SAND2013-7379P

Introduction and Overview

Course Introductions

- Introductions
  - Workshop Director
  - Class Participants
  - Instructors
- Course Overview

Workshop Objectives

After completing this workshop, you should be able to:

- Explain the design and evaluation process outline (DEPO)
- Define the elements of a physical protection system
- Develop an understanding of the fundamental principles of the different elements

Introduction of Workshop Participants

- Please introduce yourself to the class
  - Name
  - Organization and job
  - Nuclear security / physical protection experience
  - What are your expectations for this course
  - What are your favorite activities outside of work

Logistics

- Class schedule
  - Start and end time
  - Breaks
- Cellphones and pagers
- Exits

Train-the-Trainer

Training Methodology

Outline

- Instructor/Training Objectives
  - Instructor requirements
  - Learn the Course
    - Objectives and Audience for the Course
    - Structure and Components for the Course
  - Instructional Systems Design (ISD) Process
- Subgroup Instructor Objectives
  - Purpose and significance of subgroups
  - Role of subgroup instructors
  - Facilitation techniques
- Instructor Competency
- Summary

Note: This presentation has been designed and will be presented as though it were a lecture in a training course.

INSTRUCTOR/TRAINING

Instructor/Training Objectives

At the end of this module, you should be able to:

- Discuss instructor requirements
- List and discuss the 5 steps of the ISD process
- Describe the importance of learning objectives and how they relate to course components
- Define the course:
  - objectives and audience
  - Structure, components and their importance

Multiple Training Methods

- Different training methods to address different types of learners
  - Auditory
  - Visual
  - Tactile or kinesthetic
- Different training methods have different retention rates
  - 5% Lecture
  - 10% Reading
  - 20% Audio-Visual
  - 30% Demonstration
  - 50% Discussion Group
  - 75% Practice by Doing
  - 90% Teaching Others
- Combination of lecture, discussions and practice by doing in subgroups

Typical Course Structure

- Lectures
- Course/Subgroup Exercises
- Field trip, where applicable
- Final exercise
- Daily review
- Daily quiz
- Daily evaluation
- Social/cultural/team building activities

Typical Course Structure

Course Structure	Type of Learning
Lectures/ Slides	Visual/Auditory
Course Exercises	Visual/Auditory/Tactile
Text	Visual
Facility Tours, Field Trips	Visual/ Auditory/Tactile
Daily Review	Visual/Auditory
Daily Quiz/Daily Evaluation	Visual/Tactile

Course Instructors

- Qualifications
  - Subject matter experts in multiple physical protection areas. Must be technically qualified
  - Trained instructors
- Tasks
  - Present multiple lectures
  - Lead all subgroup exercises
- Commitment
  - Presence during course

Basic Instructor Qualifications

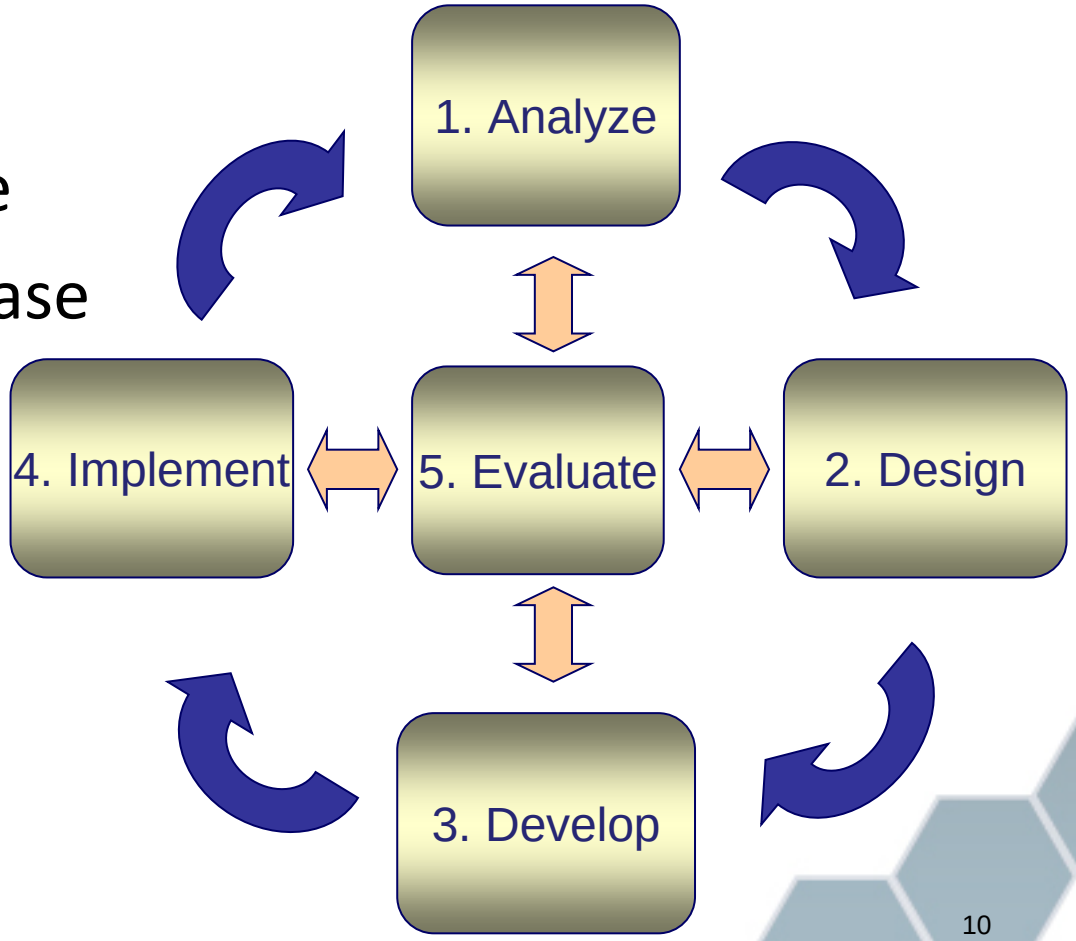
The ability to provide effective training is significantly influenced by an instructor's instructional skills and technical expertise.

Instructors should be able to:

- Use a systematic approach to:
  - implement training
  - develop and use learning objectives
  - develop and use questioning techniques
- Understand and use adult learning and motivation principles
- Teach and facilitate classroom learning
- Use student-centered activities in a classroom environment
- Manage stress in the classroom

Courses Designed and Maintained using 5 Phases of Instructional System Design (ISD)

1. Analysis Phase
2. Design Phase
3. Development Phase
4. Implementation Phase
5. Evaluation Phase



Why do I “the instructor” need to understand the ISD model?

- An instructor should understand the material they are using and the techniques used to design it
- An instructor should understand who the learners are
- An instructor should understand how to use their teaching material
  - Learning objectives
  - Quizzes
  - Reviews
- Instructors should understand the proper way to upgrade and improve a course

1. Analyze

- Conduct Needs Assessment
  - Will training fix the problem?
  - Who are the learners, what are their knowledge, skills, attitudes, and competencies?
  - What do people need to learn?
    - Course Requirements
    - Course Design
    - Course Evaluation
- Develop Course Requirements
  - Course Objective
  - Pre-requisite knowledge

2. Design

- Write Student Learning Objectives

Student Learning Objective: A specific description of tasks and abilities the student should be able to do at the end of a module.

  - These are the most important piece of the course: all presentations should focus on these.
  - These items are directly linked to quiz questions and exercises to test the students knowledge of, or ability to complete the tasks.

- Specify Instructional Strategies

Instructional strategies: Approach taken to achieve learning objectives.

  - Examples: Lectures, Subgroup, Games, Demonstrations, Reading

Example: Introduction to DEPO Methodology

Methodology based on a system engineering approach — three major steps:

1. Define physical protection system requirements
2. Design new, or characterize existing, physical protection system
3. Evaluate physical protection system performance, and redesign if necessary

Design and Evaluation Process Outline (DEPO)

Define PPS requirements

- Process of design & evaluation
- Facility characterization
- Target Identification
- Threat definition

Design PPS

Physical Protection System

- Detection
  - Intrusion detection
  - Alarm Assessment
  - Access control
  - Alarm Communication & display
- Delay
  - Delay
- Response
  - Response

Evaluate PPS

- ASD
- Single Path analysis
- Neutralization analysis
- Scenario analysis
- Insider analysis

Final PPS Design

Re Design PPS

3. Develop

- Develop instructional materials
  - Text
  - Lecture
  - Exercises
  - Test and evaluation
- Peer review
- Technical editing
- Production

4. Implement

- Instructor rehearsal and critique
  - Lectures
  - Subgroup exercises
  - Team building
  - Language skills
- Course presentation
  - Time management
- Student learning estimates
  - Daily quiz and feedback
    - Daily review
  - Instructor meetings

International Presentation Considerations

- Speak slowly, English is a second language for most participants
- Focus on the objectives as you work through the presentation
- Do not use acronyms
- Do not use idioms or slang words, few of the participants will understand them
- If asked a question, repeat the question so that everyone can hear it, and to confirm that you understood the question
- Be aware, jokes do not always translate well

5. Evaluate

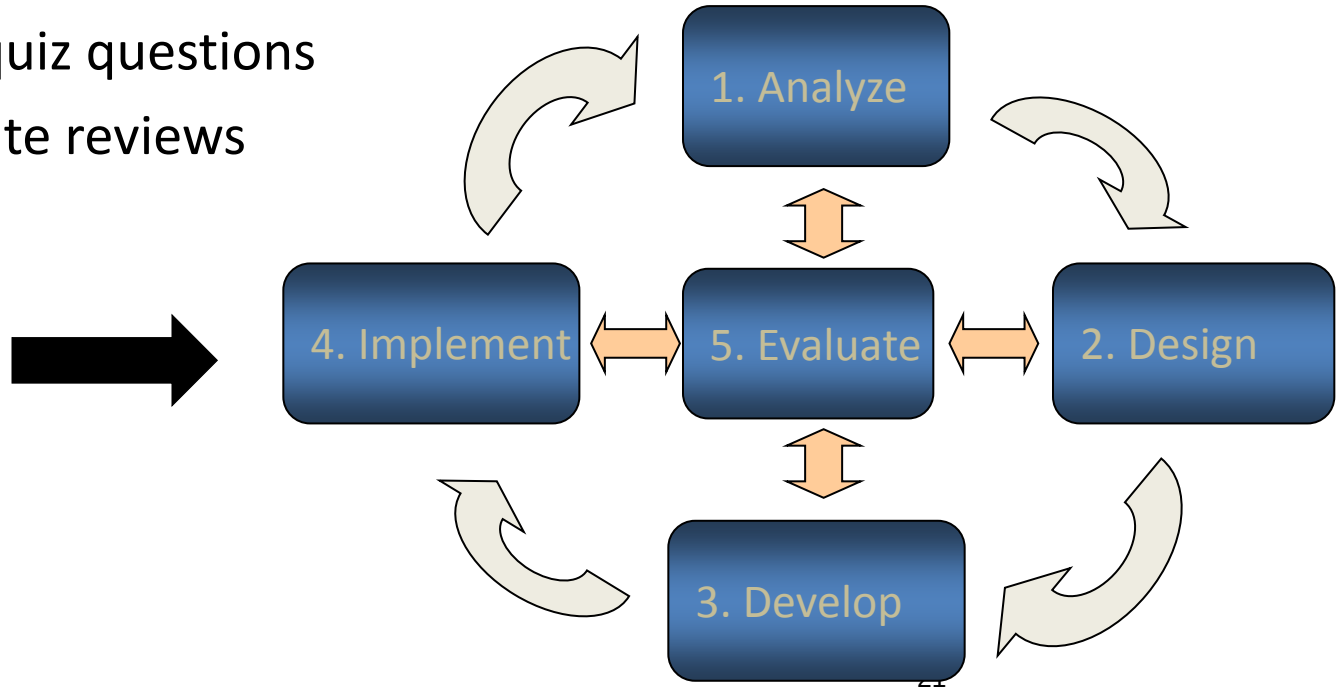
- Evaluate course activities versus objective and requirements
  - Student feedback
    - Daily Quizzes (what participants learned)
    - Daily Evaluation Forms (how participants felt)
  - Instructor input
- Updates should be done when
  - Evaluation results suggest needed changes
  - Technologies and tools have changed
- Repeat the instructional system design process

Quiz Questions

- Quiz questions should be linked directly to the objectives.
  - This allows appropriate measurement of objective comprehension
  - This keeps the message consistent throughout the course
  - Results help identify what topics were understood and retained, and what topics should be reviewed and emphasized the next morning

Instructor/Training Summary

- Courses are designed to teach individuals using visual, auditory, and tactile learning styles
- Learning objectives are key to ensuring
  - Consistent presentations
  - Focused quiz questions
  - Appropriate reviews
- ISD Process



SUBGROUP INSTRUCTORS

Subgroup Instructor Objectives

At the end of this module, you should be able to:

- Describe the purpose and significance of subgroups
- Discuss the role a subgroup instructor has
- Describe the subgroup process
- Discuss the subgroup facilitation techniques

Purpose of Subgroups

- Subgroups involve visual, auditory, and tactile learning
- Subgroups give participants experiences that emphasize the methods and techniques taught during the lectures

  "What we have to learn to do, we learn by doing"
  -Aristotle
- Subgroups share professional experiences related to each topic

Subgroup Instructors

"The best way to learn something, is to teach it to someone else." -Anonymous

- The role of a subgroup instructor is to facilitate subgroup exercises
  - *Facilitator:* A facilitator serves as a coordinator and organizer of the subgroup, and ensures everyone is participating and staying on task. Facilitators clarify issues, focus discussions, bring out viewpoints, and synthesize differences.

Subgroup Process

- At the beginning, the subgroup will rely heavily on the subgroup instructor
- As the subgroup comfort level increases, they will become more independent
- By the end of the workshop, the subgroup instructor should act as a consultant, instead of a leader. The participants should be leading themselves

Subgroup Instructor Preparation

- Prepare by working through all exercises yourself
  - You should experience it before participants do
  - This will allow you to identify areas that need to be emphasized and/or clarified
- Review the exercise the evening before, to refresh your memory
- Ensure that all necessary training aids and supplies are available for participant use

Subgroup Instructors Should:

- Build a strong bond with your group, motivate and empower them
- Direct subgroup activities, recognizing that as the group gains cohesion you should be more of an observer than a leader
- Ensure appropriate training aids and supplies are available for participants
  - Markers
  - Flipcharts
  - Posters of important facility drawings
  - Computers for software (if necessary)

Subgroup Instructors Should:

- Manage the group process: Observe group occurrences and trends, work with the group to ensure that they are completing the necessary tasks and that everyone is participating
- Most groups will go through the 5 stages of group development:
  - forming
  - storming
  - norming
  - performing
  - adjourning

Subgroup Instructors Should NOT:

- Complete the exercises for the subgroup
- Just give out the answers
- Allow one person to dominate the group and do all of the work

Facilitation Techniques

- Identify ground rules
- Give specific instructions
- Focus the subgroup

Identify Ground Rules

- As a group, take 5 or 10 minutes, and determine the rules that the group will follow
  - Allows group to work together and feel ownership of their rules
- These should not be lengthy (3-7 rules)
- Examples:
  - Be on time
  - Be respectful of others
  - Everyone contributes based on their knowledge and experience

Give Specific Instructions

- Before the subgroup begins, have times planned for each exercise
- Verbally explain that task
- Tell subgroup how long they have to do the task
- Tell subgroup what you expect them to do at the end of the task

Focus the Subgroup

- Stay on time (start, return from breaks, etc.)
- Assign roles/responsibilities when appropriate
- Keep group on track (don't allow them to waste their time)
  - Ask strategic questions to redirect if they are off track
- Manage conflict

TAKE A BREAK AND WHEN WE COME BACK WE WILL HAVE A DISCUSSION

Discussion Items (1)

1. What are the instructor requirements?

2. How do learning objectives relate to the course components?

3. How many of you are instructors? Do you feel comfortable enough to teach this material? Why or why not?

Discussion Items (2)

4. If someone is technically qualified, does that make them a good instructor? And visa-versa?

5. Who creates the training material?

6. Is a sub-group instructor different than a lecture instructor?

Subgroup Instructor Summary

- Subgroups are the most important component of a course because they allow participants to experience concepts that are taught during the course
- The subgroup instructor should facilitate the subgroup through the exercises
- The subgroup instructor should become less important as the group progresses
- 3 facilitation techniques
  - Identify ground rules
  - Give specific instructions
  - Focus the subgroup

Instructor Competency

- An instructor competency is a skill that an instructor must successfully exhibit so that they are able to teach and/or facilitate a course or subgroup.

- The following competencies should be adopted by each instructor before they are said to be proficient with facilitating this course:
  - Work experience
  - Teaching experience
  - Participation in 3 course sessions with a Subject Matter Expert (SME)
  - Pass evaluation from the SME
  - Creation of an Instructor Guide Document

Work and Teaching Experience

- Each instructor should have a technical background related to the subject of the course

Courses with a SME

- Observe a SME teach the course and participate exclusively as a student
- Co-facilitate with the SME that they observed
- Facilitate entirely by themselves with the same SME observing and providing feedback to the instructor

Instructor Guide Document

- Instructor Guide is created by each individual instructor throughout the train the trainer session
- Each module will allow 5-10 minutes to complete you guide at the end of the lecture
- Guide should consist of the following for each module:
  - Key learning points
  - Relevant examples that enhance the course materials
  - Materials needed to instruct
  - Items to prepare ahead of time

Module Summary

- Instructor/Training Objectives
  - Instructor requirements
  - Learn the Course
    - Objectives and Audience for the Course
    - Structure and Components for the Course
  - Instructional Systems Design (ISD) Process
- Subgroup Instructor Objectives
  - Purpose and significance of subgroups
  - Role of subgroup instructors
  - Facilitation techniques
- Instructor Competency

Introduction to the Design of Physical Protection Systems

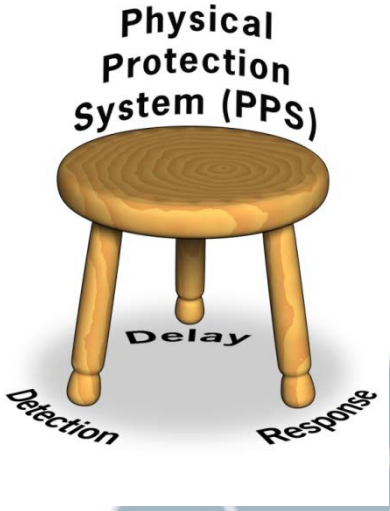
Learning Objectives

At the end of this module, you should be able to

- State two different PPS design strategies
- Identify the three functions of a PPS
  - Discuss the relationships between them
- Discuss performance measures
  - Detection, delay, response
  - System
- Describe the adversary timeline vs. PPS time requirements
- Identify system engineering design principles for an effective PPS

PPS Design Strategies

- Deter the adversary
  - Implement a PPS that potential adversaries perceive as too difficult to defeat and thus do not attack
  - Problem: Deterrence is difficult to quantify or measure
  - Problem: What if some adversaries are not deterred?
- Defeat the adversary
  - Required PPS functions: detection, delay, response
    - Integrated as a system
  - Recommended design approach and the one used in this course

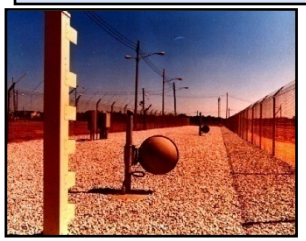


Basic PPS Functions

Physical Protection System Functions

Detection

- Intrusion Sensing
  - Exterior Sensors
  - Interior Sensors
- Contraband Detection
- Entry Control
- Alarm Assessment
- Alarm Communication and Display



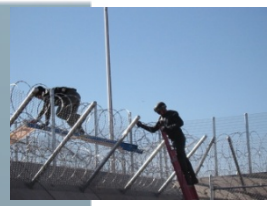
Delay

- Passive Barriers
- Active Barriers

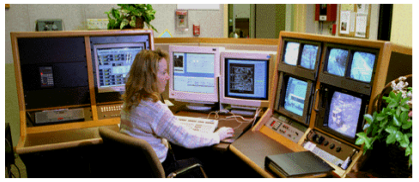
Response

- Guards, Response Force
- Interruption
  - Communication to RF
  - Deployment of RF
- Neutralization

Detection



Sensor Activated → Alarm Signal Initiated → Alarm Reported → Alarm Assessed



- Performance measures
  - Probability of sensor alarm (P_S)
  - Alarm assessment and communication time (T_A)
  - Probability of assessment (P_A)
  - Nuisance alarm rate (NAR)
  - Probability of detection $P_D = f\,(P_S, T_A, P_A, NAR)$
- A long time delay between sensor alarm and assessment lowers P_D

"An alarm without assessment is not detection"

Delay

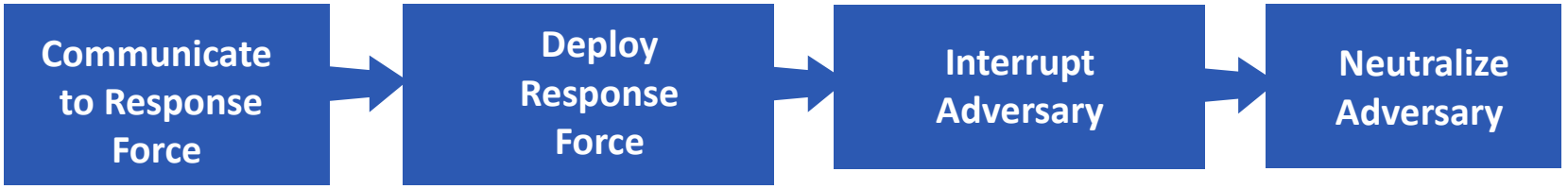
Provide Obstacles to Increase Adversary Task Time

Passive Barriers and Active Barriers

Response Force

- Performance measures
  - Time to penetrate or bypass barriers
  - Time to travel across areas
- Delay must occur after detection
  - Delay before detection is deterrence

Response



- Performance measures
  - Probability of communication to response force
  - Communication time
  - Probability of deployment to adversary location
  - Deployment time
  - Response force effectiveness

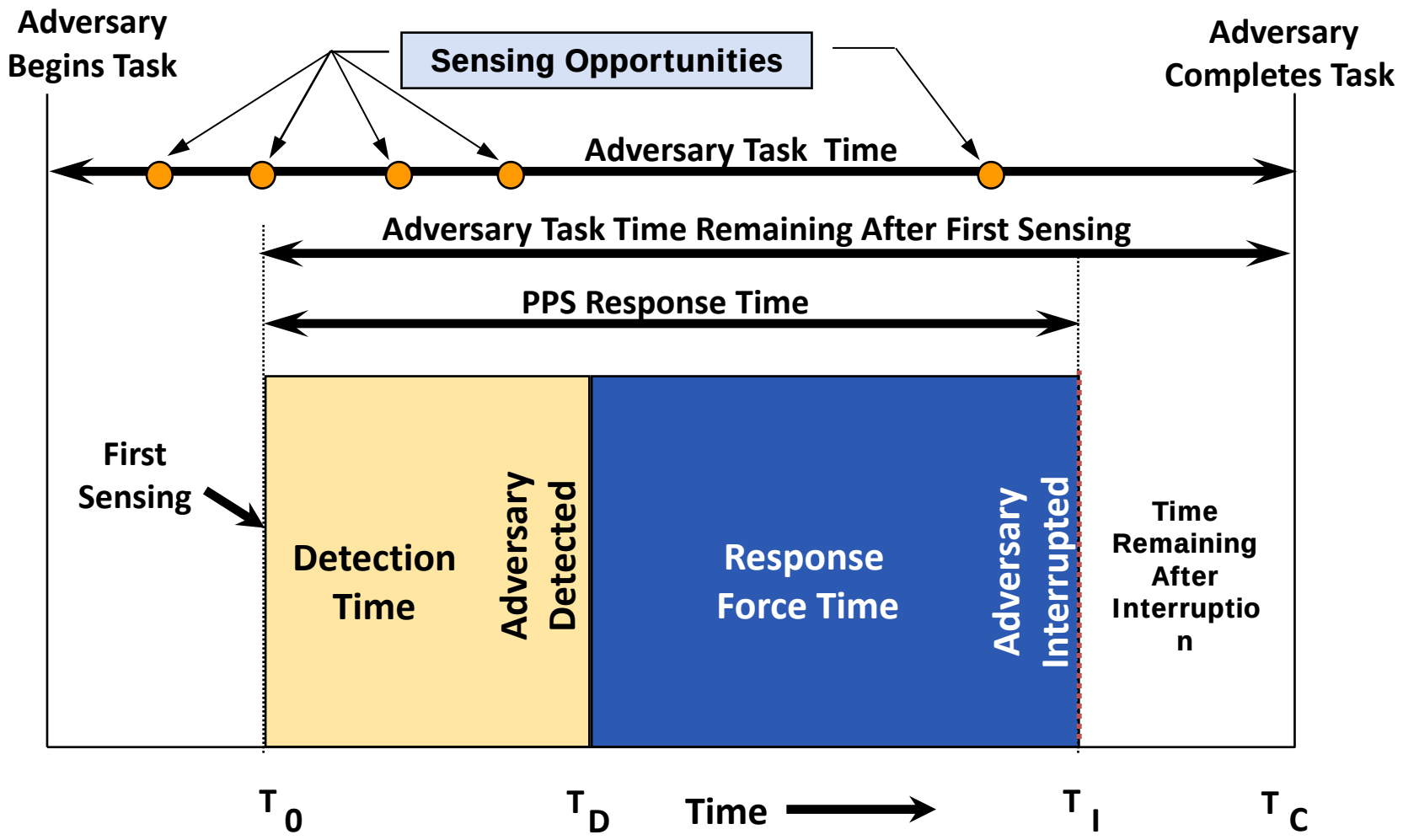
Design Practices for Effective PPS

- Timely detection
- Defense in depth
- Balanced protection
- High reliability

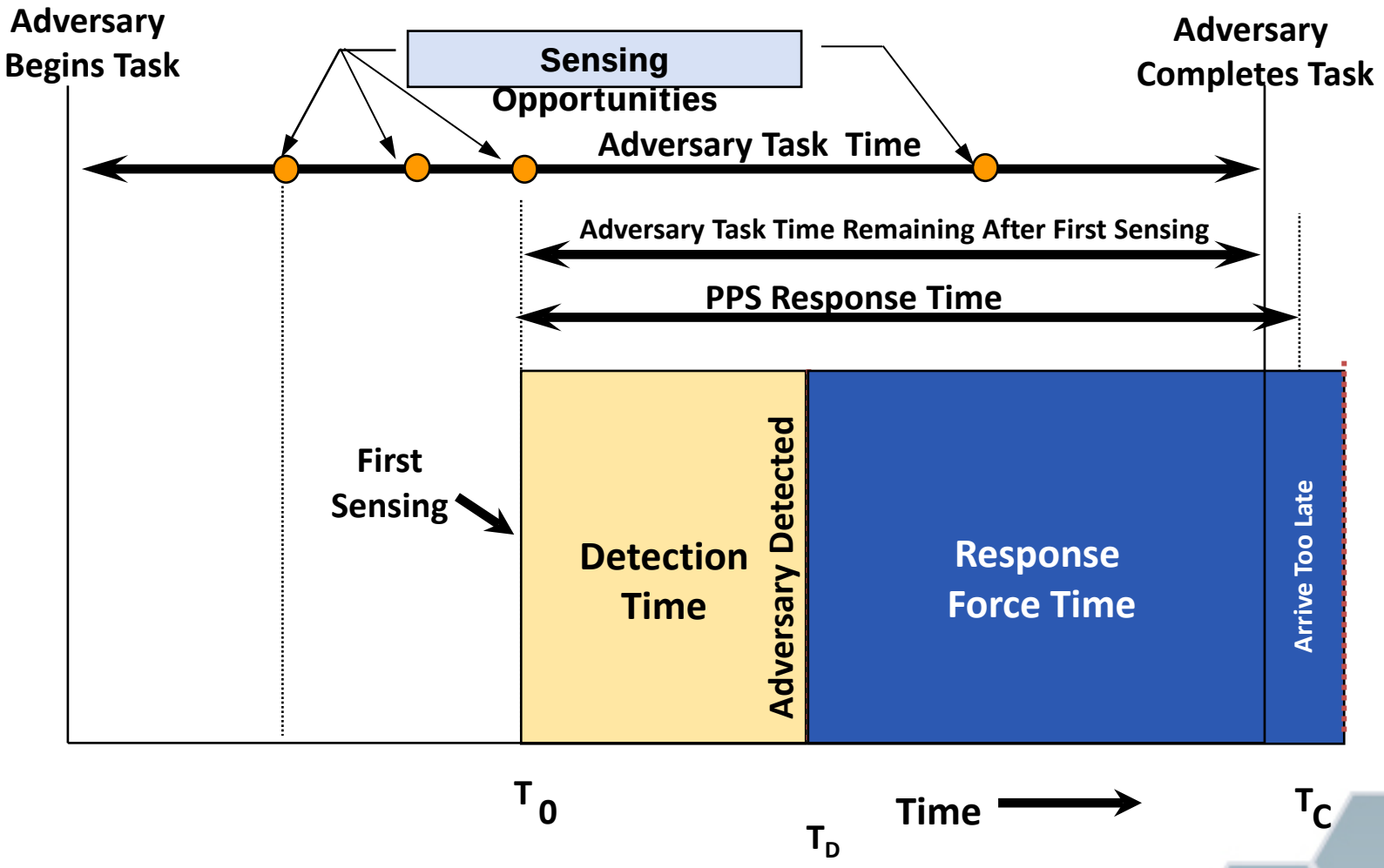
Two Competing Timelines

- Adversary Timeline
  - Cross areas
  - Penetrate or bypass barriers
  - Remove or sabotage target
- PPS Timeline
  - Detection process
  - Delay process
  - Response process
- Overlay of two timelines illustrates requirement for PPS effectiveness

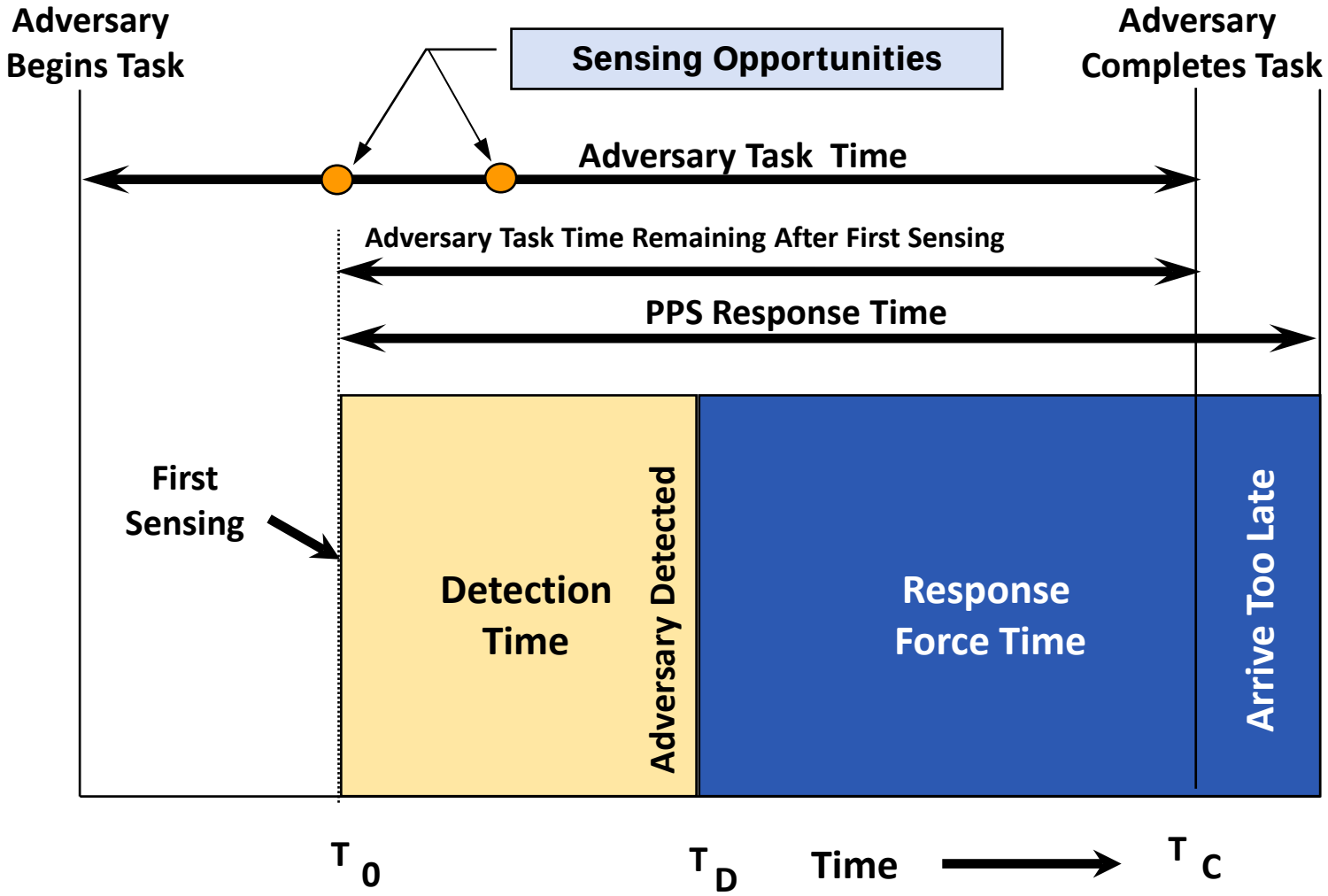
Adversary and PPS Timelines



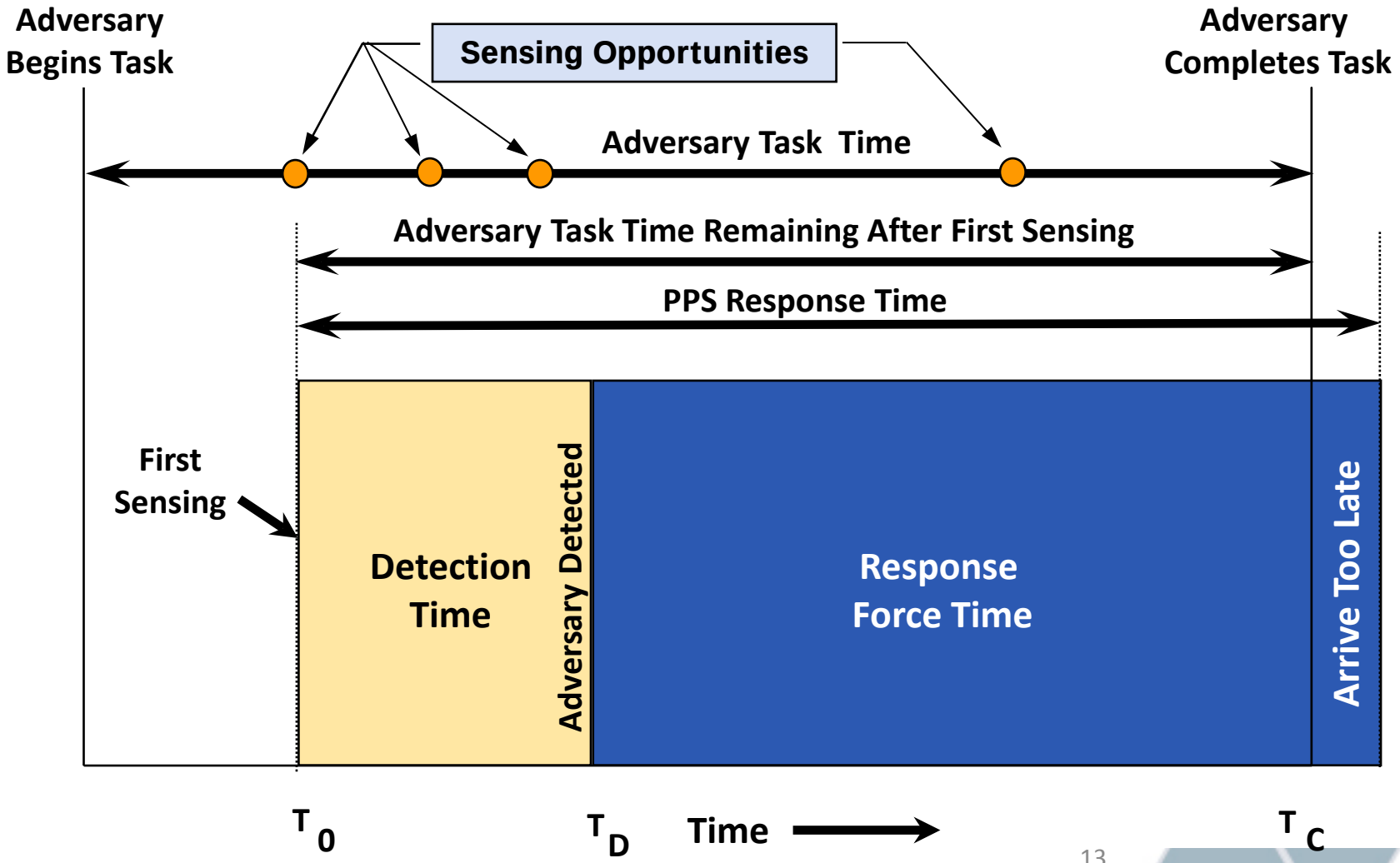
Late Detection



Insufficient Delay



Slow Response

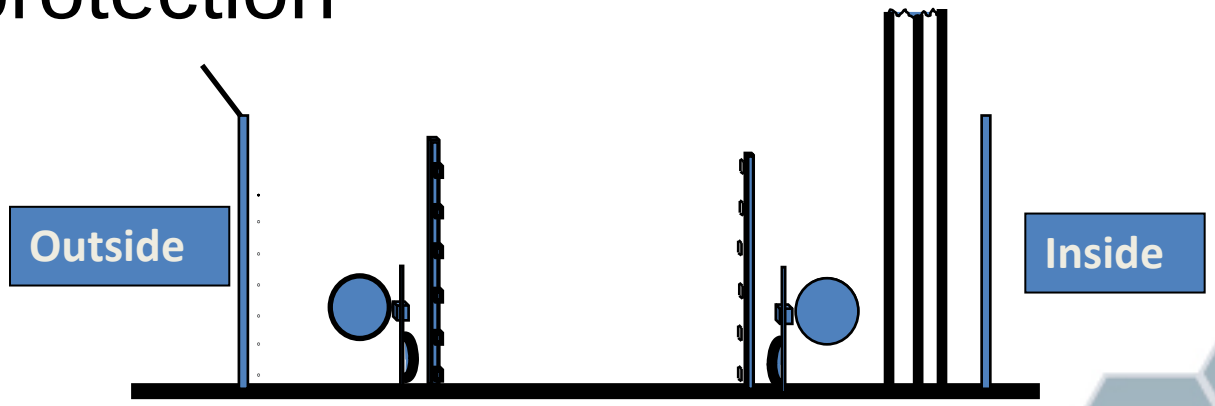


Relationship of PPS Functions

- System detection and response time must be less than adversary task time
- To increase the probability of system success
  - Detect intrusion earlier
  - Reduce assessment time
  - Increase adversary task time
  - Reduce response time
  - Increase response effectiveness

Design Principles for an Effective PPS

- Protection-in-depth
- High reliability
  - Minimum consequence of component failure
  - No single-point of failure
- Balanced protection



Protection-in-Depth

- Adversary must defeat or avoid a number of protective devices in sequence
  - Multiple layers of detection and delay are preferred
- Protection-in-depth should
  - Increase adversary's uncertainty about the system
  - Require more extensive preparations by adversary prior to attacking the system
  - Create additional steps where the adversary may fail or abort his mission

High Reliability

- Contingency plans must be provided so the PPS continues to operate after a component fails
- Redundant equipment can take over function of disabled equipment in some cases
  - For example, backup power exists if primary power is lost
- Some failures require aid from sources external to the facility
  - For example, national guard is used to supplement security during times of higher alert status

Balanced Protection

- No matter how an adversary attempts to accomplish their goal, effective elements of the PPS will be encountered
- Provides adequate protection against all threats along all possible paths
- Minimum time to penetrate each barrier is equal and the minimum probability of detecting penetration of each barrier is equal
- Maintain a balance with other facility considerations
  - Cost
  - Safety
  - Structural integrity

Summary

- Two PPS design strategies
  - Deter adversary
  - Defeat adversary (recommended)
- Three functions of a PPS
  - Detection, delay, response
- Total time for detection and response must be less than adversary task time
- Design characteristics of an effective PPS
  - Protection-in-depth
  - Highly reliable
  - Balanced protection

Introduction to Sensors

Learning Objectives

After completing this module, you should be able to:

- Provide a general overview of sensors
- Describe sensor fundamentals and principles
- Explain the different types of testing for sensors
- Describe features of an exterior and interior sensor system

Parts of a Physical Protection System

- Detection and Assessment
  - Exterior intrusion sensors
  - Interior intrusion sensors
  - Alarm assessment
  - Alarm communication and display
  - Entry control and contraband detection
- Delay
- Response

Example of Design Objective - Exterior

- Design a PPS exterior sensor system:
  - Which will detect a human intruder in the detection zone walking, running, or crawling;
  - In a speed range of 0.15 to 4 meters per second;
  - At a probability of detection of 90% and 95% confidence level
  - A nuisance alarm rate of no more than 1 alarm per day per zone

Example of Design Objective - Interior

- Interior intrusion detection system (IDS) design:
  - Volumetric sensors must detect an individual moving at a rate of 0.15 meter per second, or faster, within the total field of view of the sensor and its plane of detection
  - A balanced magnetic switch (BMS) must initiate an alarm whenever the leading edge of the door is moved 2.5 cm or more from the fully closed position
  - Upon attempted substitution of an external magnetic field when in the secured position the BMS shall generate an alarm or tamper indication

Example of Design Objective - Interior *(cont'd)*

- Interior intrusion detection system (IDS) design:
  - While maintaining proper detection sensitivity, each sensor must have a false alarm rate of less than 1 alarm per 2400 hrs of operation
  - If alarm assessment is available continuously, either visually or by CCTV, a higher false and nuisance alarm rate may be tolerated, if such alarms do not degrade the system effectiveness

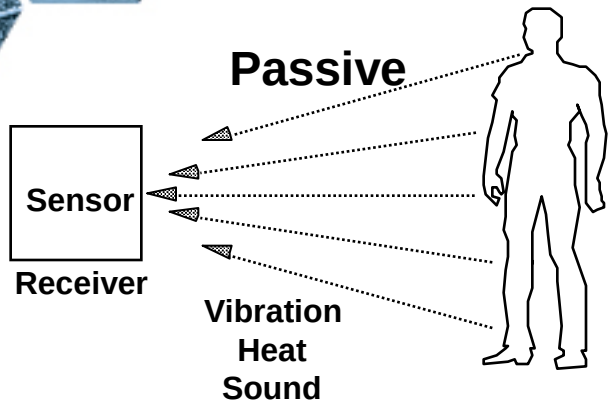
Sensor Fundamentals

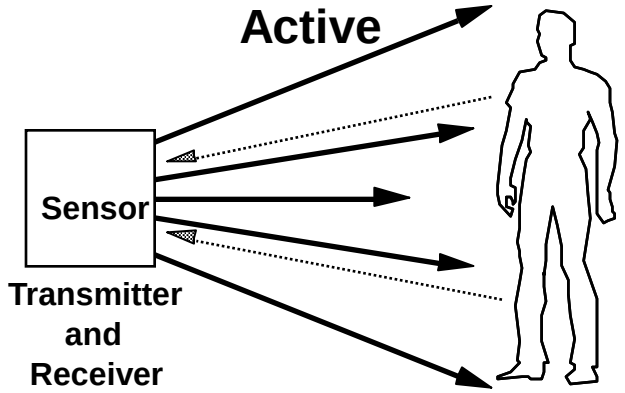
- Sensor classification
- Alarm definitions
- Sensor performance characteristics

Sensor Classification

- Passive or active
- Covert or visible
- Line of site or terrain following
- Volumetric or line detection
- Mode of application

Passive or Active



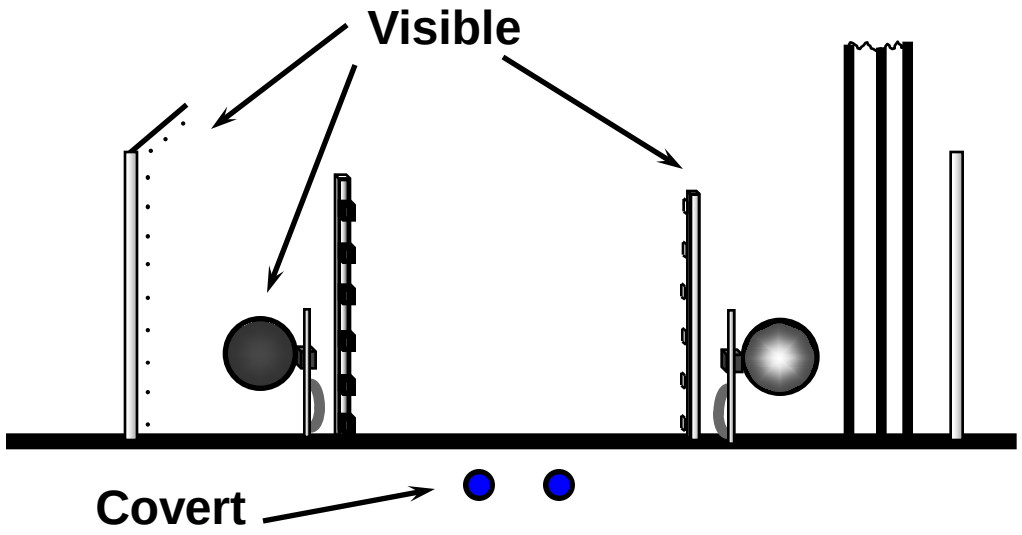


- Passive
  - Sensor receives energy
  - Sensor does not radiate energy

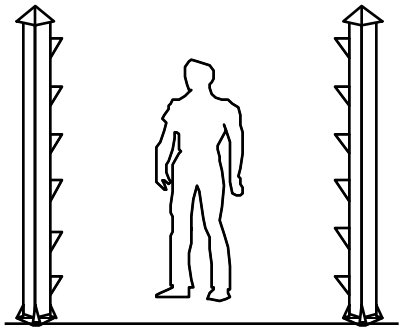
- Active
  - Sensor receives energy
  - Sensor radiates energy

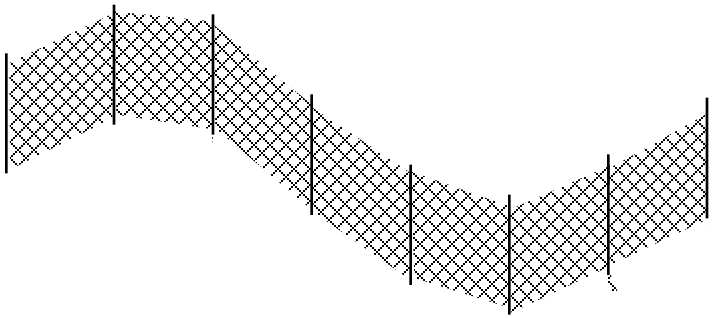
Covert or Visible

- Covert
  - Sensors hidden from view
  - More difficult for intruder to detect
- Visible
  - Sensors in plain view of intruder
  - Simpler to install and repair



