

Electronic Security Overview

Prepared by:



SONITROL®

Main Principles of Electronic Security

- *Intrusion Detection Systems (IDS)*
- *Access Control*
- *CCTV*
- *Fire*

A Security Plan Must Address.....

- *Prevention (Delay)*
- *Detection*
- *Assessment*
- *Response*
- *Evidence*

Prevention

- Increase *TIME* required to gain entry
 - Stronger doors
 - Protective glass
 - Better locks
 - Vaults
 - High visible security
- Perpetrator has to spend more time and effort to get at and remove property

Detection

- Reduce *TIME* required to detect intruder
 - Moveable openings
 - Volumetric protection
 - Sensitivity vs. False alarm
 - Verification = low false alarms

Assessment

- Provides additional information as to who, what and where
- People
- Alarm system assessment
 - Video
 - Audio
 - Alarm system design
 - Separate alarm zones within a building allows better determination of where activity has occurred or is occurring
 - Many alarm zones provide better definition and higher costs
 - Few zones result in low definition, but lower costs

Response

- Reduce *TIME* for authorities to arrive
 - Low false alarms
 - Verifiable information
 - Credibility with authorities
 - Apprehension
- Many police officers will not walk into an unknown situation without backup or additional “verified” information

Evidence

- Information deemed necessary to insure prosecution of an accusation
- More important today than ever before
- Authentication is important in legal cases (especially important in video)

**INTRUSION DETECTION
SYSTEMS
(Burglary Systems)**

Why Intrusion Detection?

- Provides detection of unauthorized entry into buildings
 - 108,000 buildings are broken into every year
- How can detection be provided?
 - **People**
 - 24 hour guard
 - Roving patrols
 - **Technology**
 - Sensors
 - Alarm Communication System

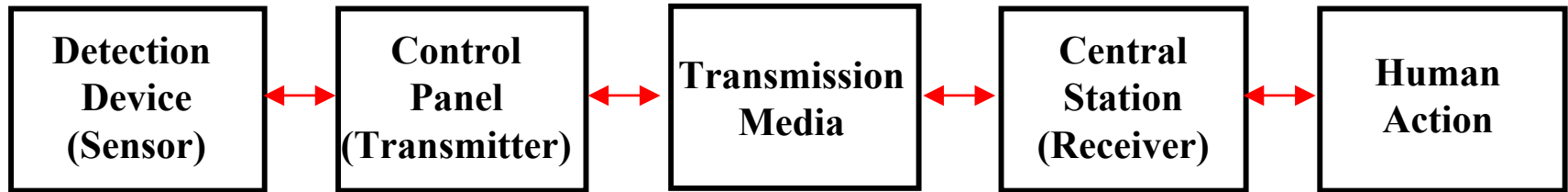
Detection and Alarm System Objectives

- Overall objective is to combat theft and vandalism during off hours
- Must be dependable and reliable
- People must have confidence in system
 - Few problems or failures
 - Problems or failures that do occur get fixed right away
 - LOW false alarm rate is very important
- A system that is known to be highly dependable and reliable will help deter some or many would-be perpetrators

Detection and Alarm System Objectives Continued..

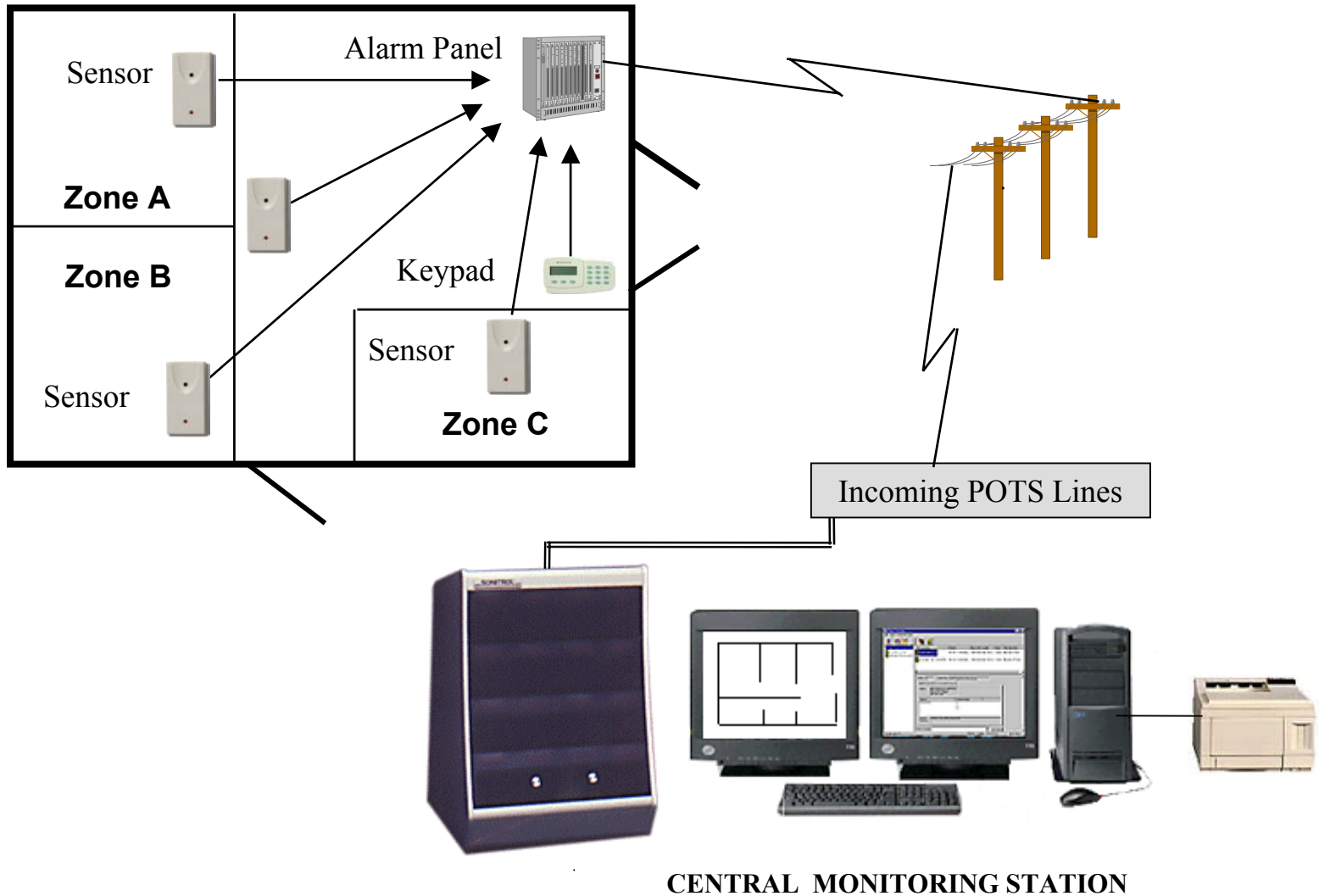
- Scare off perpetrator
 - Audible alarm - loud siren or horn
 - Some perpetrators may not leave right away
 - Need alarm communication and response
 - *NOTE*: Be aware of City noise and nuisance ordinances
- Catch perpetrator
 - Dependable, timely off-site reporting
 - Requires appropriate and quick actions by personnel at alarm reporting end
 - Response must be fast
 - Assessment and delay helps to provide information to responders and slow down perpetrator

Monitored Intrusion Detection System Requirements



NOTE: Bi-directional communication not standard in all alarm systems

Alarm, Communication and Display



CENTRAL MONITORING STATION

Alarm, Communication and Display Configurations

- Local reporting
 - Stand-alone system
 - No monitoring
 - Audible siren or horn
 - Key pad display of alarm zone status
- Off-site reporting
 - Alarm monitoring station/company
 - Normally silent alarm
 - Police response
 - Usually communicates via phone lines or cell phone
 - Includes local key pad display of alarm zone status

Electronic Sensor Application

- Designed to detect intruders at 5 points
 - **Perimeter** (surrounding complex)
 - **Exterior** (of structure)
 - **Structure** penetration
 - **Interior** (of structure)
 - **Point detection**

Sensor Technologies

- **Magnetic switches**
- **Glass break**
- **Audio**
- **Ultrasonic**
- **Passive infrared**
- **Microwave**
- **Dual technologies**
- **Photoelectric**

