICT distribution designer shall evaluate the:

- Quantity of video inputs and outputs.
- System's life cycle and potential growth.
- Other considerations when selecting the capacity of the matrix.

The traditional product is available in multiples of 8 or 16 inputs and outputs.

Matrices may be connected in single large or small systems allowing for a distributed architecture and resulting in several benefits including:

- Flexibility.
- Scalability.
- Reliability.

Processing, continued

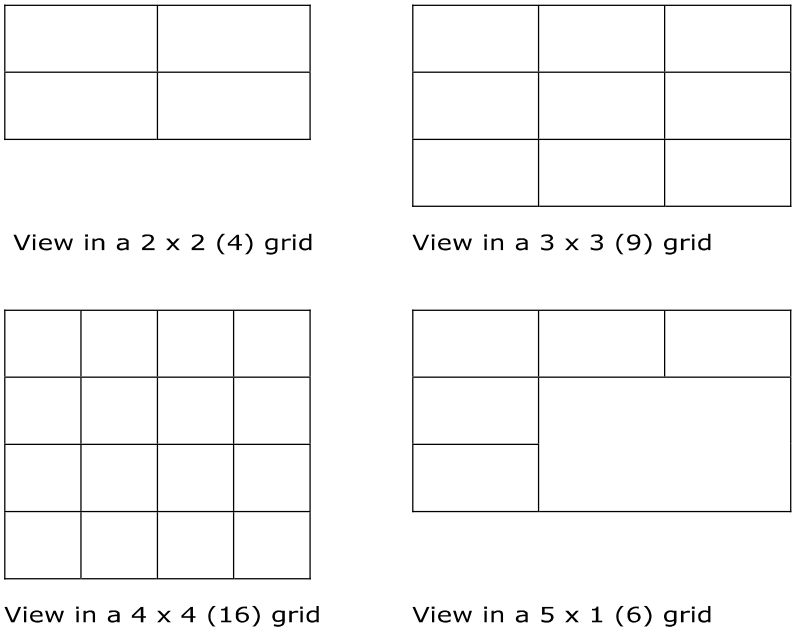
The traditional video surveillance matrix system transmits all video to the matrix at all times, regardless of whether the video is viewed or not. The digital systems, based on information technology processes, attempts to make the most efficient use of the bandwidth. The video frame rate and resolution may also be tailored to the bandwidth. These controls allow the video to share the network with other applications.

Multiview Processors

The function of the multiview processor is to take groups of video inputs and consolidate them into a single video output. The new video channel is structured to allow multiple inputs to be simultaneously displayed in a single output image.

The typical output image may consist of a grid display with multiple layouts as presented in Figure 17.10.

Figure 17.10
Grid display layouts



The ICT distribution designer should keep in mind that consolidating multiple video inputs into one video output results in lower resolution of each individual input in the grid format. To view the detail, the operator may need to display the video in a single view on a larger screen.

The ICT distribution designer should consider whether the application warrants routing the video outputs from multiview processors into a matrix as a single video input.

Digital Recording

Digital recording is the nonlinear writing of video image data to a media for the purpose of storage.

Technologies used for digital video storage include:

- Storage area networks.
- Network-attached storage.
- Redundant array of independent disks.
- Stand-alone disks and digital cards.

Analog VSS include a digital recording subsystem. This subsystem accepts analog inputs and digitizes the video. The capabilities of the units vary in both frame rate and resolution.

The current standard resolutions for National Television System Committee are:

- Common intermediate format (CIF [320 × 240]).
- 2CIF (320 × 480).
- 4CIF (640 × 480).

The traditional video surveillance camera outputs up to 470 lines of resolution; therefore, the 4CIF is close to the native camera resolution.

Digital recorders may or may not use the same frame rate as the capture device. Because of the digital nature of the information, some systems may capture frames at a high frame rate for viewing and record at a different frame rate.

The normal frame rates used are 1 fps, 3.75 fps, 7.5 fps, 15 fps, and 30 fps. The frame rate for any given application is custom to each situation, but a general rule is never to accept less than 3.75 fps.

A digital recording system also is capable of using the capture device for motion detection and altering the recording frame rates. In such an application, the system detects changes in the video frame and increases the recording rate only when motion is detected, allowing conservation of storage space. A typical recording scheme is to record motion at 7.5 or 15 fps, allowing 3.75 fps recording when no motion is detected.