Line-of-Sight or Terrain-Following

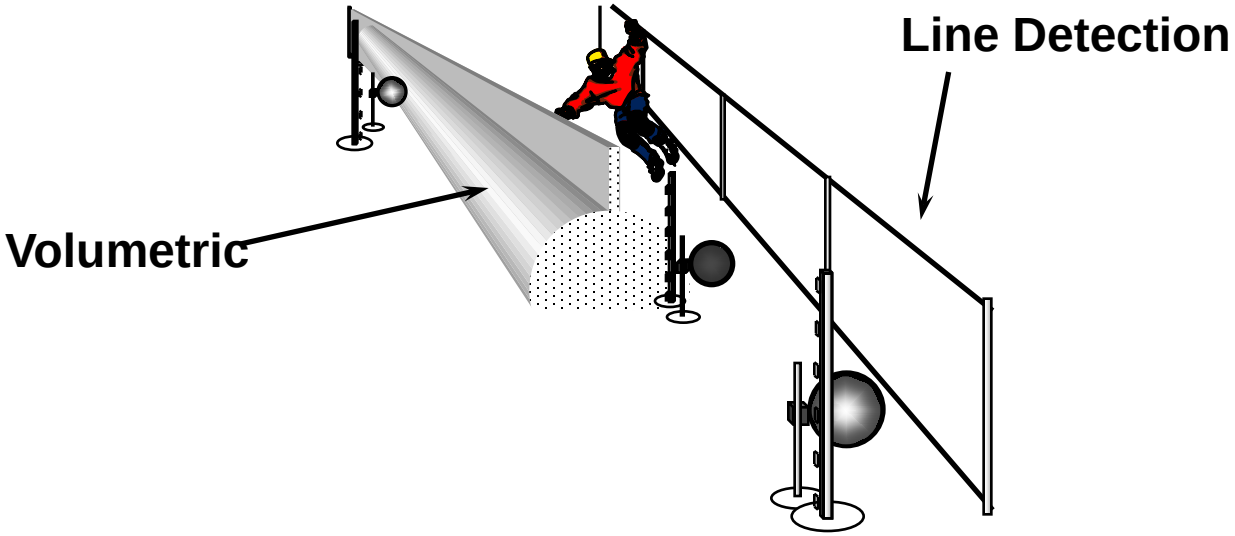




- Line of sight
  - No obstacles in the detection space
  - Requires flat ground surface
- Terrain following
  - Sensors detect on flat or irregular terrain

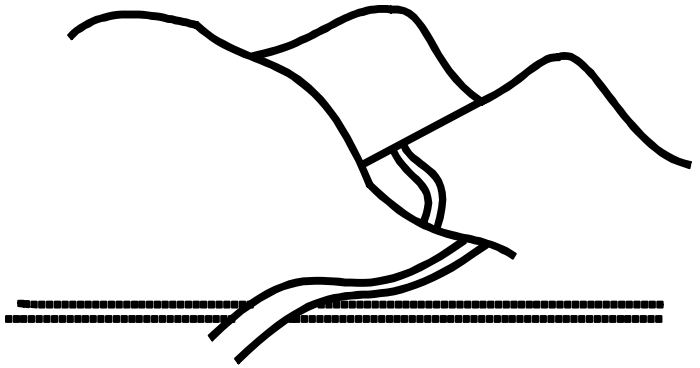
Volumetric or Line Detection

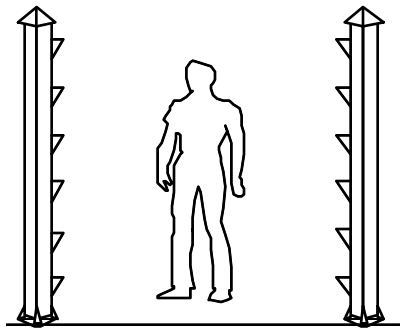
- Volumetric
  - Detection in a volume of space
  - Detection volume usually not visible
- Line detection
  - Detection along a line
  - Detection zone easily identified

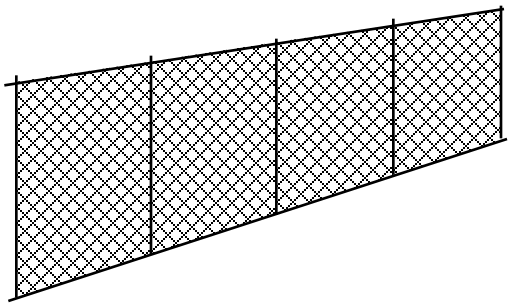


Sensor Mode of Application - Exterior

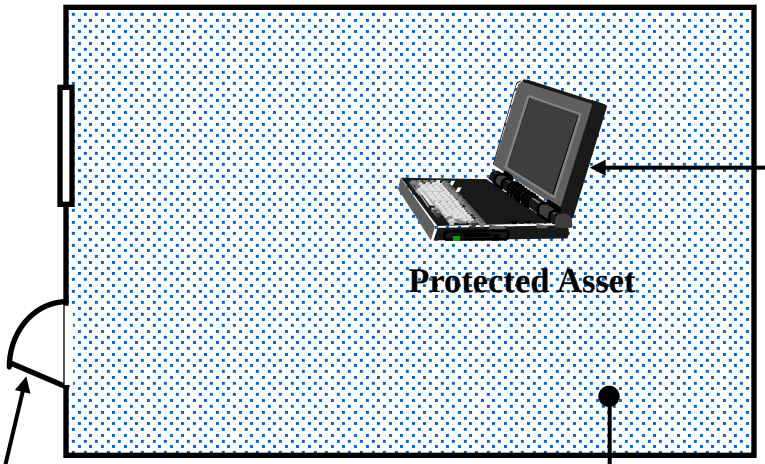
- Freestanding
- Buried line
- Fence associated







Modes of Application - Interior



- Proximity
  - Detection at an object

- Boundary
  - Detection at doors, windows, walls
  - Detection zone easily identified

- Volumetric
  - Detection in a volume of space
  - Detection volume usually not visible

Alarm Definitions

- Nuisance alarm rate (NAR)
  - Expected rate of alarms from an intrusion detection sensor unrelated to intrusion attempts
- False alarm rate (FAR)
  - Expected rate of alarms from an intrusion detection sensor not caused by intrusion attempts which cannot be attributed to known causes

Sensor Performance Characteristics

- Probability of detection (P_D)
  - Likelihood of detecting an adversary within the zone covered by an intrusion detection sensor
- NAR and FAR
- Vulnerability to defeat
  - Likelihood an intrusion detection sensor is exploitable due to design, installation, or maintenance
- All sensors can be defeated given the proper expertise, time, and tools

Performance Characteristics of Intrusion Detection Sensors

- $P_D = P_S * P_A$
  - P_D – probability of detection
  - P_S – probability of sensing
  - P_A – probability of assessment

Testing to Confidence Level

Number of Tests	*Number of Detections*	*Probability of Detection is at least XX% at 95% confidence*
30	**30 (-0)**	**90.5**
40	**39 (-1)**	**88.7**
50	**48 (-2)**	**87.9**
60	**57 (-3)**	**87.6**
80	**76 (-4)**	**88.9**
100	**95 (-5)**	**89.8**
120	**114 (-6)**	**90.4**

NAR / FAR Criteria

- Express in terms of:
  - Average number of nuisance or false alarms per week per sensor at proper P_D
  - If observed by closed circuit TV or visual, a higher value may be acceptable

Types of Testing

- Operability tests
- Performance tests
- Limited scope and whole system tests
- Evaluation tests

Operability Tests

- Simple measure of integrity on a frequent basis
  - Tests to check for significant malfunctions and continued operations
  - If the test fails, call maintenance and possibly take compensatory measures
- Examples (each shift):
  - Metal detectors
  - X-ray machines
  - One-quarter of the sectors in a perimeter

Performance Tests

- Check equipment over planned range of operation
- Perform repetitive tests on a PPS element or sub-function to develop performance values and confidence levels
  - Establishes or confirms the ability of a PPS element to meet a performance level
  - Provides comprehensive assurance of performance on a less frequent basis
  - Establish a baseline performance useful for design
  - Populate and validate analysis data

Limited Scope and Whole System Tests

- Used to determine or verify physical protection system performance
  - Test sections of the system together
  - Conduct whole system tests
  - Done initially and when PPS design changes
  - Identify areas of weakness or substandard performance in relation to design standards

Limited Scope and Whole System Test Examples

- Response force times to a particular target
- Probability of detection of contraband items during vehicle searches
- Verifying that an alarm can be initiated, communicated, annunciated, and assessed
- Force-on-force exercise

Evaluation Tests

- An independent or 3rd party evaluation to verify effectiveness of the physical protection system
- Regulatory Authority may conduct to verify the facility evaluation
- May be used as an element of licensing program

Summary of Perimeter Sensors

	Passive or Active	Covert or Visible	LOS or Terrain Following	Volumetric or Line Detection
Buried Line				
Seismic Pressure	P	C	TF	L
Magnetic Field	P	C	TF	VOL
Ported Coax	A	C	TF	VOL
Fiber Optic Cables	P	C	TF	L
Fence Associated				
Fence Disturbance	P	V	TF	L
Sensor Fence	P	V	TF	L
Electric Field	A	V	TF	VOL
Freestanding				
Active Infrared	A	V	LOS	L/VOL
Passive Infrared	P	V	LOS	VOL
Bistatic Microwave	A	V	LOS	VOL
Dual Technology	A	V	LOS	VOL
Video Motion	P	C	LOS	VOL

Features of a Good Perimeter Sensor System

- Continuous line of detection
- Protection in depth
- Complementary sensors
- Alarm combination and priority schemes
- Clear zone
- Sensor configuration

Features of a Good Perimeter Sensor System *(cont'd)*

- Site-specific system
- Tamper protection
- Self-test capability
- Suitable for physical and environmental conditions
- Integration with assessment system
- Integration with barrier delay

Features of a Good Interior Intrusion Detection System

- Protection in depth
- Complementary sensors
- Alarm combination and priority schemes
- Sensor configuration

Features of a Good Interior Intrusion Detection System *(cont'd)*

- Site-specific system
- Tamper protection
- Self-test capability
- Suitable for physical and environmental conditions
- Integration with assessment system
- Integration with delay

Sensors Summary

- Sensor classification
- Alarm definitions
- Sensor performance characteristics
- Intrusion detection system

Microwave Sensors

Learning Objectives

After completing this module, you should be able to:

- Describe the fundamental principles of microwave sensors
- Identify in what application microwave sensors are suitable for providing effective detection for given threat tactics and environmental conditions
- Evaluate and determine effective placement of microwave sensors
- List the advantages and disadvantages of microwave sensors

Sensor Classification

Microwave (MW) Sensors	
Active	Passive
Covert	Visible
Line of sight	Terrain following
Volumetric	Line
Mode	Freestanding Bistatic or Monostatic Configuration

Bistatic Microwave Sensors

- Transmitter and receiver at opposite ends of detection zone
- Received signal is vector sum of direct transmitted signal and all reflected signals
- Moving objects in zone cause a change in net vector summation causing signal strength variations
- Variations (above or below) exceeding preset level generate an alarm

MW Detection Parameters

- Detection accomplished by:
  - Beam break
  - Multi-path signal changes
  - Jamming
- Typical operating frequency
  - 10.525 Ghz +/- 25 MHz
- Typical carrier modulation frequencies - 3, 5, 8, 13 Khz
  - Beam width is determined by antenna size, design, and frequency

Exterior Bistatic Microwave

Exterior Monostatic MW Sensor

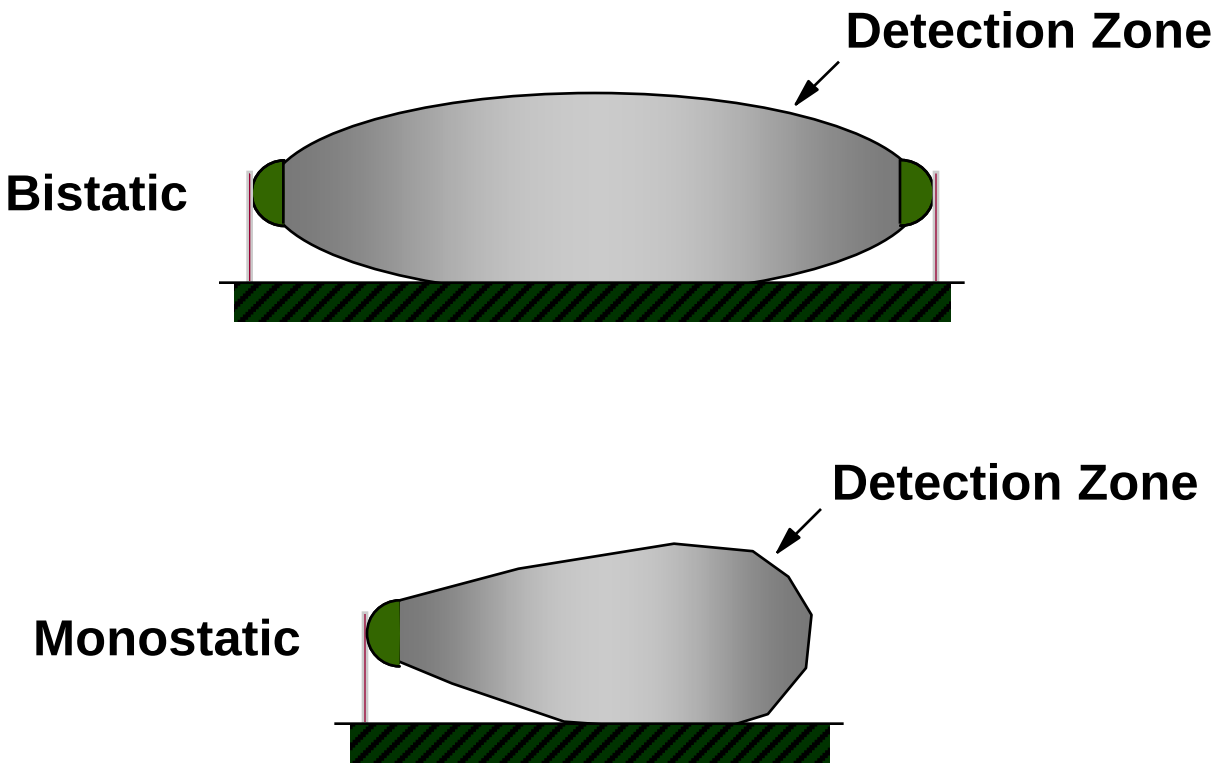
- Transmitter and receiver collocated
- Receiver establishes a reference level based on reflected signals
- Motion in detection zone causes a change relative to the reference level

Monostatic MW Detection Parameters

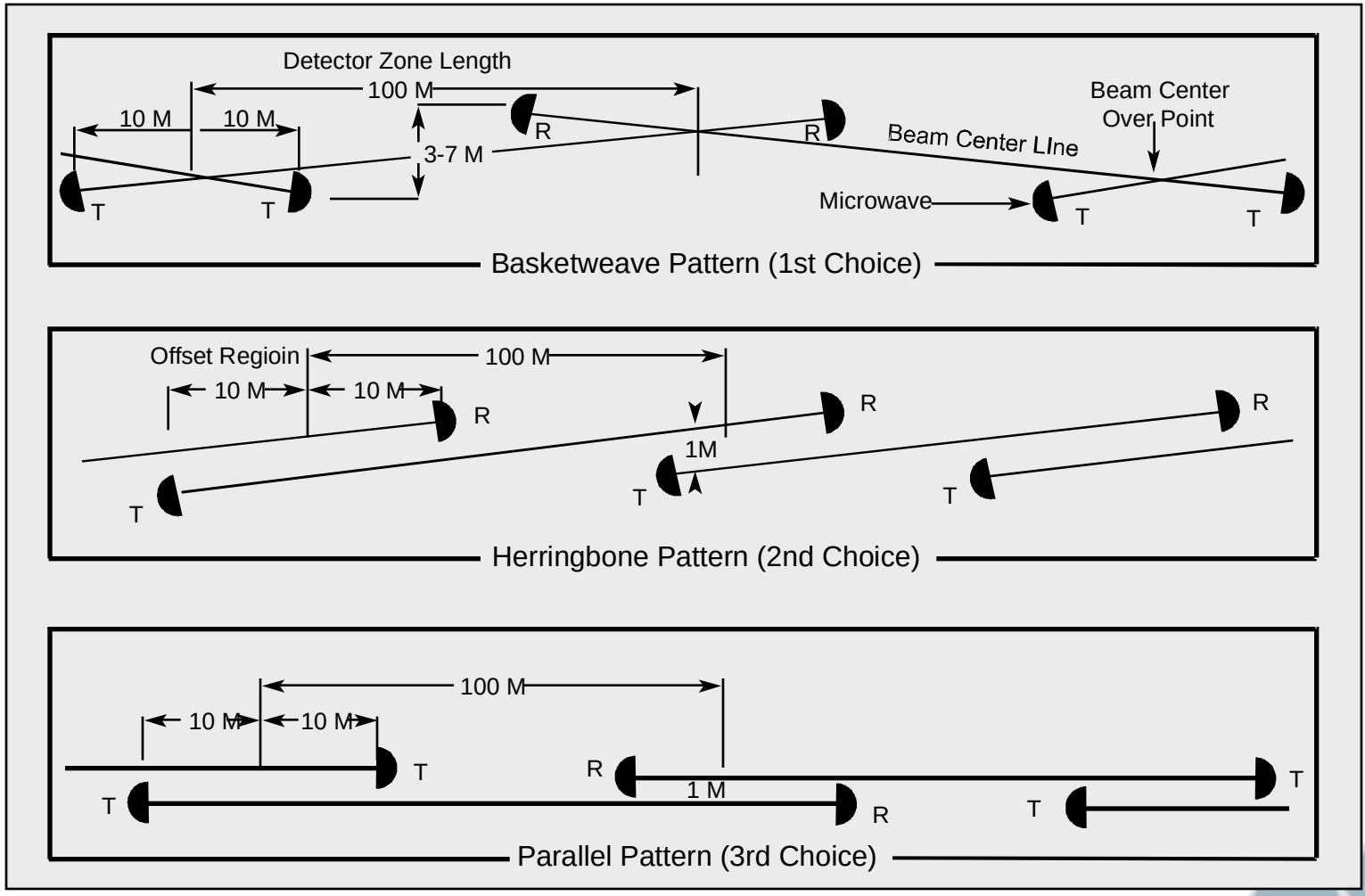
- Typical operating frequency:
  - 10.525 GHz + 25 MHz
- Detection accomplished by:
  - Change in the reflected mw signal from an established reference level
- Operating range
  - Variable from 15 to 65 m
- Beam width:
  - Vertical and horizontal approximately 11.5 degrees

Monostatic Microwave - Example

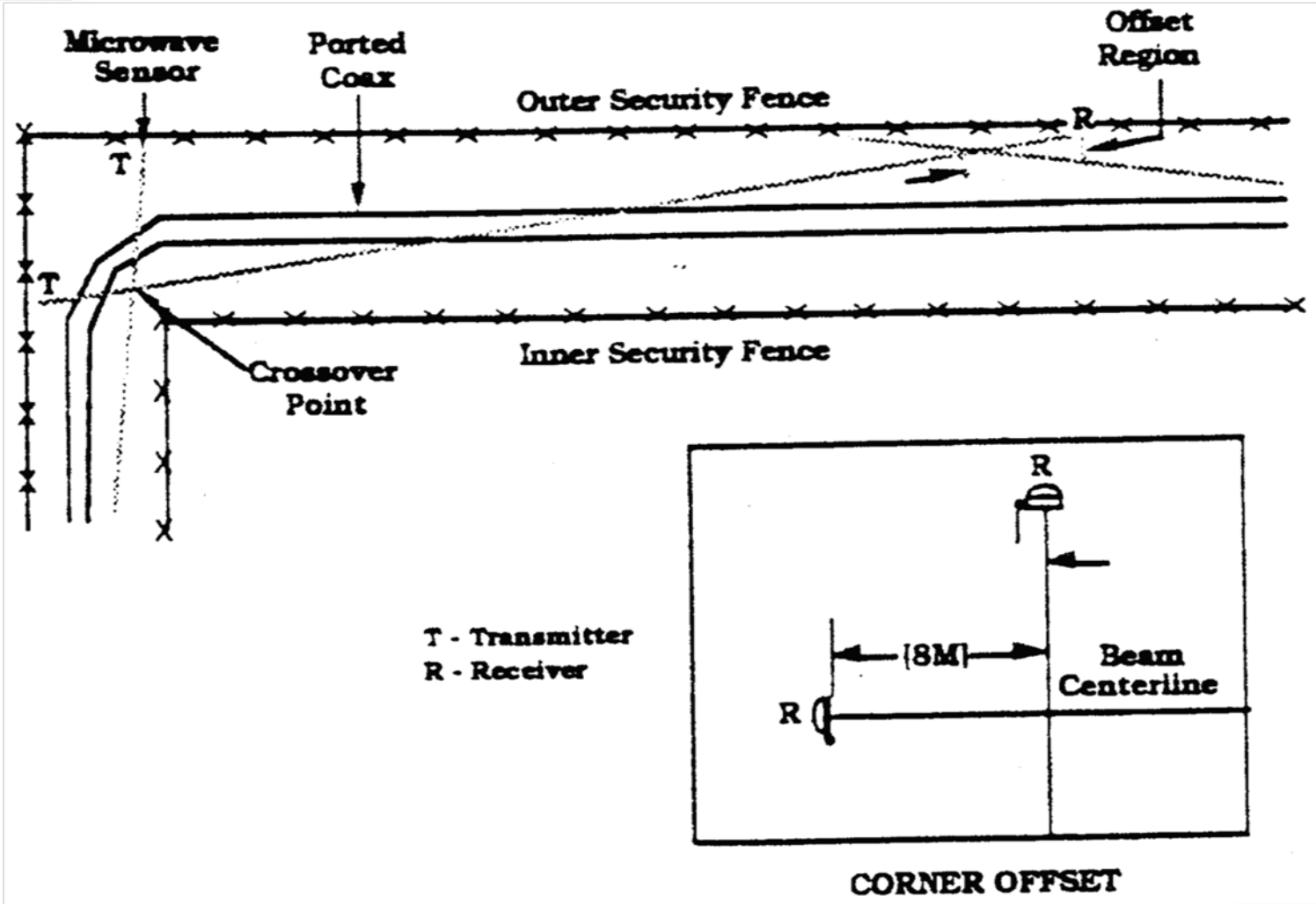
MW Detection Patterns



Examples: Microwave Installation Patterns

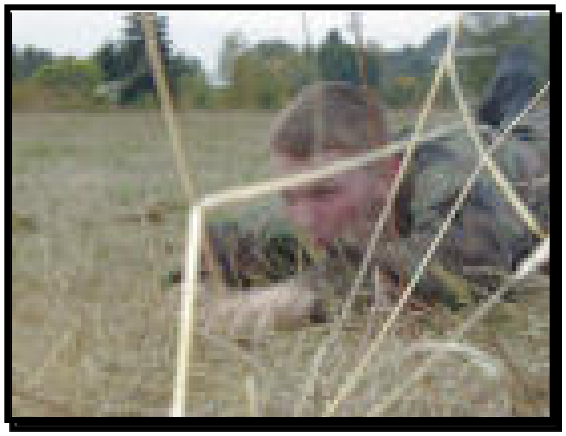


Microwave Offset Examples



Sensor Bed Requirements

- Sensor bed
  - Flatness between the transmitter and the receiver is + 0 and – 15 cm
- Antenna height
  - 30 to 60 cm above sensor bed surface
- Slope of plane
  - No more than a 0.4 cm elevation change in 3.3 m from any point on the surface of the plane



Sensor Bed Requirements *(cont'd)*

- Sensor bed surface
  - 10 cm of river bed gravel, no larger than 3 cm diameter with a neutral density color preferred
  - Crushed rock that will pass through a 2.5 cm screen may be used if fine gravel is removed
- Drainage
  - Water must not stand on the sensor bed surface or flow across the surface
  - Any rain that falls on the surface must percolate into the gravel and flow off to the side of the sensor zone beneath the sensor bed surface

Use of Reflectors

- Size of reflector
- Distance from transmitter
- Stability of reflector mounting

Reflectors mounted to a building usually work well, other applications usually cause problems!

MW Alignment and Testing

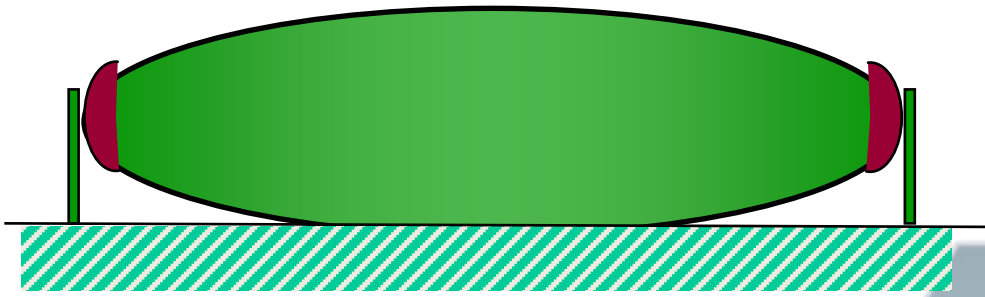
- Alignment
  - Automatic gain control (AGC)
  - Visual
- Testing
  - Crawler simulation
  - Walk test
  - Jump test

Performance Testing of Exterior Microwave Sensors

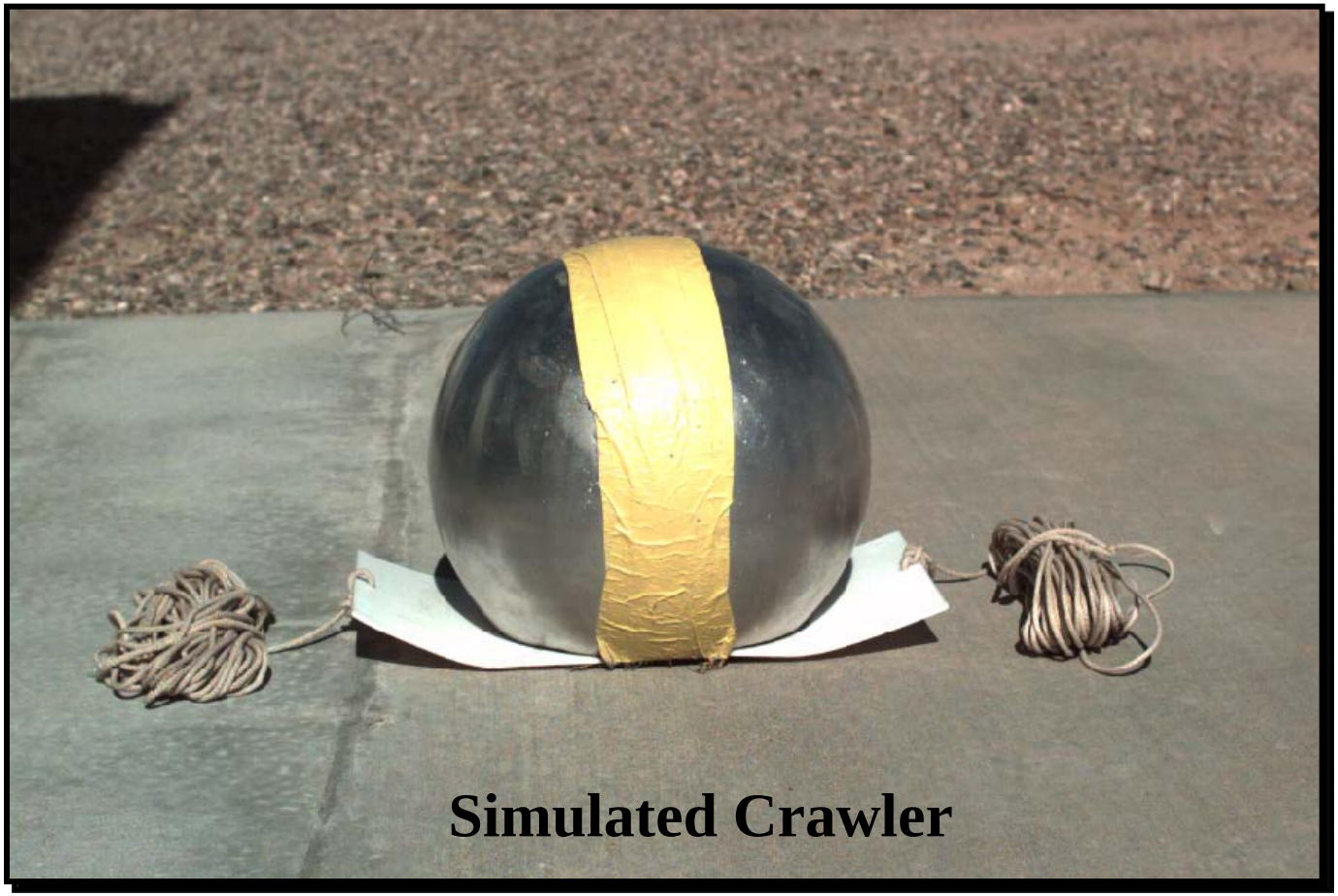
- Detection tests: average, low, and high velocity
- As a minimum, tests should be done
  - Near crossover points
  - At the center of each detection zone
- The number of trials done at each location should be sufficient to verify acceptable P_D for each velocity of interest

Performance Testing of Bistatic Microwave Sensors

- Detection envelope
  - Walk tests
- Crawl detection
  - Ball drags
- Jump-over detection



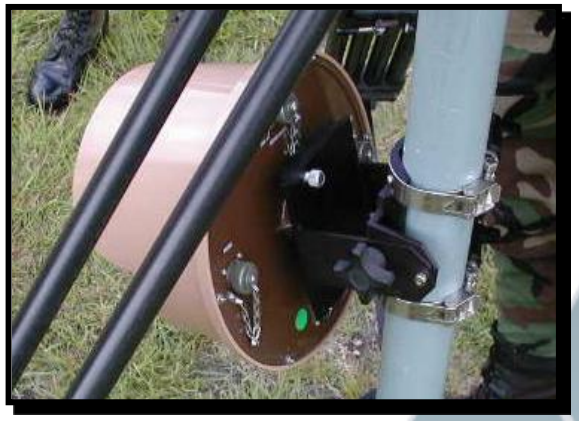
Performance Testing of Bistatic Microwave Sensors *(cont'd)*



Simulated Crawler

Microwave Sensor Maintenance

- General manufacturer guidelines
- Vegetation removal
- Inspect zone for erosion
- Visual inspection for corrosion or damage
- Test battery back-up
- Periodic performance testing



Bistatic MW Sensor Performance Characteristics

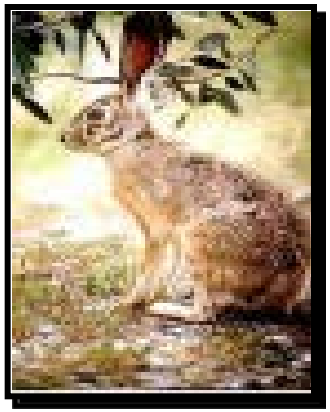
- P_D
  - Detection volume is large compared to other intrusion sensors
- NAR / FAR
  - Moving metal objects in field
  - Surface water
  - Blowing snow
  - Small animals
  - Vegetation

Bistatic MW Sensor Performance Characteristics *(cont'd)*

- Vulnerability to defeat
  - Snow accumulation reduces sensitivity
  - Tamper defeat of receiver
  - Jump or crawl
  - Slow movement
  - Receiver capture using secondary transmitter

Monostatic Microwave Performance Characteristics

- P_D
  - Large detection volume
- NAR / FAR
  - Moving metal objects in field
  - Surface water
  - Blowing snow
  - Small animals
  - Vegetation
  - Vibration

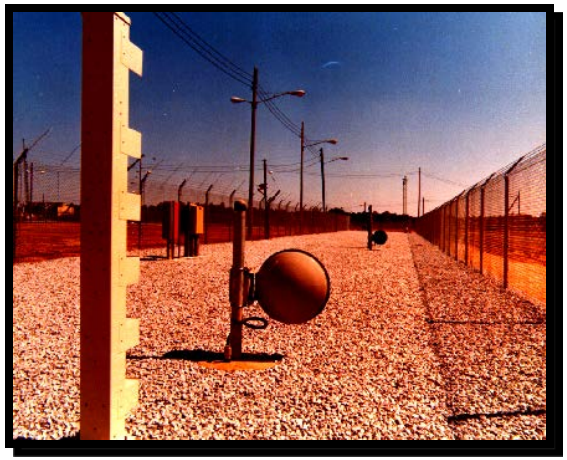


Monostatic Microwave Performance Characteristics *(cont'd)*

- Vulnerability to defeat
  - Snow accumulation
  - Tamper defeat
  - Slow movement
  - Jump or crawl
  - Re-aiming

Microwave Design Layout Factors

- Other sensors
  - Complimentary
  - Interference
- Zone width
  - Crossover angles
  - Distance from fences
  - Beam centerline angle relative to fence
- Sensor characteristics
  - Beam width, frequency, antenna design



Microwave Design Layout Factors *(cont'd)*

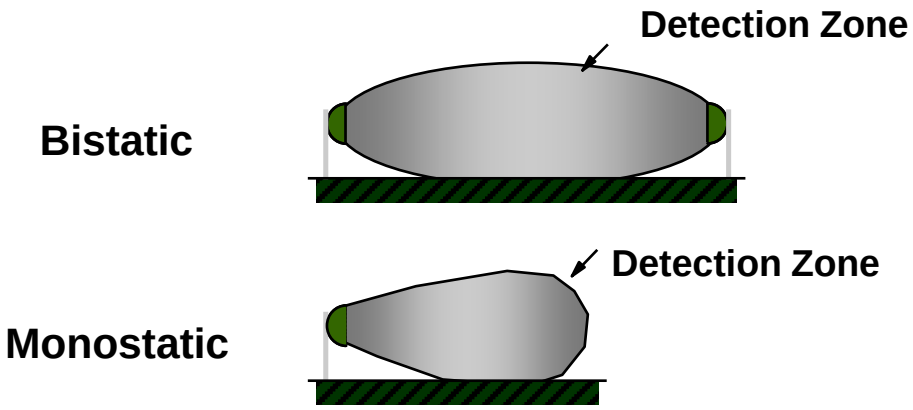
- Sector length affected by
  - Detection capabilities
  - Assessment
  - Terrain
    - Number and location of grade breaks
    - Severity of grade changes
  - Corners
    - Angles
    - Distance between
  - Portals

MW Sensor Strengths and Weakness

- Strengths
  - Large detection volume not easily defined visually
  - Combines well with other sensors
- Weaknesses
  - Requires good site preparation
  - Difficult to use in narrow zones

Microwave Sensor Summary

- Bistatic - perimeter; Monostatic - special uses
- Flat terrain required (gravel preferred)
- Overlap required to provide continuous detection
- Jump or crawl defeat
- Deep snow detection problems
- NAR / FAR - small animals, water puddles



Fence Disturbance Sensors

Learning Objectives

After completing this module, you should be able to:

- Describe the fundamental principles of fence disturbance sensors
- Identify in what application fence disturbance sensors are suitable for providing effective detection for given threat tactics and environmental conditions
- Evaluate and determine effective placement of fence disturbance sensors
- List the advantages and disadvantages of fence disturbance sensors

Sensor Classification

Fence Disturbance Sensors	
Active	Passive
Covert	Visible
Line of sight	Terrain following
Volumetric	Line
Mode	Fence mounted

Fence Disturbance Sensors

- Detect penetration / climbing fence
- Technological types
  - Mechanical
  - Electromechanical
  - Strain sensitive cable
  - Geophone

Fence Disturbance Sensor

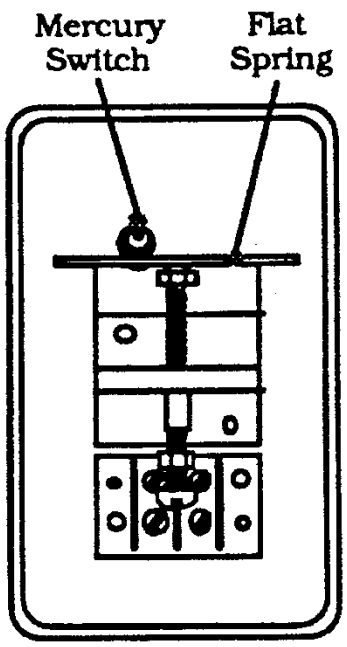
Operational Principles

- Mechanical motion
  - Usually a mercury switch
    - Activation primarily due to low frequency movement of fence
  - Detection of shock is by mechanical means
- Electro-mechanical motion (analog)
  - Detectors may be piezoelectric crystals, fence mounted geophones, electric cables, or fiber optic

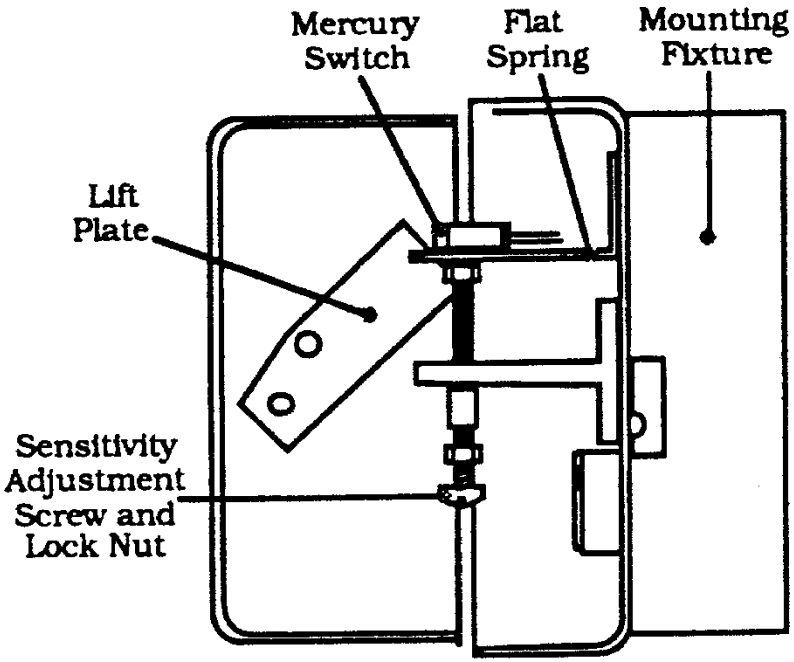
Operational Principles *(cont'd)*

- Strain sensitive cable
  - An "event" occurs when the signal exceeds a preset threshold
  - When the number of events exceeds a preset "count" within a preset time window, an alarm occurs
- Geophone
  - Moving coil in a magnetic field

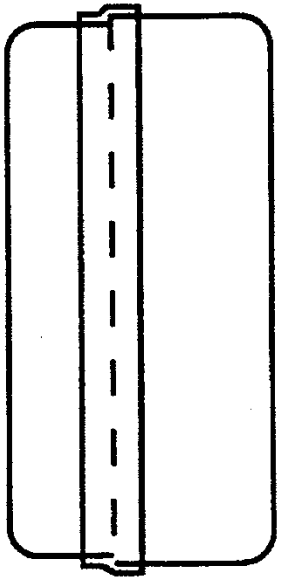
Fence Disturbance Sensor Assembly



Box with Cover Removed

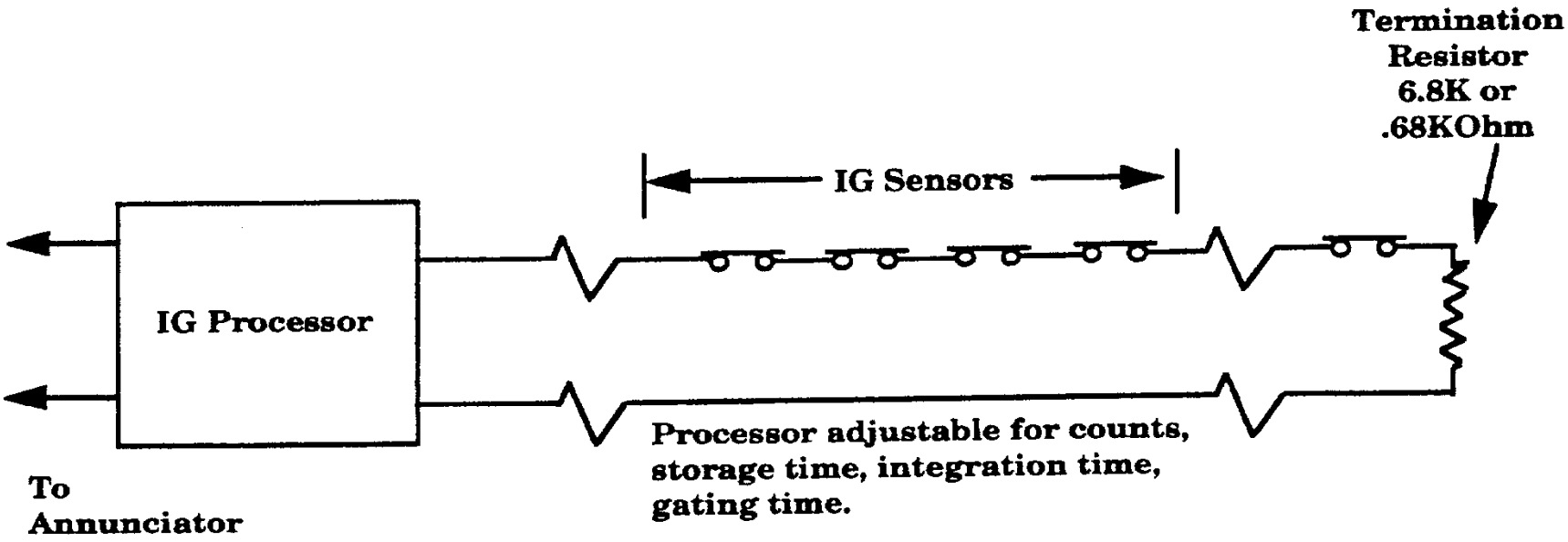


Box and Cover Open Position
[Side View/Cutaway]

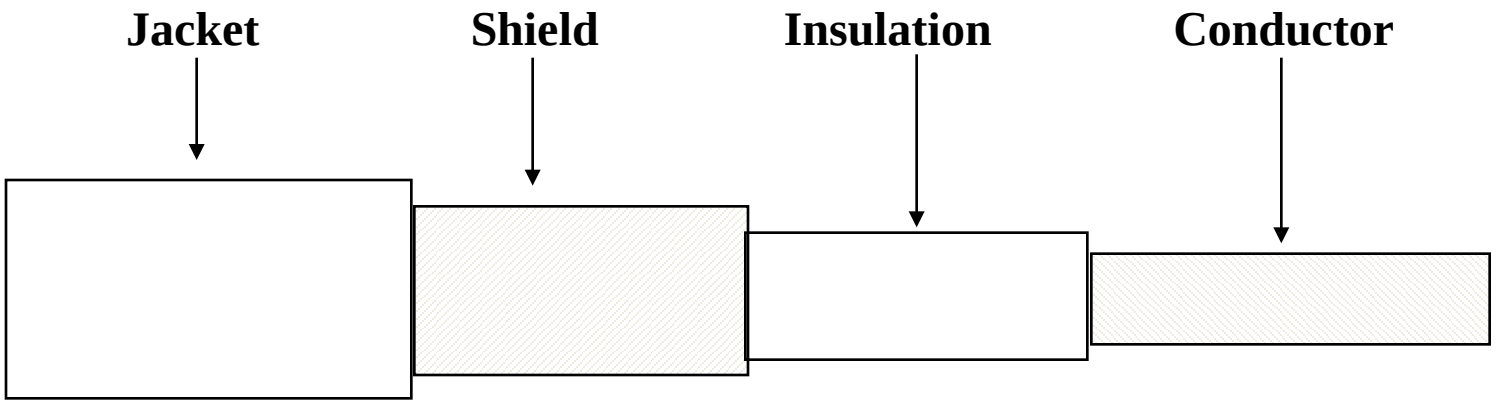


Box and Cover Closed Position

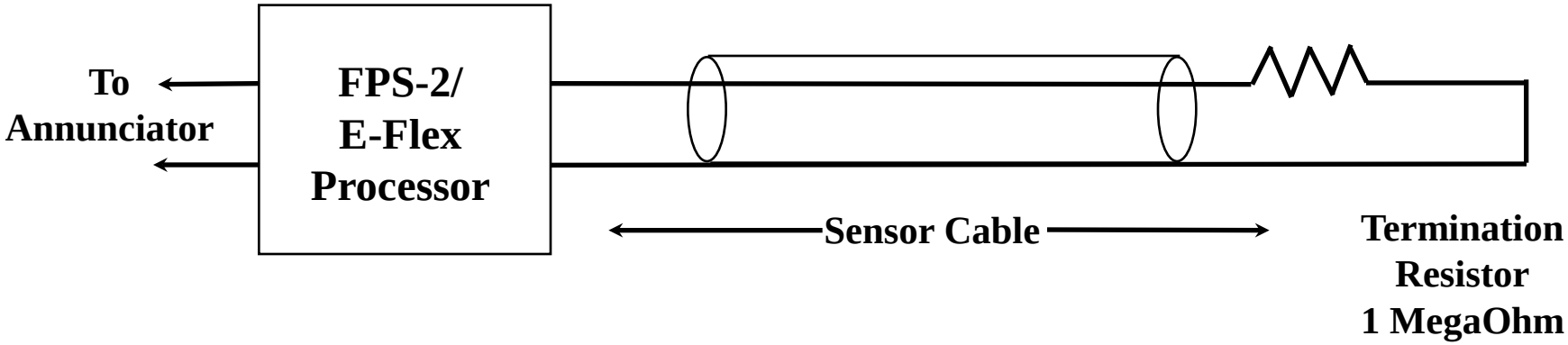
Inertiaguard Schematic



Analog Fence Sensor Cable



FPS-2 / E-Flex Schematic



Fence Requirements

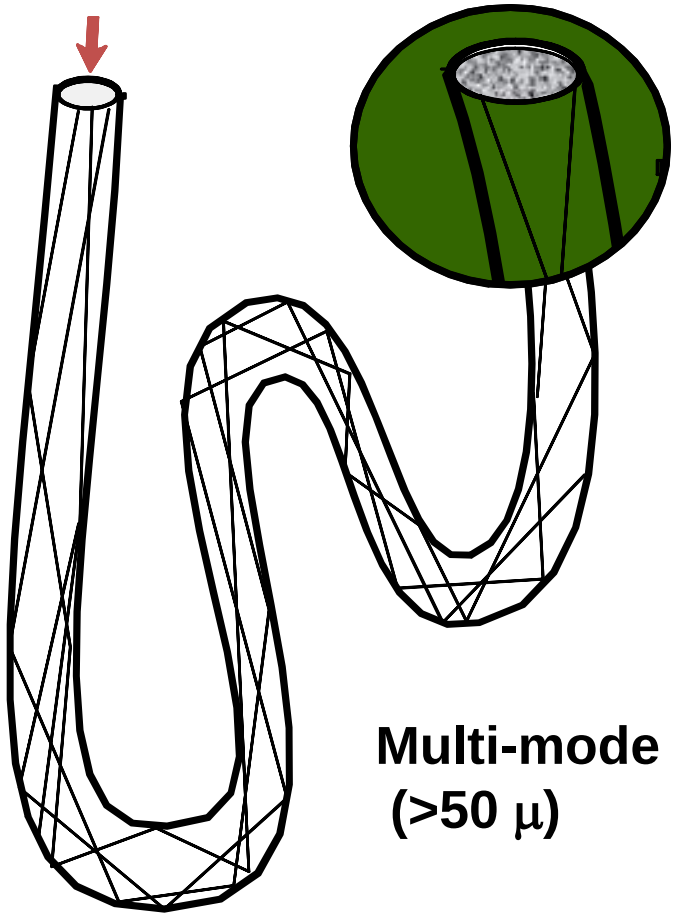
- Proper tension
  - Fabric deflects no more than 2.5” (64 mm) for a 30 lb. (13.6 kg) pull centered between posts
- Rigid posts
  - Post moves no more than ½” (13 mm) for a 50 lb. (22.7 kg) pull applied 5’ (1.5 m) above the ground
- No rattles
  - Signs, loose ties, hog rings, etc