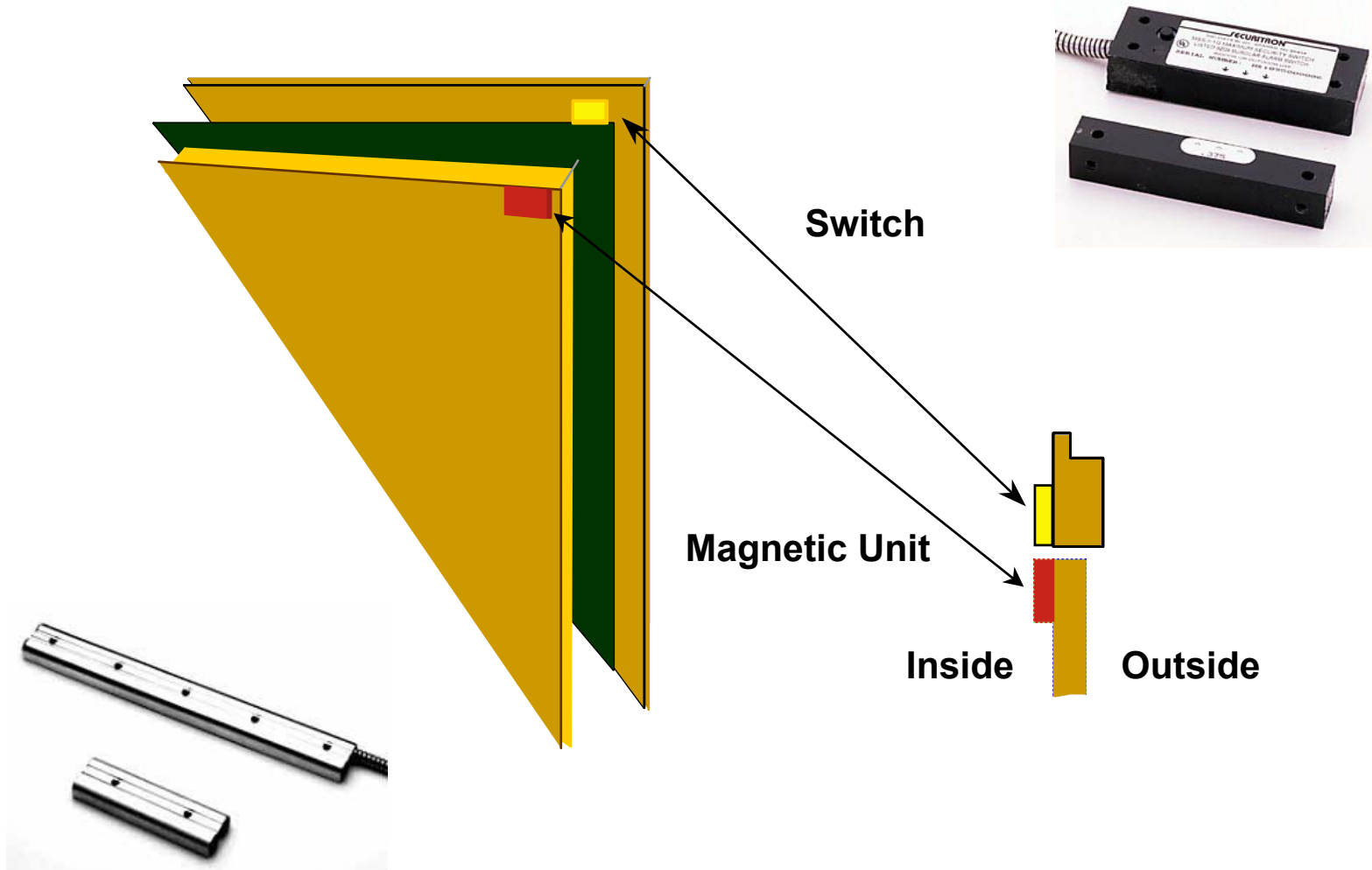


Magnetic Switches

- Installed on doors or windows to detect opening
- Must use specific switch for particular application
- Will not detect breakage of windows or holes in doors
- REACTIVE intrusion device
- **False/nuisance alarms**
 - Loose fitting or worn door hardware
 - Improper installation



Magnetic Switches



Glass Break Sensors

- Common Types
 - Frequency/Vibration
 - Look for frequency and amplitude signals
 - Acoustic (Passive Audio)
 - Provide audio listen-back
 - Dual Technology
 - Provide audio listen-back



Glass Break Sensors

- Window mounted
 - Detects vibrations or flexing of breaking glass
- Ceiling or wall mounted – dual technology acoustic
 - Detects very low frequencies associated with a blow to the glass and the high frequency audio of breaking glass
 - Curtains, blinds or other coverings need to be taken into account
- ***Typical Coverage*** – Size and type of glass coverage is usually specified by manufacturer

Audio Sensors

- Two forms of use.
 - Listen Back
 - Some other device must first activate and then the live sounds are transmitted to central station.
 - Audio Detection
 - Transmits impact activated and live audio sounds above the preset ambient level of the room.
- **PROACTIVE** intrusion device.



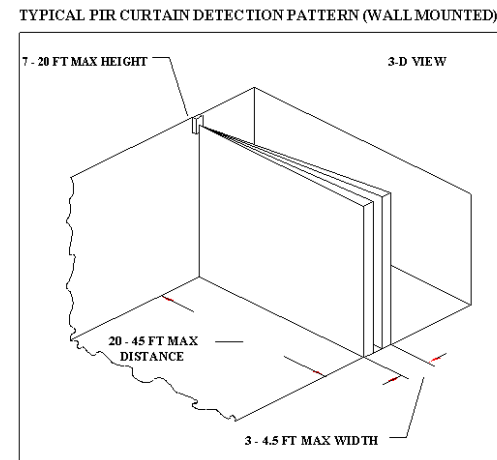
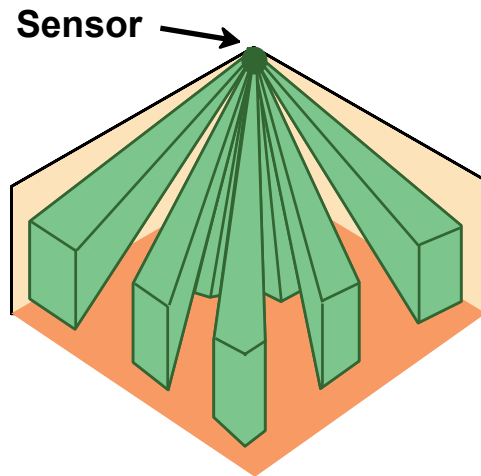
Audio Sensors

- Normally wall mounted or ceiling mounted
 - Detects and relays sounds from the protected facility
 - Environmental conditions need to be taken into account
 - Audio allows for central station *verification* of an alarm condition
- ***Typical Coverage*** – Audio coverage is omni-directional



Passive Infrared Sensors (PIR)

- Receives infrared energy from objects.
- Ceilings, walls, floors, furniture, and all other objects emit infrared energy proportionate to their temperature.
- Detection of motion is accomplished by measuring changes in the received infrared energy of the “bands or fingers”.
- **REACTIVE** intrusion device.