Digital video recording enables retrieving and viewing video without interruptions in the recording process, scanning video for activity, and viewing cameras over LAN/wide area network connections.

Monitoring

The monitor is the human machine interface for the VSS. Monitors used for surveillance are essentially computer monitors with no tuning or audio capabilities. These video-only displays accept various forms of video input from a camera or recording device and convert the video back into a visible picture on the monitor screen.

The capability of the surveillance monitor to provide an accurate image clear to the human eye is the key to any VSS. The security guard's success is dependent on the ability to accurately observe images on the monitor.

Monitor Selection

The elements that shall be considered when selecting monitors used in a surveillance system are the:

- Number, type, and quality of monitors.
- Integration with other systems.
- Physical arrangement of monitors.
- Ability to view in multiple locations.

These factors also will influence the selection of the size and design of the monitor array. A sequencing monitor placed ≈1.83 m (6 ft) from the monitoring station, sequencing through eight cameras per minute, may not provide adequate time and image quality to detect crime or other undesired events. Video monitors are now capable of displaying video from many cameras on a single large screen at the same time.

The following factors shall be included in the monitor array design to address operator fatigue:

- Positioning of the monitors
- Distance between the monitor and the operator corresponding to the size of the monitor
- Height of the monitor's placement above the floor
- Monitor's position within the array

Considering the human factor in the monitor array design, the design almost always will provide a higher rate of visual detection.

Intrusion Detection

Overview

Both EAC and intrusion detection are considered inner defenses—when sufficient threat is present, depend on perimeter protection. The purpose of the facility determines how many layers of protection are present and at what layer sensors and alarms are used. In some military and other secure locations, the perimeter barriers contain sensors (e.g., a fence that reports the location of vibrations or distortion outside of certain acceptable limits to a local or remote monitoring station).

In some instances where a low level of security is needed, only a single layer of intrusion detection (e.g., door alarms, motion detection, glass breakage) is installed. If the purpose of alarms is to detect, deter, and ultimately delay the burglar or trespasser, then a single layer of intrusion detection decreases the likelihood that the burglars will escape without apprehension.

Each building shall be evaluated for its own unique uses, traffic pattern, hours of operation, local crime statistics, and other relevant observations. The most common points of concern are typically the outside walls, doors, and windows of the building although many times the doors and windows opening into sensitive internal areas are included in the initial assessment.

The EAC section outlines many effective types of locks that can be installed to control legitimate traffic and detect intruders. The use of locks integrated with credential readers, radio frequency identification, artificial intelligence on video surveillance systems (e.g. facial recognition systems), and even traps can further reinforce sensitive areas.

It quickly becomes obvious that the practice of detecting an intrusion can combine one or more ESS system including video surveillance, EAC systems, motion sensors, or other electronic devices. The risks and threats shall be identified and evaluated for an adequate ESS strategy to be conceived and a resulting system to be designed.

Types of Alarms

The three general types of alarms are:

- FDAS—Warn the occupants and alert a fire service that:
  - A fire is in some stage of development.
  - Flow has been detected in a sprinkler system.
  - A manual alarm has been engaged.
- Intrusion alarms—Signal the entry of an unauthorized person, sometimes under a set of variable conditions (e.g., time of day, business hours, holiday schedules).
- Special alarms—Indicate that some threshold has been reached by a sensor or electronic device. While it is not a security device, chemical, biological, radiological, nuclear, or explosive sensor raises a security alert with an alarm condition.

Types of Alarms, continued

An IDS goes into alarm mode under any of the following conditions:

- Breaking an electrical circuit
- Interrupting a light beam
- Detecting a sound
- Detecting vibration
- Detecting a change in capacitance because of penetration of an electrostatic field
- Tampering with the devices or processing controller

Intrusion alarms do not initiate countermeasures; they simply provide visual, audible, or electronic notification of the problem.

There are three common components in any alarm system:

- Sensor
- Sending circuit
- Annunciator

Sensors

The intrusion detection sensor shall detect the undesired or desired activity and alarm when certain preset conditions are met. In addition, the sensor shall perform under likely environmental conditions. If a motion detector cannot operate in temperatures less than –12 °C (10.4 °F) then it does not make sense to install that sensor in certain northern latitudes.

Available alarm sensors include:

- Electromechanical.
- Motion detection.
- Pressure.
- Photoelectric.
- Audio.
- Capacitance.
- Vibration.
- Thermal.