Requirements for Satisfactory Sensor Operation

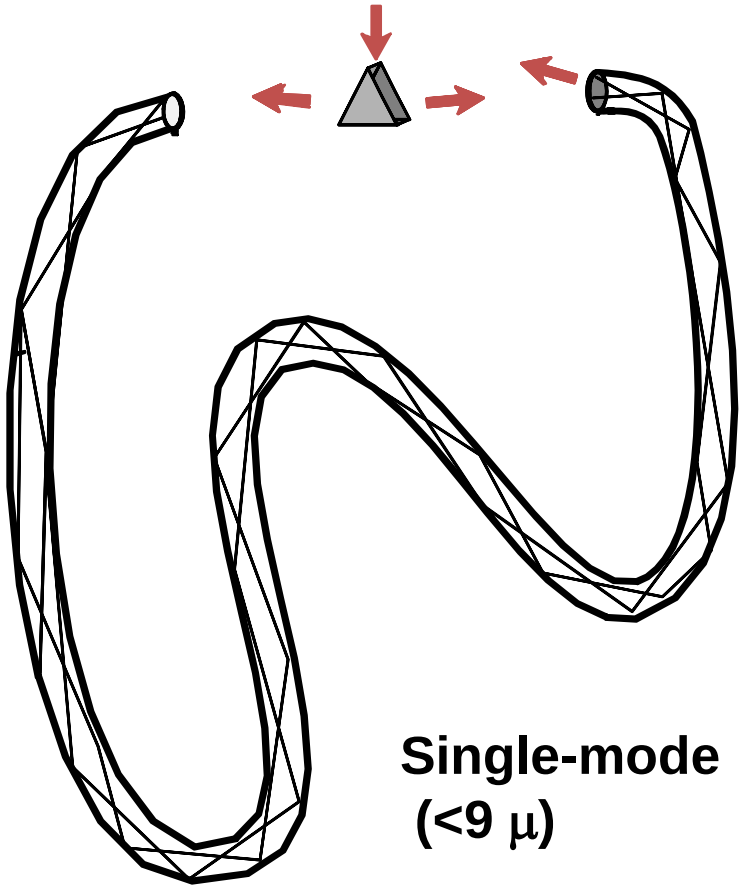
Fiber Optic Sensors

- Mode of application
  - Buried
    - Sod
    - Gravel
  - Fence mounted
- Covert (buried) or visible (fence mounted)
- Terrain-following
- Line detection

Fiber Optic Intrusion Detection Sensors

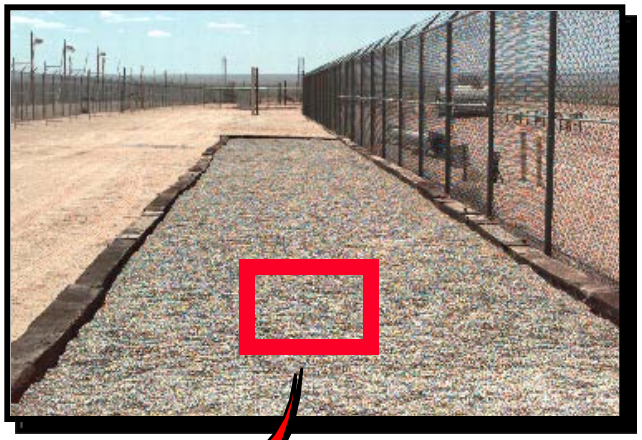


Multi-mode
(>50 μ)



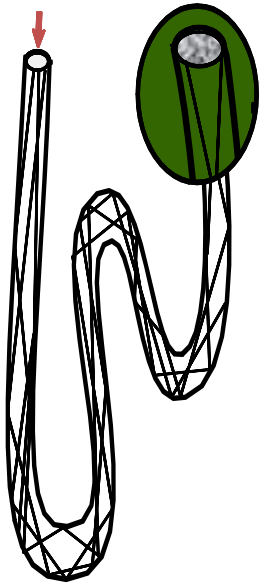
Single-mode
(<9 μ)

Buried Fiber Optic Sensors



Fiber Optic Sensor Summary

- Fiber Characteristics
  - Single mode
  - Multimode
- Mode of Application
  - Buried
    - Unique problems
  - Fence mounted
    - Very similar to other fence disturbance sensors



Fence Sensor Performance Characteristics

- P_D - affected by
  - Quality of fence
  - Processor settings (count, timing logic)
  - Method of attack and tools used
- NAR / FAR - causes of nuisance alarms
  - Loose fence fabric
  - Tree branches, signs, chains
  - Wind, rain, hail

Fence Sensor Performance Characteristics *(cont'd)*

- Vulnerability to defeat
  - Digging under fence
  - Bridging over fence
  - Knowing timing logic
  - Careful removal of sensor cable from fence
  - Weather station attacks

Fence Sensor Testing

- Climbing
- Cutting
- Simulated cut (tap or mechanical impact)

Portable Fence

Fence Sensor Maintenance

- Remove debris from fence
- Shake fence to locate and correct sources of rattles
  - Signs
  - Loose fabric ties
  - Gates
- Inspect sensor for loose cable

Fence Disturbance Sensor Summary

- Relatively high NAR / FAR during wind
- Line sensor - easily avoided by not touching fence
  - Bridging, tunneling
- Relatively inexpensive
- Easy to install
- Variety of types available
  - Mechanical
  - Electromechanical
  - Strain sensitive cable
  - Fiber optic

Volumetric Sensors

Learning Objectives

After completing this module, you should be able to:

- Describe the fundamental principles of volumetric sensors
- Identify in what application volumetric sensors are suitable for providing effective detection for given threat tactics and environmental conditions
- Evaluate and determine effective placement of volumetric sensors
- List the advantages and disadvantages of volumetric sensors

Volumetric Sensor Technologies

- Passive infrared
- Monostatic microwave
- Dual technology (Dual-tech)

Sensor Classification

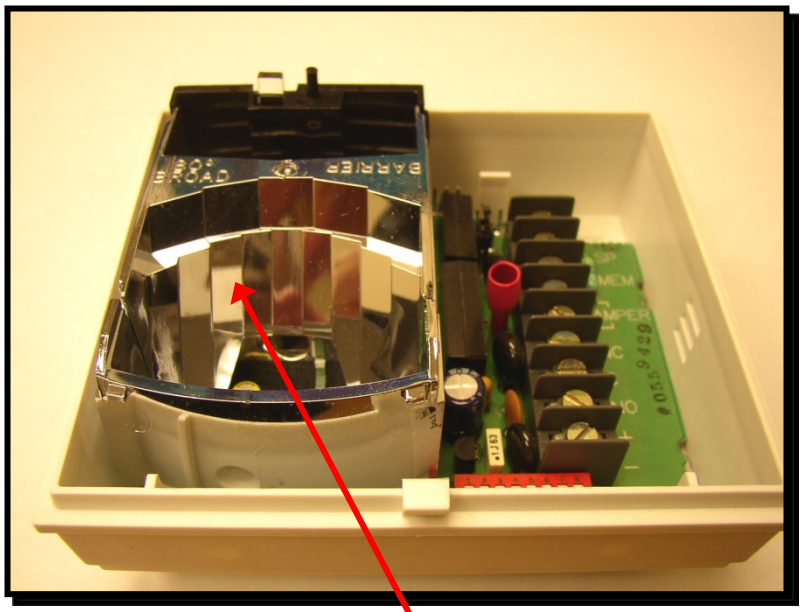
Interior PIR Sensors	
Active	Passive
Covert	Visible
Line of sight	Terrain following
Volumetric	Line
Mode	Freestanding

PIR Basic Principles of Operation

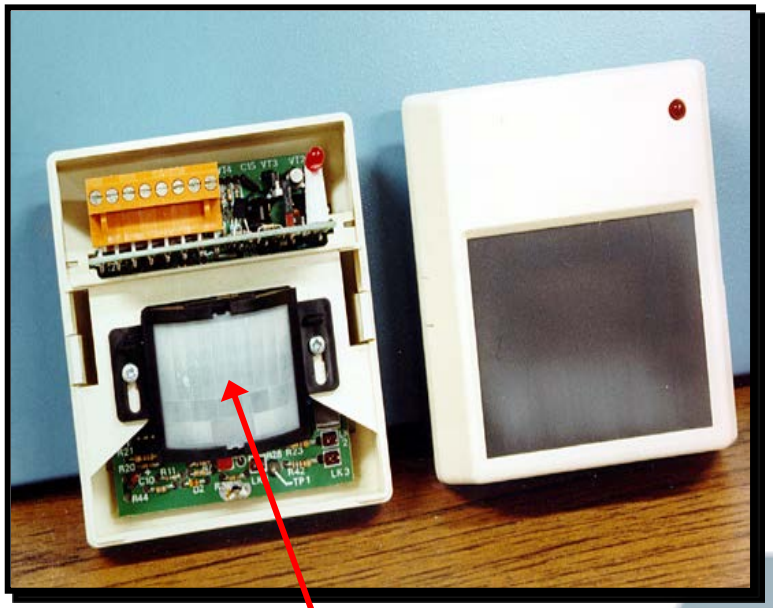
- Receives infrared (IR) energy (heat) from objects in area being protected
- Objects emit infrared energy proportionate to their temperature and emissivity
  - Ceilings, walls, floors, furniture, etc.
- Detection of motion is accomplished by measuring changes in received infrared energy

PIR Operation - Lens

- A parabolic mirror or Fresnel lens provide a field-of-view with multiple detection segments



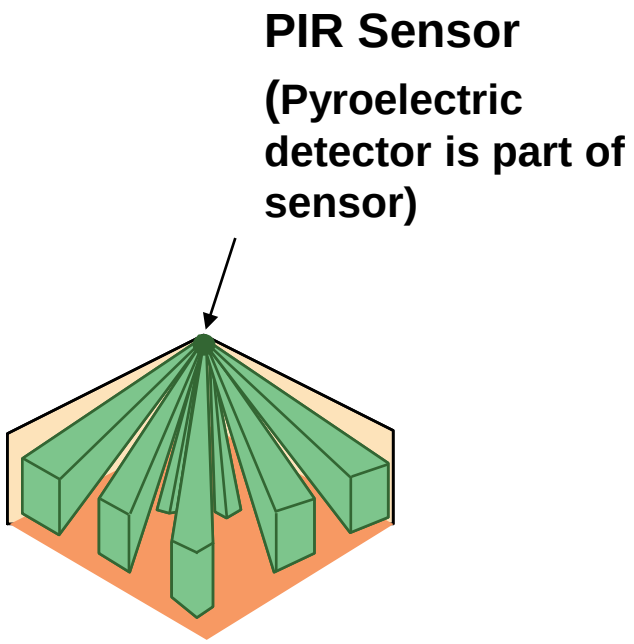
Parabolic mirror



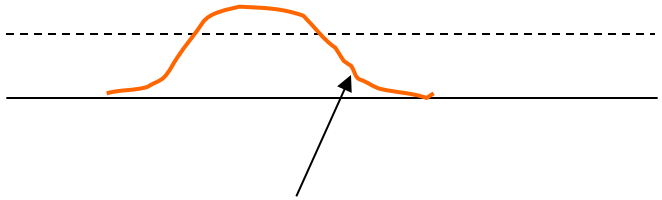
Fresnel lens

PIR Operation - Detector

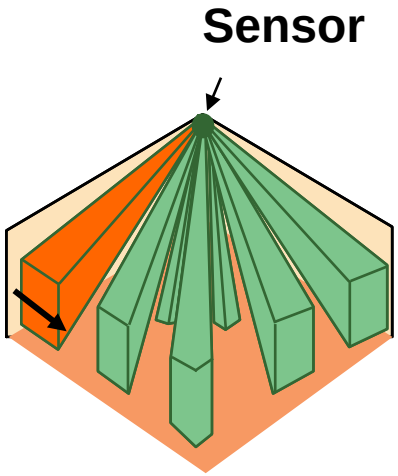
- Pyroelectric detector converts changes in IR energy (heat) to an electrical signal
- Segmented optics focus IR energy onto a pyroelectric detector



Simple PIR Operation

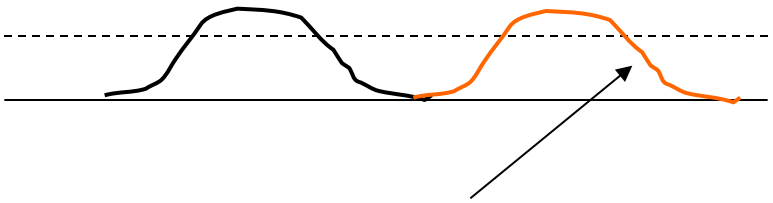


Pyroelectric detector electrical signal out

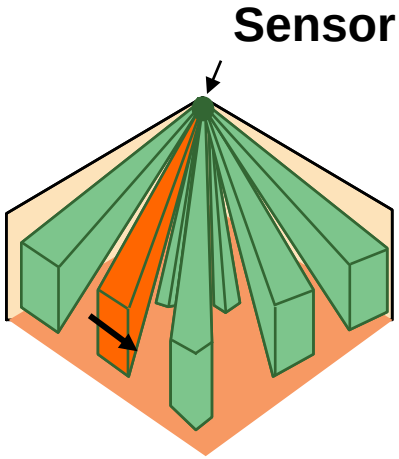


- A change in IR energy is detected by the pyroelectric detector when a person (or warm object) moves through a segment

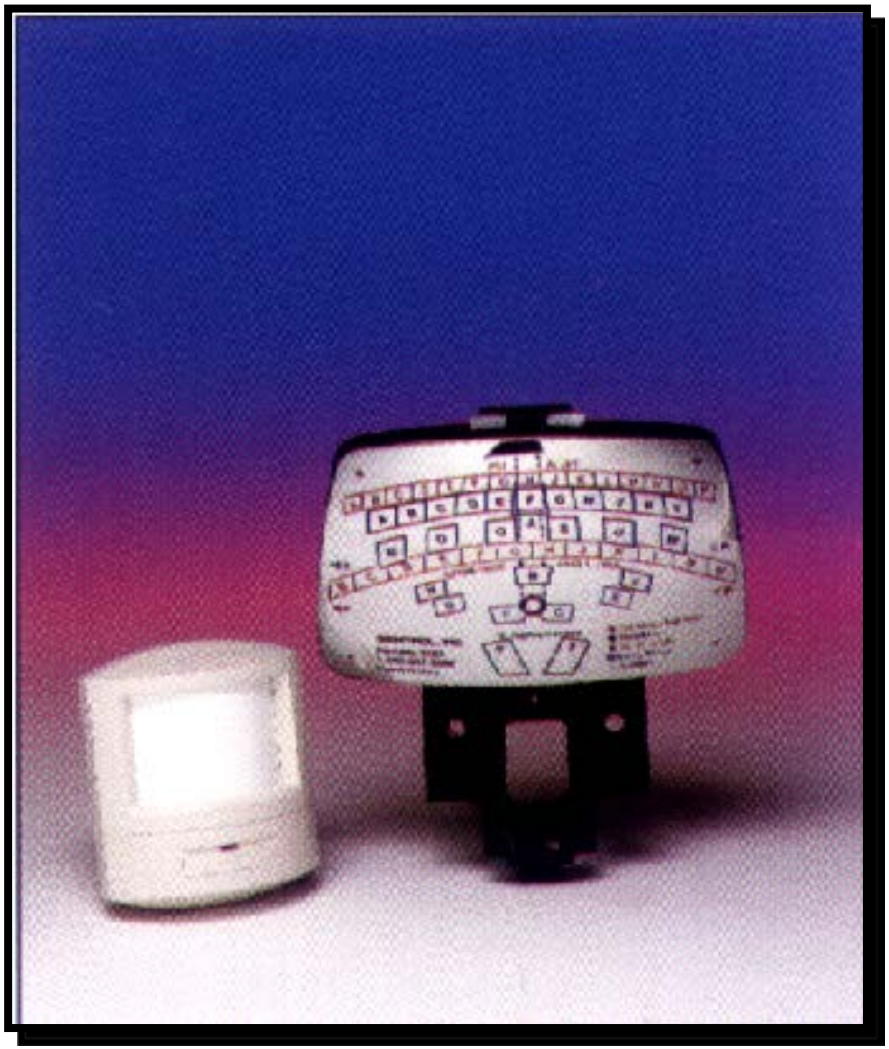
Simple PIR Operation *(cont'd)*

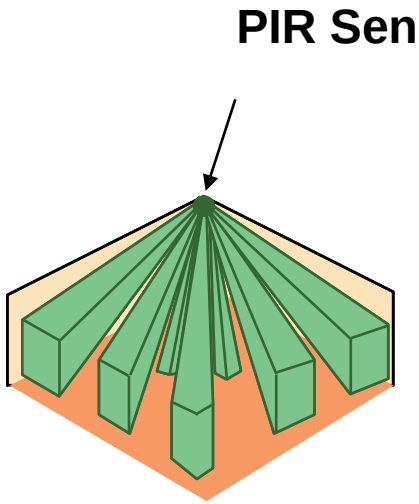


Pyroelectric detector electrical signal out

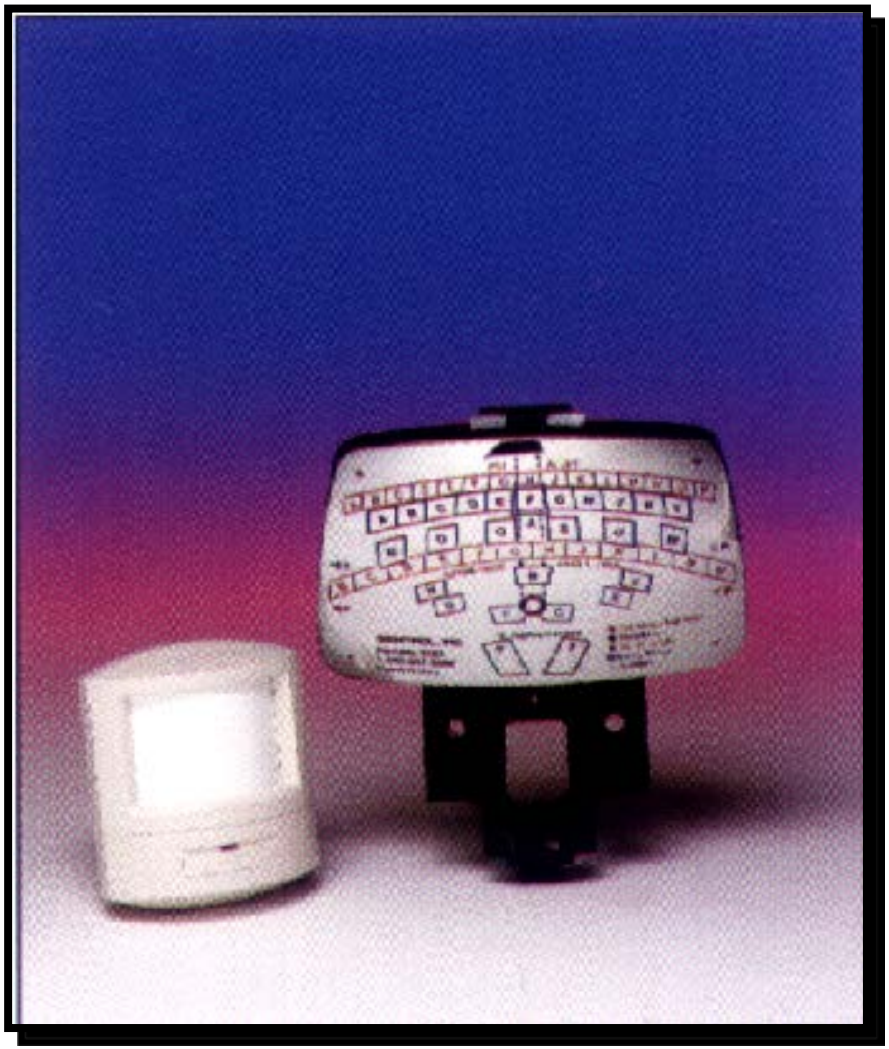


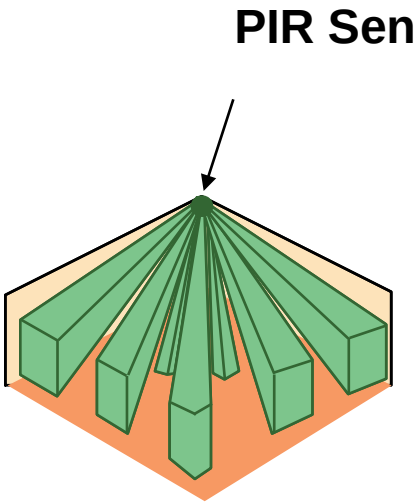
PIR Segment Locator



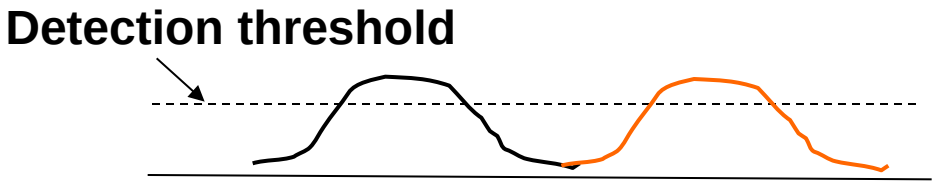


PIR Segment Locator



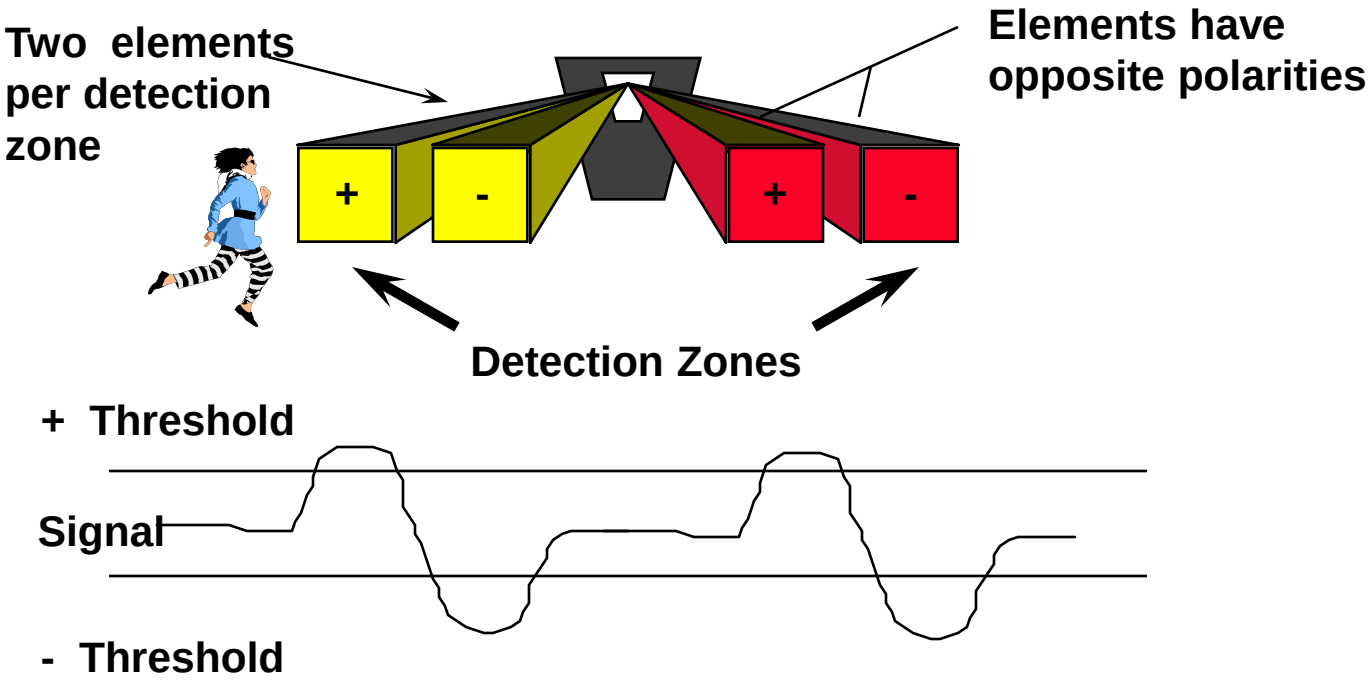


PIR Operation – Electronic Processing



- Electronic processing
  - Detection threshold
  - Count number of pulses over threshold (number of detection segments ‘seeing’ changes in IR energy)
  - Pulse count of 1 or 2 or 3, etc. within time window to generate alarm
  - Nuisance and false alarms reduced
  - Signal processing and sophistication varies among manufacturers

Dual-Element or Quad-Element Pyroelectric Detectors



Nuisance Alarms in IR Sensors

- Localized heating
  - Heaters / radiators
  - Sunlight
  - Nearby unshielded incandescent light
- Moving air
- Animals / insects
- Sensor / mounting structure vibrations

PIR Sensor Vulnerabilities

- Can be defeated by very slow motion
- May not detect intruder (sensitivity reduced) if room temperature is above 90°F
- Possible for intruder to wear “insulated” suit
- Detection effectiveness reduced for motion directly toward or away from sensor
- “Fogging” or masking of lens

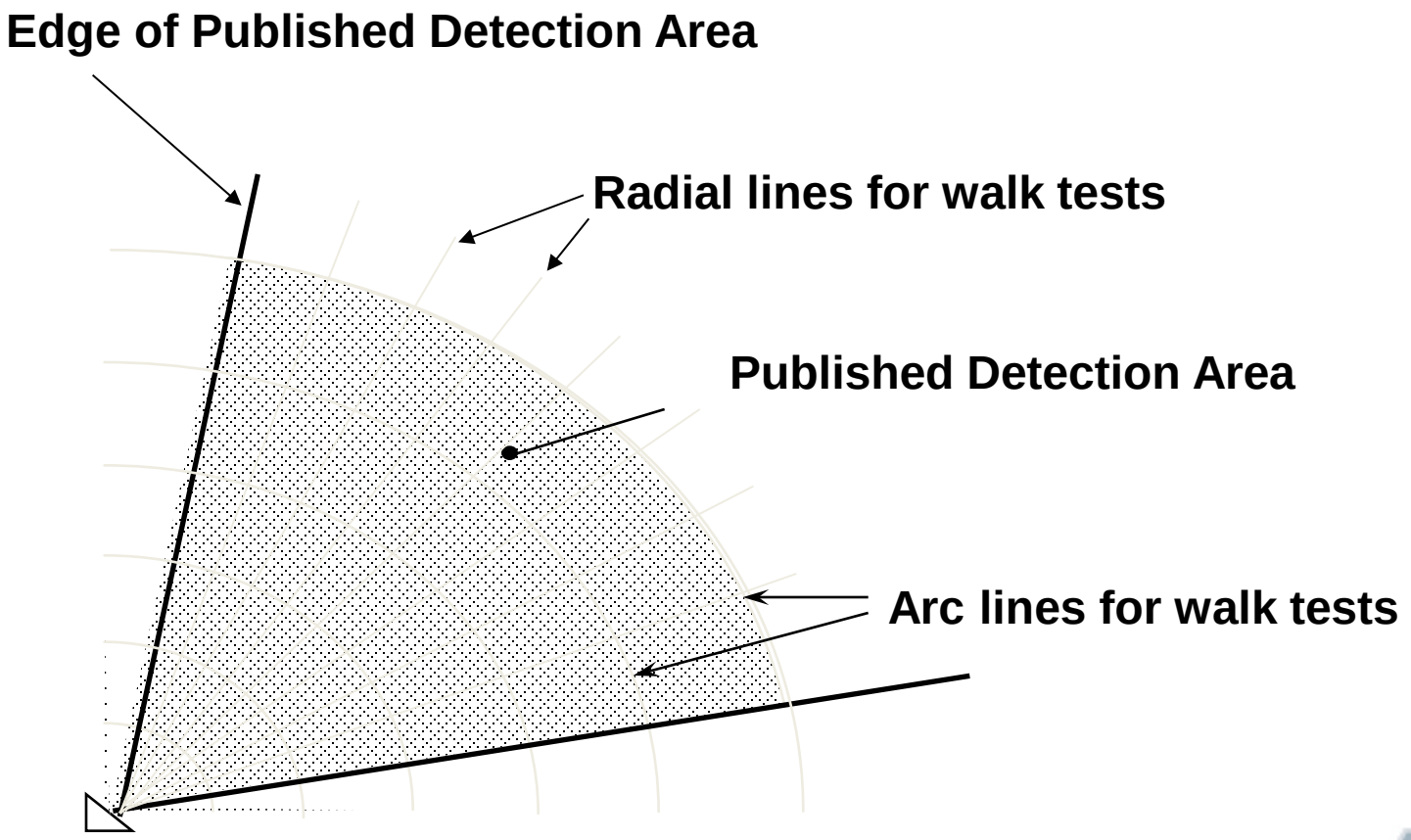
PIR Laboratory Performance Testing

- Ideal, baseline testing
  - Performed under ideal or optimum conditions
    - Room temperature 68 - 75 degrees F
    - Empty room (no equipment, furniture, etc.)
    - No or minimal nuisance alarm sources
  - Establishes sensor detection probability
  - Verify manufacturer's published detection area
  - Monitor sensor for false and nuisance alarms

PIR Laboratory Performance Testing *(cont'd)*

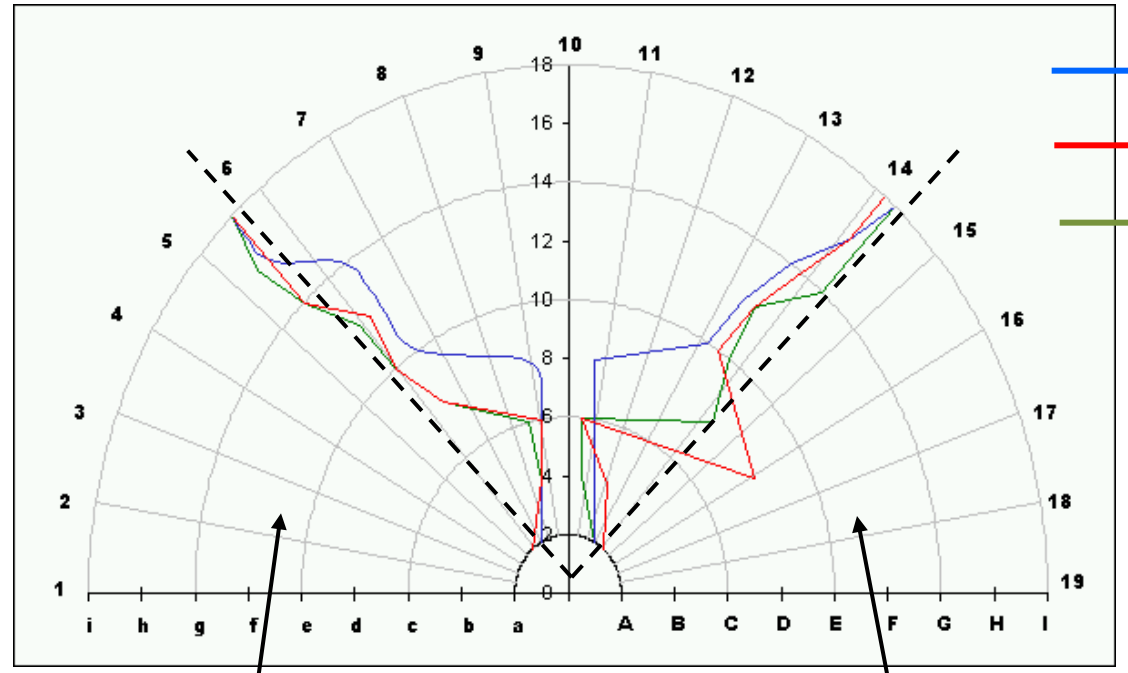
- Ideal walk testing
  - Multiple sensor units
    - Same make / model and different lots
  - Human test subject
    - Small person – 5 foot tall, weighing 90-100 pounds (40-45 kilograms)
    - Arms of test person held tightly across chest
    - Walk rate of test target at 1 ft/second (0.3 m/s)
  - Record where alarms are generated along all paths
  - Establish baseline detection pattern and probability based on performance data
  - Perform multiple sets of tests at different times

PIR Baseline Testing



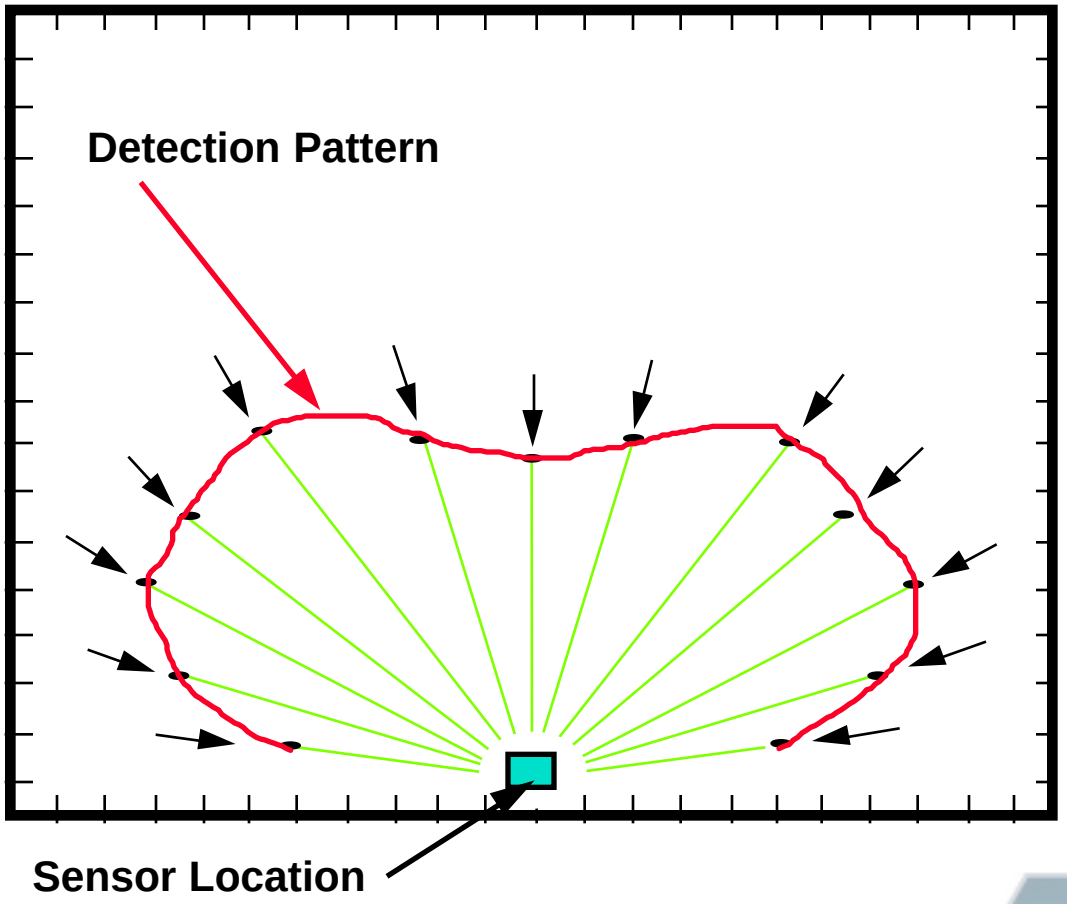
PIR: Walk Test - Most Sensitive Direction

Three individual units of the same model



PIR Detection Pattern

Basic PIR detection pattern with the intruder walking towards the sensor



Additional Performance Testing

- Slow walk (0.15 m/s)
- Least sensitive direction
  - Directly towards sensor
- Crawl
  - 1 foot / second (0.3 m/s)
- Vulnerabilities
  - High room temperature 90^{o}+ F (32^{o} + C)
  - Mask sensor
  - Mask target

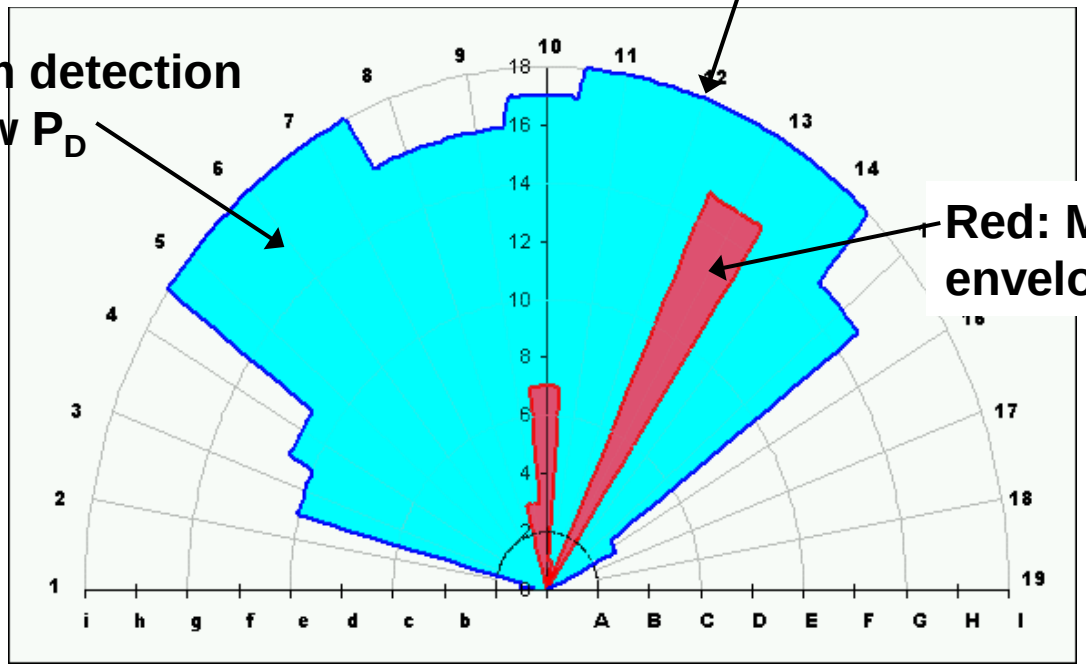
PIR: Walk Test – Least Sensitive Direction

Walk directly towards the sensor

Maximum and minimum detection envelope

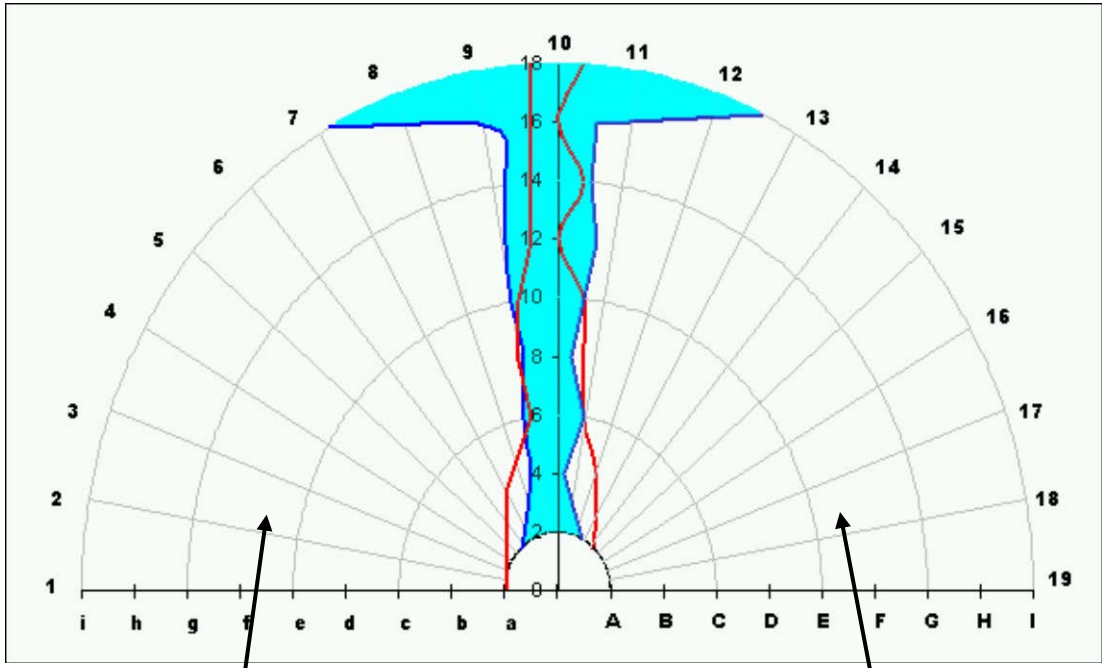
Test direction along radials

Blue: Maximum detection envelope – Low P_D



Red: Minimum detection envelope – High P_D

PIR: Crawl Test - Most Sensitive Direction



Test direction, arcs a - i

Test direction, arcs A - I

Passive Infrared Sensor Summary

- Principles of operation
  - PIR sensors detect changes in heat energy
  - Field-of-view is segmented
  - Most sensitive direction is across sensor field-of-view
- Nuisance alarm sources
  - Heat sources
  - Animals, insects

Passive Infrared Sensor Summary *(cont'd)*

- Vulnerabilities
  - Very slow movement
  - Masking
  - High temperature
  - Target insulation
- Performance testing
  - Establish probability of detection, detection envelope, and nuisance alarm sources

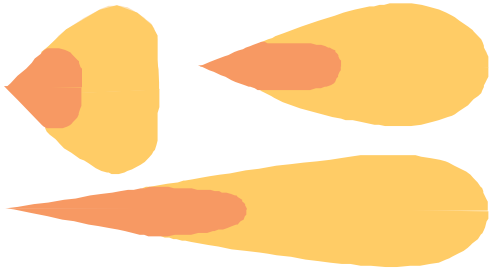
End Part 1

ANY QUESTIONS?
SEE YOU TOMORROW MORNING

Sensor Classification

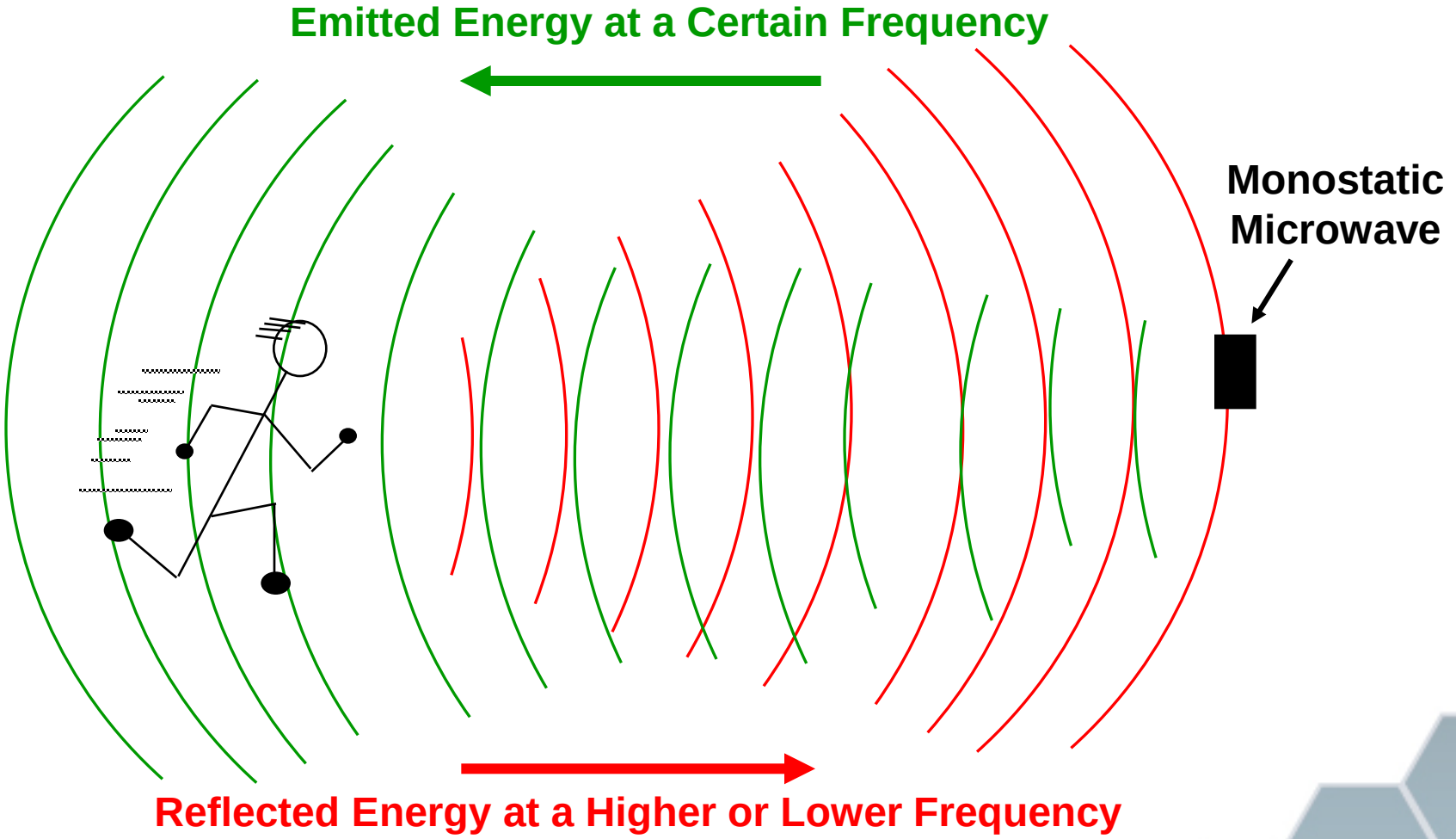
Interior Microwave Sensors	
Active	**Passive**
Covert	**Visible**
Line of sight	**Terrain following**
Volumetric	**Line**
Mode	**Freestanding**

Microwave Sensors



- Interior microwave sensors are
  - Active sensors
  - Typically monostatic
- Employ a single antenna for both the transmit and the receive functions
- Intrusion detection is based on a Doppler frequency shift
  - If the Doppler signal is of sufficient amplitude and duration an alarm will be generated