Passive Infrared Sensors (PIR)

- Totally passive device
- Many possible detection patterns
- Strength is detection across the finger pattern
- No interaction between multiple devices
- Sensitivity changes with room temperature
- Line-of-sight device
 - Field-of-view easily blocked
 - Caution with placement of cabinets/stock or when rearranging existing stock/fixtures



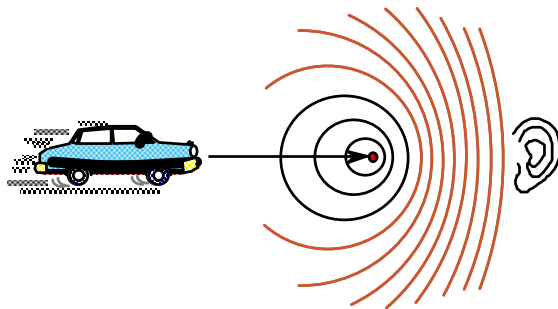
Passive Infrared Sensors (PIR)

- **False / nuisance alarms**
 - Localized heating
 - Sunlight
 - Animals (especially cats)
 - Insects
 - Sensor/mounting structure vibration
- **Typical Coverage** – Various ranges as specified by manufacturer (typical 25-50 feet)



Microwave Sensors

- A tear-shaped pattern of microwave energy is transmitted, received and monitored for changes (10ghz range)
- Intruder's motion alters microwave energy pattern/frequency.
Optimum detection - towards or away from sensor, not through the pattern
- Two sensors in same room must operate at different frequencies
- Detection based on Doppler frequency shift
- **REACTIVE** intrusion device



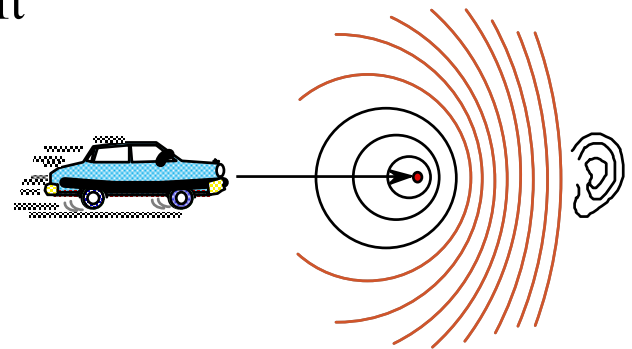
Microwave Sensors

- **False / nuisance alarms**
 - Movement of objects within and *outside* of detection zone
 - Animals/birds
 - Metal objects
 - Fluorescent lights/EMI sources
 - Sensor/mounting structure vibration
- **Typical Coverage** – Various ranges as specified by manufacturer and particular device (typical 50-100 feet)



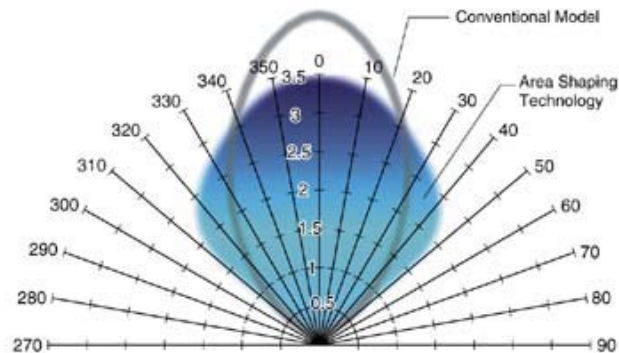
Ultrasonic Sensors

- A pattern of microwave energy is transmitted, received and monitored for changes (20 – 40 KHz range....Just above human hearing)
- Intruder's motion alters microwave energy pattern/frequency
- Detection based on Doppler frequency shift
- Not commonly used today
- **REACTIVE** intrusion device
- **False / nuisance alarms caused by:**
 - Movement of objects within detection zone
 - Heating / air conditioning ducts, drafts
 - Acoustic energy such as ringing bells, hissing noises



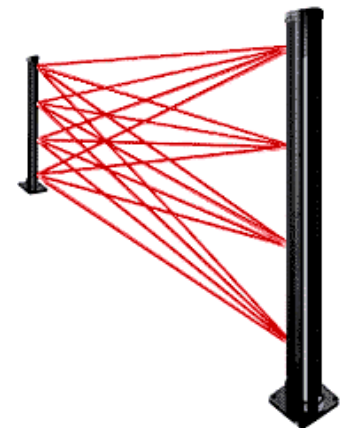
Dual Technology Motion Sensors

- Combines sensor technologies
- Most common combinations are PIR and Microwave
- Helps reduce false/nuisance alarms
- But...both technologies must trip to get an alarm (“AND” function)
- **REACTIVE** intrusion device
- *Typical Coverage* – Various ranges as specified by manufacturer and the particular device (typical 25-100 feet)



Photoelectric Sensors

- Characteristics and advantages
 - Basic configuration consists of a light transmitter and a photoelectric receiver
 - Boundary/entry protection
 - Requires line-of-sight
 - Low false alarm rate
 - False alarm sources:
 - Animals/pets, insects
- **Typical Coverage** – Long Range, typical coverage can go from 100 to 1,000 feet.



Wireless Sensors

- Wireless sensors are used today for a variety of security applications; such as panic pendants, bill traps, PIR's, door switches, temperature monitoring, smoke detectors, etc.



Wireless Sensors

- Wireless alarm systems can save on installation costs especially in older, existing buildings but additional considerations are necessary
 - Prior to installation, a thorough wireless (RF) signal testing is necessary to verify what equipment (such as repeaters) and location of equipment is necessary for reliable transmission from sensors to alarm panel
 - Batteries within wireless sensors will have to be replaced every 2-5 years depending on sensor and location
 - Supervision of the device is critical

Sensor Comparison

EVENT	Ultrasonic	PIR	Microwave	Audio
Vibration	Very few problems	Very few problems	Major problem	No Problem
Effect of Temperature change on range	Slight	Substantial	None	None
Effect of Humidity Change on range	Some	None	None	None
Reflection from large metal objects	Slight	None	Can be major problem	None
Reduction in range by drapes and carpets	Some	None	None	Adjustable
Sensitivity to overhead door movement	Needs careful placement	Very few problems	Can be a major problem	No problem
Sensitivity to small animals	Problem if animals are close to sensor	Can be aimed to be well above floor (cats jump)	Problem if animals are close to sensor	Interpretable by central station
Movement through glass walls	No problem	Needs careful placement	Needs careful placement	No problem
Drafts, air movement	Needs careful placement	No problem	No problem	No problem

Sensor Comparison Continued...

EVENT	Ultrasonic	PIR	Microwave	Audio
Sun and moving headlights through windows	No problem	Needs careful placement	No problem	No Problem
Ultrasonic noise	Can cause problems	No problem	No problem	No problem
Heaters	Problem only in extreme cases	Needs careful placement	No problem	Careful placement in noise source
Moving machinery, fan blades	Needs very careful placement	Little problem unless in field of view	Can be major problem	Careful placement in noise source
RFI or AC interference	Can be problem in severe cases	Can be problem in severe cases	Can be problem in severe cases	Can be problem in severe cases
Interference between 2 or more sensors	Must be crystal controlled or synchronized	No problem	Must be different frequencies	No problem
Radar Interference	Very few problems	Very few problems	Problem if radar close to or pointed at sensor	No problem

Important Considerations

- When considering a new system talk to a number of security companies, large and small, to get a feel for the range of systems available
- Include system performance criteria in a request for quote
- Obtain and follow up on security company references
- Funding needs to be available each year for maintenance, upgrade and eventual replacement of equipment

Important Considerations

- A new system should run for at least several weeks to verify performance before it is accepted
 - Testing of all zones and sensors should occur during this period
 - False and nuisance alarms and equipment failure data should be gathered
- Conventional and wireless systems need to be tested on a continuing basis
 - Twice per year or other determined period
 - Sensor operability and transmission to alarm panel
 - Alarm transmission to off-site monitoring station
 - Backup batteries, keypad operation

Access Control Systems

Why Access Control?

- Two biggest issues regarding security in the marketplace today
 - Internal theft
 - Workplace violence
- Industry segment growth
 - Grow approximately 11% annually
 - Approximately a \$1.2 billion in the commercial market

Statistics

- Internal theft.
 - Employee pilferage is \$5-10 billion/year.
 - An estimated 40% of business theft involves employees.
 - White collar crime is estimated at \$44 billion/year.
- Workplace violence.
 - 2 million employees victimized by workplace violence each year.

Employee Theft

- How employees look at themselves:
 - 21% - will never steal.
 - 13% - will undoubtedly attempt theft.
 - 66% - will steal if others are successful.
- A proactive security operation can have a visual impact on the two-thirds of employees who might steal.
- *Source - SDM Oct. '99 - 500 employees surveyed by Michael G. Kessler & Asso., Ltd.*

System Integration

- The concept of combining services, such as intrusion, CCTV and access control to improve efficiency and reduce false alarms
- This is the most important technology strategy that security operations will apply in the upcoming years
- Integration is also the sharing of databases among separate systems
- Over the next three years - at least 33% plan some type of integration
- *Source: Analysis by The SECURITY Group for SECURITY Magazine*

Forms of Access Control

- Keys - can be duplicated, no record, tough to administer, how to retrieve
- Cypher locks - common code, hard to change code, better on interior doors
- Security guards - costly, absenteeism, trusted?, Difficult employment times
- Receptionist - always there?, Trained in security?
- Electronic – On-site and central station based

Electronic Access Control Systems Provide...

- **System Automation**
- **Entry Control**
- **Facility Management**



System Automation

- Eliminates needs for alarm keypad
- Provides greater convenience in alarm use
- Enhances management control
 - Alarm use time parameters
 - Detailed management reports



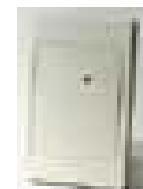
Entry Control

- Replaces mechanical keys with “electronic” keys
- Increases management control of building use
 - Prevents unauthorized entry
 - Records authorized entry
- Helps increase employee safety and security
- Reduces employer “negligent security” liability
- Reduces costs of operations



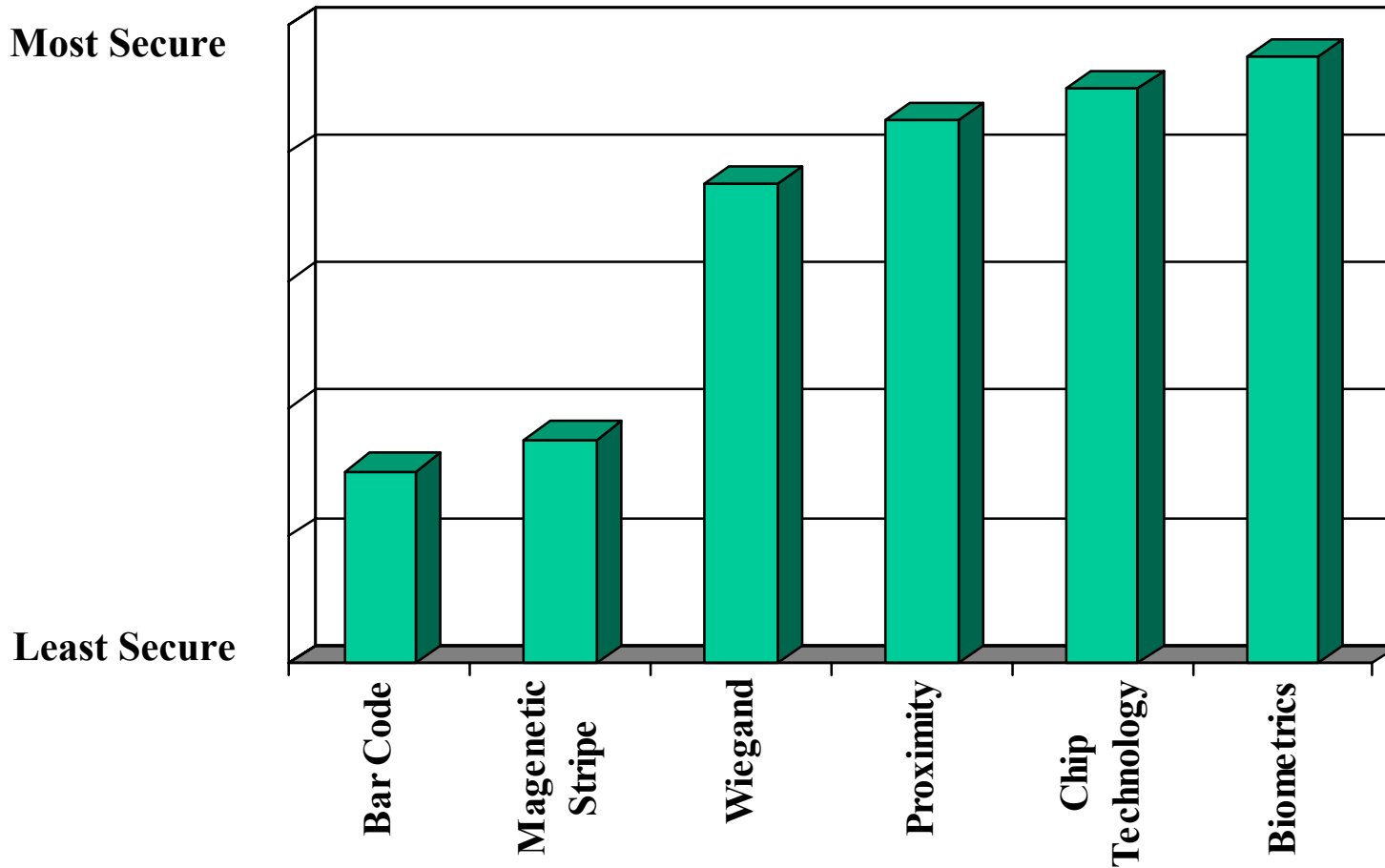
Access Control Major Devices

- Access cards
- Access card reader
- Locking device
- Door position switch
- Exit device
- Controller
- Software



Card Technologies

Relative Security



Card Reader Technologies

TYPE	Principal	Advantages	Disadvantages
Bar Code	Series of thin and thick lines forming a code that can be read by a card reader	Excellent for job costing and time and attendance. Good for low cost cards and many times as a second technology on a dual-tech card	Easy to duplicate
Magnetic Stripe	Card that has data encoded on a magnetic strip placed on a plastic card	Dependable and inexpensive. User may encode cards to further reduce costs. Works well in a dual-tech card package with Photo ID.	Subject to wear and easy to duplicate and/or copy
Wiegand	Card embedded with ferromagnetic wires to form a unique code	Easy to use, high in security and has a long life. Can be used with Photo ID systems	Limited number of site/facility codes and card numbers available

Card Reader Technologies Cont...

TYPE	Principal	Advantages	Disadvantages
Proximity	Card containing a micro-circuit. When placed close proximity to a reader, card will activate and send data	No wear on cards or readers and promotes long life. Hands free installation is possible. High on security. Can be interfaced to most access control systems and comes in various packages	Cost of cards has come down in recent years and chip can be damaged
Smart Card	Plastic card embedded with integrated-circuit chip. Card has both microprocessor and coded memory	Requires less hardware than most access card systems and can be integrated with biometrics. Can be used for other applications other than access control.	High costs of cards at present,

Access Control - Readers

- Reader must match the card technology
- Select best technology for the application. Consider:
 - Security
 - User throughput
 - Cost
 - User acceptance
 - Ease of use
 - Weather resistance
 - Mounting



Access Control - Readers

- Reader ID technologies fall into 3 groups
 - **Knowledge based**
 - Use of pin's and keypads
 - **Possession based**
 - Card has information
 - **Biometric based**
 - Hand geometry
 - Fingerprint
 - Retina scan
 - Voice verification
 - Handwriting analysis



Access Control – Locking Device

- Door configurations determine type and style of lock
 - Magnetic lock
 - Electric lock
 - Shear lock
 - Throw bolt or plunger
- Fail-safe vs. Fail-secure
- Valid read unlocks door



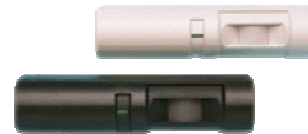
Access Control – Door Position Switch

- Function is to monitor door position
- **Door force**
 - Entry or exit without authorized request
- **Door prop**
 - A valid entry or exit request followed by failure to re-secure the door during allotted time



Access Control – Egress Device (RQE)

- Function is to unlock door and to momentarily mask door position switch.
- Numerous styles and function.
 - Push button.
 - Exit bars.
 - Motion detectors.
- **NOTE: must meet all AHJ codes and all fire/life safety requirements must be met.**