Doppler Frequency Shift

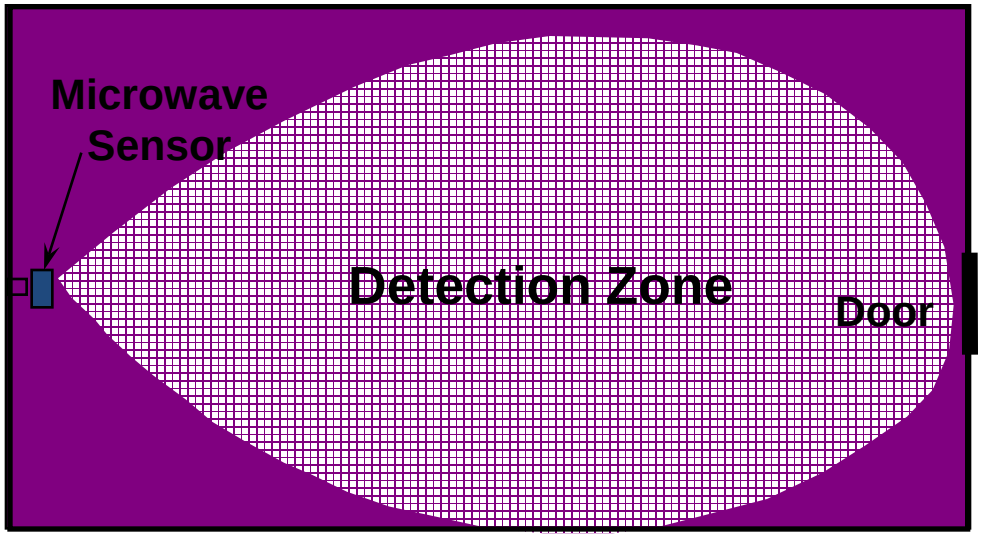


Interior MW Principles of Operation

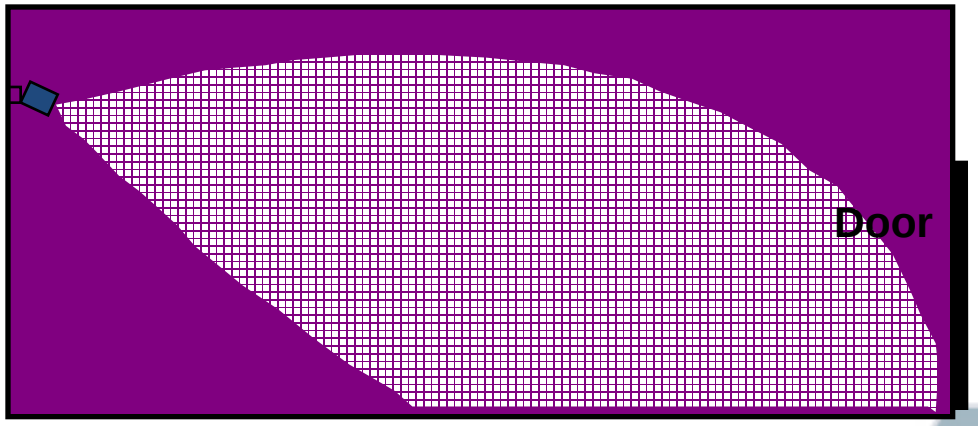
- Radiates RF signal
  - Typically 10.5 GHz +/- 25MHz
- Measures a Doppler frequency shift of the RF signal reflected from a moving “target”
- Detection pattern is largely determined by sensor antenna design
- Most sensitive to motion towards or away from sensor

Microwave Detection Pattern

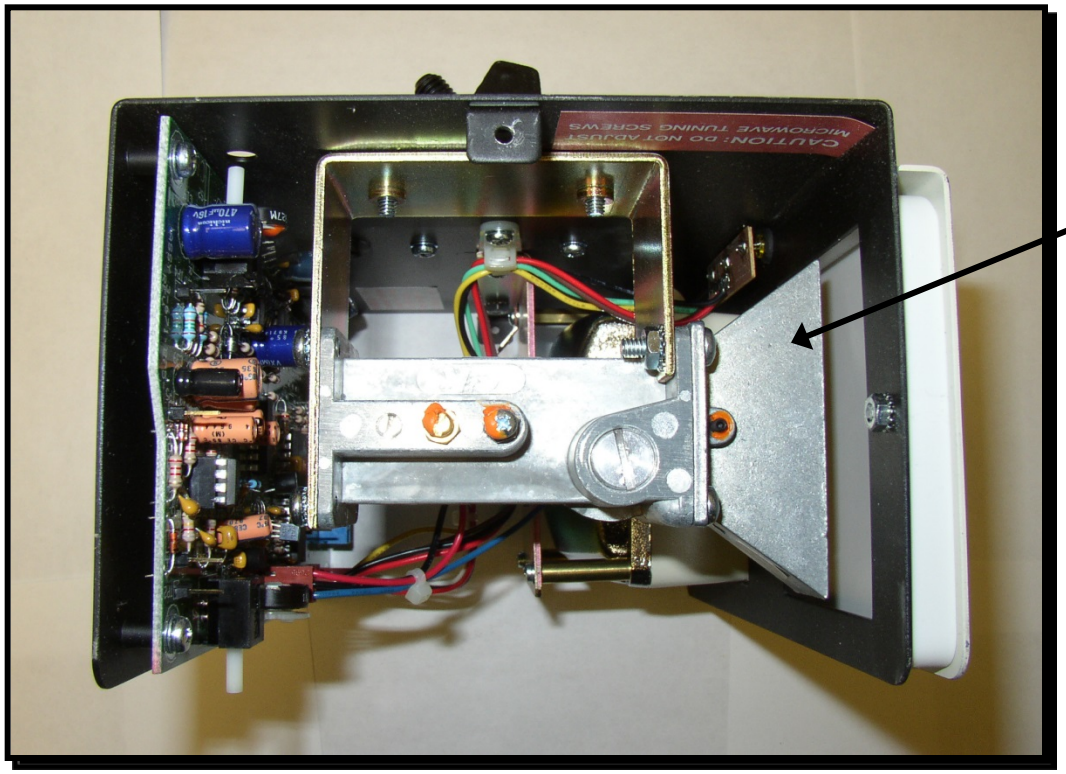
Top View



Side View



Example: Microwave Antenna



Antenna

(Also called a microwave horn for this type of antenna)

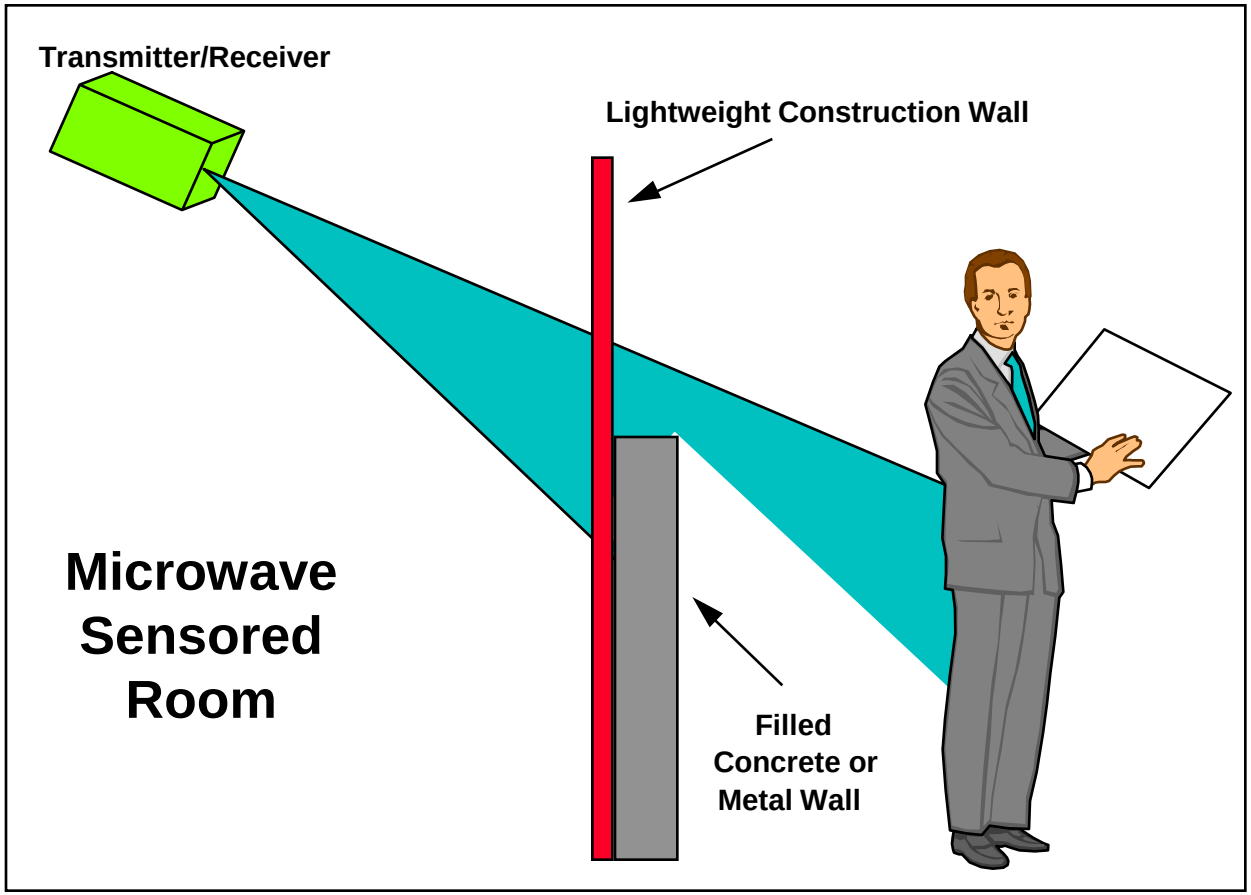
Interior MW Principles of Operation

- Processing of reflected (received) signal
  - Sensitivity
    - Related to the amount of Doppler shift needed to generate an alarm
  - Range gating
    - Detection distance adjusted using timing between transmitted and received signal
  - Rejection of minor oscillating motion
  - Signal level sensing
    - Detect if reflected signal is too weak, strong, or non-existent

Interior MW Nuisance Alarm Sources

- Movement of personnel, objects, or material on other side of windows or walls with lightweight construction
- Movement of objects within the protected area
  - Fan blades, animals, equipment
- Fluorescent lights
- Electro-magnetic impulse sources
- Sensor / mounting structure vibration
- Multiple microwave sensors in same area

Interior MW Nuisance Alarm Sources



Nuisance alarms can occur from outside a room with light construction materials (wood doors, windows, drywall, etc.)

Microwave Sensor Vulnerabilities

- Slow moving target
- Microwave absorption or reflection
- Blockage of field-of-view
- Circumferential motion
  - Difficult to defeat with normal walking

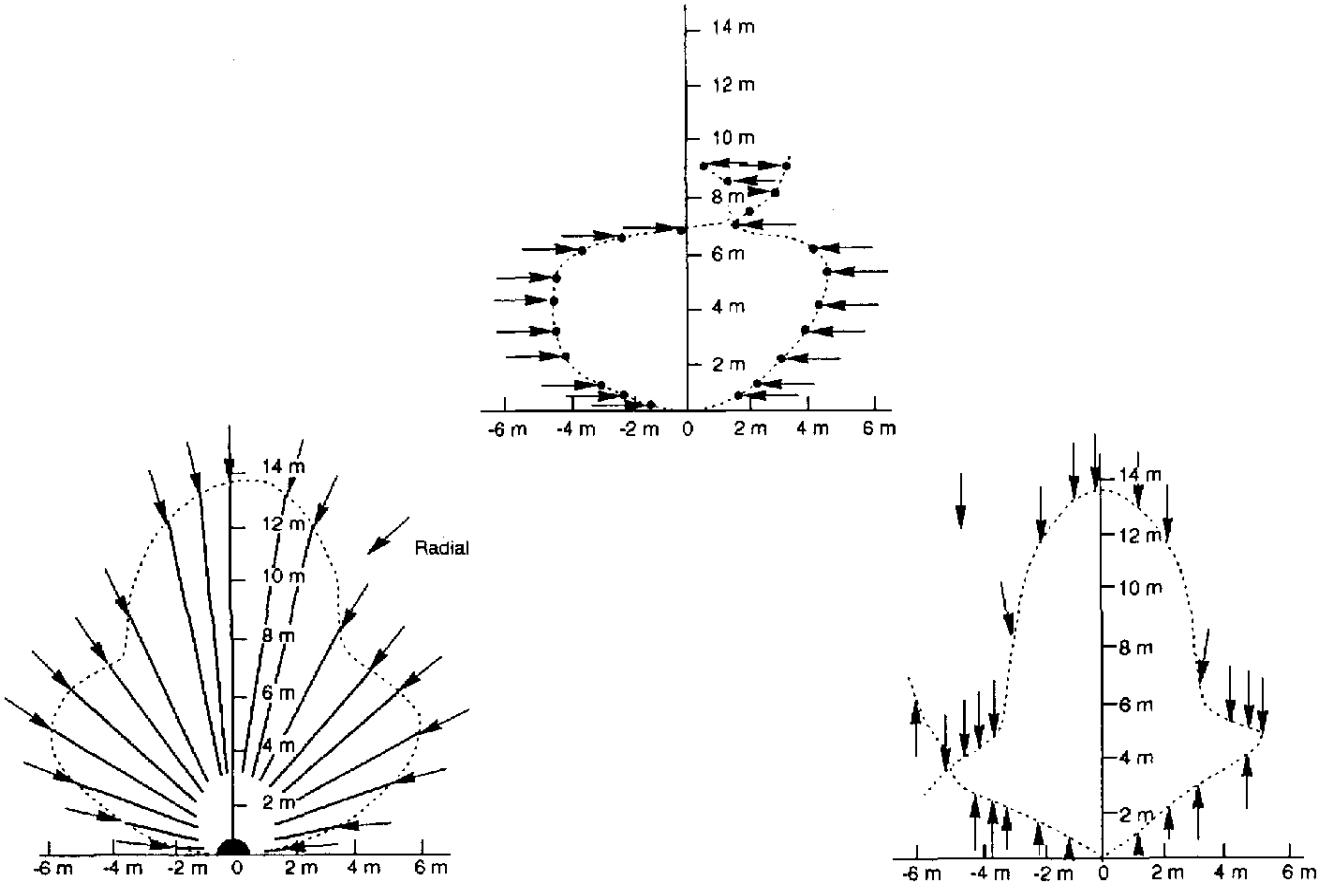
Microwave Laboratory Performance Testing

- Ideal, baseline testing
  - Performed under ideal or optimum conditions
    - Empty room (no equipment, furniture, etc.)
    - No or minimal nuisance alarm sources
  - Establishes sensor detection probability, P_D
  - Verify manufacturer's published detection area
  - Monitor sensor for false and nuisance alarms

Microwave Laboratory Performance Testing

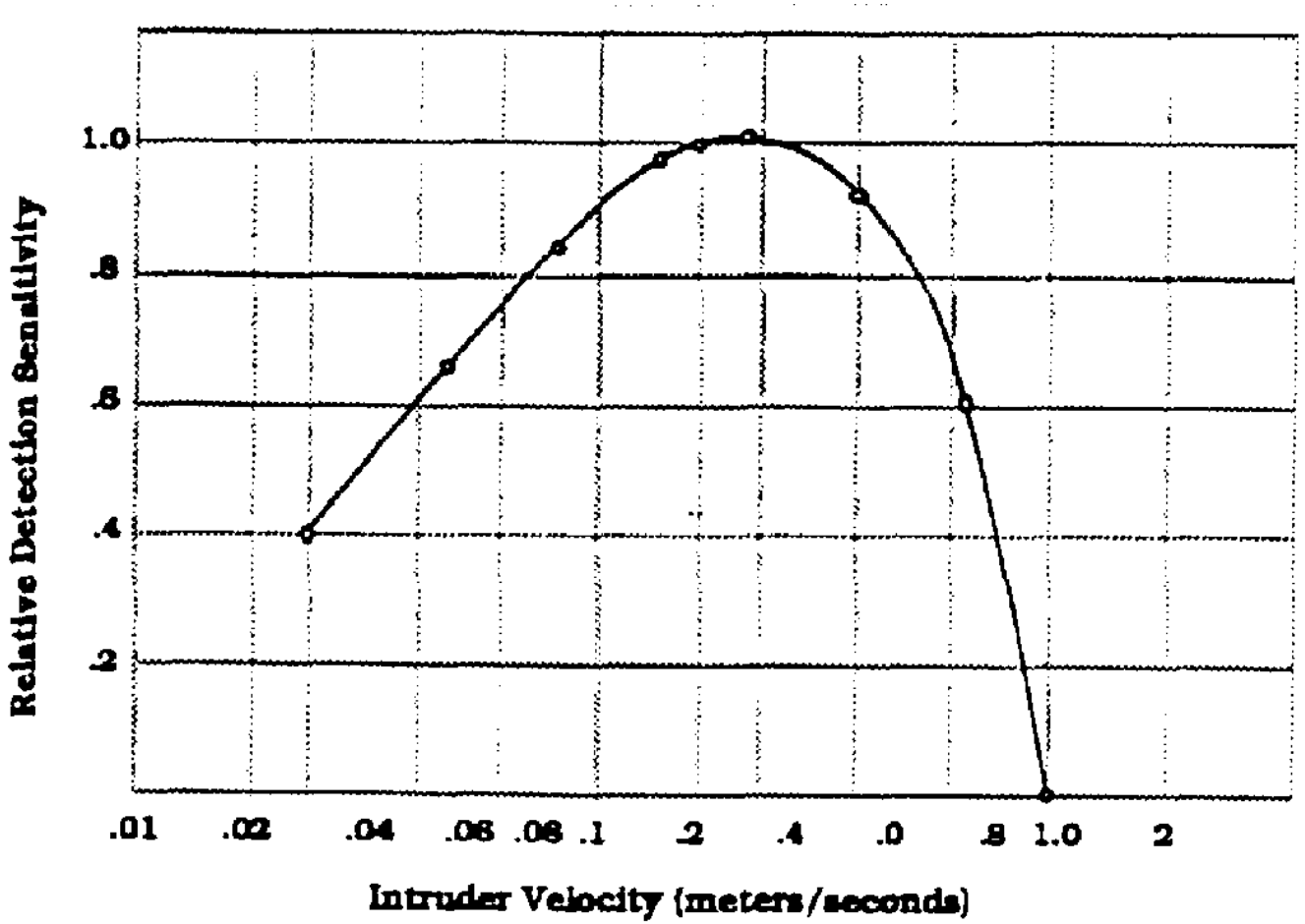
- Ideal walk testing
  - Multiple sensor units
  - Same make / model and different lots
  - Multiple human test subjects (small, medium, large)
    - Arms of test targets held tightly across chest
    - Walk rate of test target at 1 ft/second (0.3 m/s)
  - Record where alarms are generated along all paths
  - Establish detection pattern based on performance data
    - Individual sensor
    - Individual test subject

Interior Microwave Detection Patterns



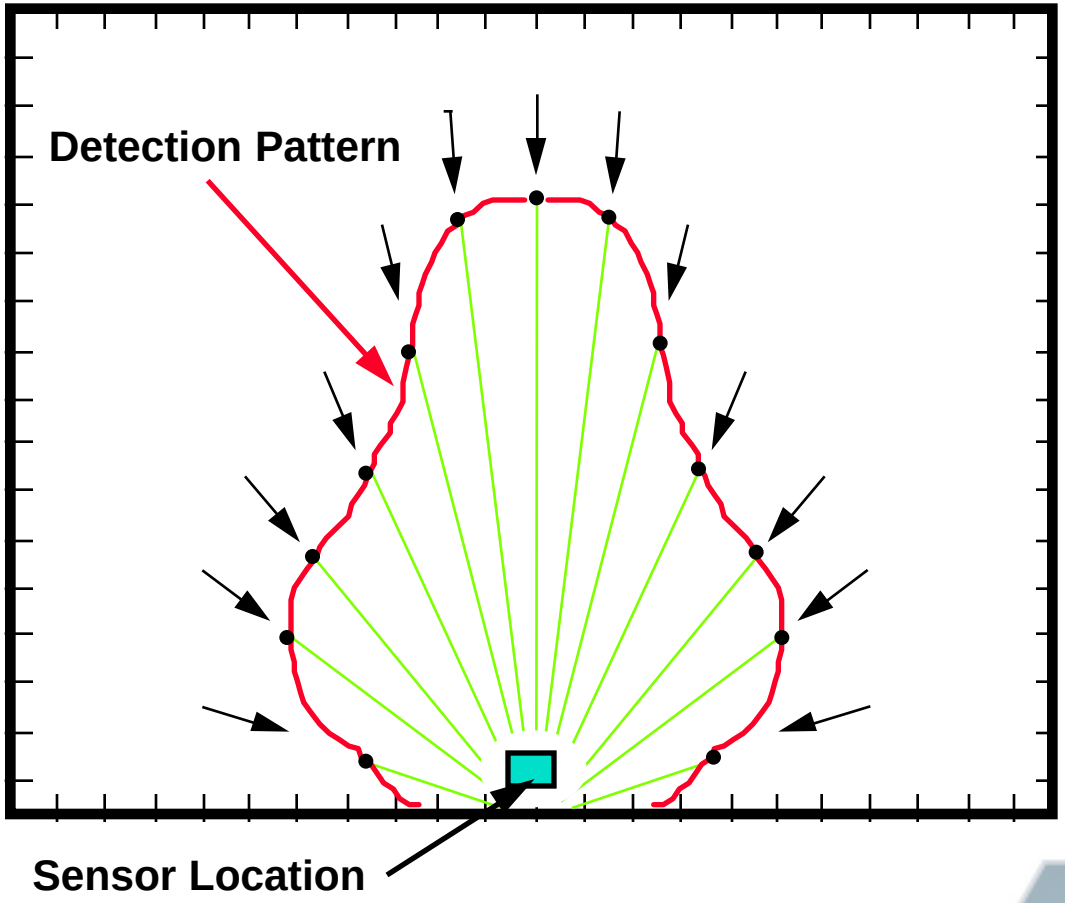
Note: Arrows indicate walk-test direction

Interior Microwave Target Speed vs. Sensitivity



Microwave Detection Pattern

Basic microwave detection pattern with the intruder walking towards the sensor



Microwave Sensor Summary

- Principles of operation
  - MW sensors are monostatic
    - Transmitter and receiver co-located
  - MW sensors detect the Doppler shift of a known transmitted frequency
  - Most sensitive direction is directly towards or away from the sensor
- Nuisance alarm sources
  - Movement of reflective objects, fluorescent lights, animals / insects, electro-magnetic interference

Microwave Sensor Summary *(cont'd)*

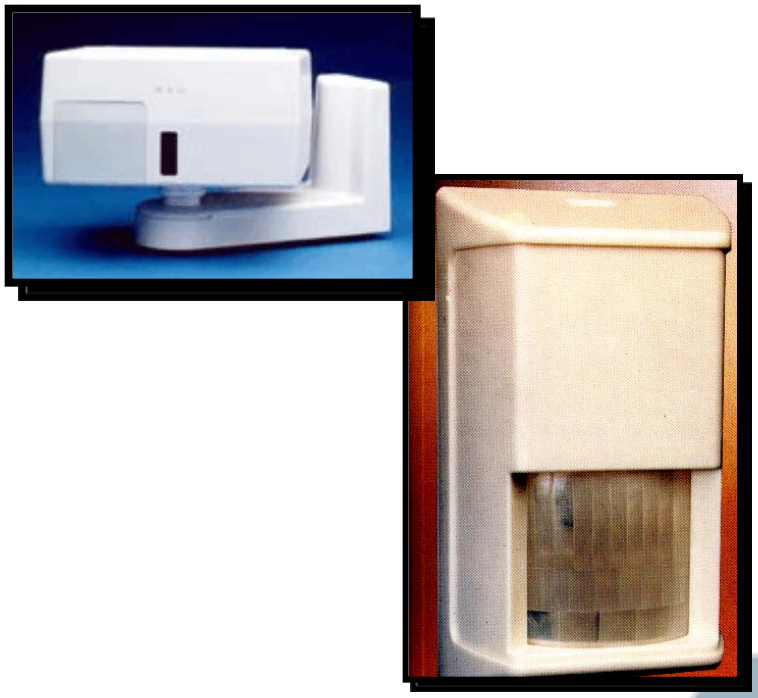
- Vulnerabilities
  - Very slow movement,
  - Blockage of microwave energy
  - Circumferential motion
- Performance testing
  - Establish probability of detection
  - Detection envelope
  - Nuisance alarm sources

Sensor Classification

Dual Technology Sensors	
Active	Passive
Covert	Visible
Line of sight	Terrain following
Volumetric	Line
Mode	Freestanding

Dual Technology Sensor Operation

- A combination of two sensor technologies
  - PIR and microwave
    - Most common
  - PIR and ultrasonic
  - PIR and glass break
- Alarm Processing
  - “AND” sensor outputs
  - “OR” sensor outputs



Dual Technology Sensor Operation

- "AND" (PIR / Microwave)
  - Both sensors must detect motion before alarm is generated
  - P_D is equal to the product of the P_D of each sensor
    - Example: PIR P_D = 0.9, MW P_D = 0.9, product = 0.81
    - The P_D of the dual-tech sensor in this example is 0.81
- Nuisance alarms are reduced
  - Most nuisance alarm sources for the PIR are not the same as for the microwave
  - A few nuisance alarm sources (such as small animals) are the same

Dual Technology Sensor Operation *(cont'd)*

- "OR"
  - If either sensor detects motion an alarm will be generated
  - This configuration is similar to placing two separate sensors in the same location.
    - If the sensor technologies are PIR and MW, one technology would be placed in a location where it is less effective with regards to direction of motion
  - Nuisance alarms are not reduced
- Individual PIR and microwave sensors installed in separate locations would be better

Dual Technology Sensor Vulnerabilities

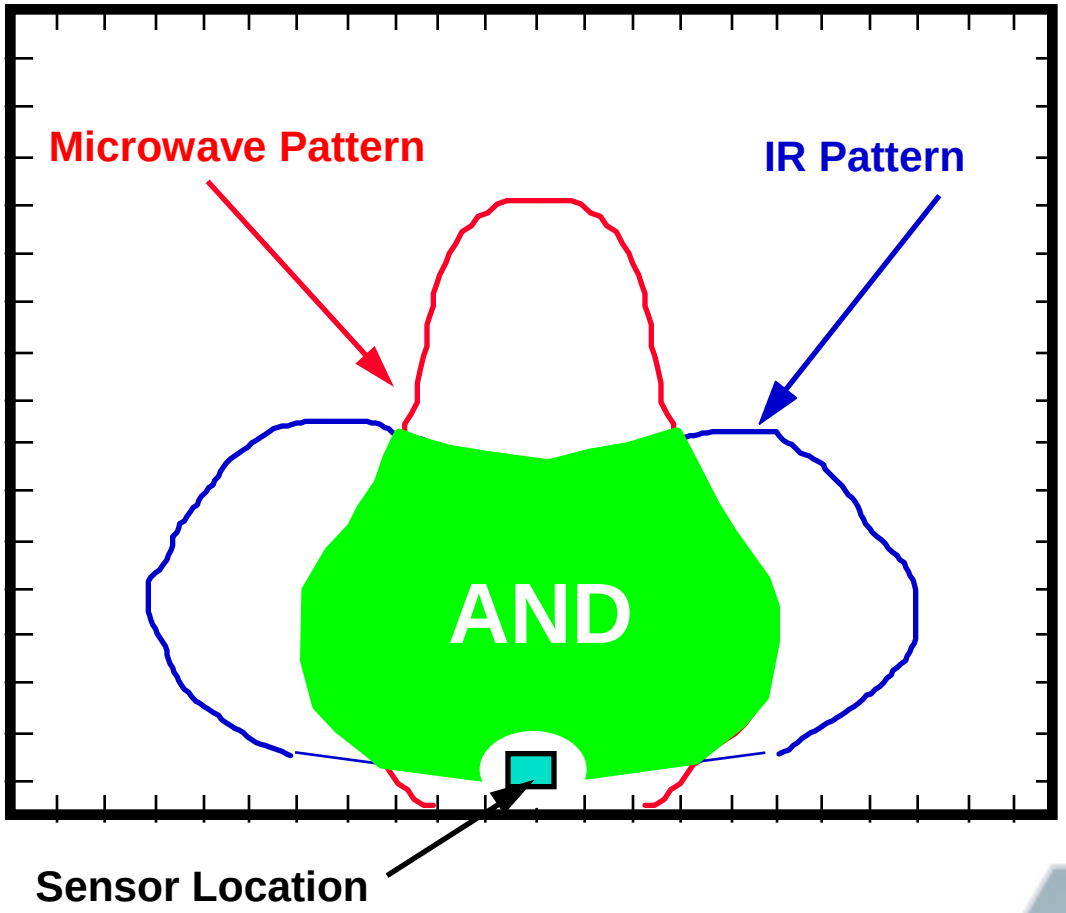
- Vulnerabilities are the same as for PIR and microwave sensors
- In the “AND” configuration if either sensor is defeated, then both are defeated

Testing, Evaluation, and Installation

- In a PIR / MW dual technology sensor the PIR sensor is primary in determining the detection pattern and volume
- PIR and microwave dual technology sensors should be tested and evaluated the same as a PIR sensor
- Sensor should be installed with primary consideration to the PIR sensor
- Do not use a dual technology as a replacement for two independent sensors in high security applications

Dual Technology Detection Pattern

Basic dual technology detection pattern with the intruder walking towards the sensor



Dual Technology Sensor Summary

- Two sensor technologies combined
  - Most common are PIR and microwave
- "AND" configuration reduces nuisance alarms as well as the P_D of each sensor technology
- If one sensor technology is defeated, then the sensor is defeated ("AND" configuration)
- Testing and installation should consider the PIR technology first

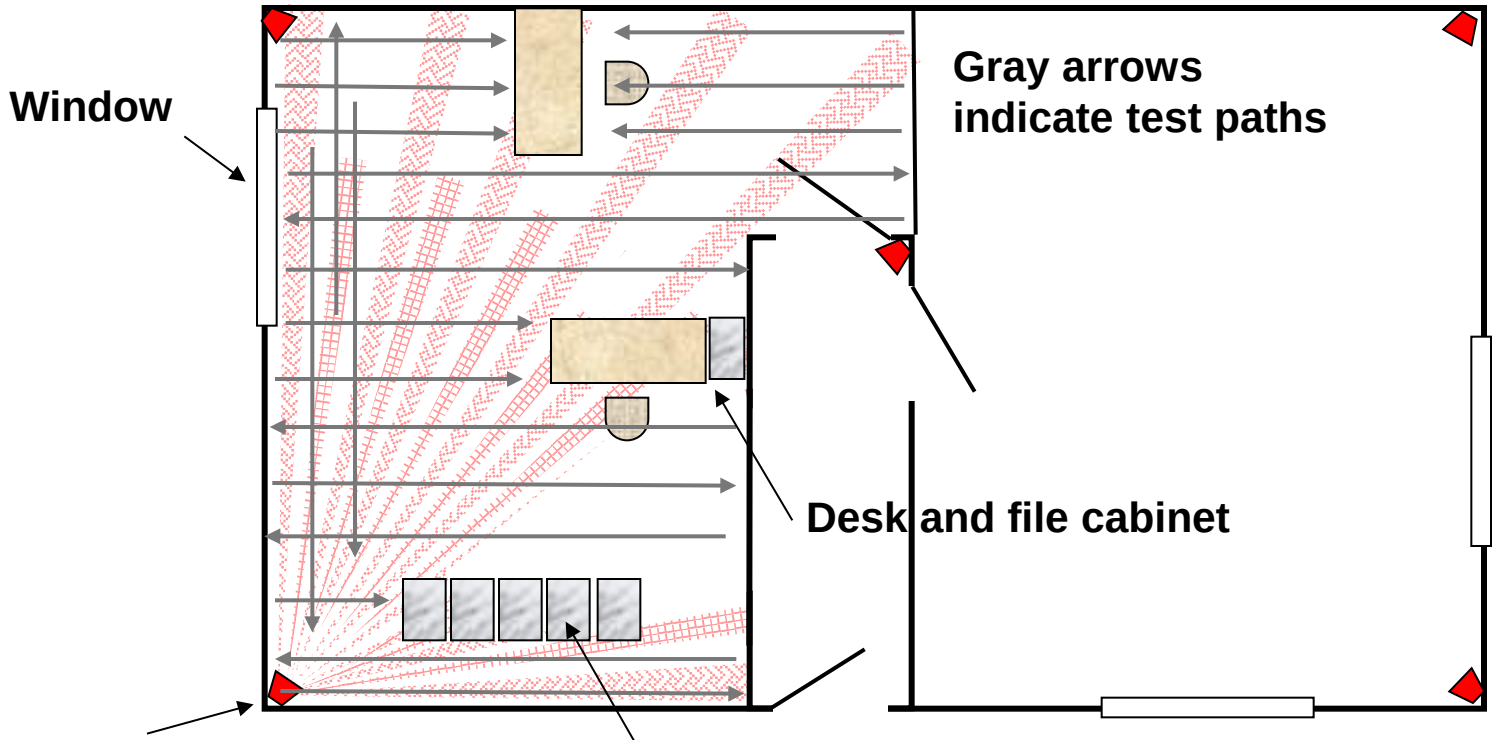
Dual Technology Sensor Summary

- For high security do not use a dual-tech sensor as a replacement for two separate sensors
- For high security multiple sensors should be used and installed so that they protect each other
  - And provide overlapping coverage of the protected area

Evaluation of Installed Sensors

- Effectiveness testing
  - Performed every 6 months, yearly, or per site requirements
  - Verify complete detection coverage and P_D
  - Verify tamper operation and communication to CAS
  - Includes review of
    - Most likely ways of entry
    - Location of furniture, equipment
    - Sensor maintenance
    - FAR / NAR histories

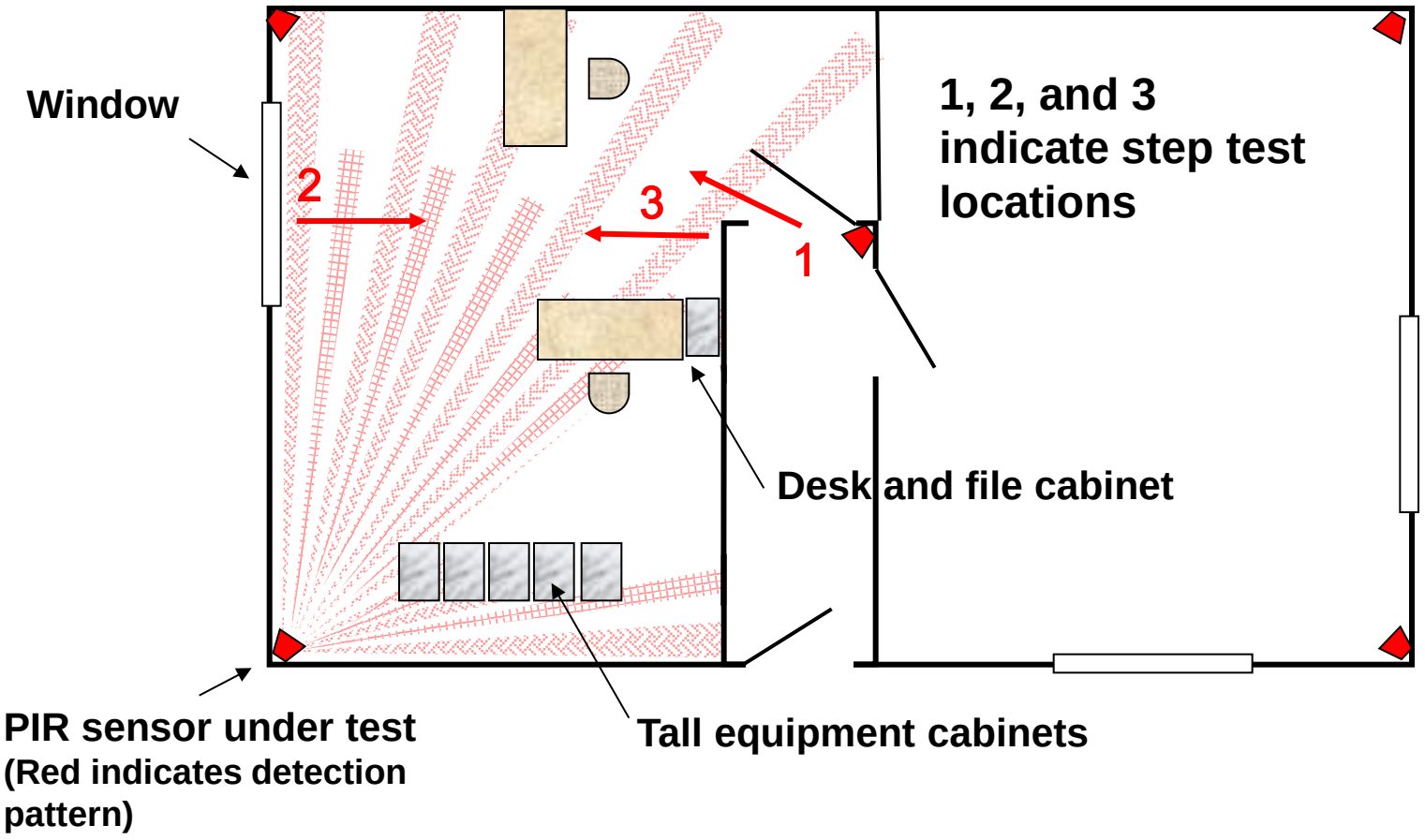
Effectiveness Evaluation and Testing – PIR Example



Evaluation of Installed Sensors

- Operability testing
  - Performed on a frequent basis (daily / weekly)
  - Verify that the sensor is operational
  - Verify correct alarm received at CAS
  - Step test
    - From likely entry points
    - From other points as defined by site requirements

PIR Operational Test Example



Infrared Sensors

Learning Objectives

After completing this module, you should be able to:

- Describe the fundamental principles of infrared sensors
- Identify in what application infrared sensors are suitable for providing effective detection for given threat tactics and environmental conditions
- Evaluate and determine effective placement of infrared sensors
- List the advantages and disadvantages of infrared sensors

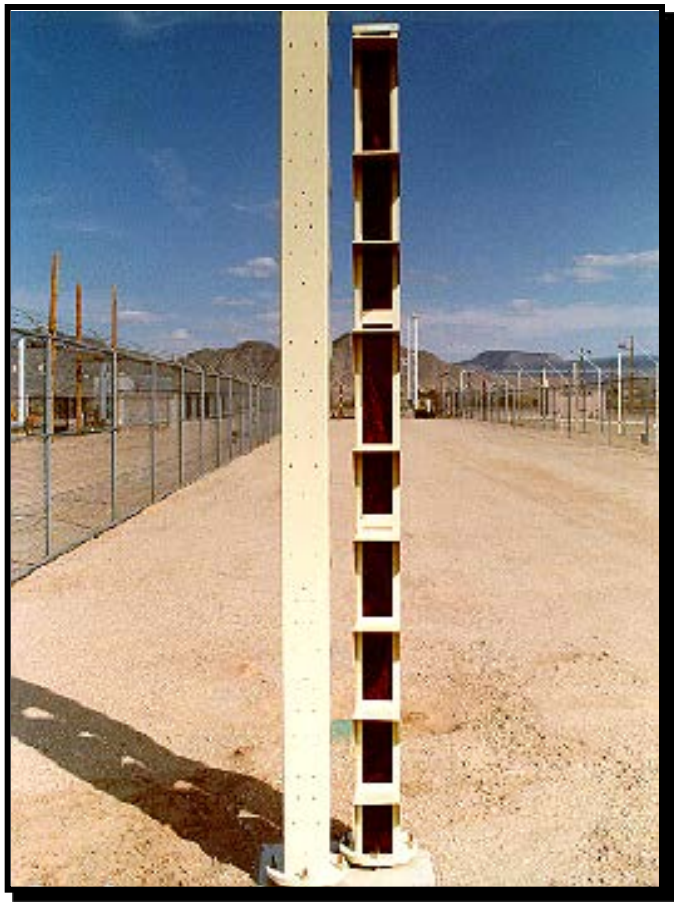
Sensor Classification

Exterior Infrared Sensors	
Active	Passive
Covert	Visible
Line of sight	Terrain following
Volumetric	Line
Mode	Freestanding

Infrared Sensor Types

- Active
  - A majority of the exterior infrared sensors used are of the active type and are multiple beam
- Passive
  - More typically used as an interior sensor but is used to cover special situations in the external environment

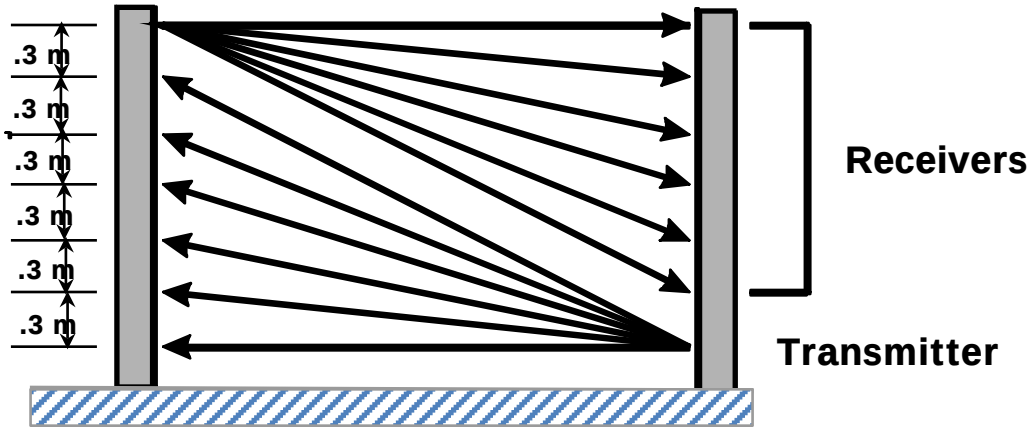
Example of Active IR

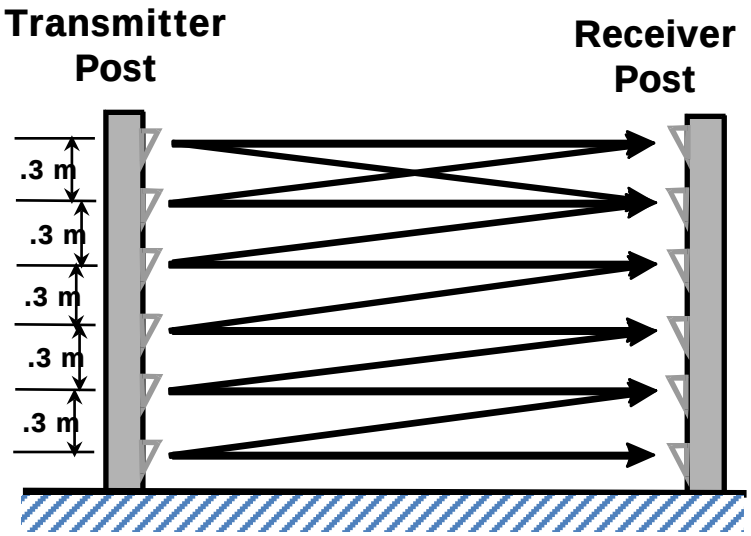


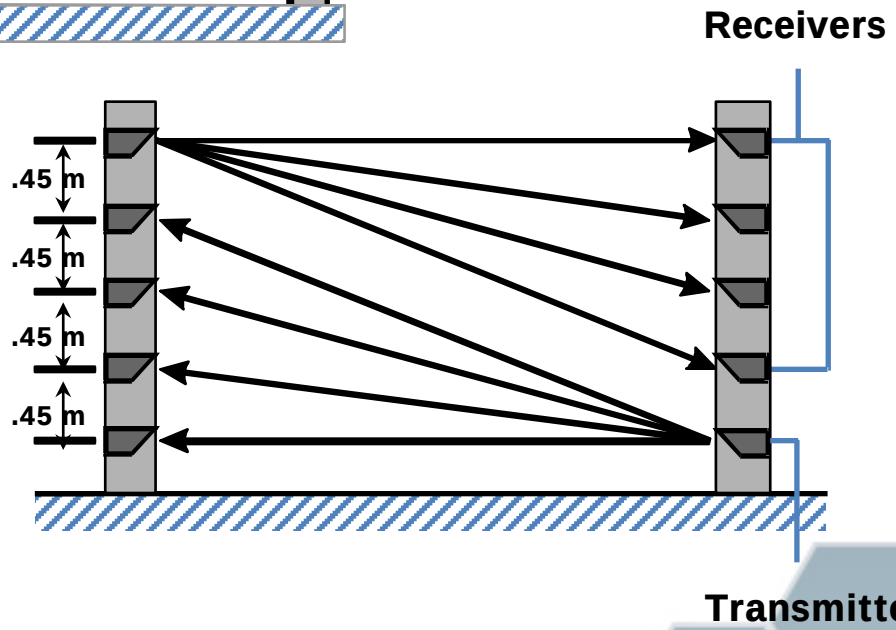
Exterior Active Multi-Beam Infrared Sensors - Operational Principles

- Pulsed IR light beams
- Beams transmitted in sequence
- Detection method - beam break
- Wavelength - 0.8 to 0.95 Microns (non-coherent)
- Radiated power - low (eye safe)
- Detection zone height - typically 2 to 3 m
- Transmitter beam angle (receiver also) - nominally 1/2 degree (half power points)
  - Some sensors / angles can be as much as 3 degrees

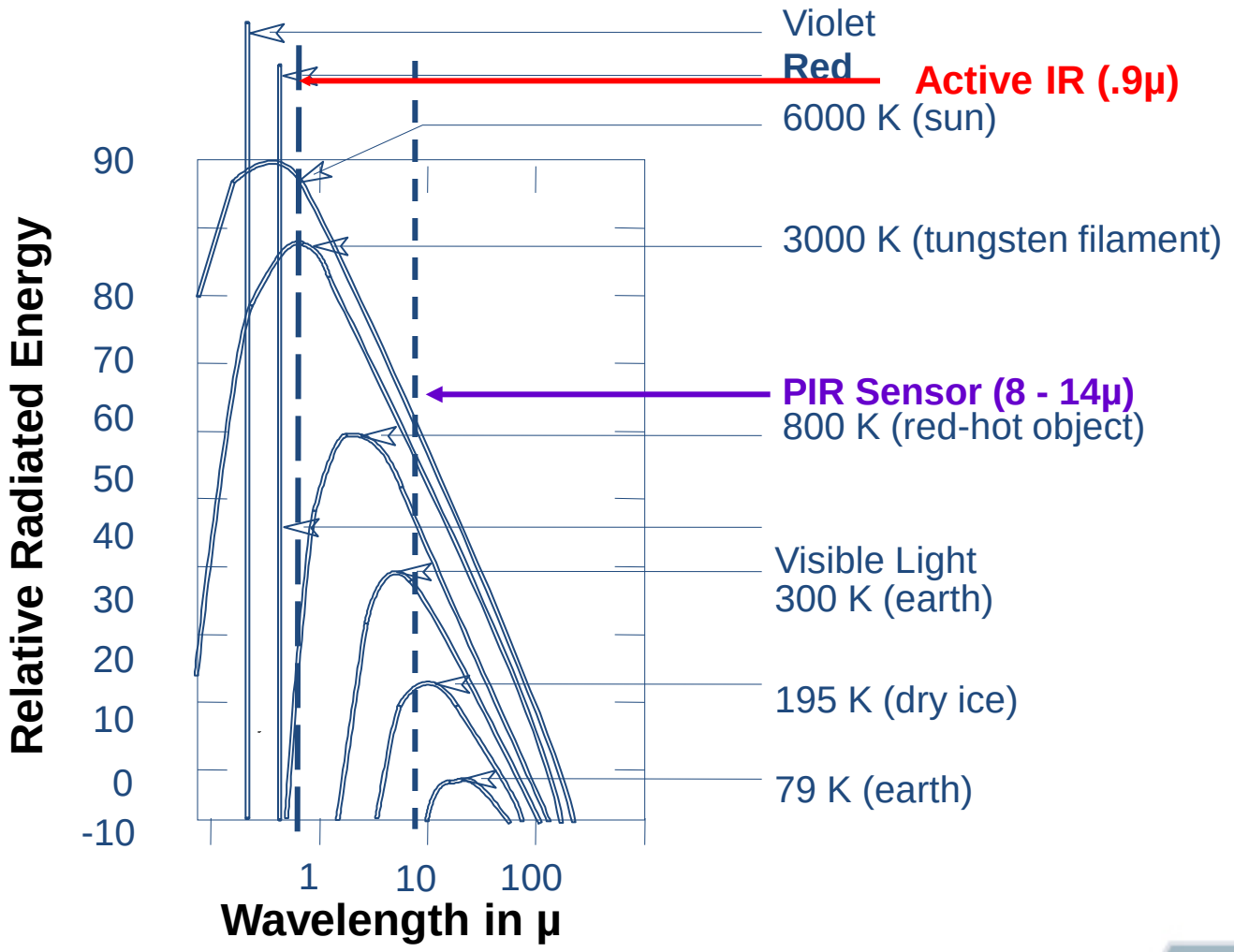
Examples: IR Sensor Beam Pattern







Relative Radiated Energy



Active Infrared Performance Characteristics

- P_D
  - Very high for multiple beam sensor
  - Detection zone narrow and high,
    - Not in contact with ground
- Vulnerability to defeat
  - Bridging
  - Shallow tunneling or trenching