Access Control – Controller

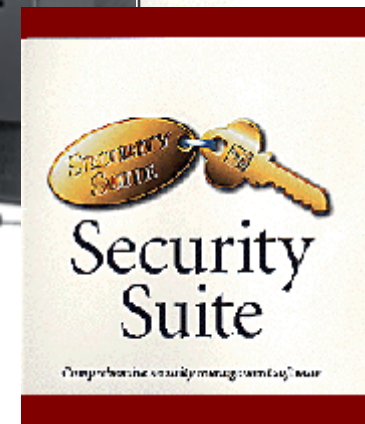
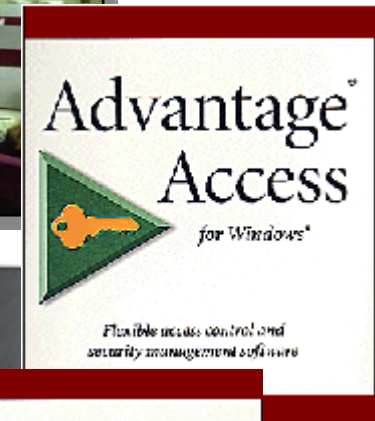
- Single door with *integrated* reader/controller
- Single door with *separate* reader and controller
- Multi door with *separate* reader and controller

- Controls all functions and controls of the door(s)
- Most today use *distributed processing*



Access Control - Software

- Provides central programming, monitoring and control of one or multiple controllers
- Provides real time monitoring
- Provides for storage and customized report generation
- Typical configurations are:
 - Central Station Based
 - On-Site Based
 - Shared



Access Control – Code Compliance

- AHJ – building inspector, fire marshal
- Building / electrical codes
- Fire codes / life safety
- ADA
- UL 294, UL 1076, electrical safety
- NFPA 101 (delayed egress)

Access Control – Wiring Standards

- Follow manufacturer's guidelines
- Twisting prevents wire from acting as an antenna
- Shielding helps stop RFI and EMI from being given off and absorbed
- For powered devices, wire size critical to proper operation
- Stranded wire is preferred type
- Do not install lock control wiring in same conduit as other circuits
- Avoid running wires near lights and other devices that may cause interference
- Determine if plenum or other special rated wire is required

CCTV Systems

Three Reasons for CCTV in Security

- **SURVEILLANCE** - use of video system to manually view a particular area. These systems typically involve an operator constantly watching activities on display devices. - *(To obtain visual information about something that **IS** happening)*
- **MONITORING** - use of video system to record information on particular activities and / or areas. These systems involve operators and / or recording devices for later review. – *(To obtain visual information about something that **HAS** happened)*
- **DETERRENT** - use of video system as a deterrent to a crime. The system is established in an open fashion with customer & employee awareness. - *(**Deterrence** can only be used under specific circumstances)*

Why Use CCTV?

- Market is demanding - biggest drivers are internal theft, workplace violence, personal safety.
- Industry segment growth -
 - Growing approximately 10% annually.
 - Generate revenue of approximately \$4.5 billion in the non-residential segment.
 - Accounts for approximately 15% of total security purchases.
- Tops on the list of planned purchases.

Common Types of CCTV

- **Overt** - standard cameras recognizable by the general public. Generally act as a deterrent.
- **Discreet** - cameras designed to blend into the environments and be less intrusive. Will be in the shape of a dome or ball.
- **Covert** - cameras hidden or disguised from public view. Designed to detect rather than deter.



Cameras

- CCD (charged coupled device) describes a small image sensor used in most cameras.
 - The chip takes the information from the lens converts light to transmit to the monitor.
- Cameras are designed to work with a wide variety of lens.
- There are two specifications commonly used to judge a cameras performance:



Resolution and Sensitivity

- *Resolution* - often expressed as TV lines (TVL). This is an indication of the cameras ability to resolve detail. (Ex. 400 TVL).
 - The higher the resolution the sharper the picture, better the detail.
- *Sensitivity* - is the minimum light level (measured in LUX) required to produce usable picture. Lighting levels are quite high for most applications and should not be a concern.

Black/White vs. Color

- *Visual recognition* - color will provide more information than B&W.
- *Resolution* - B&W can produce higher resolution. Color maximum TVL of 480. B&W maximum TVL of 600.
- *Light levels* - B&W works better because it requires less available light to produce usable picture.
- *Cost* - Color and B/W are getting closer in costs. Color used to be more expensive.

Cameras and Lighting

Application	Color	Black / White
Indoor fixed lighting	Good	Good
Indoor low light	OK	Better
Outdoor daytime	Good	Good
Outdoor nighttime/low light	OK	Good

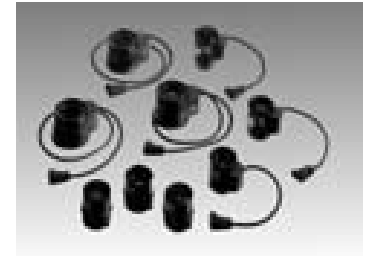
Can add infrared illumination (IR) devices for very low light conditions



Lens Variables

The CCTV lens has four basic functions:

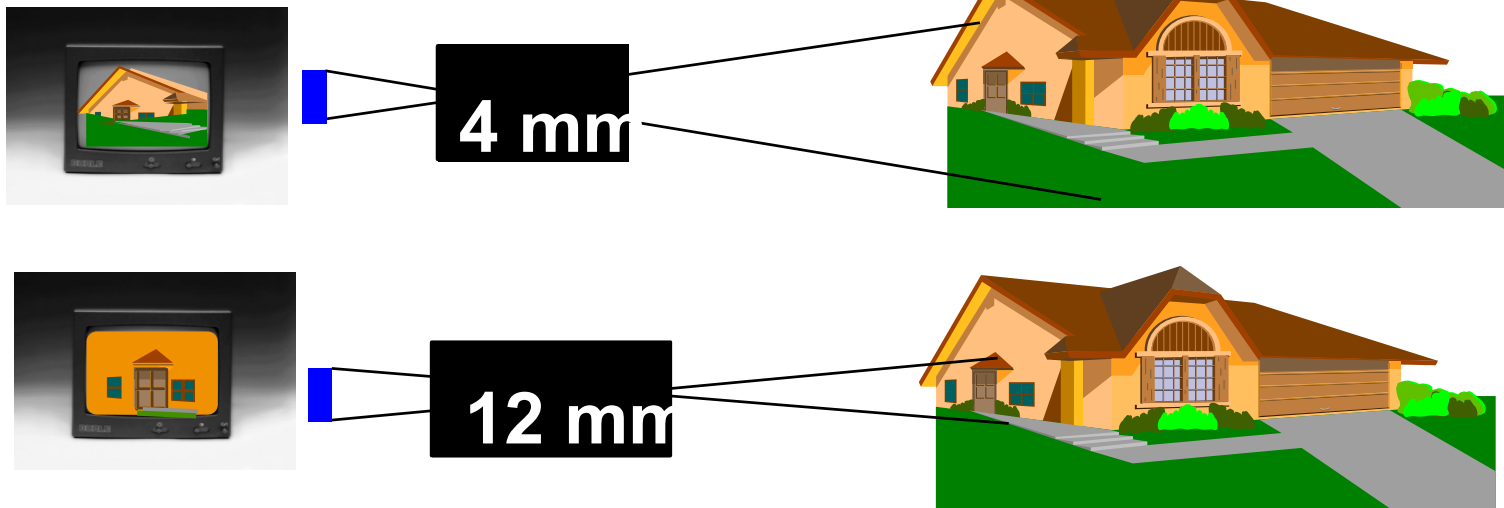
1. Fill the camera imager (CCD) with light
2. Provide a proper field of view
3. Control amount of light to imager (camera)
4. Focus light on the imager (camera)