Active IR Performance Characteristics *(cont'd)*

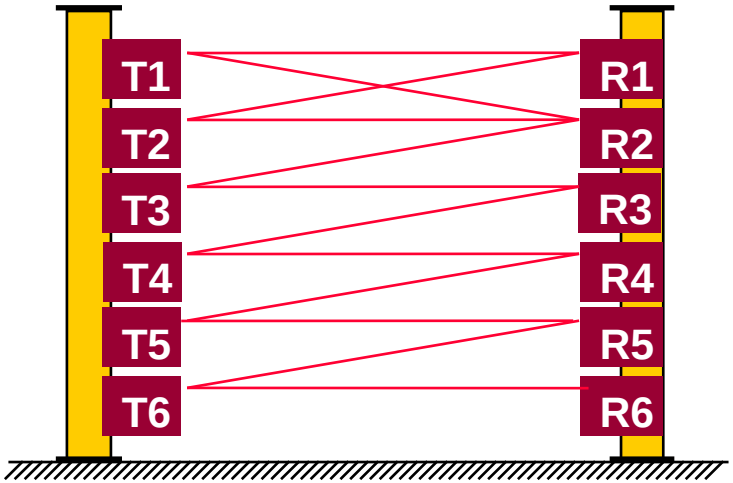
- NAR / FAR
  - Animals, birds,
  - Vegetation
  - Snow accumulation
  - Blowing debris
  - Weather conditions which reduce visibility
    - Fog, heavy snow, dust
  - Ground heaving caused by freezing and thawing
  - Function of optical alignment
  - Sunlight

Active IR Sensor Installation

- No objects protruding into detection zone
- Constant grade below bottom beam
  - Concrete sill or curb is preferred
- Stable mounting bases are required
- Heated face plates or environmentally sealed housings required to prevent lenses from fogging
- Pillars mounted perpendicular to grade
  - Not always vertical

Active IR Sensor Installation *(cont'd)*

- Proper alignment is critical to minimize nuisance alarms
- Overlap or climb detection required
- Avoid aiming towards sunrise or sunset
- Avoid aiming at adjacent sensor sectors

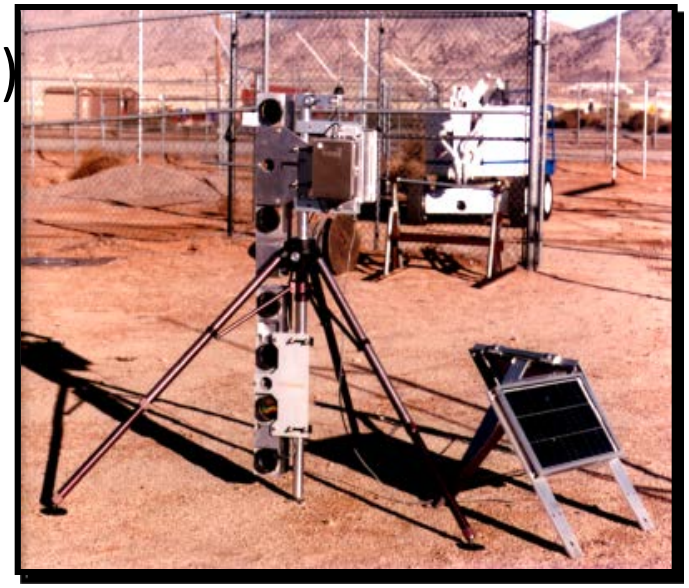


Active IR Sensor Maintenance

- Clean optical lenses
- Check for possible soil erosion
- Proper alarm margin
  - 1 dB per 8 m
- Check heater operation
- Snow removal

Active IR Sensor Detection Testing

- Walk / run test
  - Velocities
    - Low - 0.2 m/s (0.5 ft/s)
    - High – 5.0 m/s (15.2 ft/s)
- Crawl test
- Slow obscuration
- Alarm margins
  - Optical filters
  - Opaque plate



Active IR - Strengths and Weaknesses

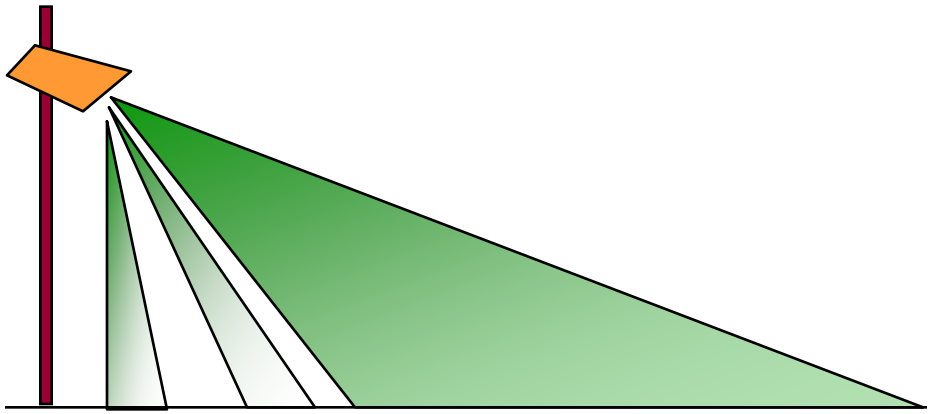
- Strengths
  - Narrow detection zone
  - Unaffected by nearby motion
  - High P_D
- Weaknesses
  - Poor sensor choice for snowy climates
  - Well defined detection pattern

Example of Passive IR

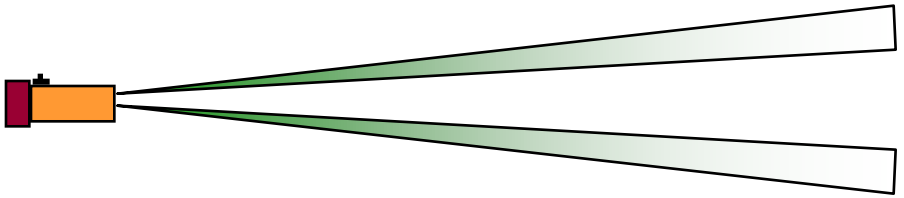
Exterior Passive Infrared Sensors - Operational Principles

- Detection method: detects a change in the received infrared energy
  - In most situations the target must be in motion
- Wavelength - 9 to 10 microns
- Detection pattern - most have a detection beam width of under 6 degrees

Common Exterior PIR Detection Pattern



Side View



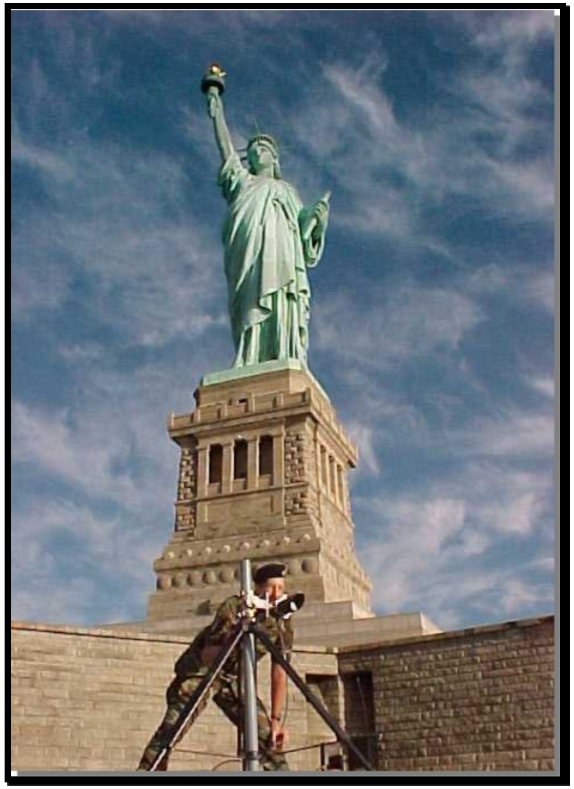
Top View

PIR Performance Characteristics - P_D

- Probability of detection (P_D)
  - Most sensitive to movement across the field of view
  - Velocity of intruder
  - Temperature of intruder relative to background
  - Height and angle of installation

PIR Performance Characteristics *(cont'd)*

- NAR / FAR
  - Weather conditions
    - Dust, rain, snow
  - Blowing debris
  - Animals and birds
  - Detector not aimed at solid background
- Vulnerability to defeat
  - Shielding of detector
  - "Insulated suit" worn by intruder



Dual Technology Sensors

- Sensor will not alarm until both sensors have detected
- Example
  - Monostatic microwave and passive infrared
- “AND” output
- Reduces nuisance alarms
- Allows sensitivity to be set high

Dual Technology Sensors *(cont'd)*

- Adversary always approaches one technology in the least sensitive direction
- If one sensor is defeated, then an alarm is not activated
- Currently not in common use in exterior environment

Active IR Sensor Summary

- Flat terrain required
- Direct sun can cause alarms
- Blowing debris can cause alarms
- Fog and heavy rain can cause constant alarms
- Snow depth reduces performance
- Alignment is critical
- High P_D
- Low NAR

Passive IR Sensor Summary

- Detection volume (range) changes with background and target temperature
- Detects hot objects at greater distances
- NAR / FAR sources
  - Dust devils, small animals
- More easily defeated than some sensors
- Difficult for intruder to determine detection zone
- Relatively low cost

Exercise 6.4

Fence Disturbance Sensors

Session Objectives

1. Provide "hands-on" experience with fence disturbance sensors in the exercise field.
   - Peridect Vibration Sensor

2. Give participants practice in testing and evaluating fence disturbance sensors. Participants will use questions and evaluation checklists as a guide and for documentation of test results from the exercise.

.

Exercise: Fence Disturbance Sensors

OBJECTIVES: The objective of this exercise is to give participants practice in evaluating fence sensors.

The participants will evaluate the fence sensor and document these tests on Evaluation Sensor Checklists.

PROCESS: As a sub-group, participants will complete (as a group) the evaluation sensor checklist, which includes not only measuring sensitivities but also attempting to exploit vulnerabilities.

During the testing, use the "cutting" or "simulated cutting (tapping)" test as well as the climbing test. Document this test on the sensor checklist.

Evaluate sensitivity at a fence post and at the fence fabric between the posts.

If time permits, test the sensor enough to conclude the probability of detection and the confidence level of that probability.

FENCE DISTURBANCE SENSOR CHECKLIST Date

Evaluator Facility / Location

A. Equipment Data

1. Type _____
2. Manufacturer & Model

B. Climbing Performance Tests

1. Unaided Climbing Test - attempt to climb over fence. Repeat test three times at each fence post.
   (a) How many attempts were successful with no alarm generated? _____
   (b) Did any post allow three successful attempts? Y N
   (c) Were the missed detections evenly distributed along the fence? Y N
2. Can the fence be bridged without generating an alarm? Y N

   Describe _____
3. Can an intruder dig under the fence without generating an alarm? Y N

   Describe _____
4. Are the sensors equipped with tamper switches? Y N
5. Is wiring in conduit? Y N
6. Is the sensor line supervised? Y N

C. Cutting or Simulated Cutting (tapping) Performance Tests

1. Cut or simulate cut at the center of each fabric span. Repeat test three times at each span.
   (a) How many attempts were successful with no alarm generated? _____
   (b) Did any span allow three successful attempts? Y N
   (c) Were the missed detections evenly distributed along the fence? Y N
2. Can the fence be bridged without generating an alarm? Y N

   Describe _____
3. Can an intruder dig under the fence without generating an alarm? Y N

   Describe _____
4. Are the sensors equipped with tamper switches? Y N
5. Is wiring in conduit? Y N
6. Is the sensor line supervised? Y N

D. Factors Affecting Performance

1. Are fence posts spaced properly? Y N
2. Are fence posts vertical within 4° in two planes? Y N
3. Is fence fabric attached in at least five places, evenly spaced on each post? Y N
4. Is fabric secured to upper tension wire at least every foot? Y N

5. Check fence fabric tension:

   (a) When a force of 30 lbs. (13.5 kg,133 Newtons) is applied to the center of the fabric panel, does the mesh deflect more than 5 cm (2 in.) ? Y N

   (b) Does the fabric return to its original position when released? Y N

6. When a force of 50 lbs.(23 kg) Is applied perpendicular to the fence at the top of the post, does the post deflect more than 2.5 cm (1 in.) where the force is applied? Y N

7. Is the fence area clear of tree branches or other objects that could mechanically disturb the fence? Y N

8. In case of loss of electrical power:

   (a) Does the sensor have backup standby power? Y N

   (b) Is a loss of power alarm initiated? Y N

9. Are there signs of physical abuse? Y N

10. What serves as backup detection if this sensor is inoperable?

Describe

FENCE DISTURBANCE SENSOR CHECKLIST *(cont.)*

Notes / Miscellaneous

Exercise 6.5

Microwave and IR Stacked Sensor

Session Objectives

1. Provide "hands-on" experience with the following sensors:
    - Securit IR and microwave stacked sensor

2. Give participants practice in testing and evaluating sensors. Participants will use questions and evaluation checklists as a guide and for documentation of test results from the exercise.

Exercise: Microwave and IR Stacked Sensors

OBJECTIVES: The objective of this exercise is to give participants practice in evaluating different kinds of microwave and IR units.

The participants will evaluate both the microwave and IR sensors and document these tests on Evaluation Sensor Checklists.

PROCESS: As a group, participants will complete the evaluation sensor checklist for each unit, which includes not only measuring sensitivities but also attempting to exploit vulnerabilities.

A copy of "installation, alignment, and testing" for both microwave sensors and infrared sensors is included in this workshop that may give more explicit instructions about the testing.

Perform the walk tests at 0.2 m/second (0.6 ft/second) and the run test at 4.5 m/sec (15.2 ft/second).

Instead of using the crawl test of the microwave, use the radar pull target described in 3.1.3.

EXTERIOR MICROWAVE SENSOR CHECKLIST

Date

Evaluator

Facility / Location

A. Equipment Data

1. Type _____
2. Manufacturer & Model

B. Performance Tests

1. Walk Test
   (a) Is an alarm generated by movement immediately behind the transmitter? Y N
   (b) Is an alarm generated by movement immediately behind the receiver? Y N
   (c) If a sensor is located parallel to a fence, walk along length of detection zone, 3 ft.(1 m) from fence - does an alarm occur? Y N
2. Run Test - Run across the center of the zone. Does an alarm occur? Y N
3. Shuffle Walk Test - Walk very slowly (5cm (2 in.) steps, 2 step/sec.) across the zone at mid-range without swinging the arms - does an alarm occur? Y N
4. Crawl Test - Stomach crawl across detection zone at 3m (10 ft.) intervals - does an alarm occur on each attempt? Y N

   If not, note locations of successful intrusions. Note: It is not necessary to perform crawl test before crossover point. _____
5. Can the microwave beam be easily bridged without generating an alarm? Y N

   Describe

C. Factors Affecting Performance

1. Is the terrain flat and regular between the transmitting and receiving antennae? Y N
2. What material forms the surface of the sensor bed? _____
3. What is the distance between transmitting and receiving antennae? _____
4. What is the height of the antennae from the center line? Transmitter _____ Receiver _____
5. Are mounting posts fixed in location with a permanent concrete footing? Y N
6. Can one sensor induce an alarm in another sensor (crosstalk)? Y N
7. Do antennae provide proper overlap at the crossovers? Y N
8. Is there evidence of erosion or low spots? Y N
9. What is the expected maximum snow accumulation around detection zone? _____
10. Is the detection zone near a parallel chain-link fence with loose mesh that flexes in the wind? Y N
11. Is the detection zone free of surface water and melting snow? Y N
12. Is the detection zone free of animals? Y N
13. Is wiring in a conduit? Y N
14. Are both transmitter and receiver equipped with tamper switches? Y N
15. Is the sensor line supervised? Y N

EXTERIOR MICROWAVE SENSOR CHECKLIST *(cont.)*

C.	Factors Affecting Performance					
	13. Is the sensor line supervised?	Y	N			
	14. In case of loss of electrical power:					
		(a) Does the sensor have a standby power source?			Y	N
		(b) Is a loss of power alarm initiated?			Y	N
	15. Are there visible signs of physical abuse?	Y	N			
	Describe					
	16. What serves as backup detection if this sensor is inoperable?					
	Describe					

Notes / Miscellaneous

INFRARED SENSOR (BOUNDARY PENETRATION) CHECKLIST

Date

Evaluator

Facility / Location

A. Equipment Data

1. Type _____
2. Manufacturer & Model

B. Performance Tests

1. Walk-test - proceeding at a normal pace across the path of the beam, is an alarm initiated? Y N
2. Run-test - running quickly across the path of the beam, is an alarm initiated? Y N
3. Can the beam(s) be bypassed by:
   (a) Crawling under beam(s)? Y N
   (b) Jumping over beam(s)? Y N
   (c) Digging under beam(s)? Y N
4. What is the separation between beams? _____
5. Can receiver be "fooled" by an external infrared source? Y N
6. Is the device line supervised? Y N
7. Is wiring in conduit? Y N
8. Is an alarm initiated when:
   (a) Cover is removed from device enclosure? Y N
   (b) Electrical lines are disconnected? Y N

C. Factors Affecting Performance

1. Are the infrared source and detector properly aligned? Y N
2. Are optics clean? Y N
3. Is the most likely intrusion path across the beam(s) rather than directly into or away from the beam(s)? Y N
4. Are transceivers, receivers, and control units located away from radio transmitters? Y N
5. For multiple sensor applications, do all sensors function properly providing the required area of coverage? Y N
6. Is the area clear of animals, birds, large flying insects, and blowing debris? Y N
7. In case of loss of electrical power:
   (a) Does the sensor have battery standby power? Y N
   (b) Is a loss of power alarm initiated? Y N
8. Are there visible signs of physical abuse? Y N

   Describe _____
9. What serves as back-up detection if this sensor is inoperable?

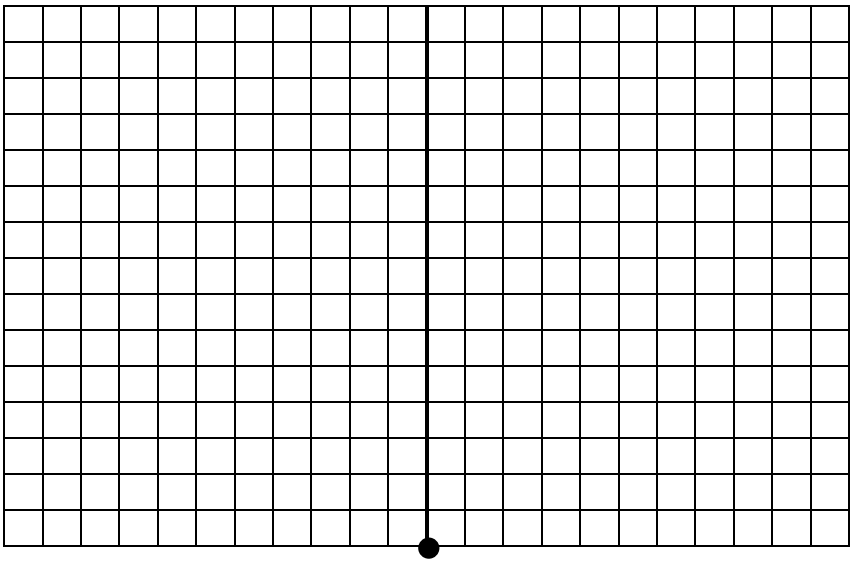
   Describe _____

INFRARED SENSOR (BOUNDARY PENETRATION) CHECKLIST *(cont.)*

Notes / Miscellaneous

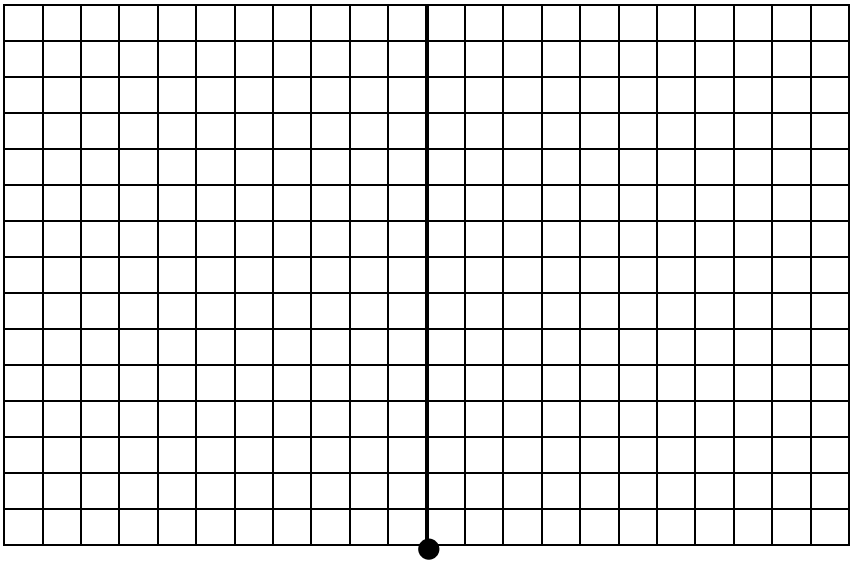
INFRARED SENSOR CHECKLIST

Walk-Test Worksheet



Sensor Location

Notes/Miscellaneous



Sensor Location

Notes/Miscellaneous

Mark location of alarm with a dot and direction of approach with an arrow.

INSTALLATION, ALIGNMENT, AND TESTING

The following procedure applies to Racon-manufactured equipment

Step	Instructions	Check
1.0	**Microwave Sensors** CAUTION: It is critical for the infrared and microwave that the batteries be maintained at charge during cold weather. If heads are installed and will remain in the field for long periods without power from a power junction box (PJB), remove the batteries from the heads and store them inside until charge can be maintained under field conditions. References: Manuals and drawing	
1.1	**Receiving Inspection** Part 1: Inspect all components for damage upon receipt. Unpack; lay out and identify components for future installation. Part 2: Select a matched transmitter/receiver pair. Install appropriate-sized supervision resistors within each microwave head. Select the specified frequency channel by installing appropriate jumpers within each microwave head.	
a.	Install batteries in sensor heads per manufacturer's instructions. • Identify each head for future installation.	
b.	Set up a transmitter/receiver pair about 3m (10 feet) apart.	
c.	Power up each pair of microwaves for initial operational test. • Confirm operation in accordance with manufacturer's instructions.	
d.	Verify that an alarm is generated as the transmitter beam is blocked.	
2.0	**Microwave Installation**	
a.	Install microwave heads at the mounting heights specified on drawings.	
b.	Roughly align each pair of microwave heads by rotating the heads to be perpendicular to the centerline between each head. *The rough alignment is designed to boresight a microwave pair so that the transmitter and receiver are aligned both horizontally and vertically with respect to each other*. Required equipment: • 60 cm (24-inch) carpenter's square • One set of stair gages • One small bubble level	
c.	**NOTE**: The following procedure applies to Racon-manufactured equipment. *There is a slight bow in the plastic face of a microwave antenna as well as a windlace around the circumference of the antenna that prevents finding a flat, usable alignment surface on the antenna. The stair gages used with the square will provide for an equal and uniform standoff for the square from the plastic face of a microwave antenna.* • Place one each stair gage on the long side of the 24-inch carpenter's square at the 4 cm (1½-inch) point and the 58 cm (23-inch) point. • Tighten the thumb screw on each stair gage after the gages are firmly seated on the square.	

Step	Instructions	Check
d.	Place the square horizontally across the face of a microwave head with the short side of the square facing outward toward the opposite head. *It is important that the long side of the square be truly horizontal across the surface of the head and that the stair gages rest directly on the faceplate just inside the windlace so that the square does not touch the center bow of the faceplate.*	
e.	Sight along the short edge of the square that is parallel to the microwave beam. • Rotate the head so the sight line along the edge of the square lines up with the corresponding edge of the opposite microwave head. • Secure the mounting clamps while maintaining the proper height and sight line along the square. **NOTE**: Tightening the screws on one side of the mount more than on the other side will cause the head to rotate around the pole.	
f.	Loosen the two allen screws on each side of the antenna to prepare for vertical alignment.	
g.	Place the square vertically on the faceplate with the short edge on top and parallel with the microwave beam.	
h.	Sight along the short edge to match to the top of the opposite microwave head.	
i.	Tighten the two allen screws.	
j.	Check the height and the horizontal and vertical alignment to ensure that the head has not moved.	
k.	Repeat the process for the opposite microwave head.	
l.	Terminate the ground wire from the sensor foundation.	
m.	Terminate the signal and power cables within the control enclosure junction box on each head.	
3.0	## Microwave Sensor Alignment and Testing **NOTES for Procedure Goals:** There are many factors that affect the operational characteristics of the microwave pairs. Some of the major factors are: a) The antenna mounting height b) The microwave frequency c) The microwave reflection properties of the PIDAS bed d) The flatness and irregularity of the surface between the units e) The distance between the transmitter and receiver f) The final alignment is obtained when the best compromise between all of the factors has been achieved so that there is acceptable detection of a prone crawling target. The signal strength at the receiver is the combination of that part of the transmitter beam which is line-of-sight and that part which reaches the receiver by reflections off the gravel surface. Maximum signal strength at the receiver, and usually the best detection sensitivity, is found when those two beam parts combine in-phase. The sensor manuals contain graphs of theoretical mounting heights for the first four nodes of constructive interference. Manuals should indicate maximum mounting heights. Experience has shown, in some cases, that directing the units toward the ground at the zone mid-point results in a good balance between prone crawling detection and false-alarm rate. The alignment procedure achieves that balance by measuring the signal strength at the receiver during the adjustments.	

Step	Instructions	Check
a.	Certify the alignment by conducting pull tests using the microwave target test spheres. *There are 30 cm (12-inch) diameter spheres that correspond to the radar target cross-sections of prone crawling targets.*. • Use the 30 cm (12-inch) diameter target for certification, and use the other targets for troubleshooting; they are also helpful in aligning troublesome zones. • During the pull tests, rake the gravel surface as necessary to remove any regions of poor detection. It is reasonable to plan for 4 to 6 hours to align and test each microwave pair. **CAUTION**: Exercise care not to disturb the gravel surface following microwave alignment. Eliminate non-essential traffic by not allowing people to wander within the PIDAS corridor. Essential traffic should remain within 2 feet of either fence and cross the bed at zone boundaries, if possible.	
3.1	Microwave Alignment	
3.1.1	Mechanical	
a.	Before proceeding with initial alignment, look at the gravel surface between the microwave heads and smooth any obvious low spots or high spots.	
b.	Verify that microwave heads are installed at the mounting heights specified on the design drawing. • If the heads do not appear to be roughly aligned, or if they were moved to reset the mounting heights, perform the following rough alignment procedure. Otherwise, proceed to part 3.1.2.	
3.1.2	AGC Measurements, PIDAS Surface Work, and Radar Target Pull Tests	
a.	Adjustments made during any of the following steps may modify that height. Final height after alignment will become the pair-mounting height for future reference. The frequency selection for each sensor is part of the system design and should not be changed as part of this procedure. Change could adversely impact the operation of other sensors. • Verify the proper frequency settings at the beginning of each test that follows.	
b.	The alignment procedure will adjust the microwave units for optimum sensitivity. Make adjustments to maximize that energy for a prone crawling target. Refer to system diagrams to locate circuit-board test points. • Certain measurements should be made during alignment and at least once per year to document the state-of-health of a transmitter. Make measurements with a 10M ohm or greater input impedance meter.	
c.	Measure voltages on the circuit boards in accordance with system documentation.	
3.1.3	Alignment and Target Testing	
a.	Using the described boresight alignment procedures, re-aim the transmitter and receiver heads slightly in the vertical direction only. • Vertically boresight align each head to point to a spot on the gravel surface that is either 30 m (100 feet) in front of the head or midway between the two heads, whichever distance is greater.	

Step	Instructions	Check
b.	Measure and verify that the vertical alignment of both heads did not increase the receiver automatic gain control (AGC) voltage more than 0.25 V above the baseline measurement.	
c.	Close both the transmitter and receiver electronic enclosures to prevent stray RF energy from entering the enclosures during target testing.	
d.	Open the appropriate signal junction box (SJB) so that the test terminals of the receiver under test can be monitored. *These contacts will normally be open and will close upon alarm. An audible device can be connected across these terminals for a more convenient indication of alarm than meter readings.*	
e.	Pull the 30 cm(12-inch) diameter radar target perpendicular to the fence and across the microwave zone using the nonmetallic sled (polyethylene) to map the zone detection. *Acceptable performance occurs when the target is detected prior to crossing zone centerline.* • Pull the target across the zone and from both fences beginning 3m (10 feet) from one crossover point and continuing at 3m (10-foot) intervals until 3m (10 feet) from the other crossover point. *It is useful to use brightly painted wooden blocks to mark each point of target detection as the target is being pulled into the zone from either fence.*	
f.	No more than two people shall be within 9m (30 feet) of the microwave zone being tested. The individuals performing the tests must remain within 0.6m (2 feet) of either fence line and must limit movements for at least 2 minutes prior to and during the pull of the target until the target is detected. • Once the target is detected, place a marker at the sled location. • Continue to pull the sled to the opposite fence, then cross to the other side to repeat the sled pull back across the zone.	
g.	Pull the sled into the zone from one fence line. • Detect, observe, and mark it with a block, then pull the sled into the zone from the other fence line along the same line to complete a test at each interval. *This method of testing should yield a symmetrical football-shaped pattern of blocks. Asymmetry or missing blocks (nondetection) help identify areas of the gravel surface that need work.*	
h.	The acceptance criteria include detection for each pull before the target crosses microwave centerline. In some cases, the block pattern may not be exactly symmetrical because of an external interference, but the zone can be certified if the acceptance criteria are met. • If the criteria are not met, examine the gravel surface for high spots between two adjacent points of no detection or low spots near one point of no detection. • Rake the gravel surface to fill low spots and level high spots, then retest the entire zone. It is useful to begin retesting by pulls across the troublesome points to see if raking fixed the problem.	
i.	Perform a set of additional target pulls 5 feet before each crossover point to document adjacent zone overlap coverage.	
j.	Raking should be sufficient to produce acceptable zone performance. If there are a few exceptions, perform special combinations of horizontal alignment changes and/or adjustments of alarm threshold voltage on a case-dependent basis.	

Step	Instructions	Check
4.0	Testing	
4.1	Microwave Walk-Test NOTE: No more than one person shall be within 9m (30 feet) of the microwave zone being tested. The individual performing the tests must remain within 0.6m (2 feet) of either fence line while moving to a new location and must limit movements for at least 2 minutes prior to walking across the PIDAS bed. Refer to the system diagrams for each microwave pair. • Walk across the PIDAS bed every 10 feet between microwave heads and observe an alarm signal. • Upon completion of a walk-test, initiate a self-test by closing the self-test terminals and observe the alarm for the microwave zone.	
4.2	Microwave Tamper Tests Refer to the system diagrams for each microwave pair.	
a.	Open, in turn, the electronic enclosures at the receiver and transmitter heads. • Observe the tamper signal.	
b.	Following the successful tamper tests, remove microwave power from the transmitter and receiver. • Observe that no alarms or tampers occur.	
c.	Walk through the microwave beam, and open either the transmitter or receiver electronic enclosure. • Observe alarms, then tamper signals, respectively.	
d.	Restore power to the microwave heads.	
4.3	Junction Box Tampers Perform these tests as part of normal maintenance as well as at the time of walk-testing the PIDAS bed.	
4.3.1	Junction Box Tamper Test Refer to the system diagrams for all junction box tamper circuits. Open each box cover as indicated to observe the tamper signal.	

INSTALLATION, ALIGNMENT, AND TESTING

Infrared Sensors

Step	Instructions	Check
1.0	**Infrared Sensors** **CAUTION**: It is critical for the infrared and microwave that the batteries be maintained at charge during cold weather. If heads are installed and will remain in the field for long periods without power from a power junction box (PJB), remove the batteries from the heads and store them inside until charge can be maintained under field conditions. References: Manuals and drawings	
1.1	Receiving Inspection Part 1: Inspect all components for damage upon receipt. Unpack; lay out and identify components for future installation. Part 2: Install end-of-line resistors. Select an infrared transmitter/receiver pair. Remove top covers and red plastic lens. NOTE: Do not scratch the plastic lens.	
a.	Install batteries and chargers inside the pillars per manufacturer's instructions.	
b.	Re-install plastic lens and top covers.	
c.	Lay out a transmitter/receiver pair about 6m (20 feet) apart on a floor.	
d.	Temporarily wire the pair together per manufacturer's instructions.	
e.	Power up the pair, and observe that an alarm occurs when each transmitter beam is blocked.	
1.1.1	Installation of Infrared Pillars	
a.	Clean dirt and other debris from top of concrete foundation.	
b.	Coat anchor bolts with WD-40 lubricant.	
c.	Remove and save top nut and washer to leave only the leveling nut and washer on each anchor bolt.	
d.	Use a leveling plate with the same hole pattern as the anchor bolts to set the height of the leveling nuts. Optimum height is when the lowest position of all the leveling nuts will allow insertion of an open-end wrench between the concrete foundation and the pillar baseplate. The leveling plate shall have the same slope as the PIDAS grade after adjusted.	
e.	Remove top covers and red plastic lens. NOTE: Do not scratch plastic lens.	
f.	Remove leveling plate. • Install pillars at the specified location and facing in the specified location. **NOTE**: Use care not to damage signal or power cables when pillars are lowered onto foundations.	

Step	Instructions	Check
g.	Rotate each pillar for coarse alignment by sighting along the flat edge of the pillar until the pillars are facing along the center line between pillars.	
h.	Secure pillars with a washer and lock nut on each anchor bolt.	
i.	Terminate the ground wire from the sensor foundation.	
j.	Terminate signal and power cables at each pillar.	
k.	Re-install plastic lens and top covers. Secure covers and rain shields.	
2.0	Alignment of Infrared (IR) Pillars	
2.1	IR Pillar First Alignment	
a.	Verify that each IR pair is perpendicular to the PIDAS slope and that the pillars are facing each other. • Sight along the flat edge of each pillar to verify that the pillars face each other along the center line between pillars.	
b.	Adjust as required. • Accomplish sighting by using a carpenter's square with the short side contacting the back of each pillar in turn. • Sight along the top edge of the long side of the square to ensure that the pillars are parallel to each other and perpendicular to the PIDAS grade. *Most portal areas are relatively flat, but the pillars will not necessarily be plumb. Reference points on the top of each pillar can be sighted to the same reference points on the opposite pillar.*	
2.2	IR Pillar Second Alignment	
a.	Carefully remove top covers and the red plastic lens from transmitter and receiver pillars. **NOTE**: Do not scratch the plastic lens. • Replace the top covers.	
b.	Remove pillar A.C. power. • Remove backup power by disconnecting battery leads within each pillar.	
c.	Connect transmitter and receiver alignment meters to the appropriate pillars. • Set both attenuation controls to maximum position.	
d.	Apply power from the PJB and begin adjustment.	
e.	Use the IR viewer to look at each transmitter beam. • Adjust the alignment screws for each transmitter to direct the beam onto its corresponding receiver.	
f.	View signal strength on the analog meter at the receiver; use the attenuation control on the receiver meter.	

Step	Instructions	Check
g.	Adjust the receiver module adjustment screws for maximum reading on the meter.	
h.	Change the meter to transmitter position at the transmitter pillar. • Adjust the spring-mounted transmitter module adjustment screws for maximum reading on the meter.	
i.	Change the meter to receiver position at the receiver; repeat the adjustment process. • As the meter readings begin to saturate, increase attenuation controls in gradual steps to return the meter readings to usable range.	
j.	Repeat the above process until adjustments no longer produce a change in signal strength.	
k.	Set the alignment meter switches to read the next beam to be aligned. • Return the attenuation controls to maximum. • Repeat the adjustment procedure for each beam.	
l.	Remove power at the PJB.	
m.	Unplug alignment meters.	
n.	Remove top covers from each pillar.	
o.	Carefully re-install battery leads within each pillar.	
p.	Carefully re-install the red plastic lens and then the top covers.	
q.	Reapply PJB power.	
2.3	Grout Grout the bottom of each IR base immediately under each pillar and provide 1:1 finished slope from the edge of the pillar baseplate to the concrete foundation.	
2.3.1	IR Pillar Post-Grout Alignment The signal margin test is the most useful test to perform on a periodic basis for maintenance and performance certification. Signal margins are the true measure of the IR performance. The measurement determines the dynamic range or the range of best-case to worst-case conditions under which the IR will give reliable results. Weather conditions such as rain, fog, snow, etc., will attenuate the transmitted IR beam so less signal will be received by the receiver. The IR units, however, are designed to operate over a very large range of signal level. Most of the IR units should have a minimum acceptable margin of at least 30 dB. The minimum acceptable level for the larger spacing at a vehicle portal, however, should not be less than 20 dB. These margins correspond to changes in received power of 1000:l and l00:l. The actual value measured for each IR pair during the signal margin measurements will become the performance rating for that pair and, in some cases, may be higher than 30 dB.	
a.	Use a set of neutral density filters to measure signal margins. The filters may be calibrated in either neutral density or dB of attenuation (dB is 10 times the neutral density). **CAUTION**: Exercise care in the handling of the filters. Handle the filters only at the edges; do not touch the center of a filter.	

Step	Instructions	Check
b.	Measure the dynamic range by first blocking each beam, in turn, at the receiver pillar and verifying that an alarm is generated.	
c.	Place a neutral density filter in front of each receiver, in turn; allow 15 seconds for the receiver to stabilize. • Verify that the receiver is not in alarm, then block the receiver beam in front of the filter to again verify that an alarm is generated.	
d.	Repeat the process with a filter having larger neutral density until the unit no longer responds to beam block. *The largest filter that still allows operation defines the signal margin for that particular beam.* NOTE: The neutral density filter set contains filters with values of 0.1, 0.3, 0.5, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0, 4.5, and 5.0 in density. Do not stack filters because that introduces more attenuation than the simple sum of neutral density and can lead to nonrepeatable results. Stacking of the 0.3, 0.5, 1.0, and 1.5 filters, for example, will result in more attenuation than a single filter with a density of 3.3. The filter values below 2.0 are most useful for identifying problems and finding weak beams. One filter from the values below 2.0, however, may be stacked in front of one filter with density above 2.0 to determine performance that may lie between the larger density values. As an example, the IR beam may function with the 3.0 filter and not function with the 3.5 filter. Stacking the 3.0 filter and the 0.1 filter for one test and then stacking the 3.0 and 0.3 filters for another test can be done to provide an acceptable measure of signal margin.	
e.	Begin the test with the 2.0 filter and work to larger values. • Document the filter value found for each receiver at each IR pair.	
3.0	Infrared (IR) Testing	
3.1	IR Beam Breaks Test Refer to the system diagram for each IR pair.	
a.	Block each beam, in turn, at the receiver pillar and observe that an alarm is registered.	
b.	Initiate a self-test by closing the circuit between the transmitter self-test terminals within the appropriate SJB.	
c.	Observe that an alarm is registered.	
3.2	IR Tamper Test Refer to the system diagram for each IR pair.	
a.	Push down on the pillar cap of the transmitter and the receiver, in turn, and observe the tamper signal.	
b.	Remove the pillar cap from the receiver pillar and observe the tamper signal. • Replace the cap and observe that the tamper is no longer present.	
c.	Remove the pillar cap from the transmitter pillar and observe the tamper. • Replace the cap and observe that the tamper is no longer present.	
d.	Following successful tamper tests, remove IR power from the transmitter and receiver, and observe that no alarm or tamper occurs.	

Step	Instructions	Check
	• Block one beam, then press down upon the transmitter and receiver top caps, in turn, to observe alarm tamper signals, respectively. • Restore power to the IR pair.	

Exercise 6.6

PIR Testing

Session Objectives

1. Involve the participants in PIR sensor testing in order familiarize the participant with sensor performance and acceptance testing.

2. The testing in these exercises will demonstrate the determination of the detection envelope for the most sensitive and least sensitive directions for the sensor using different target orientations and speed (slow walk, crawl), to look at common nuisance alarm sources, and to review sensor vulnerabilities.

Volumetric Sensor Laboratory Baseline Testing

Baseline testing establishes the performance characteristics of the sensor under optimum conditions. This will help a user to determine if a particular sensor will suit the needs of a particular installation and threat. Conditions in an actual installation may degrade from the baseline performance. Evaluation of an actual sensor installation is covered in the section tiled “Evaluation of Installed Volumetric Sensors”.

Baseline testing is performed under conditions that are as ideal or as optimum as possible for the sensor. For volumetric sensors ideal conditions include an empty interior room area with a tile or concrete floor, room temperature between 65-75^{o}F, no windows (or windows that are covered) and no or minimal nuisance alarm sources within the test area. The area should be large enough so that all of the detection envelope of the sensors can be walk tested. An additional ideal condition for a microwave sensor would be room construction from heavier construction materials such as concrete, concrete fill block, or metal siding.

For this exercise we will be using the exterior mono-static PIR.

Volumetric Sensor Testing Exercises

The purpose of the test exercises is to involve the participants in sensor testing in order familiarize the participant with sensor performance and acceptance testing. The testing in these exercises will demonstrate how to verify the detection envelope for the most sensitive and least sensitive directions for the sensor using different target orientations and speed (slow walk, crawl), to look at common nuisance alarm sources, and to review sensor vulnerabilities.

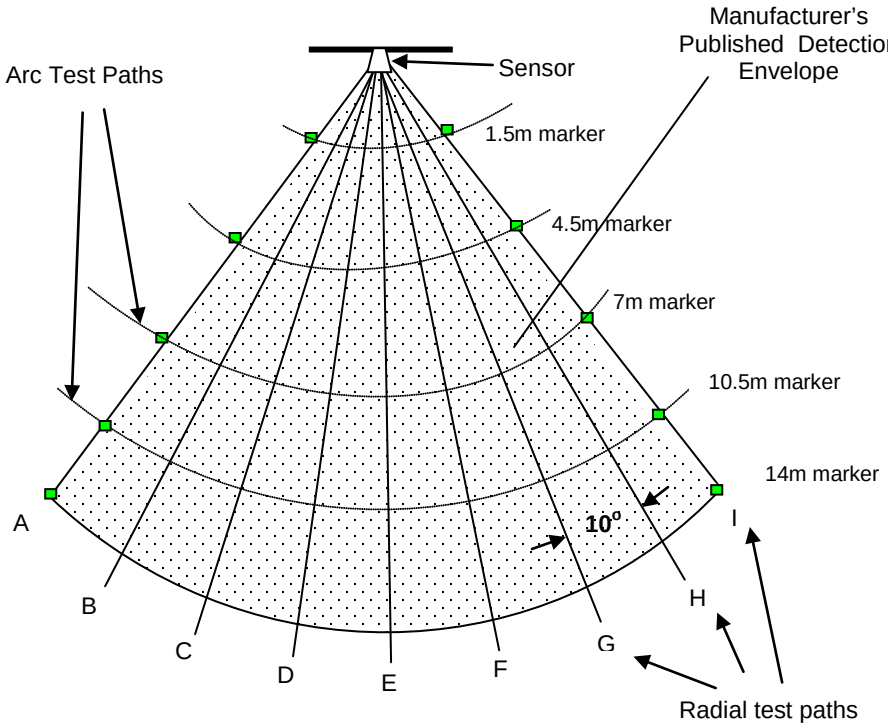


Figure 1 – Example of PIR Test Pattern of Sensor with a 14 m (45 foot) Detection Range and 90° Detection Envelope

Most sensitive direction for the PIR sensor (across detection pattern, along the test path arcs).

Beginning outside the detection envelope wait 20 seconds after the sensor resets. Walk at 0.3m (1 foot) per second with arms folded across chest along the arc path at the 1.5 m (5 foot) marker. When alarm occurs, stop. Measure the distance from the detection envelope edge to the point along the walk test arc where the alarm occurred. Record this distance on the test data sheet. If no detection occurs annotate with "ND".

Stand still for 20 seconds after sensor resets and continue to walk through the detection envelope along the test path until outside the detection envelope on the opposite side. Verify detection occurs throughout the continuous walk.

Repeat both tests beginning from the opposite side in the opposite direction along the same walk test arc.

Repeat the test cycle (in one direction, then other direction) along the same path for an additional number of times that is required to establish the desired minimum Pd and confidence level.

Perform the above tests along each of the 3m (10 feet) spaced test path arcs.

For test each direction along each test arc and using the test data, take the largest distance from the detection envelope edge where detection occurred, and mark this point on the sketch or drawing of the detection area. Once all of the detection points are marked, an outline of the smallest detection area can be drawn.

Least sensitive direction for the sensor (directly towards the sensor).

Along the radial test paths in a direction directly towards the sensor, walk test at 0.3m (1 foot) per second with arms folded across chest. Beginning outside the detection envelope wait 20 seconds after the sensor resets. For the test paths along the edges of the detection envelope make sure the tester walks just inside of the detection envelope edge.

If the test area is not large enough for the test subject to be out of the detection envelope (the test area is smaller than the maximum published detection distance), the test subject should stand very still with arms folded for 20 seconds after sensor resets before beginning each walk test. This allows the test subject to “fade” in to the background so the sensor can reset.

Along test path A begin the walk test and stop when an alarm occurs. Measure this point from the manufacturers advertised maximum detection distance or from the position where the test started. Record this distance on the test data sheet. If detection occurred before reaching the maximum detection distance, record zero. Repeat this test the additional number of times along the same test path to establish the minimum Pd and confidence level.

Repeat the above tests along each radial test path.

Using the test data, take the largest distance from the detection envelope edge where detection occurred (or from test beginning points) and mark this point on the sketch or drawing of the detection area. Once all of the detection points are marked an outline of the smallest detection area can be drawn.

Additional testing:

Perform slow walk tests 1 cm (3 inches) per second similar to the previous walk tests along each arc test paths and along each radial paths. Annotate where detection occurs and determine Pd along those paths for the slow speed tests. Sketch the detection envelope for the slow walk.

Perform crawl tests along the arc test paths at the 1.5 m (5 foot) marker and every other marker for 2 additional arc paths (total of 3 arc paths). Crawl tests can be performed using an auto mechanics creeper. Each crawl tests is performed beginning outside the detection envelope and stops where detection occurs. Annotate the distance where detection occurs for each test. Sketch the minimum detection envelope for the arc path tests.

Perform the same crawls tests along three radial paths. The radial paths should be on one side of the detection envelope beginning with the center path followed by two additional paths on either the left or right side.

Sensor Vulnerability Tests

1. Cover lens: From a location out of the sensor view (behind or side) slowly move a cover in front of the sensor unit. Try this several times from top down and side to side. Can the sensor be covered without generating an alarm?
2. No target temperature: Several methods can be tried. One way is to put on a well insulated suit that includes covering head, hands and feet. Another method is to construct a light-weight insulated box (cardboard box)to enclose the test subject. The enclosure will need to completely surround the tester. The suite or enclosure needs to be at the test room temperature. Perform tests using different speeds, orientation and backgrounds. Include obstacles (furniture, desk, file cabinet, etc) in one background and a blank wall as the other background. Can the sensor be by-passed?
3. High room temperature: increase room temperature to 32^{o} C (90^{o} F). With no test targets in the detection area, monitor sensor for nuisance alarm while room temperature is rising. The 32^{o} C (90^{o} F) temperature needs to be maintained for 8 hrs in order to allow all items within the room (furniture, equipment, walls) to equalize at this temperature. Perform detection tests at different speeds and orientation. Record testing results. If air conditioning is turned on to cool the room after testing is complete, monitor sensor for nuisance alarms during the cool down period.

Nuisance Alarm Source Tests

1. Position a variable speed fan space heater with a 500 W heater element 9m (3 feet) in front of the sensor along the E radial line. Setup an extension cord and power strip in order to remotely switch power to the heater. Switch heater on with maximum air flow. Alternately switch power on for 2 minutes, then off for 2 minutes. Record the sensor response during the on-off cycle. Repeat this cycle 10 times.
2. Repeat the above test with the heater positioned 30cm (12 inches) above the detection envelope so that it will blow hot air straight down into the detection envelope. Record sensor response
3. Locate heater outside the detection area on the floor around the 3m (10 feet) to 4.5m (15 feet) marker location so that it will blow warm air across the sensor field of view. Perform on-off cycle tests. Record sensor response.

Extra Reference Material

Evaluation and Testing of Installed Volumetric Sensors

This section discusses the on-site evaluation of sensor installation. The evaluation discussed here assesses sensor performance in the environment where it is installed and includes review of room/area configuration and characteristics, location of sensors with respect to entry paths and other sensors, review of any site procedures for testing and maintenance, review of past sensor performance and maintenance history, as well as actual performance testing the sensor. Some facilities may have criteria defined for sensor performance. Below are some examples

- Volumetric sensors shall detect an individual moving at a rate of 30 cm (1 foot) per second, or faster with a Pd of 90% at a 95 % confidence level within the total field-of view of the sensor.
- The sensor shall have no more than 1 false alarm per 2400hrs.
- The sensor shall be installed and maintained in such a way to provide reasonable assurance that the number of nuisance alarm does not reduce alarm reporting credibility. If alarm assessment is continuous and timely, either by CCTV or visually from a guard post, a higher nuisance alarm may be tolerated provided it does not result in protection system degradation.

PIR Effectiveness Testing

An effectiveness test is performed at the initial or new installation of a sensor, and when a sensor has been moved, repaired or replaced. In the case of a new installation this test can be used as an acceptance test. The objective of this test is to establish that each sensor detects throughout the intended detection area at the Pd confidence level specified in the site requirements. In order to establish the Pd and confidence level, a number of tests are required along number of paths within the detection area. In this exercise 10 tests along each path will be conducted. If the sensor passes all 10 tests along each path, we will have verified the sensor coverage and a Pd of at least 70% Pd at 95% confidence More tests will need to be conducted to verify a higher Pd level.

Two persons will be required when conducting this test. One to perform the test, the other to document test results.

1. Review previous installation, testing, maintenance and repair records. Review nuisance and false alarm records. Make a note of any previous deficiencies or issues and sensors that have an on-going or recent high NAR/FAR
2. Make a drawing sketch of the area or room. Include the location of sensors, furniture, equipment, other objects, and likely entry points and paths that an intruder would take to get to protected items. Include

necessary annotation of the sensor such as type, model no, serial no. etc. Using the manufacturer's data sheets obtained from the installation and maintenance records, sketch in the published detection area for the sensor.

3. Draw in sensor test paths. Include the starting points and ending points for each path. This test grid should be based on locations of windows, doors, ventilation ducts, other likely ways of entry and protected assets. There should be enough test paths to provide confidence that the sensor detection envelope is correct and provides the intended coverage.
4. If furniture, equipment or other items block the sensor line of sight in certain areas so that the sensor is blind along a viable path, verify that another sensor(s) cover that area. (Effectiveness testing of the other sensors will verify their coverage.)
5. Note the room temperature.
6. Visually inspect the sensor under test and look for signs of tampering, damage and other items that could degrade performance.
7. Verify that the sensor wiring after it leaves the sensor housing is protected and cannot be accessed easily.
8. Remove sensor cover and verify with the CAS operator that a tamper alarm for that sensor is displayed.
9. Place the internal jumper within the sensor so that the alarm indicator lamp operates.
10. Establish within the room where the detection area should be for the sensor under test. If necessary mark off this detection area using masking tape or other marker.
11. From outside the detection area, begin walking at 30 cm (1 foot) per second along the first path. When an alarm occurs document on the drawing the point where the test walker was detected.
12. The test walker returns to outside of the detection area and waits for a minimum of 30 seconds after the sensor has reset. Perform step 11 again.
13. Repeat steps 11 and 12 until at total of 10 tests have been performed along the path. If all of the walk tests have been detected, the sensor passes testing for this path.
14. Perform steps 11, 12 and 13 for the remaining paths
15. At the conclusion of effectiveness testing place the alarm lamp indicator to the off position.
16. Perform operational tests and verify that the alarm signals are received at the CAS.

PIR Operational Tests

Operational testing is performed on a periodic basis such as when the protected area is placed into the secure condition at the end of a work day or on a weekly/monthly basis. The objective of this test is to verify that the sensor is operational and that the alarm signal is received and displayed at the CAS.

One person can perform this test. The tests are performed beginning at the likely paths of entry. There may be only one likely entry path or several.

Before beginning the test it will be necessary for the test person establish communications with the CAS to let the operator know that an operational test of the specific sensor is about to begin.

1. For each likely entry path the tester will remain outside the protected area or sensor detection area for 30 seconds in order make sure that the sensor has stabilized in the secure mode.
2. After this period the tester takes 3-30 cm (1 foot) steps (approx 1m or 3 feet), into the protected or sensor detection area and stops. The tester contacts the CAS operator to verify that an alarm for the sensor under test has been displayed on the console. If an alarm is displayed, the test is complete.
3. If no alarm has been displayed, the tester returns to the starting point and repeats the test with 4 steps (approx. 1.2 m or 4 feet into the area). This repeat test is performed provided that the tester within the 4 steps cannot reach any items under protection. If no alarm occurs after this test, a problem with the sensor is indicated and needs to be investigated.

PASSIVE INFRARED SENSOR CHECKLIST

Date

Evaluator

Facility / Location

A. Equipment Data

1. Type _____
2. Manufacturer & Model

B. Performance Tests

1. Walk-tests - determine range and shape of detection zone:

   (a) With the system armed (or using a walk-test light if available), walk across the sensor field with a slow, steady walk (5 in/sec 13 cm/sec) while keeping arms motionless; note on worksheet where an alarm occurs.

   (b) Repeat the test several times with different directions of approach to map detection zone.

2. Could the sensor be defeated by very slow motion? Y N
3. Is the device line supervised? Y N
4. Is wiring in conduit? Y N
5. Is an alarm initiated when:

   (a) Cover is removed from device enclosure? Y N

   (b) Electrical lines are disconnected? Y N

C. Factors Affecting Performance

1. Are sources of infrared energy (open heating elements; incandescent light bulbs; direct sunlight on windows, floors, and walls; and convective heat currents) present? Y N
2. Are there periods when the room temperature is 26-32° C (80-90° F)? Y N
3. Is the most likely intruder path across the field of coverage rather than directly into it or away from it? Y N
4. Can the intruder approach the sensor from the rear? Y N
5. Is the desired detection zone interrupted by windows, partitions, or furniture? Y N
6. For multiple sensor applications, do all sensors function properly providing the required area of coverage? Y N
7. Is the field of the sensor clear of::

   (a) Suspended lamps? Y N

   (b) Animals, birds, and large flying insects Y N

   (c) Blowing debris? Y N

   (d) Fast heat sources? Y N

8. Are transceivers, receivers, and control units located away from radio transmitters? Y N
9. In case of loss of electrical power:

   (a) Does the sensor have battery standby power? Y N

   (b) Is a loss of power alarm initiated? Y N

10. Are there visible signs of physical abuse? Y N

Describe

11. What serves as back-up detection if this sensor is inoperable?

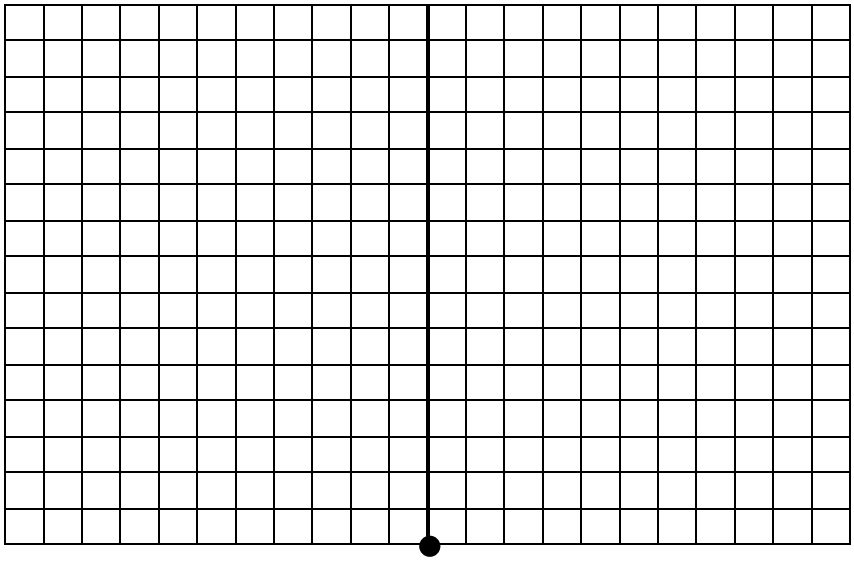
Describe

PASSIVE INFRARED SENSOR CHECKLIST *(cont.)*

Notes / Miscellaneous

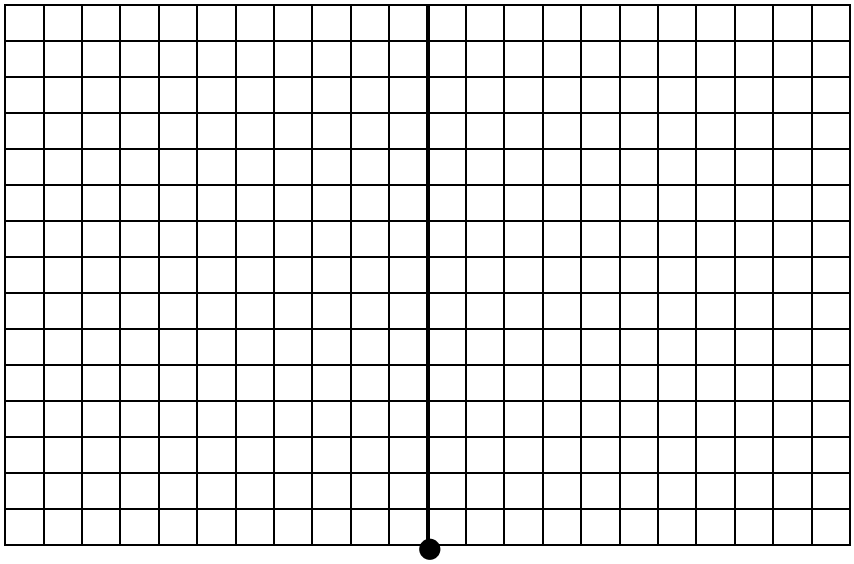
PASSIVE INFRARED SENSOR CHECKLIST *(cont.)*

Walk-Test Worksheet



Sensor Location

Notes/Miscellaneous



Sensor Location

Notes/Miscellaneous

Mark location of alarm with a dot and direction of approach with an arrow.

Other Sensors

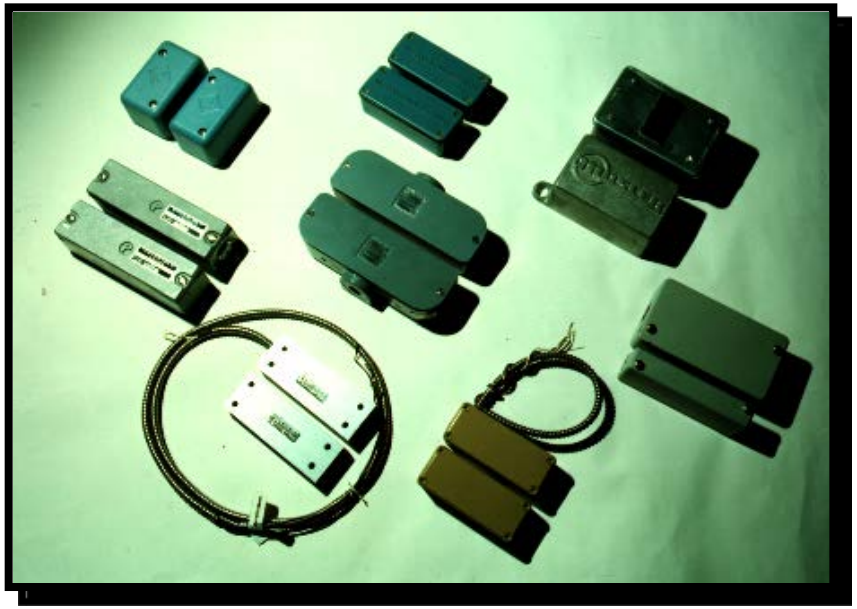
Learning Objectives

After completing this module, you should be able to:

- Describe the fundamental principles of the different sensors
- Identify in what application these sensors are suitable for providing effective detection for given threat tactics and environmental conditions
- Evaluate and determine effective placement of these sensors
- List the advantages and disadvantages of these sensors

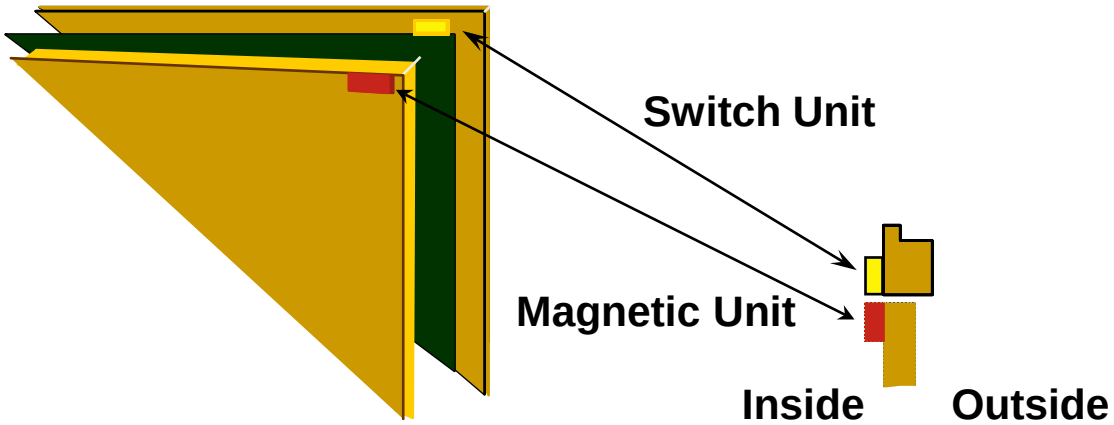
Balanced Magnetic Switches

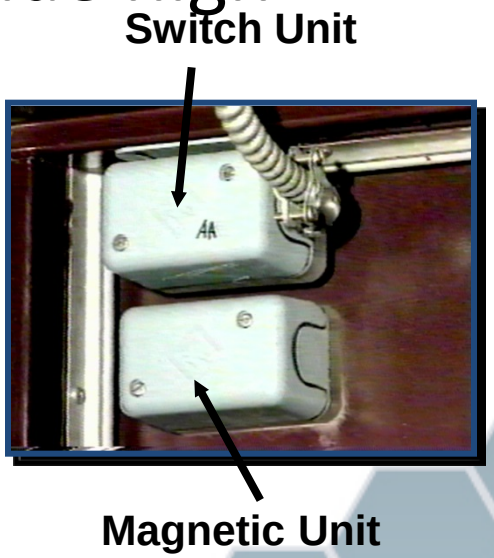
- Sensor classification
  - Passive
  - Visible
  - Boundary Penetration Sensor



Balanced Magnetic Switches

- Mounts on doors / windows
- Alarm generated by magnetically controlled switch (reed switch)
- Magnetic field balanced to provide high level of defeat protection

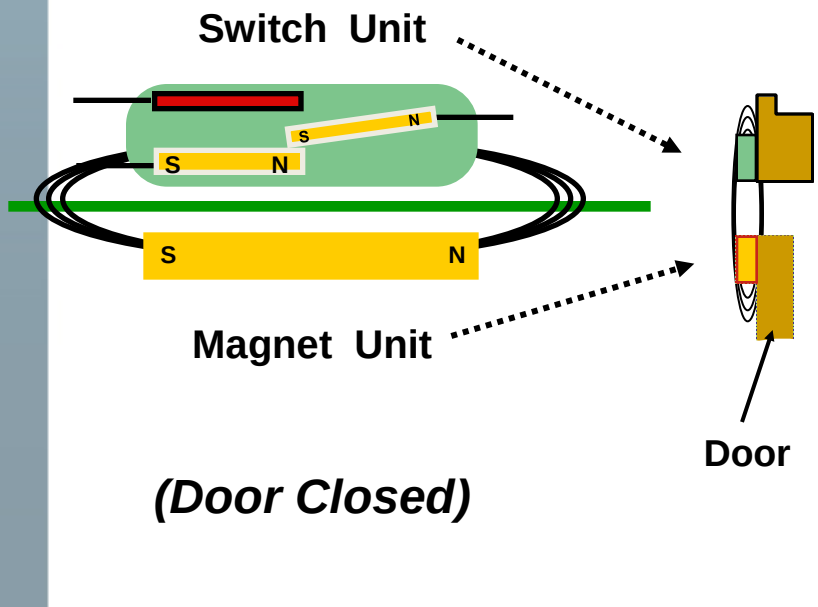


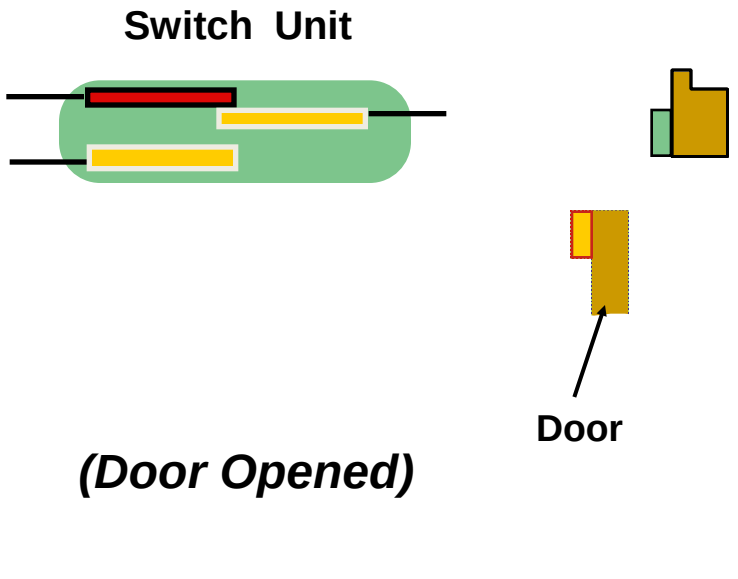


Operational Principle of BMS

- Consists of a reed switch with bias magnet and a door mounted magnet unit
  - Bias magnet and door magnet create a magnetic loop, resulting in a balanced condition around the reed switch
  - Some BMS sensors employ multiple reed switches and bias magnets, and multiple magnets in door unit
    - Provides even higher defeat protection
- Alarm occurs when balanced condition is upset
  - Such as when the door magnet is moved far enough or when an external magnet is placed close by

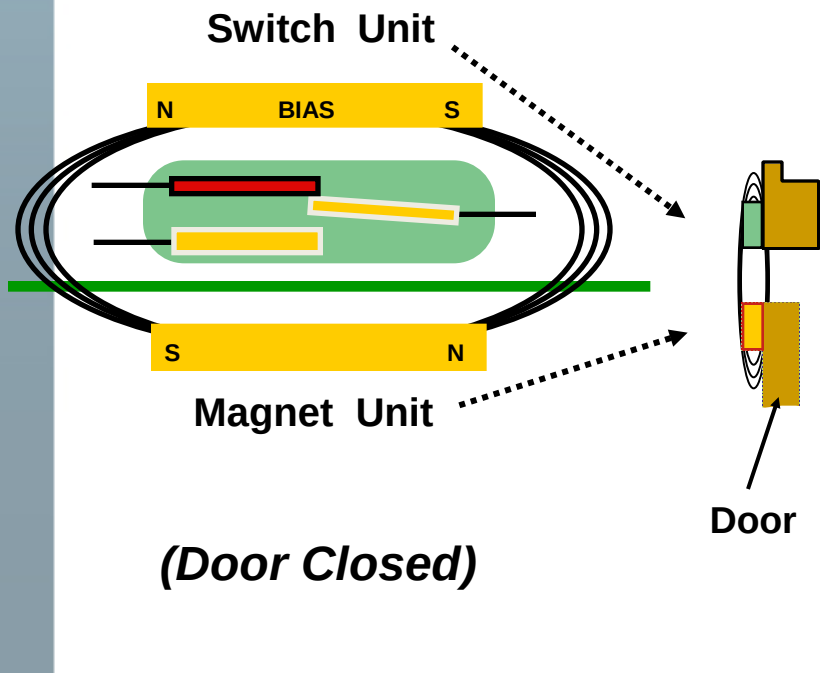
Simple Magnetic Switch

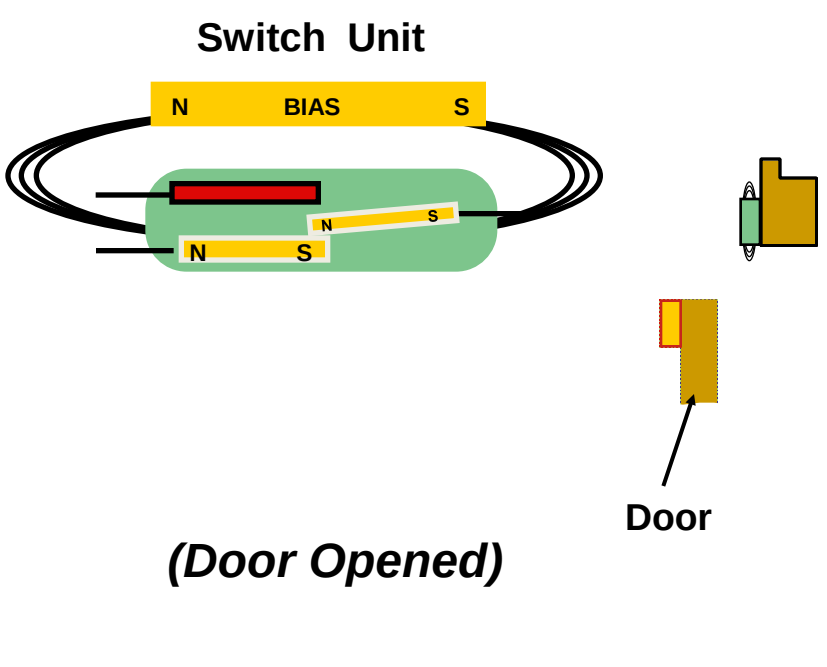




Non- Magnetic =

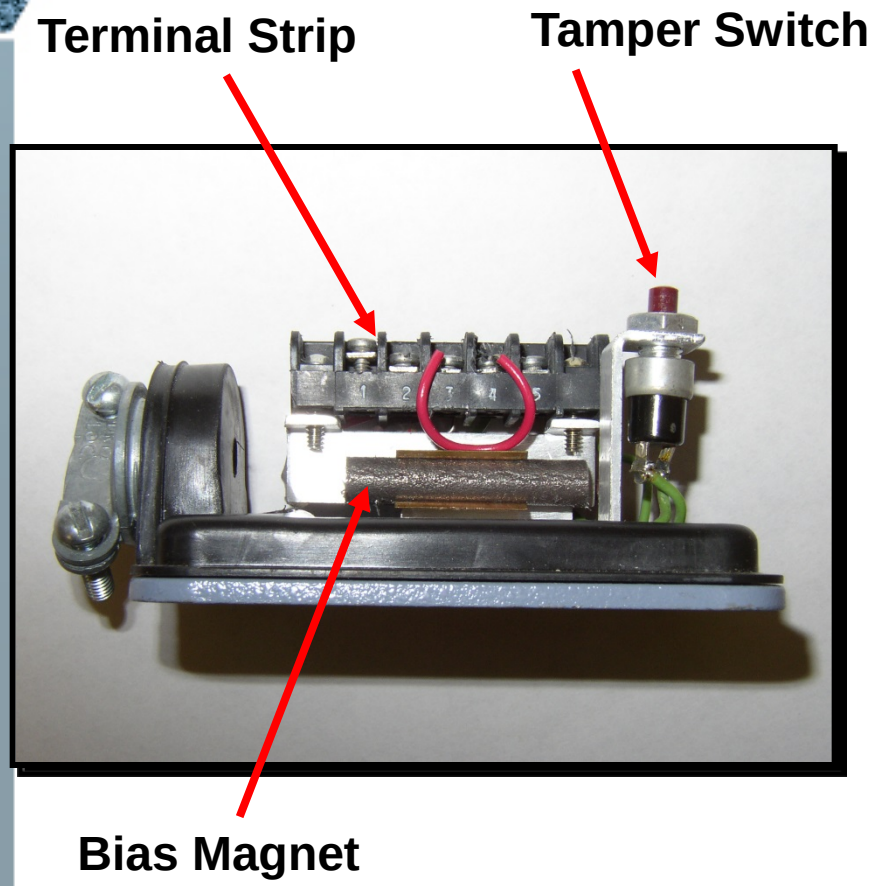
Balanced Magnetic Switch

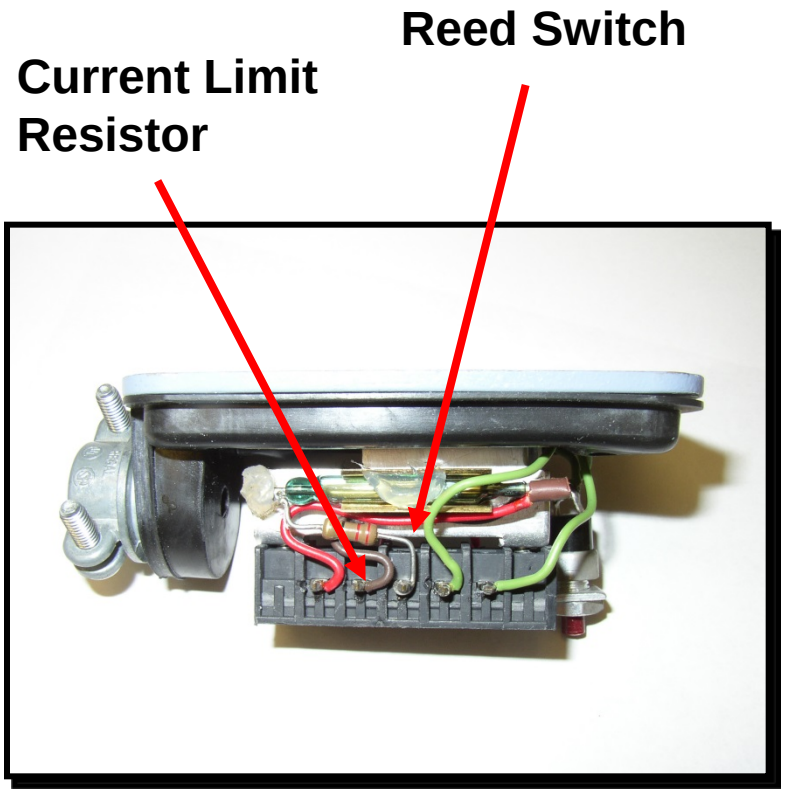




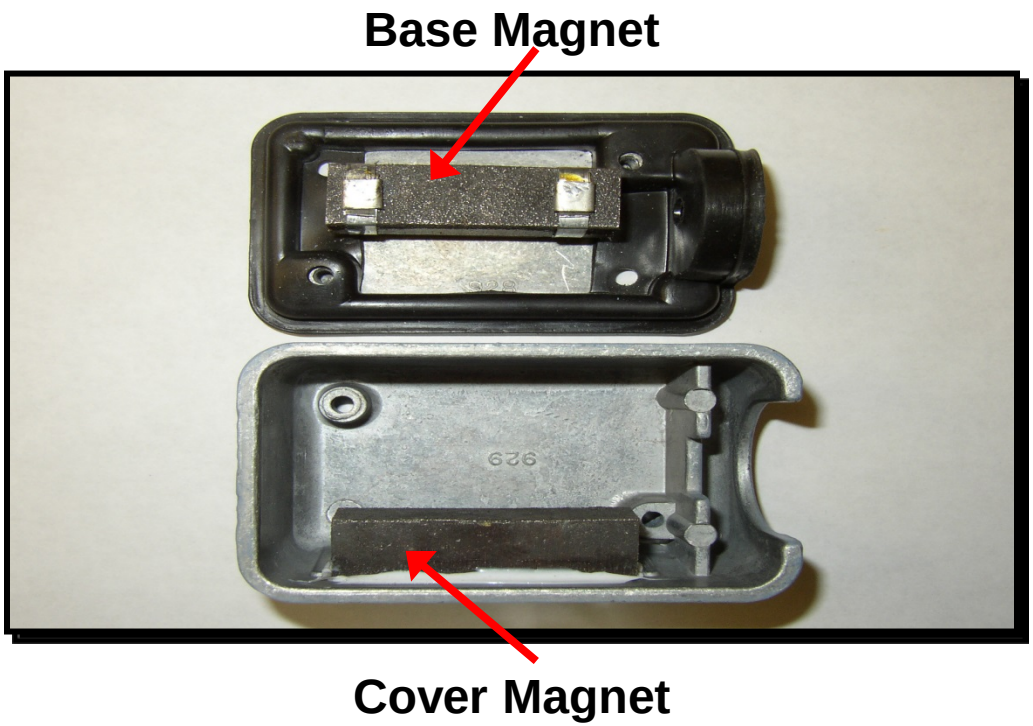
Non- Magnetic =

BMS Switch Unit Example





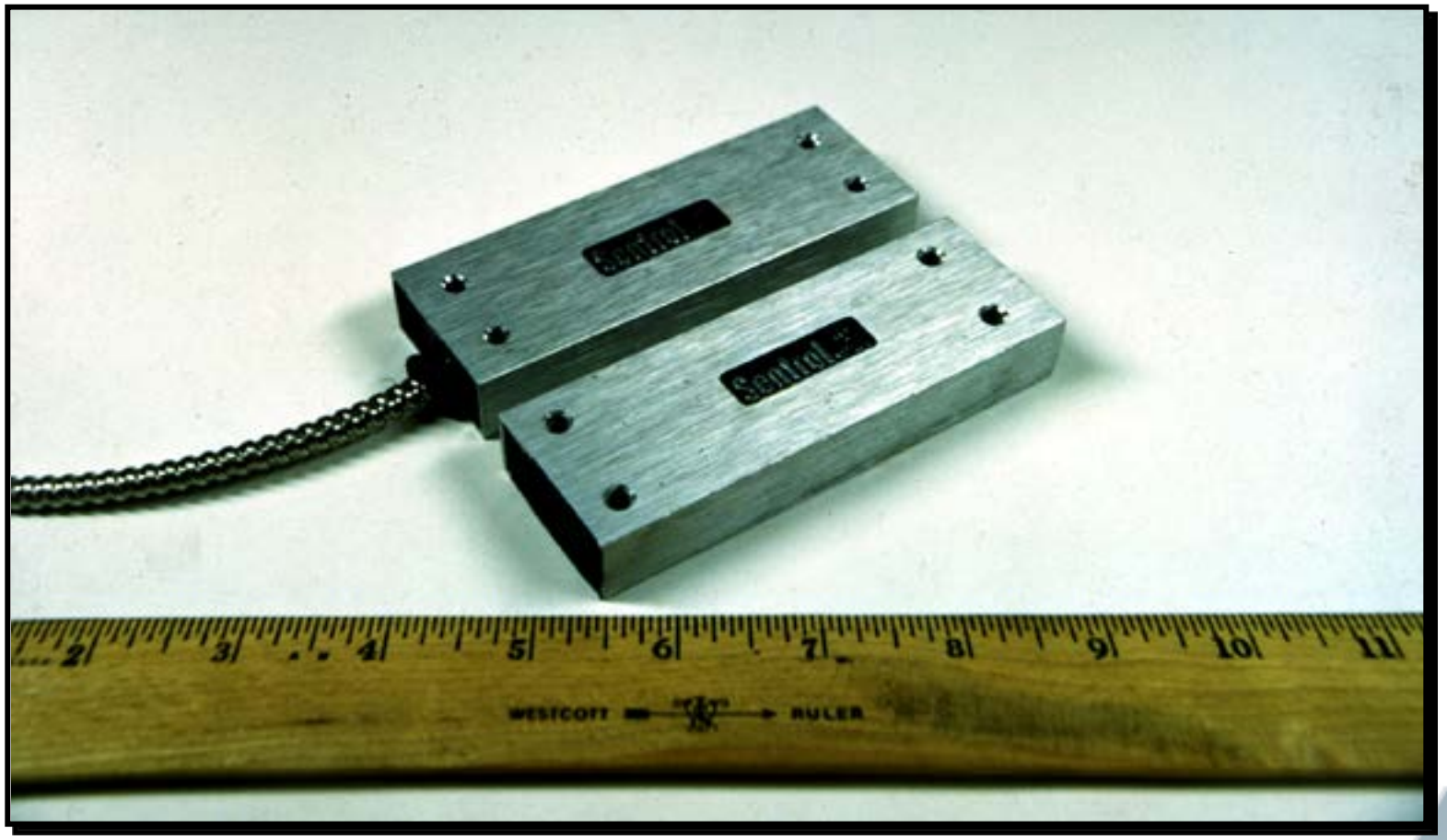
BMS Magnetic Unit Example



Triple Biased Magnetic Switch

- Three reed switches, bias magnets and door magnets
  - Polarity of magnets different
- Hermetically sealed
  - No internal access
- Pry tamper
- Magnetic tamper
- Options
  - Self test
  - Six biased reed contacts

Example: Triple Biased Magnetic Switch

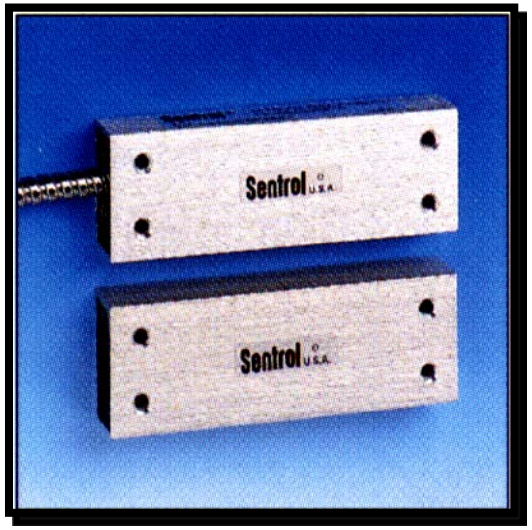


BMS Nuisance Alarms

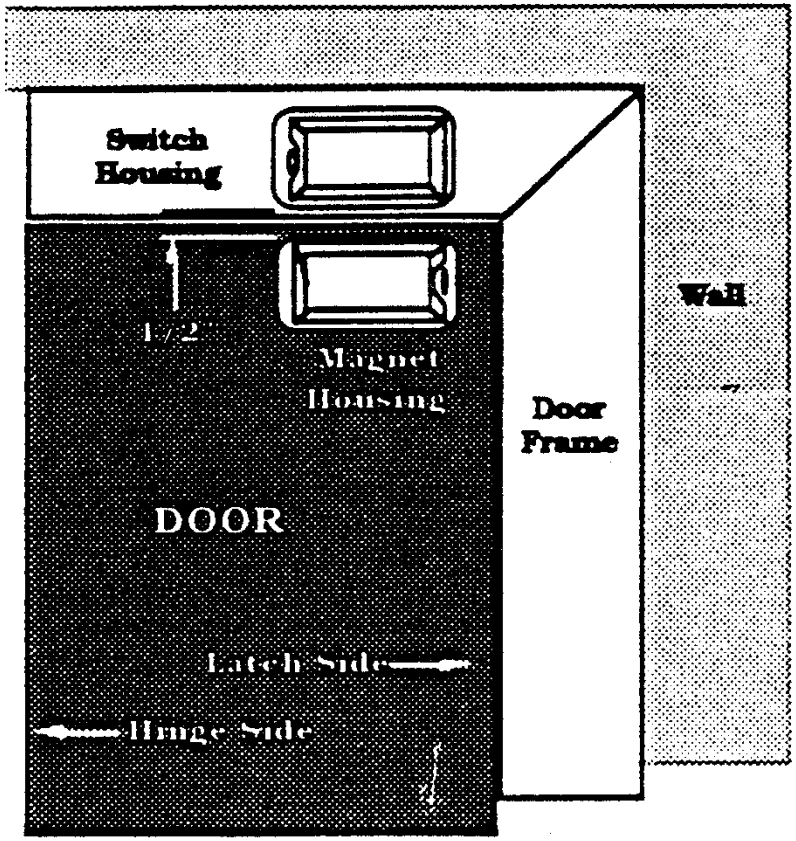
- Sensors seldom nuisance alarm by themselves
- Nuisance alarms
  - Almost exclusively caused by worn or improperly adjusted door hardware that results with door movement due to wind, human or animal activity
  - Also, improperly installed or adjusted BMS
- BMS Systems should be thought of as the sensor plus the device that it is installed on (door, window, etc.)

BMS Vulnerabilities

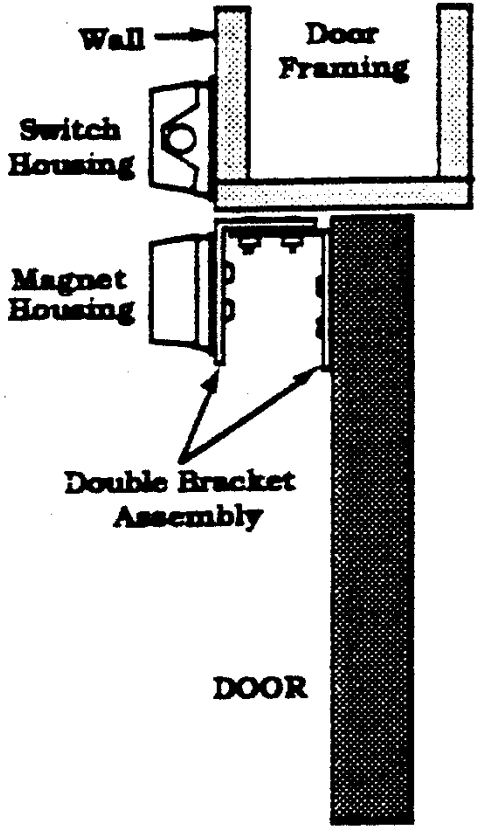
- Externally introduced magnetic field
- Switch or door magnet removal
- Physically by-passing switch



BMS Installation Example



NORMAL MOUNTING



MOUNTING RECESSED DOOR

BMS Performance Testing

- Effectiveness testing
  - Performed every 6 months, yearly or per site requirements
  - Verify tamper operation and communication to CAS
  - Verify tamper or alarm when foreign magnetic field is introduced
  - Verify that alarm occurs within specific door movement distance
    - Typically before the leading edge of door has moved 1 inch (2.5 cm)
  - Verify that no alarms occur during any slight door movement when latched

BMS Performance Testing *(cont'd)*

- Effectiveness testing (cont'd)
  - Door and hardware condition
    - Hinges, latch, scraping door jamb
  - Sensor maintenance
  - FAR / NAR histories
  - Switch location within protected area
  - Non-ferrous mounting surface or non-ferrous spacers between BMS units and metal surfaces
  - Tamper switch(es) continuously monitored and line supervision
  - Wiring in conduit

BMS Performance Testing *(cont'd)*

- Operability testing
  - Performed on a frequent basis (daily / weekly)
  - Verify that the sensor is operational
  - Simple test
    - Open door and verify correct alarm is received at the CAS
    - Close door and verify secure state

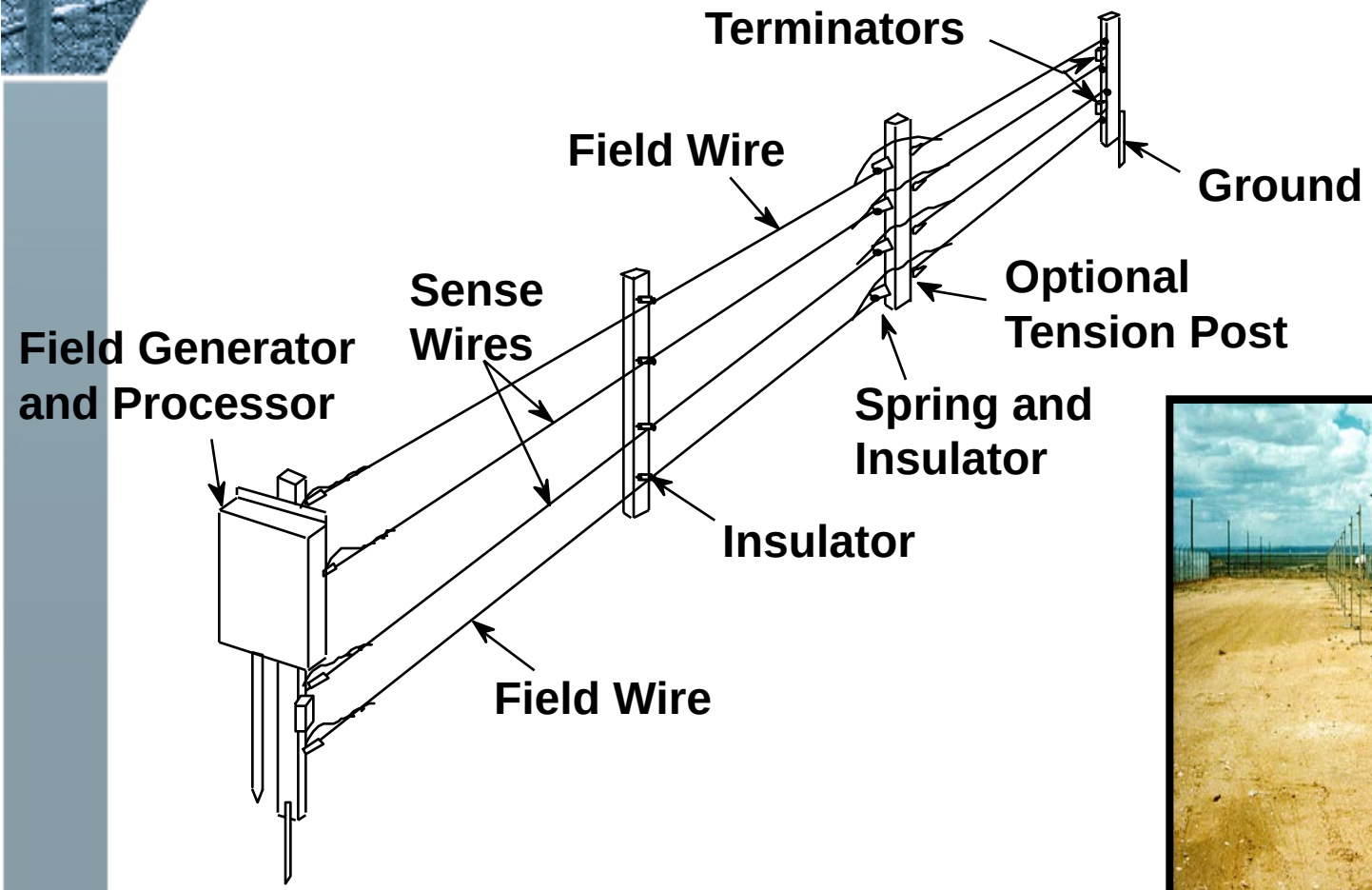
BMS Summary

- BMS application
  - P_D
  - Nuisance alarms
  - Vulnerability to defeat
- Integration of sensors into an interior sensor system must consider the skill level of the intruder, the design goals and effects of environmental conditions
- Physical operations should determine sensor placement to achieve optimum performance

Capacitance/ e-field Sensor Classification

Capacitance or E-Field Sensors	
Active	Passive
Covert	Visible
Line of sight	Terrain following
Volumetric	Line
Mode	Free Standing or Fence Mounted

Example of Early Analog Sensor



Example of Newer Digital Sensor

Capacitance Operational Principles

- Detects change in capacitive coupling between sense and field wires
- Multiple pairs of wires are used to discriminate between environmental effects
- Early versions use analog processing - newer versions are digital

Performance Characteristics

- P_D
  - Detection volume affected by;
    - Wire spacing
    - Freestanding or fence mounted
    - Sensitivity settings
  - Detection depends on size, speed, and grounding of intruder and proximity of intruder to wires

Performance Characteristics *(cont'd)*

- NAR / FAR causes of nuisance alarms
  - Birds, animals
  - Lightning, heavy rain, wet snow
  - Wind, blowing debris, blowing vegetation
  - Electrical interference
- Vulnerability to defeat
  - Tunneling
  - Bridging
  - Slow Movement

Capacitance Installation

- Site preparation
  - Uniform grade of terrain between posts
  - Area near sensor clear of vegetation
- Fence mounted
  - Fence fabric tightened
  - Motion dampened
- Can be used over buildings
- Good earth ground is critical

Capacitance Sensor Maintenance

- Check wire tension to reduce wire vibration
- Remove vegetation or debris near wires
- Check for damage to insulators, wire insulation
- Clean insulators to remove spider webs, salt spray, or dust

Capacitance Sensor Testing

- Walk tests
- Slow penetration attempts
  - Grounded and ungrounded adversary
- Currently, good testing simulations do not exist

Capacitance/e-Field Sensor Summary

- Can follow variations in terrain
  - Even up and over buildings
- Volumetric detection
- Early versions prone to high NAR / FAR
- Significant improvements due to digital signal processing

Introduction to Alarm Assessment

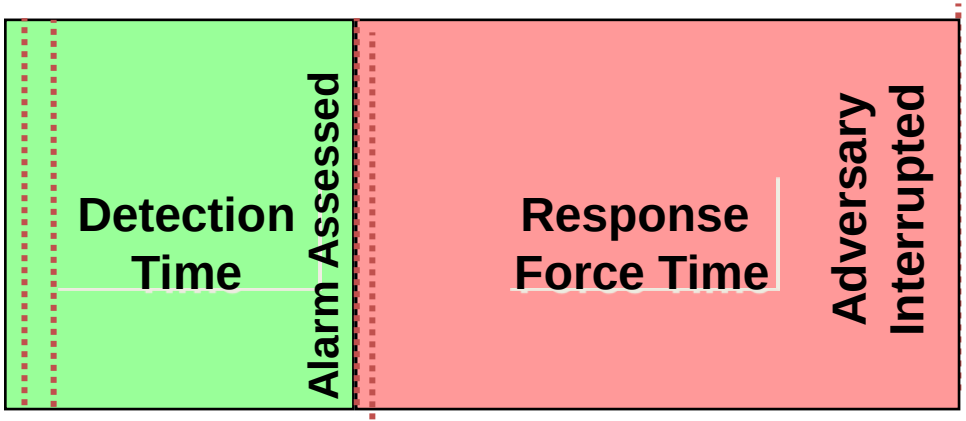
Learning Objectives

After completing this module, you should be able to:

- Discuss the basic fundamentals of alarm assessment
- Describe the purpose and importance of alarm assessment for a physical protection system
  - Review the different methods: people and technology
- Explain the differences between assessment and surveillance
  - Discuss the key points

Purpose of Alarm Assessment System

- Determine cause of each sensor alarm
- Provide information about an intrusion – relay to response force
- End detection time



Class Exercise 1: Detection Time

Question: Which Step ends Detection?