To operate properly, all four must be achieved

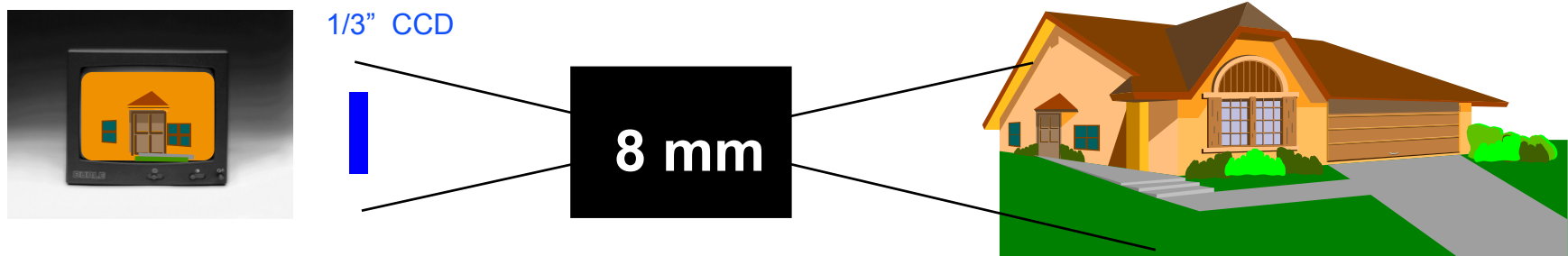
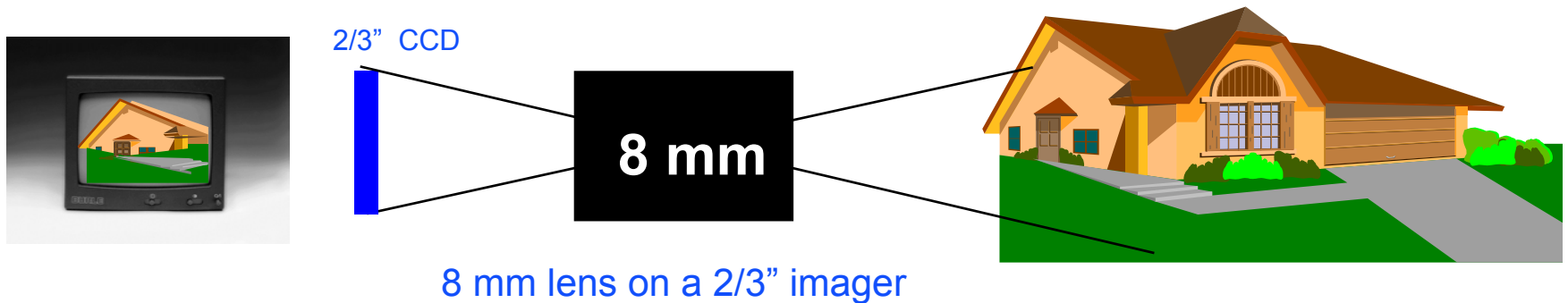
Determining Camera/Lens Field of View

- The lens is designed to provide a particular field of view
(**Lens Function 2**)
- The smaller the mm# (focal length) the wider the view



Determining Camera/Lens Field of View

- The camera imager format will affect the field of view.



Same 8 mm lens on a 1/3" imager. Only half of the lens' "cone of light" is used.

Determining Camera/Lens Field of View

Common viewing angles and associated camera formats

<u>Horiz View</u>	<u>Reference</u>	<u>Application</u>	<u>1/3" Format</u>	<u>1/2" Format</u>	<u>2/3" Format</u>
80 degrees	Extreme Wide Angle	Elevators, "tight" viewing areas	< 2.8 mm	< 3.7 mm	< 6 mm
60 degrees	Wide angle	Small lobbies, check out counters	4 mm	6 mm	8 mm
30 degrees	Standard View	Lobbies, general views	8 mm	12 mm	16 mm
15 degrees	Telephoto	Hallways, corridors	> 12 mm	> 16 mm	> 25 mm
Variable	Zoom	Detailed, distant views	5.8-58 mm	7.7-75 mm	10-100 mm

General Rule: the smaller the focal length number, the wider an area will be covered

1/3" "standards"

- Standard wide angle - 4 mm
- Standard angle - 8 mm
- Vari-focal - "best of both worlds" -manual adjust 3.5mm - 8mm

Lens Iris Types

The iris controls the amount of light to the imager (CCD) (**lens function 3**).

Manual iris: these lenses provide a manual adjustment for an acceptable picture in stable lighting conditions.

DC or direct drive iris.

DC iris lenses rely on electronics inside the camera to tell the lens to open or close. (I.E. The camera must support DC iris lenses). DC lenses have a good light range handling capability and are ideal for inside use and limited outside use.

Auto-iris: these lenses provide automatic adjustments to variations in lighting conditions for improved camera viewing performance. Full auto iris lenses include all necessary electronic circuitry inside the lens. These lenses have a excellent light range capability and are can be used in ALL lighting conditions (inside and outside).

Indoor Mounts and Housings



- **PRIMARY PURPOSE AND USE**
 - aesthetics
 - prevent tampering
 - concealment
 - maintain a good operating environment
 - camera location requirements
 - general protection.
- **Indoor dome housings:** these can be broken down into two types: those for fixed cameras and those for pan/tilt/zoom cameras. The most popular models are tinted and come in both drop-ceiling and full pendant models.
- **Standard indoor housings:** these are used to improve aesthetics and provide protection from tampering and/or the environment. Corner and security housings contain integral mounting hardware for cameras while standard housings typically require a mount with an adjustable head accessory.



Outdoor Housings & Accessories

- **Outdoor dome housings:** most applications for outdoor domes utilize pan/tilt/zoom cameras. Similar to the indoor domes, they are often tinted. Options are usually necessary such as heaters and blowers to provide a proper operational environment for the cameras and lenses.
- **Standard outdoor housings:** these can be broken down into two types: those for fixed cameras and those for pan/tilt/zoom cameras. Options are usually necessary such as heaters to provide a proper operational environment for the cameras and lenses.



Outdoor Housings & Accessories

- **Accessories:**
 - **Heaters:** provide lower operating temperature ability, helps reduce internal condensation, helps improve lens motor performance in low temperatures.
 - **Sunshield:** provides higher operating temperature ability, provides extra protection against falling elements.
 - **Transformers:** provide extra protection or power isolation for camera/lens and accessory elements.

Mounts & Housings

Typical Applications

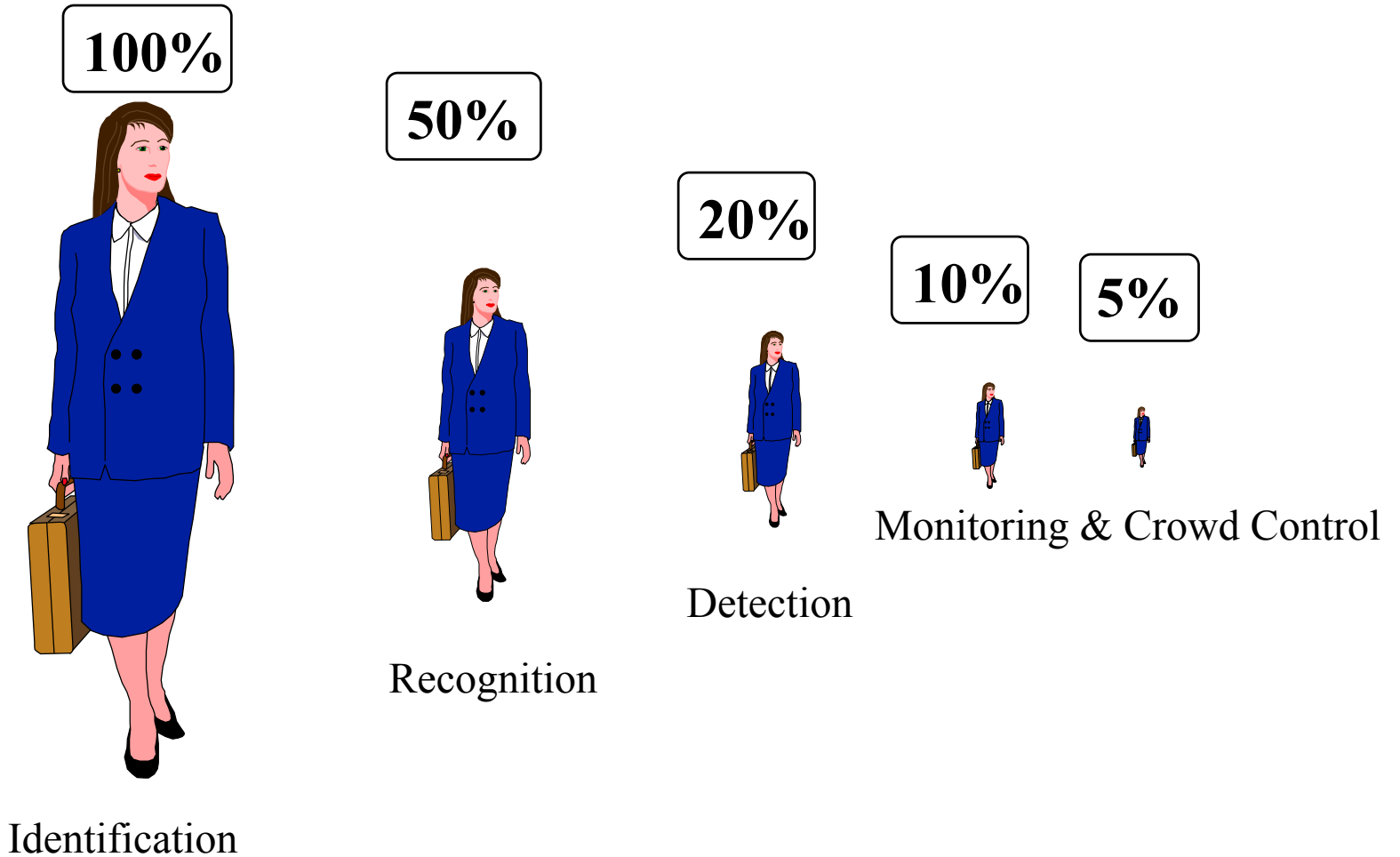
Style	Feature	Benefits	Mount Location
Standard Ceiling Mounts	T-bar Clamp	Mounts to drop ceiling grid	Aisles and entry ways
Mini-tinted dome	Discreet ceiling dome	Helps mask camera position and mounts into ceiling grid	Aisles and entry ways
Cylindrical housing	Aesthetic design	Blends in with retail decor	Halls and shipping/receiving
Environmental Housing	Cylindrical design and internal transformer	Aesthetics, camera position	Outdoors and public areas

Monitor Variables

Monitor Size	Benefit	Application
9"	Small footprint	Small office or desk top
13"	More viewing area	Manager office, desk top, good quad display, deterrent
>17"	Full screen image	Mux or quad display, deterrent

* The size of the monitor is typically a function of the location and its primary use.

Subject Size vs. Monitor



Monitor Viewing Distances

Monitor Size	Minimum	Maximum
9"	3 feet	7 feet
12"	3.25 feet	10 feet
15"	3.5 feet	12 feet
17"	3.75 feet	14 feet
19"	4 feet	17 feet
21"	5 feet	19 feet

Video Recorders

- Two Types
 - **VCR** – (Time Lapse Recorders) Images stored on tape. Most popular method utilized in recent years. Industrial strength versions designed for commercial use.
 - **Digital Video Recorders (DVR)** – Images stored on a hard-drive component. Provides better quality, retrieval and management. Benefits are starting to outweigh costs. Multiplexing devices are being built in.

Video Recorders - Digital vs. Analog

- **Analog (VCR)**
 - Scans image, converts to digital values and then converts back to analog before recording information onto a video tape
- **Digital (DVR)**
 - Scans image, converts to digital values, compresses the digital data and stores information in a digital format.

Video Recorders - VCR



- **VCR**
 - *Time Lapse Recording*: VCR records segments of time, records at a slower speeds. Records all fields - 60 fields/sec. Records 2, 12, 24, 48, 72, 120, 168, 240, 360, 480, 600, 720 hours.
 - *Real Time*: VCR records continuously. Records in “pseudo-real-time” format - 20 fields per second. Typically 6, 18, 30 hour record modes.

Video Recorders - VCR Issues

- The analog signal on the tape can degrade due to
 - VCR head wear
 - VCR tape wear
- Stored images degrade with each use
- Limitations on distances to monitor
- Complicated setup
- Complicated and tedious event search



Video Recorders – DVR Issues

- Important issues in digital recording
 - *Video Acquisition* (start with good signal)
 - *Video Compression* (reduce size of the image)
 - JPEG, MPEG, AVI, Wavelet, etc
 - *Storage* (hard drive issues)
 - Size, capacity, environment
 - *Image Display* (match resolution)
 - *Authentication* (for legal issues)
 - Digital watermark, check sum, etc



Video Recorders – DVR Benefits

- Copies of the digital images do not degrade
- Increased reliability and flexibility
- Accessibility to information
- Offers remote access to information
- Instant access to events
- Multiple user viewing



Video Processing Equipment

- **Quads:** primary function is to display 4 views on one screen. There are single page (4 inputs) and dual page (8 inputs) units. Advanced units have built-in switcher features.
- **Multiplexers (“Mux”):** primary functions are to process multiple video inputs onto one display device and/or enable recording (“encoding”) of multiple inputs onto one video recorder. Also processes pre-recorded encoded tapes for intelligent playback.
- **Switchers:** primary function is to provide the ability to selectively display a number of video inputs to a particular output device such as a monitor and/or recorder.
- **Matrix switchers:** primary function is to provide an expandable, modular product for the selective display of a number of video inputs to a variety of output devices such as a monitor and/or recorder.



Cabling and Transmission

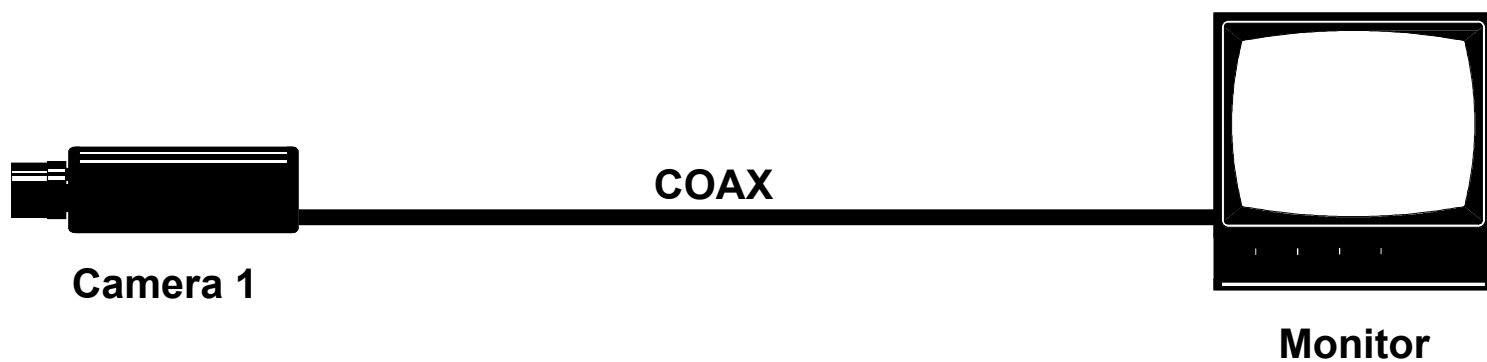
- **Coax cable** - most common form and transmits through copper conductor. Low cost and easy to install. Typical: RG59/U (<750 ft); RG6/U (1,000 ft); RG11/U (1,500ft)
- **Twisted pair** - alternative to coax. Can run over longer distances. Allows use of existing cat 5 or 3 cables.
- **Fiber optics** - uses light to transmit signals. Can run over larger distances. More expensive but less susceptible to interference.
- **Others** - phone lines, networks, infrared, & microwave.