1. Sensor alarm signal is generated
2. Alarm signal is transmitted to console
3. Operator is alerted by incoming alarm
4. Operator scans images on a monitor of the alarmed detection zone
5. In searching for cause of alarm, operator observes an unauthorized person in that area
6. Operator calls up response force, identifying nature and location of intrusion
7. Response force interdicts intruder

Determine Cause - People

- Roving patrols, or
- Fixed patrol stations

Determine Cause - Technology

- CCTV cameras and appropriate lighting provide full coverage of sensored areas
- Thermal cameras provide full coverage of sensored areas without illumination
- Images are displayed to an alarm station operator for assessment

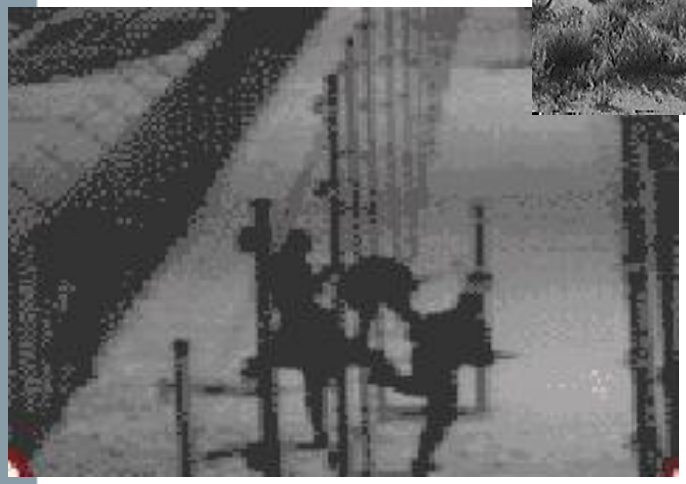
Class Exercise 2: Detection Time

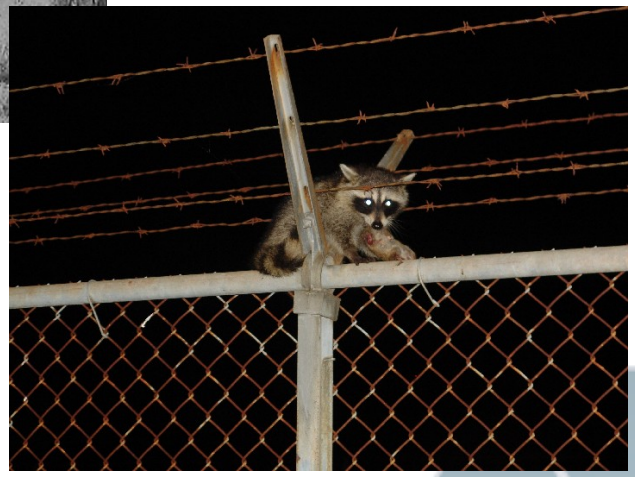
Question: Which Step ends Detection?

1. Sensor alarm signal is generated
2. Alarm signal is transmitted to console
3. Operator is alerted by incoming alarm
4. Operator sends roving patrol to investigate since the video system is offline
5. The patrol radios to the operator that they have arrived at the sensored area
6. After 1 minute the operator sends another patrol to investigate, why the first patrol has not responded

Provide Information

- Detection, Classification, and Identification





Levels of Assessment Resolution

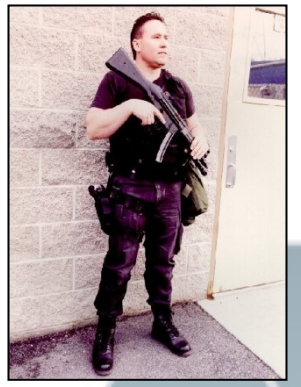
Detection	Classification	Identification
		
Determine presence of object	**Determine nuisance or real alarms**	**Determine identity of object**
2-3 pixels/30 cm	6-9 pixels/30 cm	10-16 pixels/30 cm

Important factors are *contrast, motion, and upright human figure*

People – Advantages and Disadvantages

- Advantages
  - Can provide on-site visual observation and detection capabilities
  - Flexible deployment
  - Can provide delay or immediate response

- Disadvantages
  - Significant time may have passed between an alarm and assessment
  - Can tolerate only a very limited number of nuisance alarms
  - Manpower costs
    - May be expensive over long term



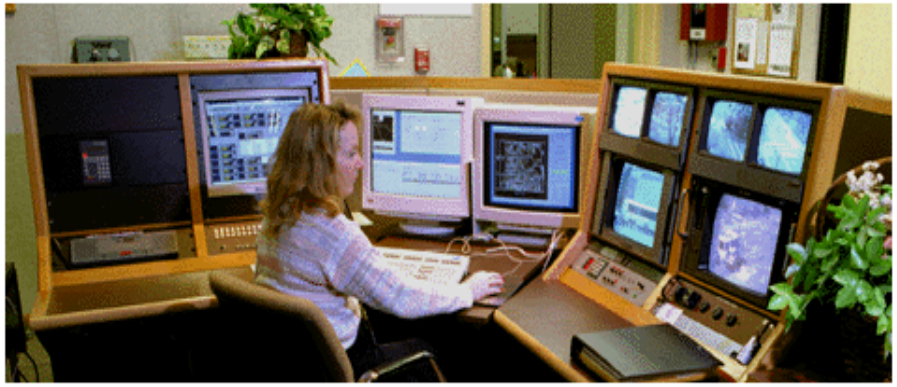
Technology – Advantages and Disadvantages

- Advantages
  - Alarm assessment can occur almost immediately
  - Pre-event and post-event recording
  - Efficient use of people

- Disadvantages
  - Requires infrastructure for effective video assessment
  - Initial cost may be high
  - Requires testing and maintenance

Assessment vs. Surveillance

- Assessment definition
  - Alarm information directed by sensor activation to a human to determine if an intruder has penetrated a sensored area



Assessment vs. Surveillance

- Surveillance definition
  - Continuous use of a human as a intrusion detector to monitor several restricted areas that are NOT sensored by intrusion technologies.

Assessment Key Points

- Technologies efficiency or accuracy of reporting events does not significantly change
- Technologies can be a force multiplier
- Humans are alerted to alarmed events
- Proper application of multiple technologies can assist the human in making a quick and accurate decision to an event
- Use of multiple technologies does not leave a single point failure in the system

Surveillance Key Points

- Technology usually is visible to public and used as a deterrent
  - Can you measure this?
- Human as a detector has a low probability of detection
  - Generally given a P_D of 0.01 to 0.02
- Used when time is not critical to an event
- Loss of video leaves a single point failure in both the assessment and detection of the intrusion
- Used for compliance criteria

Summary

- Detection is not complete without assessment
- Humans make poor detectors but are good at assessment
- For an effective on-site response, the time between an alarm and assessment must be short

Alarm + Assessment = Detection

Overview of Video System Components

Learning Objectives

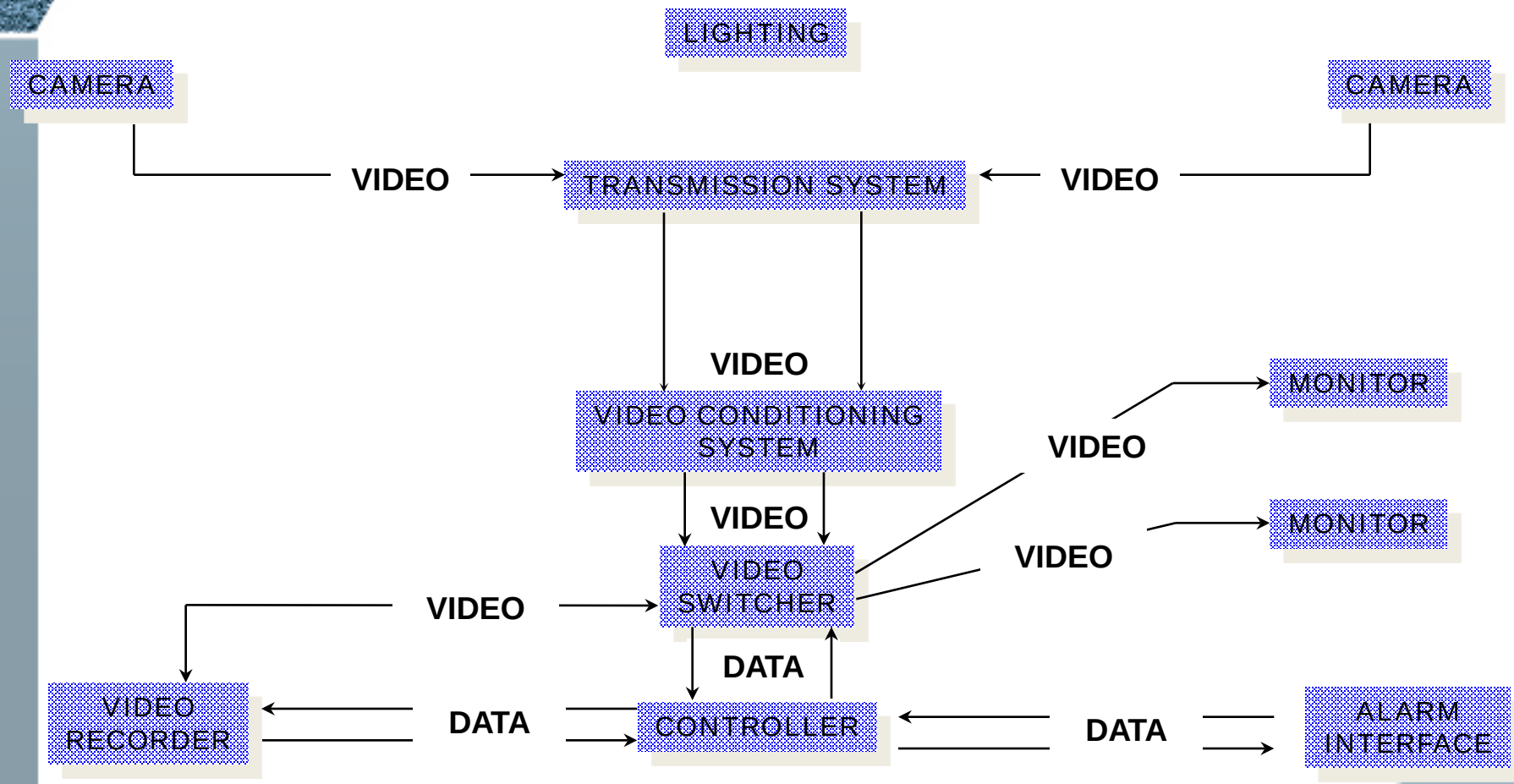
After completing this module, you should be able to:

- Identify the major components of a video system for alarm assessment
- Compare analog and digital video systems
- Explain the performance requirements of a video system for alarm assessment
- Discuss the concepts of detection, classification, and identification of objects in the assessment zone

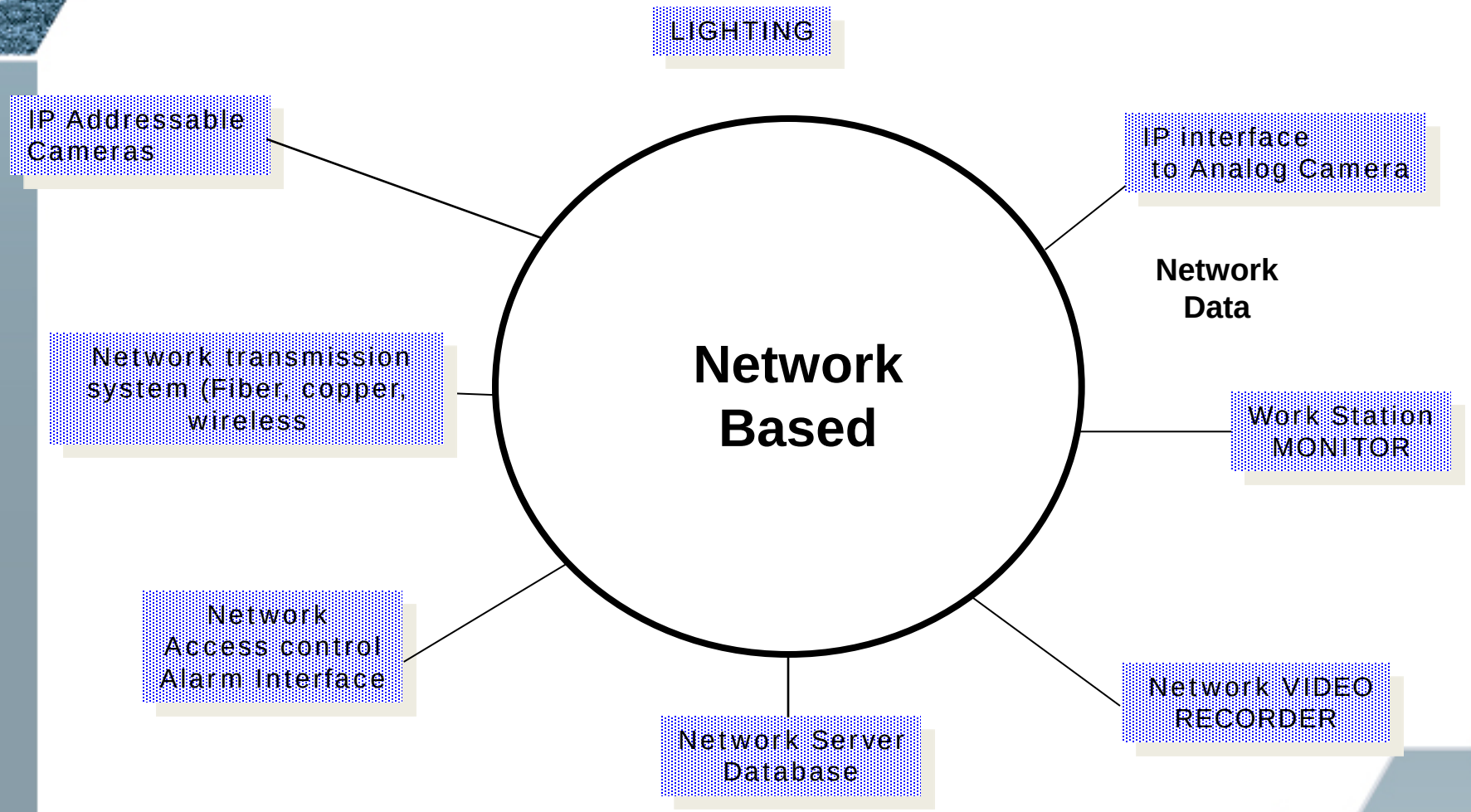
Component Performance Requirements

- Analog Block Diagram
- Digital Block Diagram
- Performance Requirements

Analog Video System Diagram



Digital Video System Diagram



Compare Analog or Digital

Analog

- Camera, mount, and lens
- Lighting system
- Video Transmission
- Video conditioning
- Video switching
- Video recording
- Video monitor
- Video controller

Digital

- Network camera, mount, and lens
- Lighting system
- Network Transmission
- Network conditioning
- Video/Database Software
- Network recorder
- Workstation
- Network Server

Performance Requirements

Assessment System

- Camera and lens
- Lighting system
- Video Transmission/Conditioning
- Video switching
- Video recording
- Video monitor
- Video controller

Video / Thermal Camera

- Function - convert visible or thermal radiance to video waveform
- Solid-state image device (analog / digital)
- Contrast
- Sensitivity
- Resolution
- Filters
- Thermal

Lenses

- Format
  - Size 1/2”, 1/3”,…(12 mm, 8 mm,…)
  - Spherical / Aspherical
- Focal length
  - Relative magnification of an object and field of view
- F-Stop (F-number)
  - Measure of the ability to gather light
- Transmittance (T-number)
  - The amount of light that can pass through the lens

Requirements for Camera

- High sensitivity
- Low light requirements
- High signal to noise ratio
- Automatic gain control (AGC)
- Automatic iris control
- Electronic shutter
- High resolution
- Environment specifications

Requirements for Camera Tower

- Stable in wind
- No sensor interference
- Minimum obscuration

Lighting System

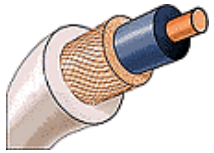
- Function
  - Illuminate scene for nighttime operation
- Major types
  - Incandescent
  - Mercury vapor
  - Sodium vapor (High/Low pressure)
  - Very Near infrared (VNIR)

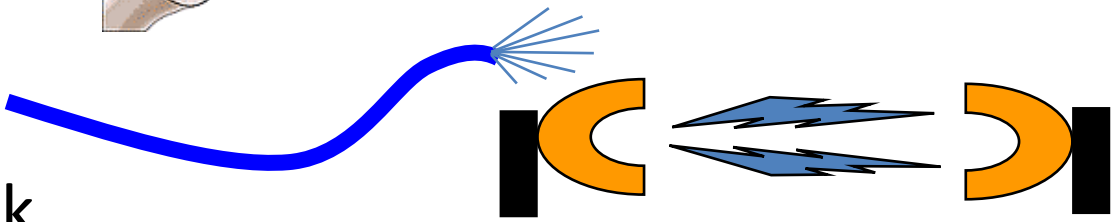
Lighting Requirements

- Minimum intensity
  - 1.0 fc for solid-state or tube camera
- Uniform illumination
  - 6:1 light-to-dark ratio, maximum
  - 4:1 design goal
- Extent of coverage
  - 70% of field of view, minimum
  - 30% ground cover reflectance

Transmission System

- Function
  - Path for video signal from camera to monitor
- Major types
  - Coaxial cable
  - Optical fiber
  - Microwave link
  - UTP (Unshielded Twisted Pair)
  - Network Data System





Video Conditioning System

- Function
  - Reduce video signal degradation from cable transmission system
- Major types
  - Transient protection (Lightning, High Current)
  - Equalization (High Frequency)
  - Clampers (DC restore)
  - Isolation Transformers (Hum)

Video Switching System

- Function
  - To connect cameras to recorders and monitors in a variety of ways
- Major types
  - Manual switching
  - Sequential scanning
  - Alarm activated

Video Recording System

- Function
  - Record video signal for instant replay, or historical information
- Major types
  - Video cassette recorder
  - Digital recorders
  - network recorders
  - networked cameras

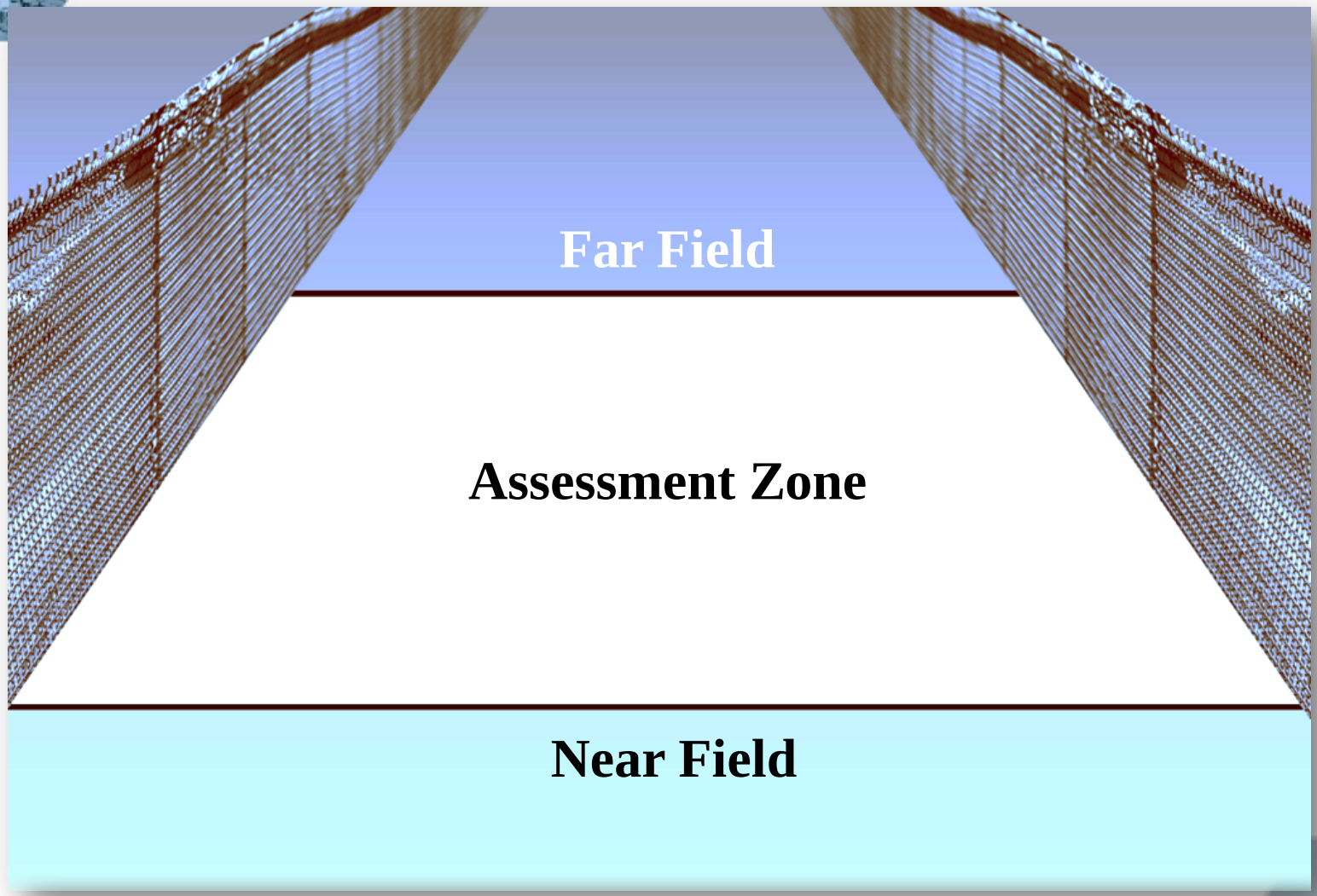
Video Monitor

- Function
  - Convert video signal to visual image
- Major types
  - Black and white
  - Color
    - CRT
    - Flat Screen (LCD, Plasma)

Video Controller

- Function
  - Interface between sensor alarm system and video assessment system
  - Controls display and recording of multiple video signals

Assessment Area Monitor View



Performance Requirements of Video Assessment

- Minimum time between sensor alarm and video display
- Complete area coverage of intrusion detection zone/sensors
- Classify 1 foot (0.3 meter) target at far edge of detection zone
- Field of view at far edge of sensor zone (height / width)
- Continuous operation 24 hours per day, 7 days per week
- Minimal sensitivity to adverse weather conditions

Levels of Resolution

Detection	Classification	Identification
		
Determine Presence of Object	**Determine Class of Object**	**Determine Identity of Object**

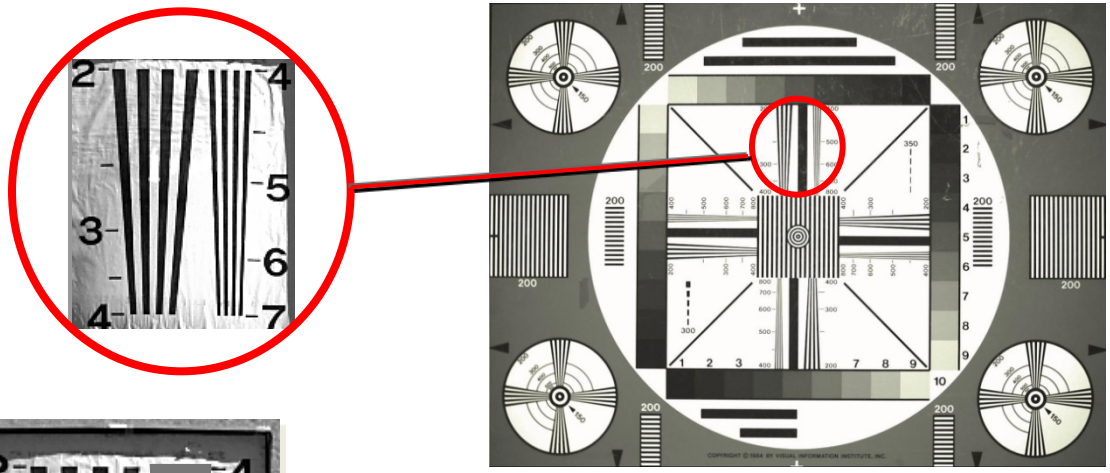
Assessment Resolution - Detection

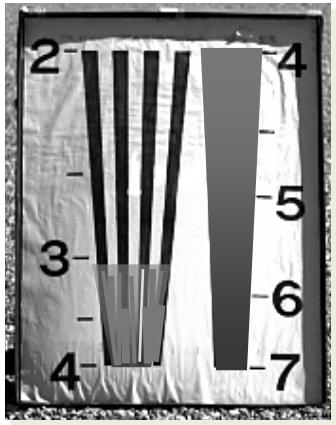
Assessment Resolution - Classification

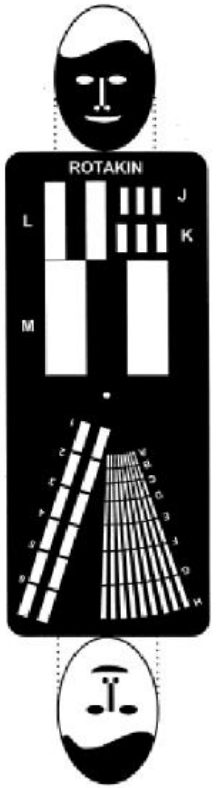
Assessment Resolution - Identification

Camera Resolution Measurements

Camera resolution is commonly measured using a standardized resolution chart







A laboratory chart, field chart, and Rotakin field resolution chart are shown

Resolution limitation is the location where distinct black and white lines are no longer distinguishable

Assessment Resolution (cont)

- Dependent on
  - Camera resolution
  - Lens focal length
  - Size of object
  - Object contrast to background
  - Object stance and motion
- Objective: distinguish (classify) between animal and crawling person with head facing camera
- 8 pixels on a 30 cm target far field viewing width is minimum to classify a human shape
- Easier if a human target is standing
- Test cameras for specific application; don't rely on manufacturers' data

Far Field Resolution

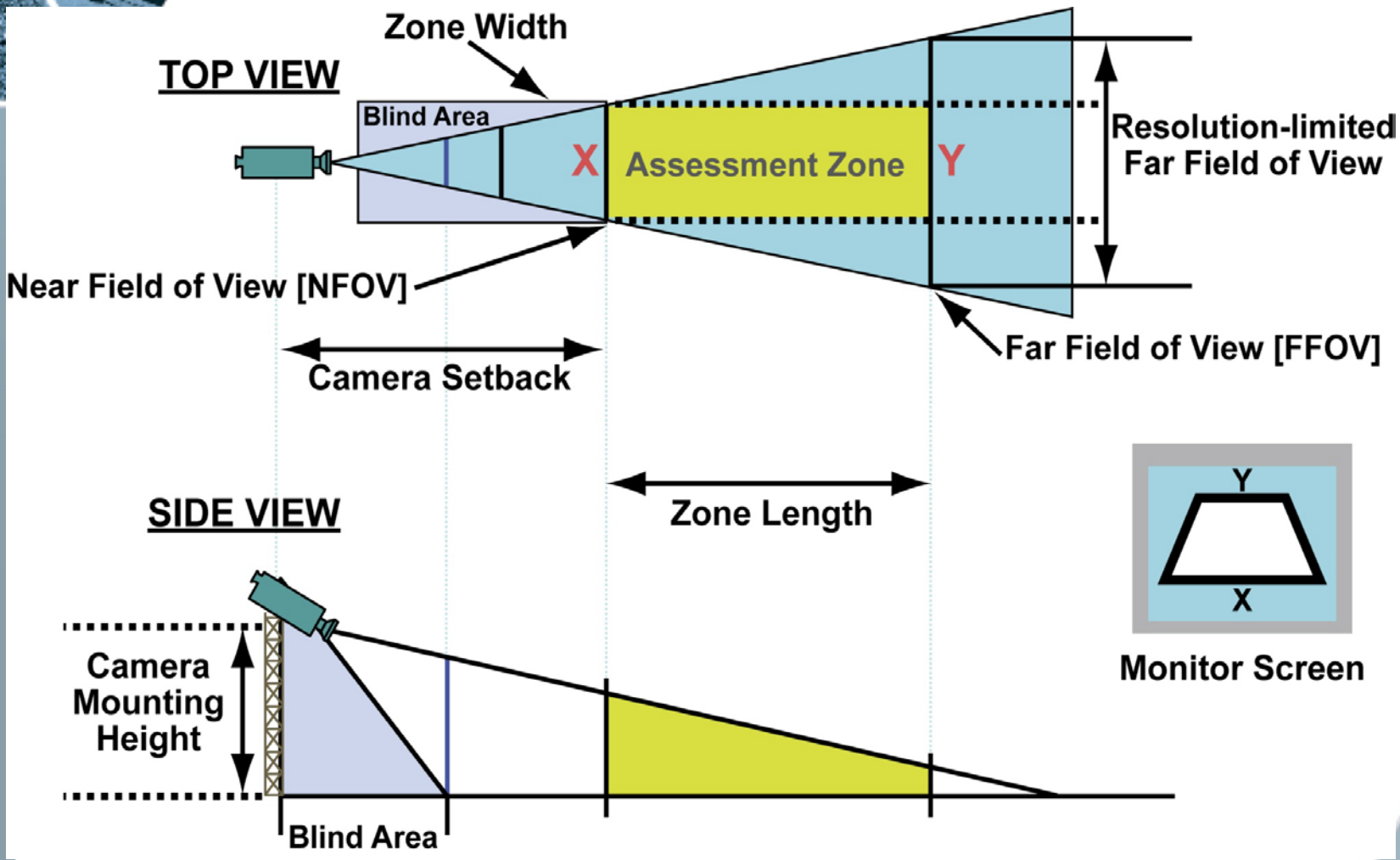
760 x 480 pixel resolution

1376 x 1032 pixel resolution

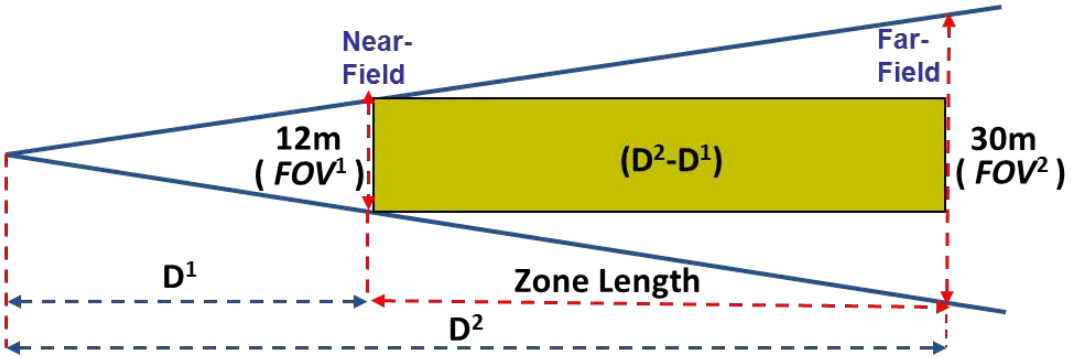
Field of View and Resolution Testing

Using circle, triangle, and square to determine far FOV resolution adequacy

Geometry of Assessment Zone



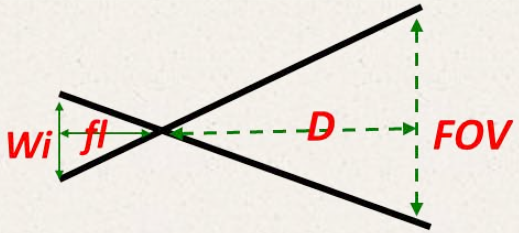
Calculation for Zone Length



Use to calculate HFOV and distance to camera

$$\frac{D}{FOV} = \frac{fl}{Wi}$$

$$D = \frac{FOV \times fl}{Wi}$$



fl - Focal Length of lens

Wi - Width of imager

FOV - Width of camera view at a distance (D)

D - Distance from camera

$$D^1 = \frac{FOV^1 \times fl}{Wi} \qquad D^2 = \frac{FOV^2 \times fl}{Wi}$$

wi = 6.4 for 8mm (1/2 inch) format

wi = 4.8 for 6mm (1/3 inch) format

wi = 3.2 for 4mm (1/4 inch) format

wi = 1.6 for 2mm (1/8 inch) format

Zone Length = $D^2 - D^1$

Resolution at Far Field

30 cm at 8 pixels = no more than **3.75 cm per pixel**

If a camera/monitor provides **800** pixels of horizontal resolution, then maximum field of view width is:

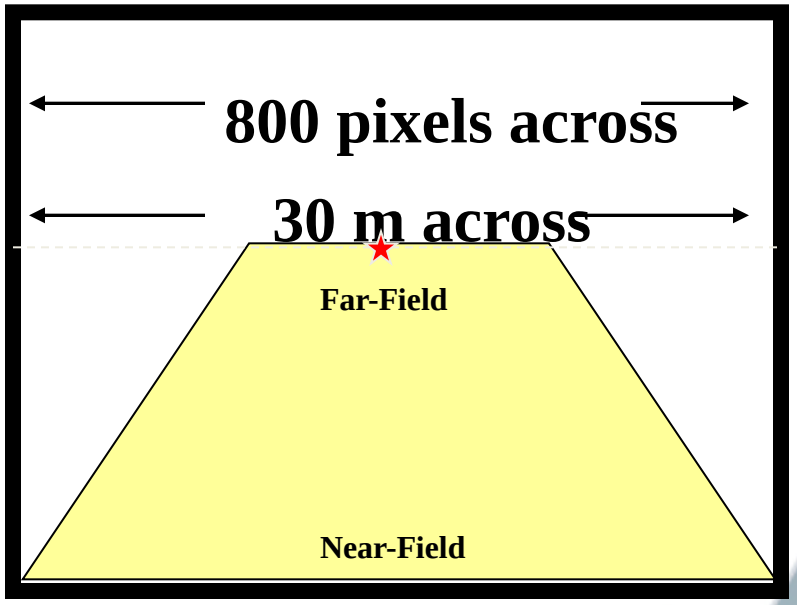
3.75 cm x 800 **pixels** = 3000 cm = **30 m**

Another way to calculate is using ratios:

8 pixels to 30 cm = 800 pixels to X

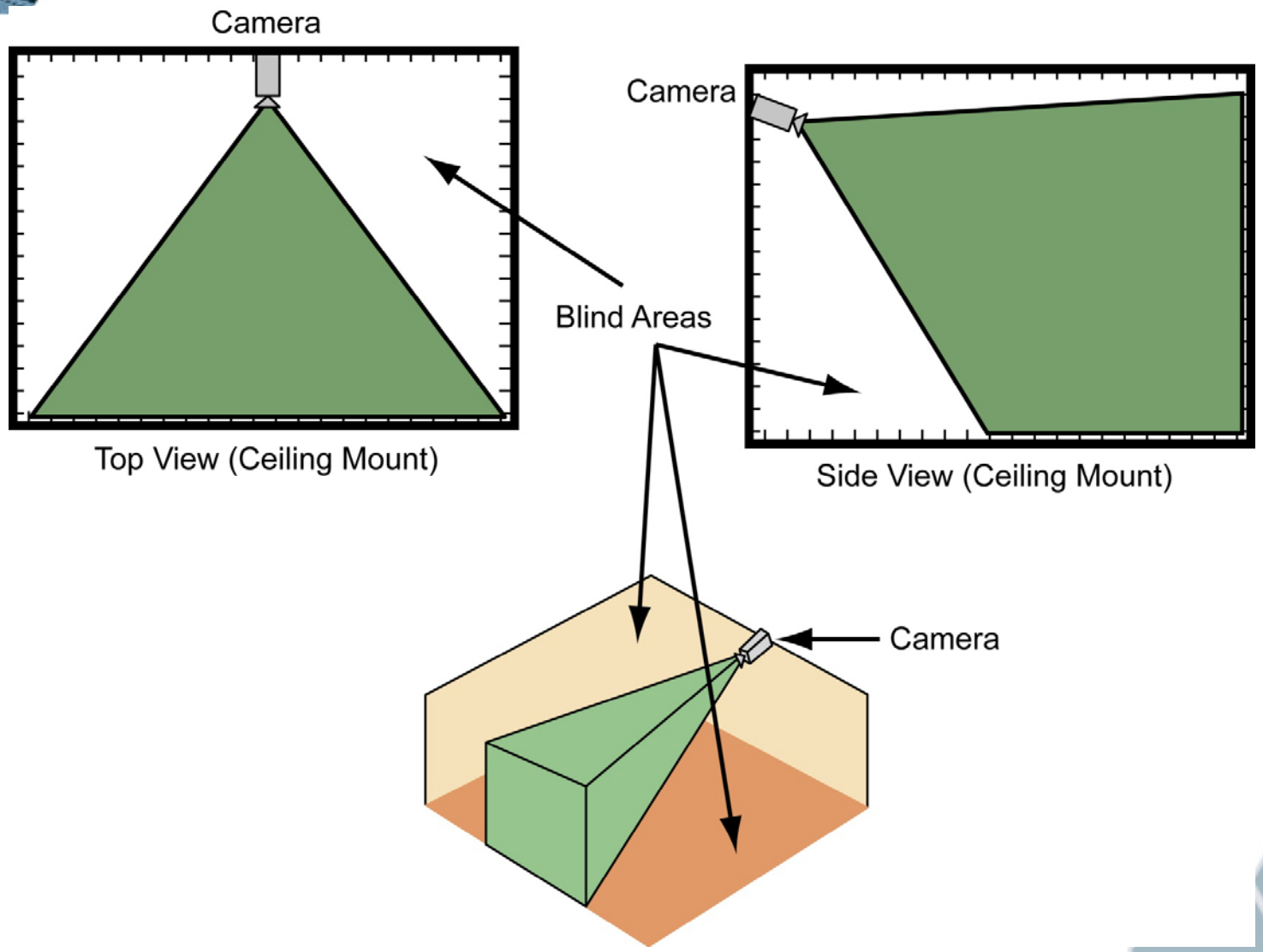
$$\frac{8 \text{ px}}{30 \text{ cm}} = \frac{800 \text{ px}}{X}$$

Solve for X = 30 m



What if the camera imager was **400** pixels?

Geometry for Interior Assessment



Summary

- Components of video system
  - Camera and lens
  - Lighting system
  - Transmission system
  - Video switching equipment
  - Video recorder
  - Video monitor
  - Video controller

Subgroup 9
Alarm Assessment

Session Objectives

After the session, the participants will be able to do the following:

1. Recognize the relationship of using different lenses to the length of sectors.
2. Identify hardware that is necessary for a complete video alarm assessment system.
3. Evaluate the effectiveness of an assessment system.

Exercise 1 - Object Distance

1) Using one of the existing cameras in the test field identify the following characteristics
    a. ___ format imager
    b. ___ lens focal length
    c. ___ width of the test perimeter
2) Calculate the distances for Near Field of View (D_N), Far Field of View (D_F) and Zone Length (D_{ZL}) and write the distance numbers in the chart below. The formula for calculating Field of View Distances is shown in the box below.

D= FOV (*fl*/*wi*)	**Where:** **D** is distance from camera (m) **FOV** is width of field of view (m) at distance D ***fl*** is focal length of lens (mm) ***wi*** is width of imagers sensitive area (mm)

The end of the assessment zone is indicated when the field of view is 30m wide, why would this distance be chosen?

_____

_____

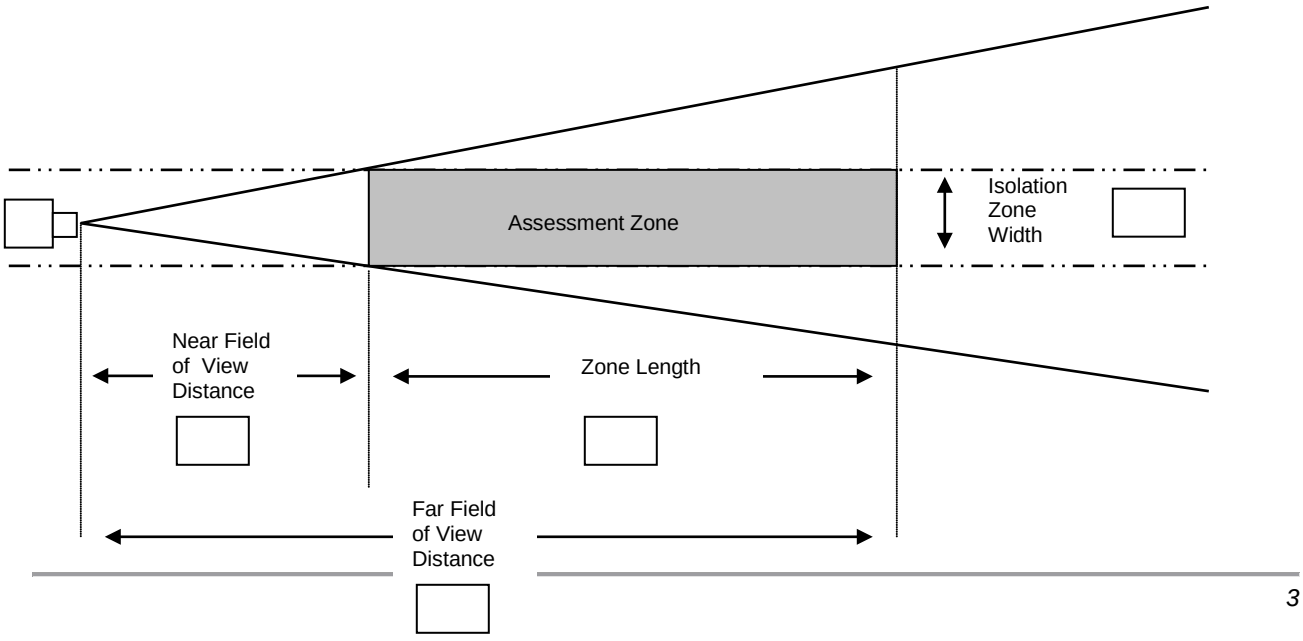
How wide is the camera Field of View at the 8 pixel/30cm resolution limit? _____*m*

3) Complete the following table for the different focal length:

	Lens Focal Length ***(fl)***				
Field of view	4mm	12mm	25mm	35mm	50mm
Near field of view distance D_N, **(**beginning of assessment zone, width of field of view, **FOV**, is 12 meters**)**	D_N =	D_N =	D_N=	D_N =	D_N =
Far field of view distance D_F **(**end of assessment zone, width of field of view, **FOV**, is 30 meters)	D_F=	D_F =	D_F=	D_F =	D_F =
Zone length $D_{ZL} = D_F - D_N$	D_{ZL}=	D_{ZL} =	D_{ZL} =	D_{ZL} =	D_{ZL} =

4) From the calculations in the above table, Insert the dimensions in the boxes in the diagram below for a 35mm lens showing the beginning of the assessment zone, the end of the assessment zone, and the zone length. Write the appropriate number in the boxes shown below for:

- Isolation Zone Width,
- Near Field of View Distance ,
- Far Field of View Distance and
- Zone Length



Exercise 3 - Video Alarm Assessment System

1) Identify the hardware that is necessary for a digital video alarm assessment system

_____

_____

_____

_____

_____

2) How will snow, rain, fog, and other environmental factors impact performance of this proposed system?

_____

_____

3) How will the proposed Video technology perform compared to simply using human response force personnel to assess alarms?

_____

_____

4) Exercise 4 - Lighting Equipment

List the requirements for a perimeter lighting system

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

Alarm Communication and Display Integration with Alarms, Sensors, and Access Control Systems

Learning Objectives

After completing this module, you should be able to:

- Explain the integration of alarm, communication, and display with sensors, video assessment and access control systems
- Evaluate possible human interface problems for alarm assessment in stand-alone, loosely integrated and tightly integrated systems

Role of Alarm Communication and Display

An alarm communication and display (AC&D) system transmits alarms signals from electronic devices and systems to a monitoring station and displays the information to an operator for action.