Network Video Issues

- Utilize existing backbone (LAN/WAN) for video transmission
- Requires network compatible (IP addressable) cameras or converters
- Bandwidth is critical for proper operation
- IT Department will be part of decision
- Cost still a factor, but technology is driving applications

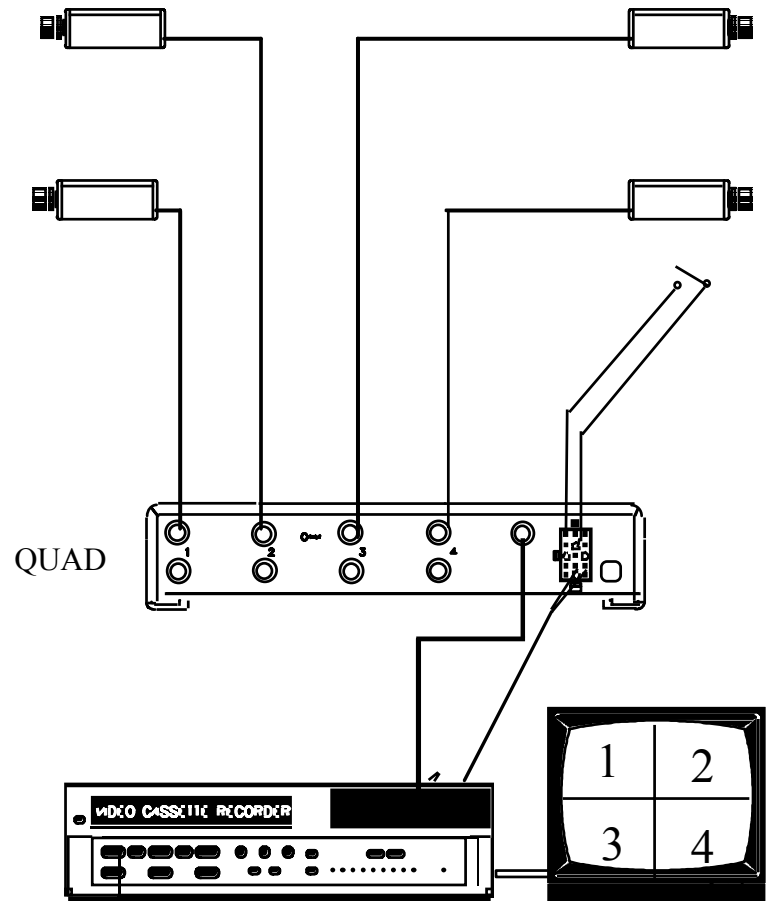
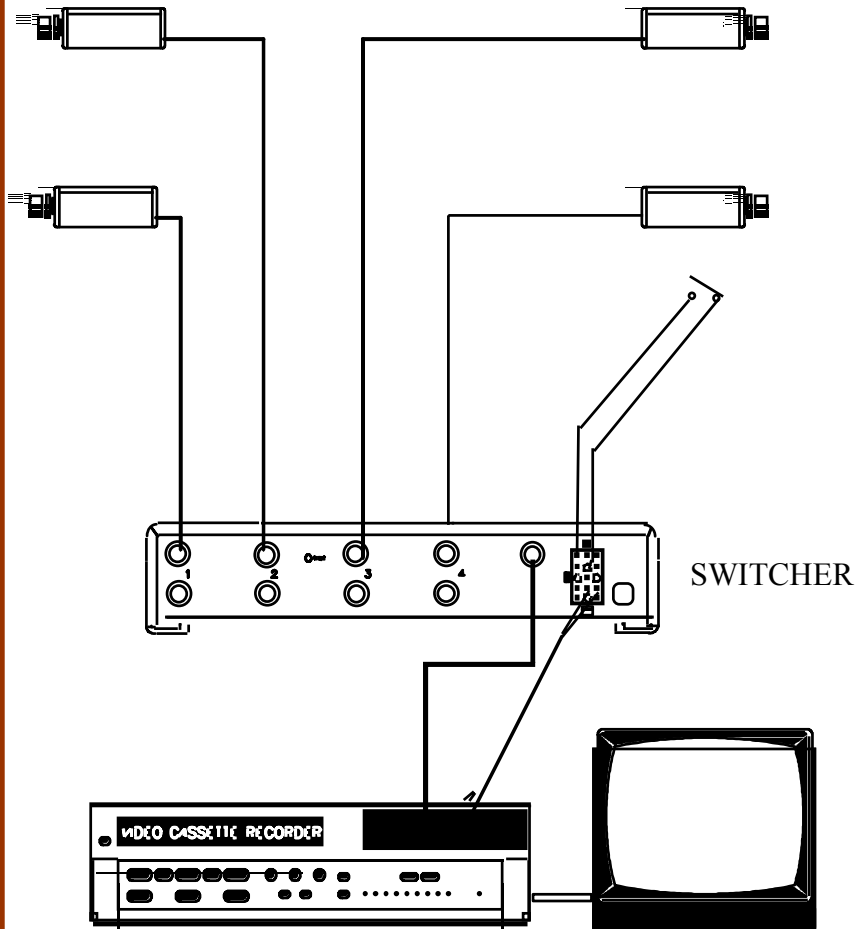
Typical Simple System

Single Camera



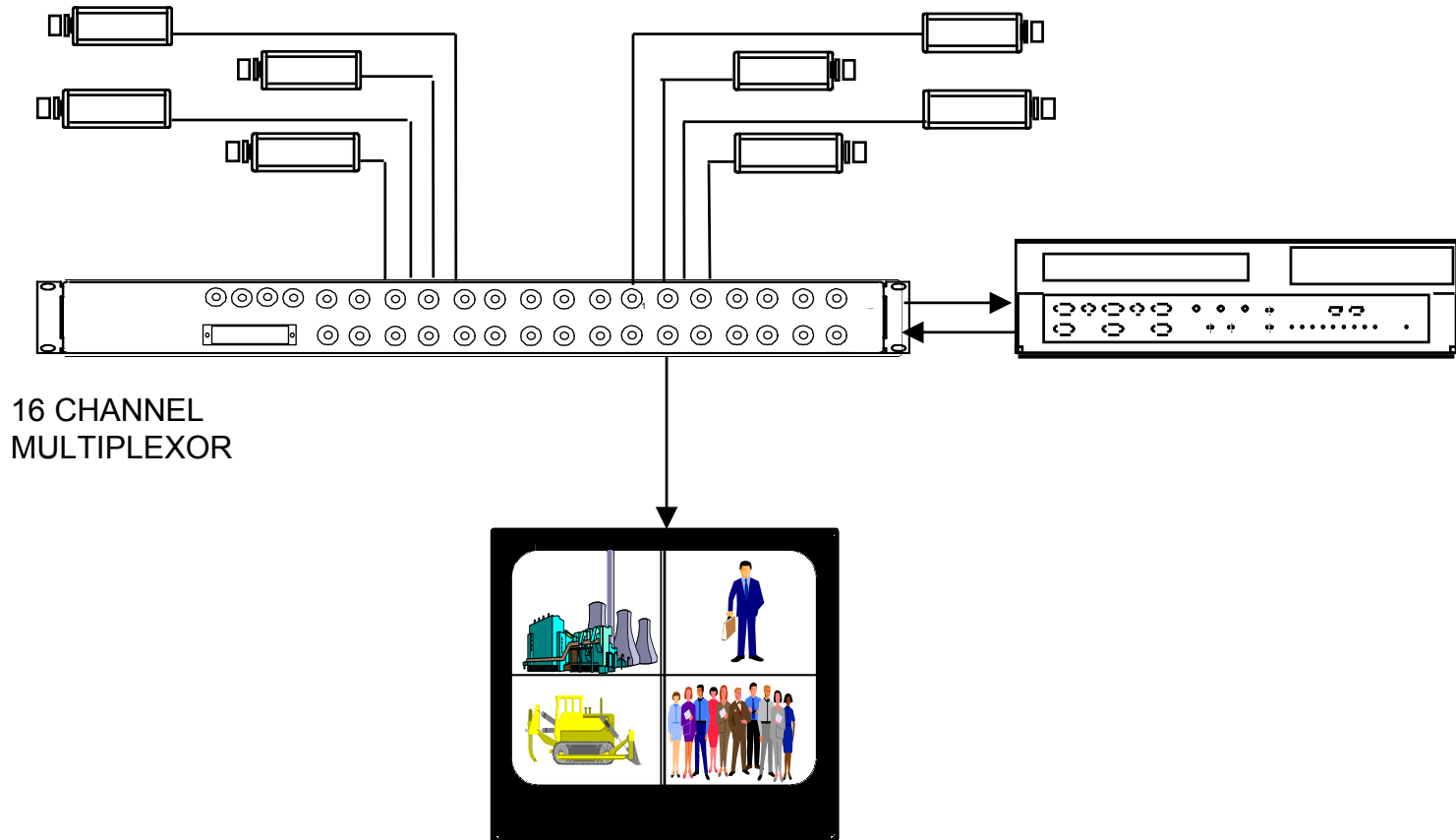
Typical System

Four Camera



Typical System

Multiplexers



Fire Systems

Fire Systems



Contact your local
Sonitrol Dealer for
specific information



*For more information, contact your
local Law Enforcement or your local
Sonitrol Dealer at
1-800-328-5607
or
www.sonitrol.com*



SONITROL®