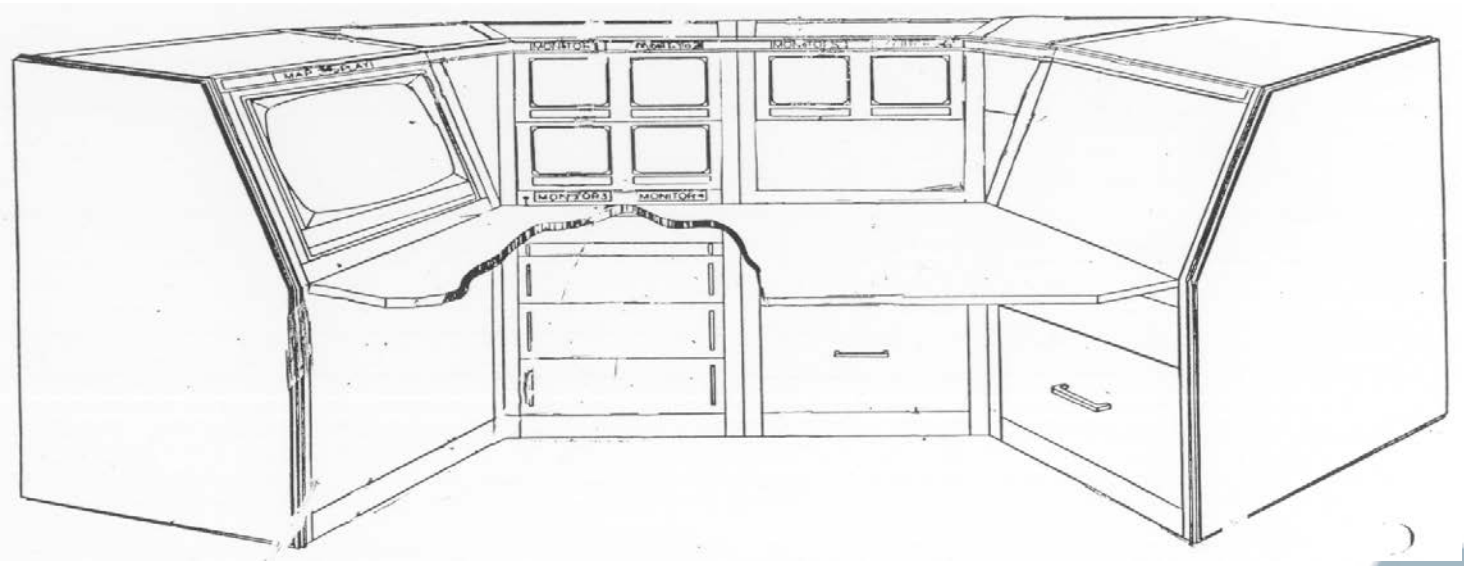
Role of Alarm Communication and Display, continued

- Collect and Display Data from the PPS
  - Alarm System (Intrusion Detection)
  - Entry Control (Access Control)
  - Assessment (Video assessment and Surveillance)
- Provide the human/machine interface
  - Proved overall status of site security system
  - Provide mechanism for operator input
- Support communication with others
  - Guards and response forces
  - Emergency personnel
  - System Administrator and Maintenance personnel
  - Site Personnel

Operator effectiveness ?

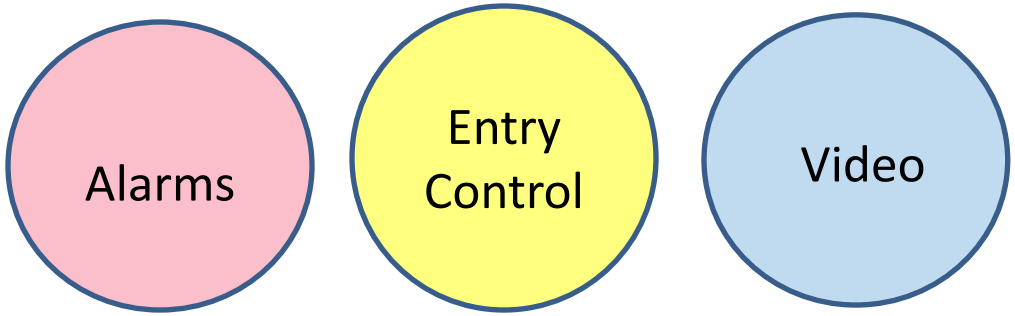
Assessment Display Dependence

- All functions of assessment must be integrated with an alarm communication subsystem.
- These functions must be presented to the operator in a coordinated human engineered fashion.

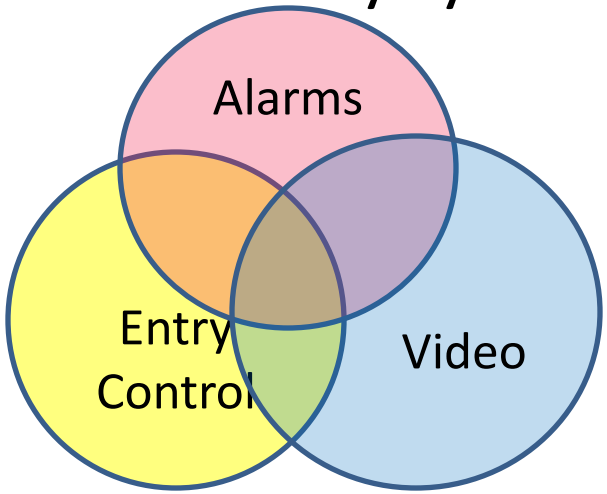


Alarm Display – Data Processing, continued

- Types of AC&D Systems
  - Independent Systems – many systems, many displays

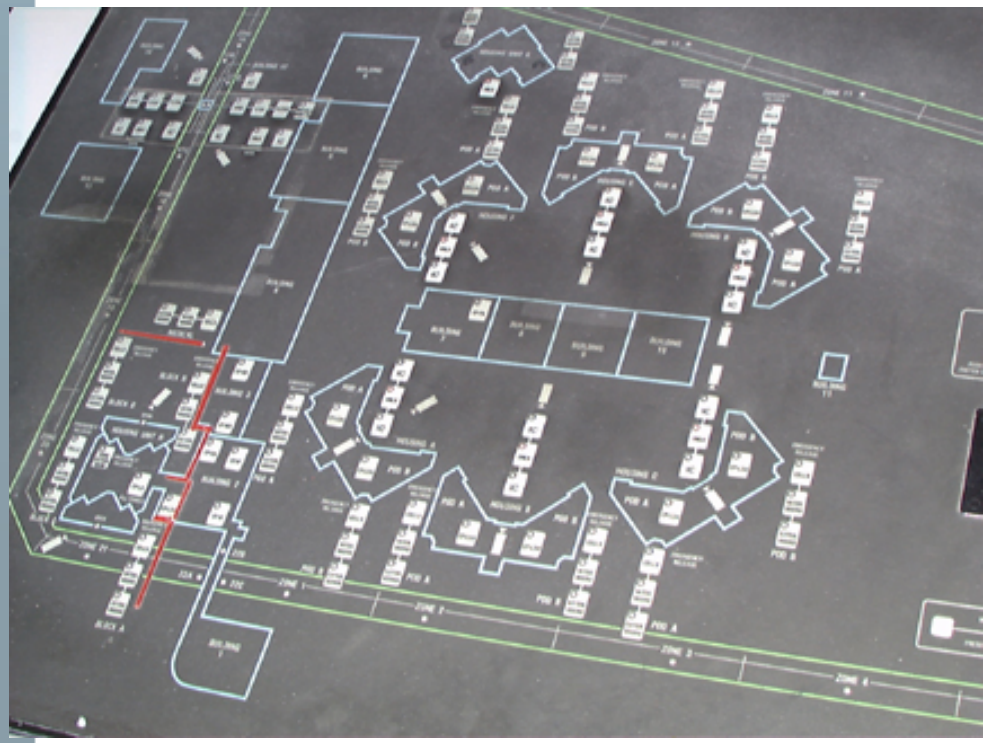


  - Integrated System – many systems, one display



Stand - Alone

Integration – Video?



Independent – Advantages and Disadvantages

- Advantages
  - More information from more sophisticated systems
- Disadvantages
  - Difficult to learn and operate
  - Each system has to be setup separately
  - Integration by operator(s)

Independent Advantages and Disadvantages *(cont'd)*

Graphics screen showing alarmed sector's relative location on perimeter map

Text screen showing alarmed sector's sensors description

Independent DVR control used to present live and alarm assessment video

Loosely Integrated

Setup is performed on each systems interface

Console Functions

Graphics screen showing alarmed sector's relative location on perimeter map

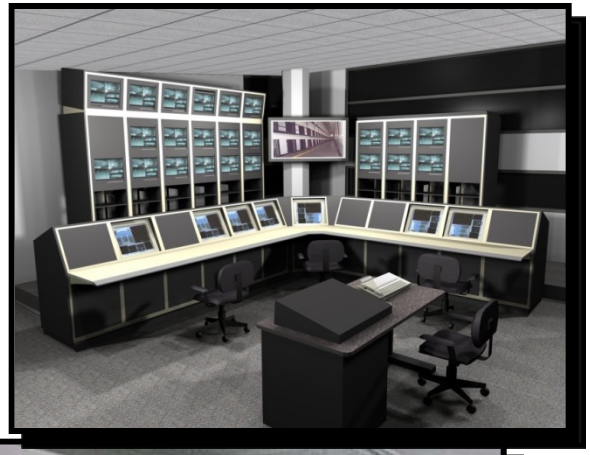
Text screen showing alarmed sector's sensors description

Video Monitors indicating live and recorded images of alarmed sector

Phone, intercom, and radio communications

Tightly Integrated

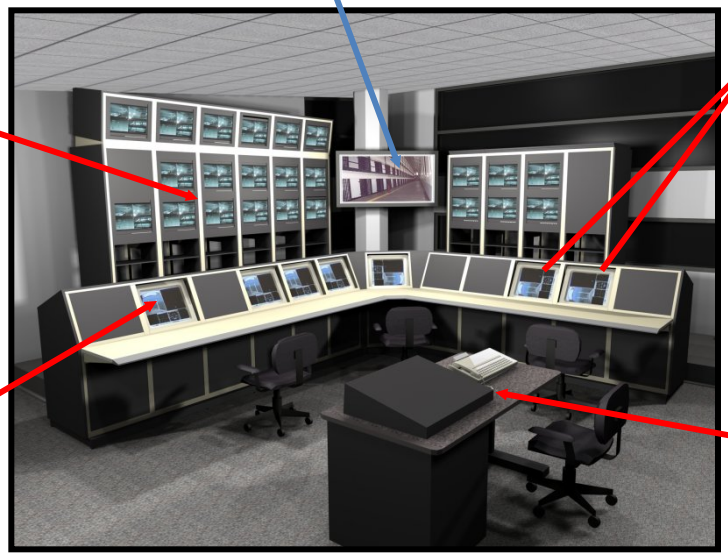
- Advantages
  - Easiest to operate
  - Distributed information per station capabilities
  - Setup of all devices through one setup process
- Disadvantages
  - Most difficult to design



Tightly Integrated

Large screen display controlled by supervisors station or task orientated workstations

Video monitors indicating live and recorded images of alarmed sector



Task orientated workstations to divide the alarm events by area

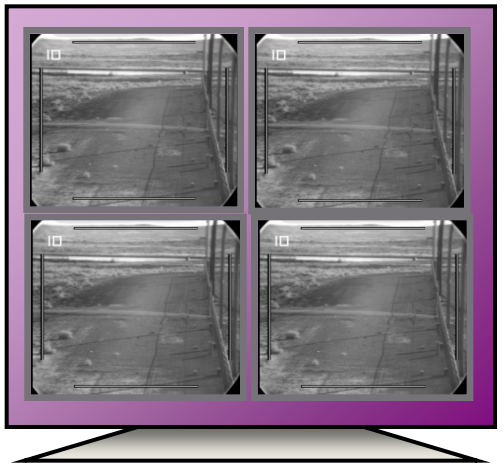
Text screen showing alarmed sector's sensors description

Supervisors stations to observe or assist with high priority tasks

Monitor Information

Graphics or Text

Full Video
Which event?

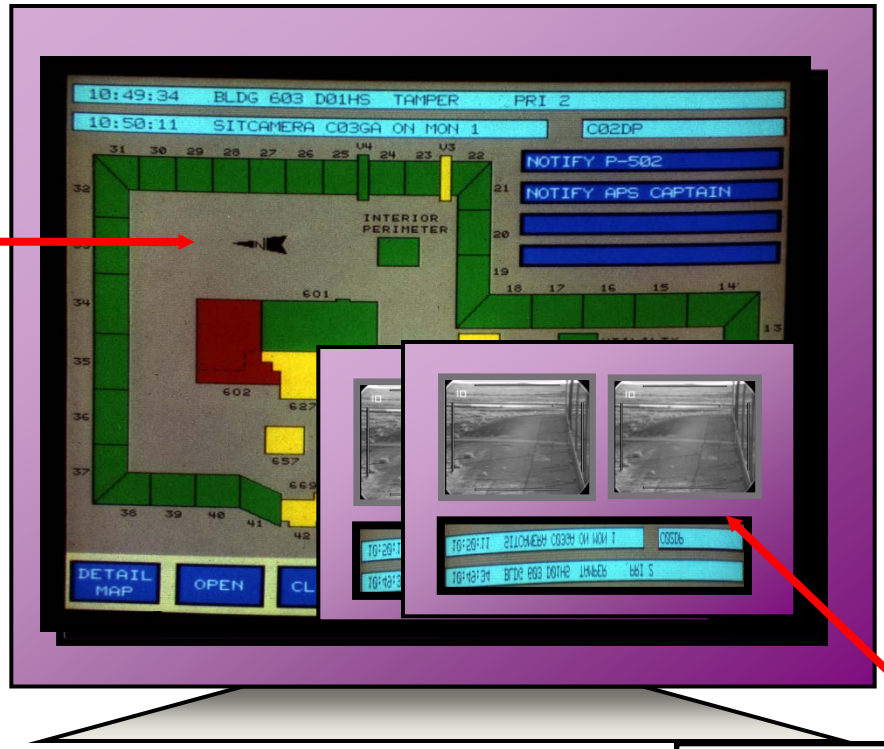


Multiple Video Events
Live? Recorded?

Although integrated the operator still has issues

Integrated Digital Monitor

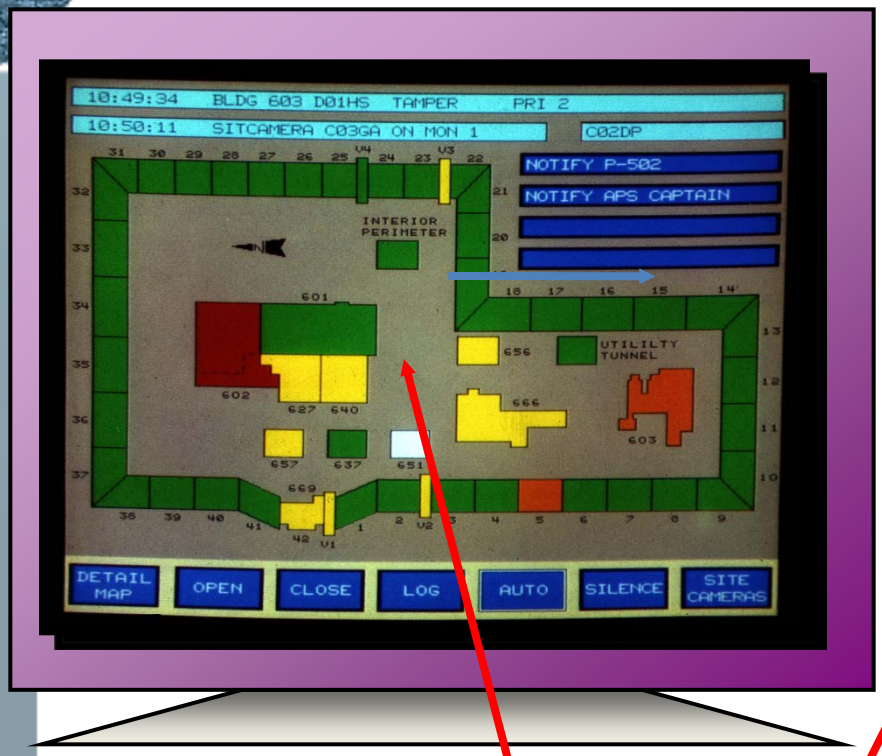
Overall situation graphics or streaming text

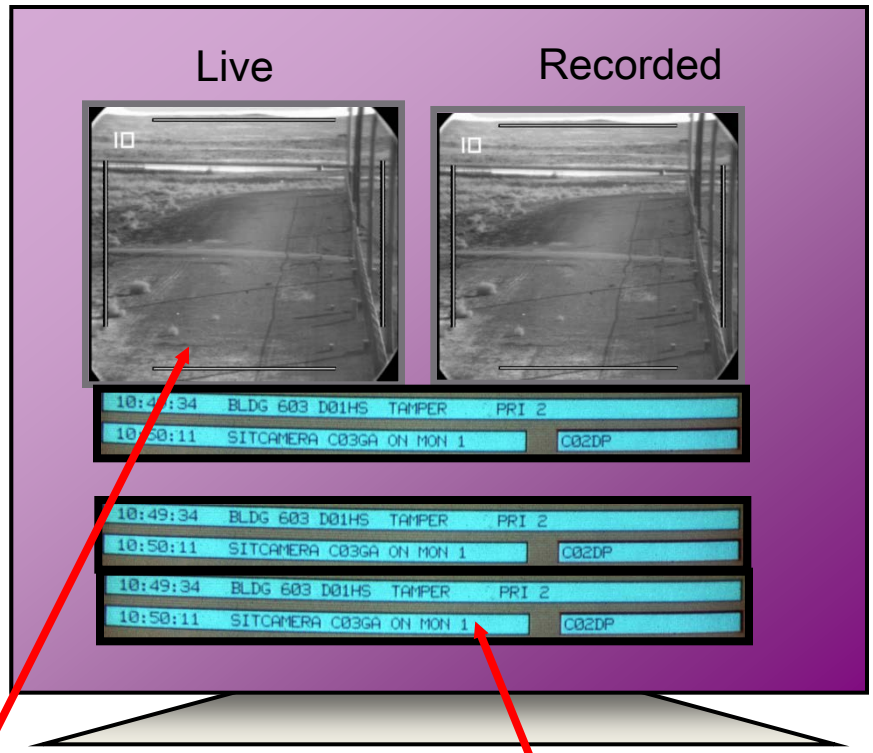


Still problems with multiple event priorities

Multiple Event windows Live, recorded, alarm text

Integrated Dual Monitors





Situation Map(s) or Streaming Text

Text alarmed event coupled to live and recorded video

Prioritized list of next events, clicking on switches to upper area

What Information is Displayed

- Overall system status
- Site layout, zone status (secure, access, alarm)
- Site maps / Building layouts
- Alarm System
  - Location of the alarm
  - Time of the alarm
- Video
  - Live video
  - Assessment video
  - Surveillance video
- Entry Control
  - Events
  - Logs

Control Center Design Criteria

- Topology – Command center
  - Centralized, manned center
  - Distributed, manned centers
  - Redundant control, centers
    - Activation by “Unanswered Alarm Condition”
  - Periodically manned, center

Open Systems Architecture

- Operating system
- Database
- Network
- Browser interface
- Application interface
- Device interface

Integration Evaluation

- What does the operator see or do?
  - Intrusions alarms
    - Detect, classify, or identify
  - Access control violations, visitor control
  - Other - fire, environment, chemical, bio-hazard
- How fast does the system display alarm and video information?
- How does the operator communicate with the system? patrols? response teams?

Summary

- Evaluation of the operations center includes understanding of how system components are:
  - Setup, operated, maintained
  - Operator information flow
    - What the operator has to observe
    - How many actions the operator has to perform
      - Single events, multiple events, routine tasks
  - Performance of human with the technology

Introduction to Entry Control

Learning Objectives

After completing this module, you should be able to:

- Discuss the general concepts of entry control systems, including:
  - Principles of identity verification
  - Methods of controlling access
  - Integration of entry control with other aspects of security systems

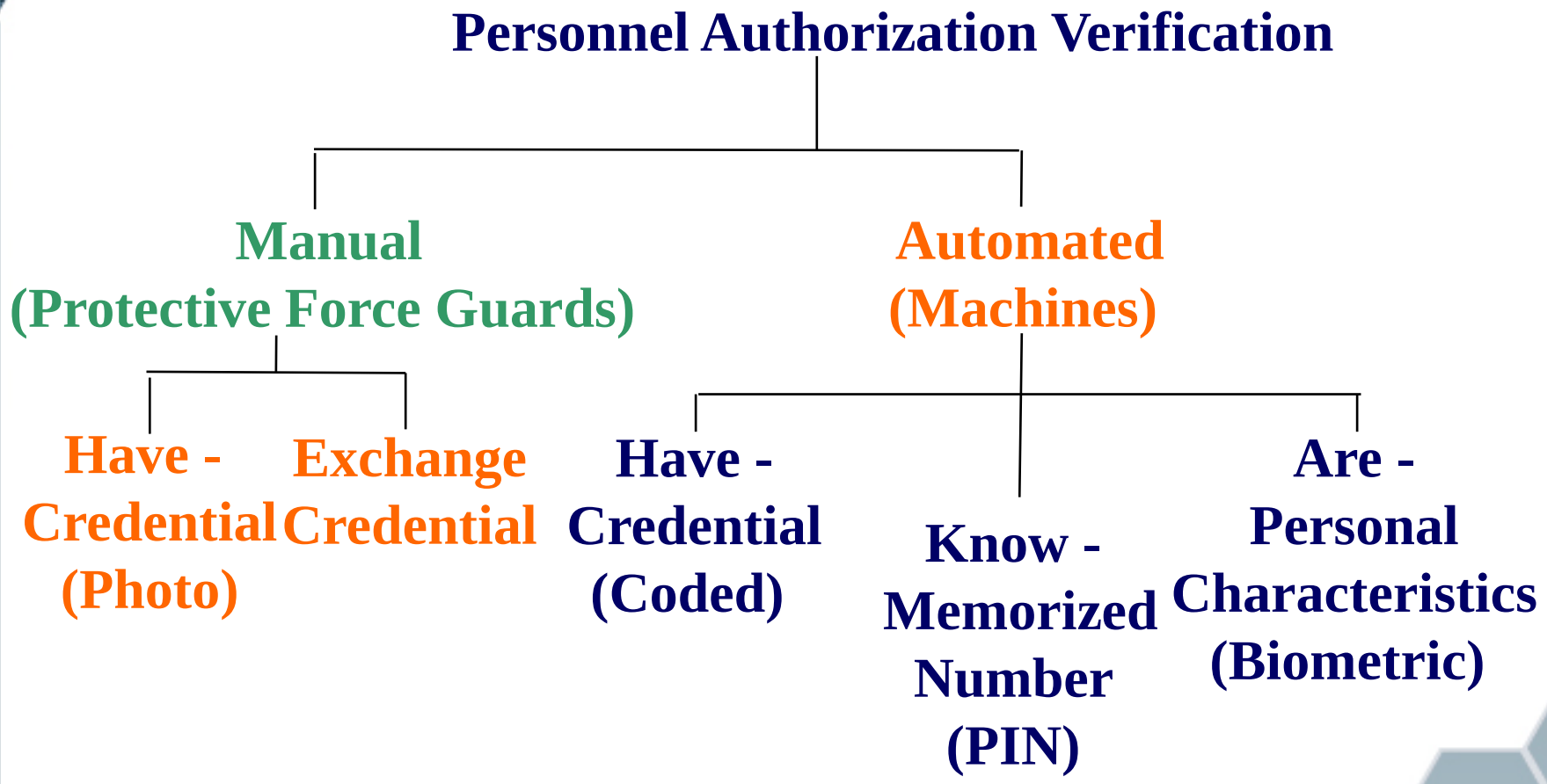
Purpose

- The purpose of a physical security system is to provide a boundary around an area to prevent or detect unauthorized penetrations
- The purpose of entry control is to complete that boundary in a way that securely allows authorized persons and materials to move in and out through that boundary

Objectives of Entry Control System

- To permit only authorized persons to enter and exit
- To detect and prevent the entry or exit of contraband material
- To provide information to security personnel to facilitate assessment and response

Types of Personnel Entry Control

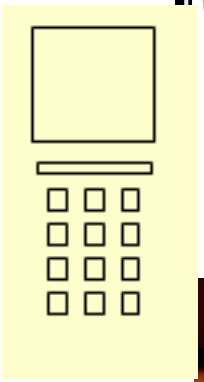


Identity Verification

- Identity verification is achieved using one or a combination of two or more of the fundamental criteria of identity verification
- The three criteria of identity verification are:
  1. Something known
  2. Something in the possession of the person requiring access
  3. Something inherent about the person requiring access

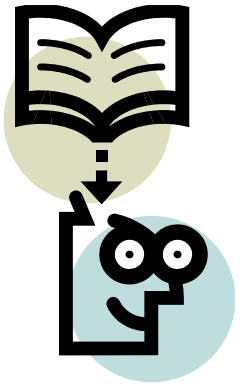
Identity Verification: Something You Know

- Something known that is shared between the authority and the person requiring access takes the form of passwords, PINs, etc.
  - Unique personal knowledge unique to the individual
- PINs are easiest to enter into electronic security systems
- Combinations are another method of interacting with both mechanical and electronic security systems



The Use of PINs and Passwords

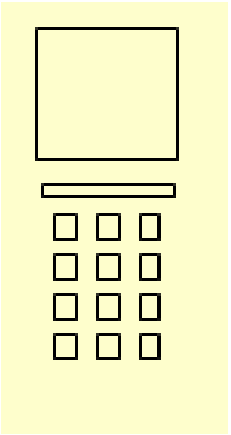
- Passwords and Personal Identification Numbers (PINs) are information shared between an authorized individual and the controlling authority
- Passwords and PINs are used in Entry Control systems as part of the identity verification process
- Passwords and PINs fall into the category of the “Something known” criterion of identity verification



Passwords

- Typically, the use of passwords is restricted to computer access
- Since passwords are alphanumeric a full “QWERTY” keyboard is required
- In many respects, a password is the general case while a PIN is a special case (numeric only) of passwords
- Passwords and PINs have the same requirements for security purposes

PINs



- PINs are used mainly at locations where it is unreasonable to provide a full keyboard
  - Automated Teller Machines (ATMs) are a good example of the use of PINs
- PINs only require a numeric keypad for entry
- PINs as the only criterion for identification is not very secure
- Visual screens or other means for preventing PIN capture by adversaries is recommended
- PINs are best used in conjunction with other criteria (something possessed or something about you)

Passwords and PINs Selection

- Passwords and PINs can be either
  - generated and assigned to the individual by the authority or
  - user selected
- If “user selected,” there is no guarantee of uniqueness
- Without uniqueness, the system cannot know who is requesting entrance (for systems that only use Passwords or PINs as the only criterion)

User Selection

- User selection often leads the user to choose one that is easy to remember, which means that it may be easy to guess or discover by an adversary
- Easy-to-remember information is often information related to the individual, e.g.,:
  - Birthdays
  - Names of family members or pets
  - Used for multiple applications (ATM PIN, email account password)

PIN and Password Length

- PINS with longer lengths are more difficult to guess but may be difficult to remember
- PINs with short lengths do not have enough combinations for larger enrollment populations
  - For example: For a company of 1000 employees, a 3-digit PIN is insufficient
    - If each PIN is unique, ALL combinations will be used; any guessed PIN will be one that is enrolled
    - Even if not all PINs are unique, the probability of correctly guessing an enrolled PIN is high

Password and PIN Length *(cont'd)*

- Passwords can use the entire alphabet and can be case sensitive as well as using numbers
- This means that shorter length passwords can have very many more possible combinations than an equivalent length PIN

59634

st6Qn8d

PIN as the Only Criteria for Identification

- Systems that use PINs as the sole means of identification are not recommended for high security applications
- For systems that use only PINs for identification it is good practice to detect and report repeated attempts to enter PINs that are not in the enrolled database
- For all systems, the number of possible combinations should greatly outnumber the number of people in the database (a factor of ten at least)

Lock Combinations

- A combination that opens a lock is another example of “something known” as a means of gaining entrance or access
- For most combination locks only one combination is set for that lock
- Since only one combination is possible for most locks the combination has to be shared between all who need access
- Once the combination is compromised the combination has to be changed and distributed to all who still need access

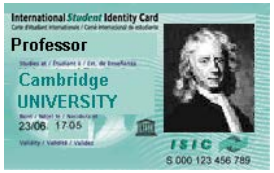
Summary

- Passwords and PINs are “something known” criteria
- The length relates to security
- Passwords and PINs can be quickly deactivated when compromised
- Passwords and PINs used in an electronic system can
  - Allow access or entry based on time of day/day of week
  - Keep a log on all transactions
- Best used in conjunction with other criteria (“something possessed” and/or “something about the individual”)

TOKENS AND CREDENTIALS

Identity Verification: Something You Have

- Something possessed by the individual, such as keys, tokens, and/or credentials
- Credentials can be checked manually or coded credentials can be used to enter information into electronic security systems
- Coded credential types include:
  - Picture
  - Magnetic stripe
  - Proximity
  - Smart card



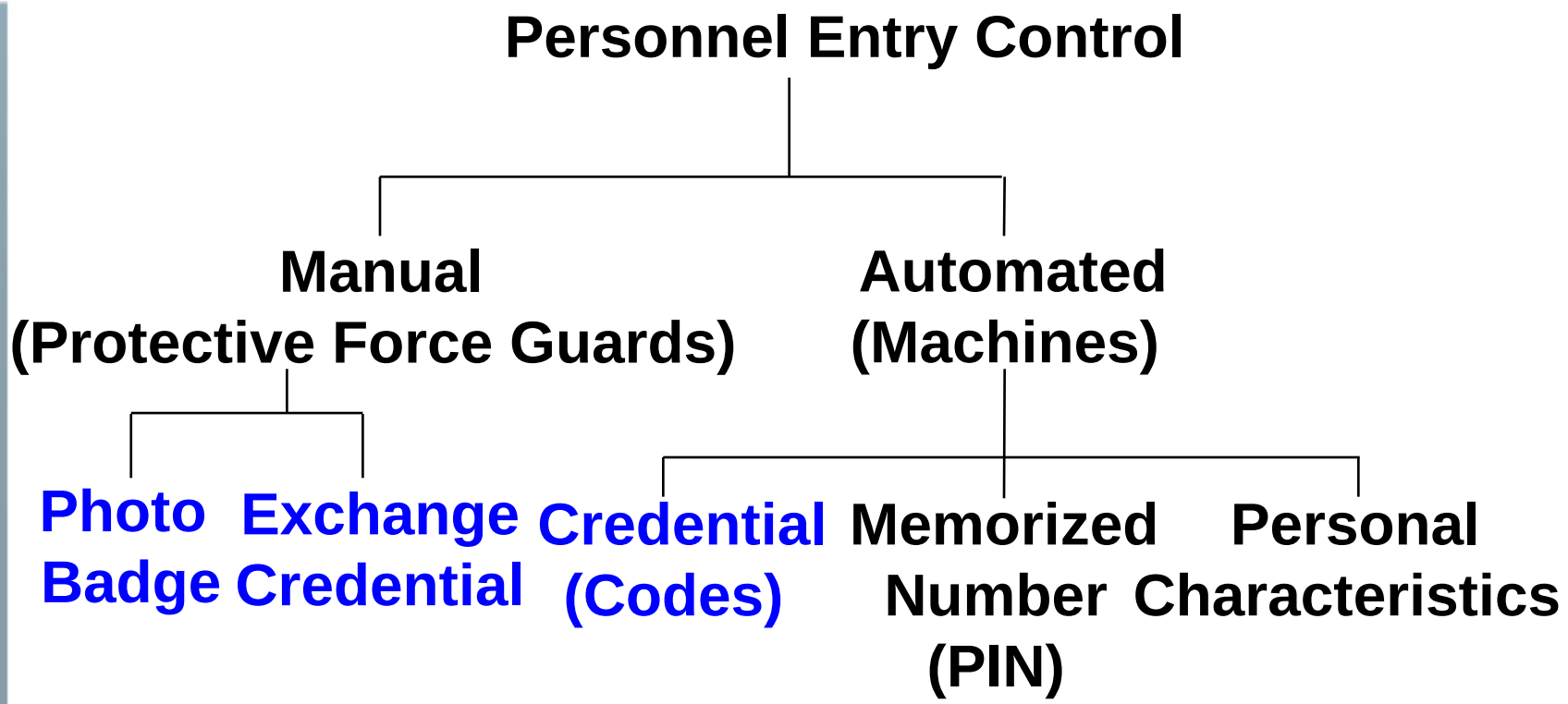
Tokens and Credentials Defined

- A token is something given or shown as a symbol or guarantee of authority or right
  - Example: crown or uniform
- Credentials are something that provides confidence or shows that a person is entitled to exercise official power
  - Example: driver's license or employee badge
- Coded credentials can be identified uniquely and therefore can distinguish between users
  - Example: magnetic stripe or smart card

Basis of Entry Control

- Something you possess
  - Key
  - Card
- Something you know
  - PIN
  - Password
- Something about you
  - Biometric feature

Techniques of Personnel Entry Control

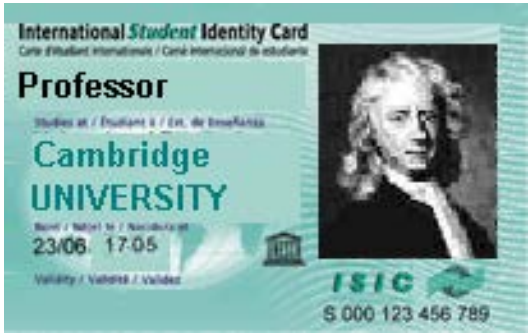


Types of Credentials

- Photo identification badge
- Exchange badge
- Stored-image badge
- Coded credential
  - Magnetic stripe
  - Bar code
  - Wiegand wire
  - Proximity badge
  - Smart card
  - Optical badge

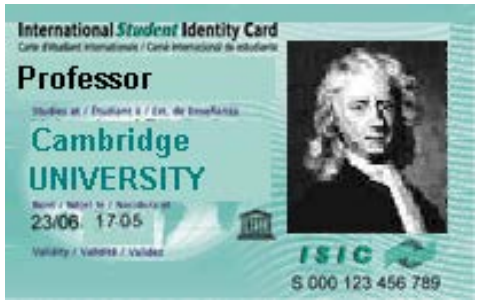
Picture ID Badge

- Only suitable for low security applications
- Cannot be used by automated entry control systems
- Human examines badge for cues to verify authenticity
- Human compares picture to possessor

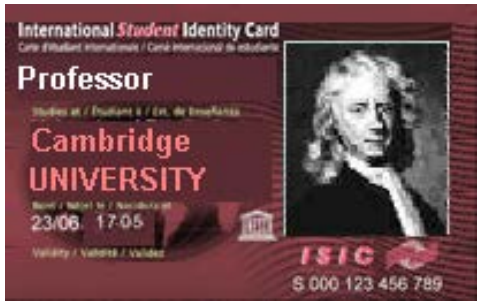


Exchange Badge System

- The exchange badge system relies on multiple credentials
- One credential is take-home while the other stays within a secured area
- These credentials must look different



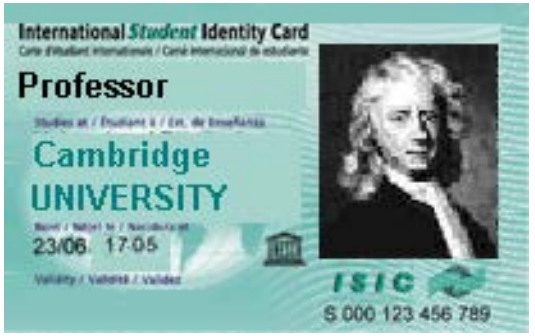
Take-Home



Exchange

Stored Image

- Similar to an exchange badge; however, this approach relies on a computer-stored image
  - Protected database
- Requires a visual verification
- Two important features
  - Enrollment capacity
  - Access time
- Difficult to tamper with the stored image



Coded Credential Capabilities

- Maintenance of entry authorization records
- Provision of unique identification code numbers
- Termination of entry authorization without recovering the actual badge
- Provision for several levels of entry authorization

Magnetic Stripe Characteristics

- Density: 300 to 4,000 Oerstead, three tracks
- Size and Placement: per ANSI X4.16 - 1983
- Durability
- Electronic Data
  - Track 1 - alphanumeric
  - Track 2 - numeric only
  - Track 3 - alphanumeric

Bar Code Characteristics

- Image of varying width lines (bars) and spaces
- Linear barcode or one-dimensional (1-D)
- Two-dimensional (2-D) barcode
- Creation and use
- Ease of copying and ways to mitigate

1-D Bar Code

2-D Bar Code

Wiegand Wire Characteristics

- Card has strip of embedded magnetic wires
- Reader - swipe similar to magnetic stripe
- Output format is an industry standard

Proximity Badge Characteristics

- Potentially minimize operational impact
  - Hands-free operation
  - Transparent to user
- Induction powered (passive)
  - Coded RF transmitter
  - Very common in today's market

Smart Card Characteristics

- Based on ISO 7816 Standards
- Uses embedded microcomputer with CPU, ROM, RAM
- Polyvinyl chloride card
- Contact / Contactless
- Main advantages
  - Large memory
  - High degree of resistance to forgery or compromise
- Disadvantage – high cost

Optical Badge Characteristics

- Write Once / Read Many
- Up to 2.8 MB of storage
- Multilayer polycarbonate
- Conforms to ISO / IEC standards
  - Size
  - Durability

Photo by LaserCard

Personnel Credentials

- **Coded Credentials**
  - Bar Code
  - Magnetic Stripe
  - Weigand
  - Proximity
  - “Smart”

Advantages	Disadvantages
• Control access by area and time	• Identifies badge, not person
• Logs each access (or exit)	• Require maintenance
• Have low false rejection rate	• May be defeated by counterfeit badge
• Perform consistently	

Badge - Physical Standards

- Dimensions: (2.123, 2.127) x (3.375, 4.250) inches
- Monolithic construction
- Material compatibility
- Durability
  - Resistant to abrasion, color fading, wear, cracking and delaminating
- Card standards are covered by both ANSI and ISO standards

Elements to Consider

- Ease of Integration
  - A factor of how many different systems support a specific technology
- Performance
  - Expressed as error rates associated with the specific technology and expected life
- Cost
  - Acquisition cost, integration cost, and life cycle maintenance cost
- Availability
  - Composed of order to delivery time, manufacturer viability, and technology maturity

Elements to Consider *(cont'd)*

- Usability
  - A rate of user acceptance and flexibility of use
- Throughput
  - Expressed as time required to read and validate encoded data
- Security
  - In terms of counterfeit and tamper resistance
- Reliability
  - Expressed in terms of resistance to loss of data

Tokens and Credentials Summary

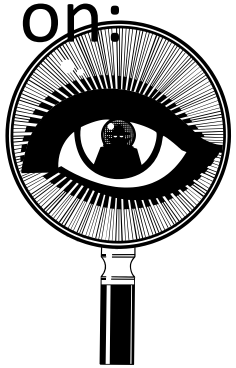
- Manual Entry Control
- Automated Entry Control
- Technologies Available
- Choosing a Technology

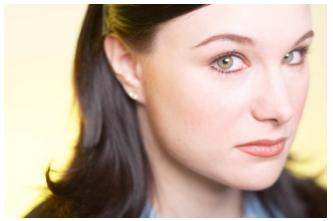
BREAK FOR LUNCH

BIOMETRIC IDENTIFICATION

Identity Verification: Something You Are

- Identity verification devices based on measurements of physical or behavioral features of individuals are called biometrics and can be based on:
  - Eye features
  - Hand and finger features
  - Voice
  - Face
  - Other



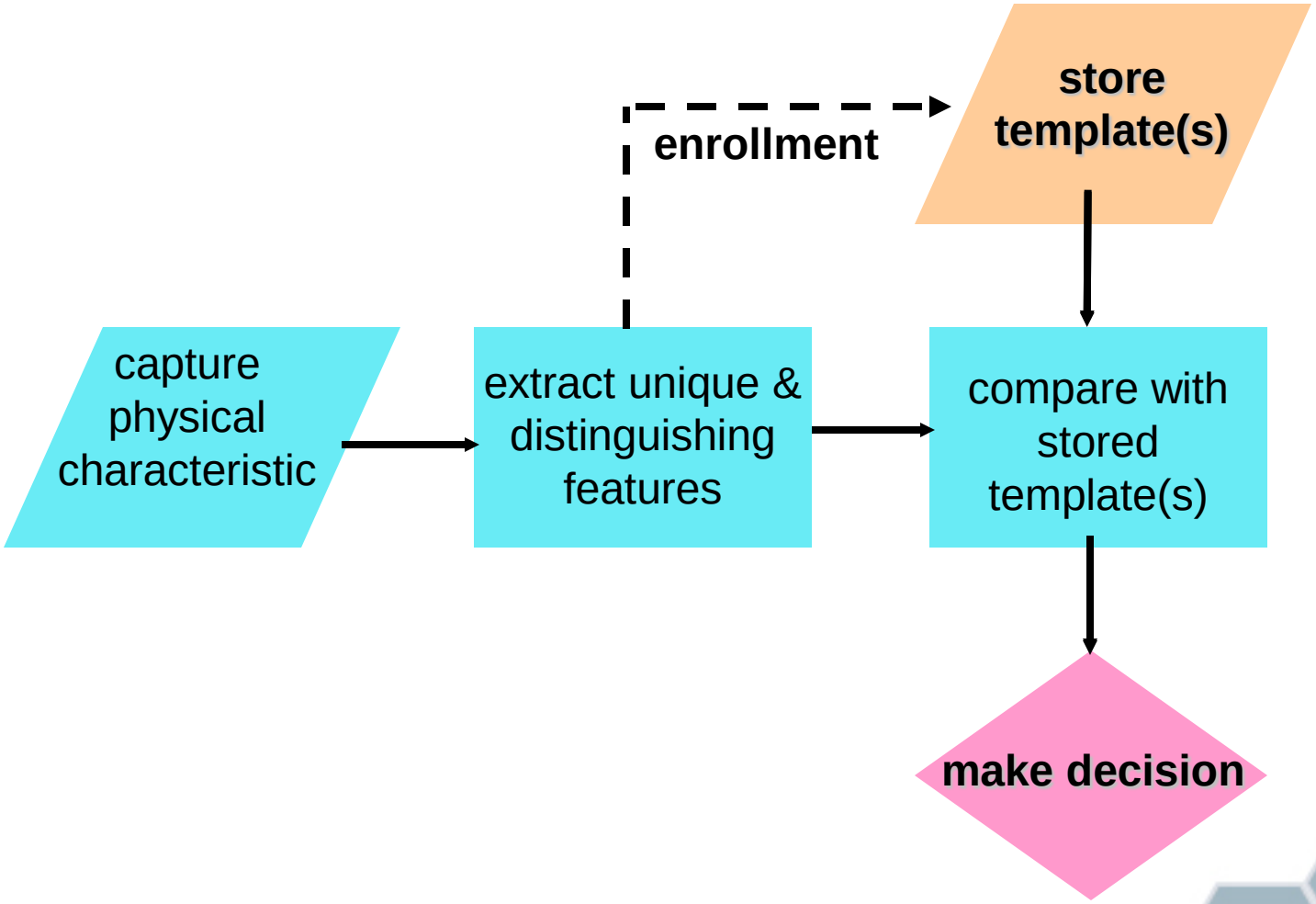


Definition

What is “Biometrics Identification”?

Biometrics Identification is the electronic verification of a person’s identity based on the measurement of some unique characteristic of that person

Generic Biometric System Processes



Elements of Identification

The elements or basis of identification:

- Something you *know* (PIN or password)
- Something you *possess* (badge, card, or token)
- Something you *are*
  - Physical biometrics - your fingerprint, eye feature, hand features, voice, face, etc.
  - Behavioral biometrics - how you walk, type, speak, sign your name, etc.

Verification

- Most biometric systems *verify* identity
  - An individual claims to be someone by presenting a card or PIN
  - The system compares the recorded template for the claimed identity with the live biometric
    - *One-to-one*
  - Also known as “verification mode”

Recognition

- Some biometric systems *recognize* who you are
  - The individual does not initiate the claim
  - The system searches through its entire database to find a match
    - *One-to-many*
- Also known as the “recognition mode”

Biometric Technology Areas

Physiological

- Fingerprint
- Hand Geometry
- Eye
- Iris
- Face
- Ear Shape
- Odor

Behavioral

- Voice
- Signature
- Keystroke (typing patterns)
- Gait (walking patterns)
- Lip movement

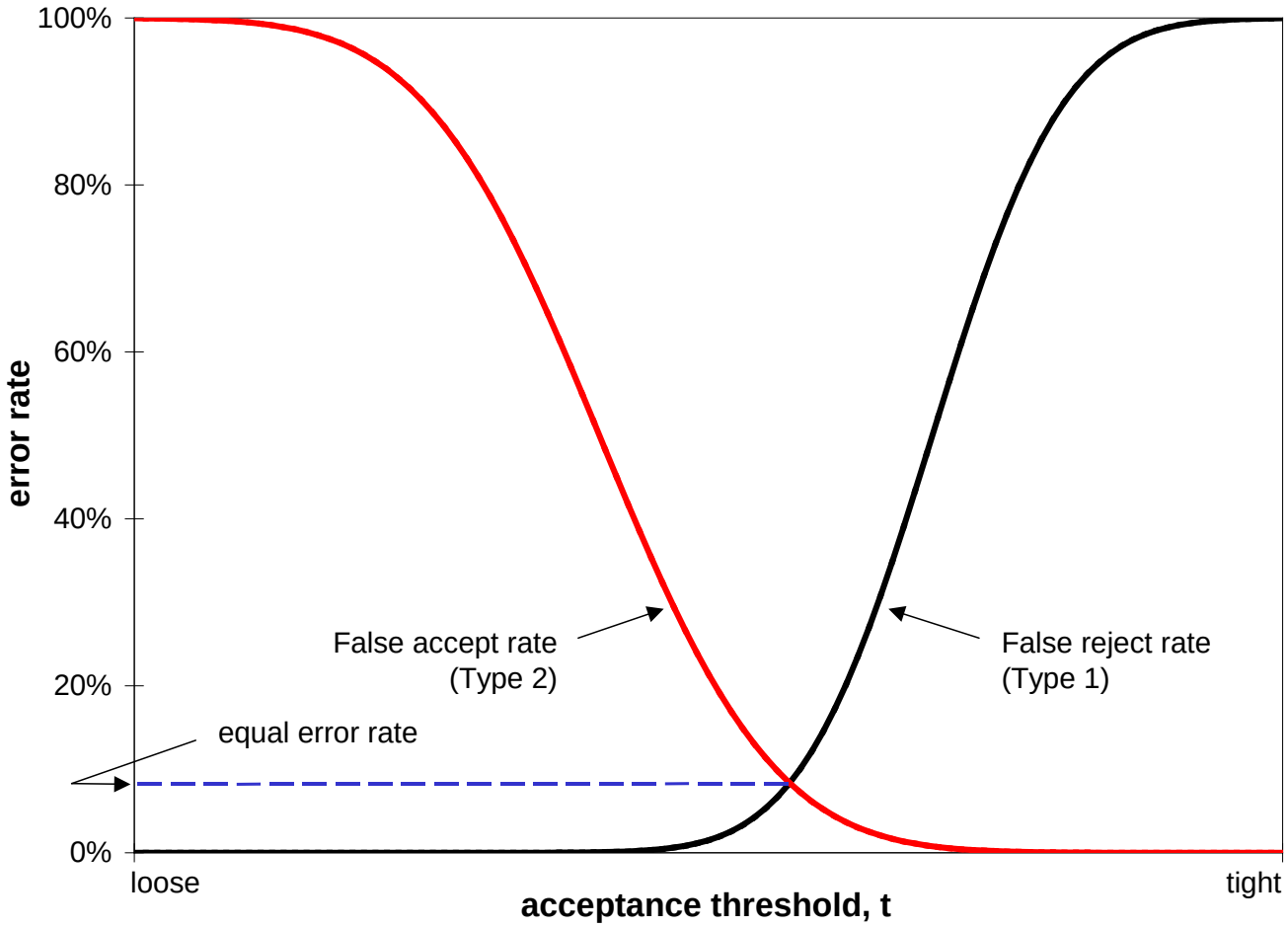
Characterizing Performance

- False Rejection Rate (FRR)
  - Ratio of false rejects to total attempts at verification
  - Typically expressed as a percentage
- False Accept Rate (FAR)
  - Ratio of false acceptances to total imposter attempts
  - Typically expressed as a percentage

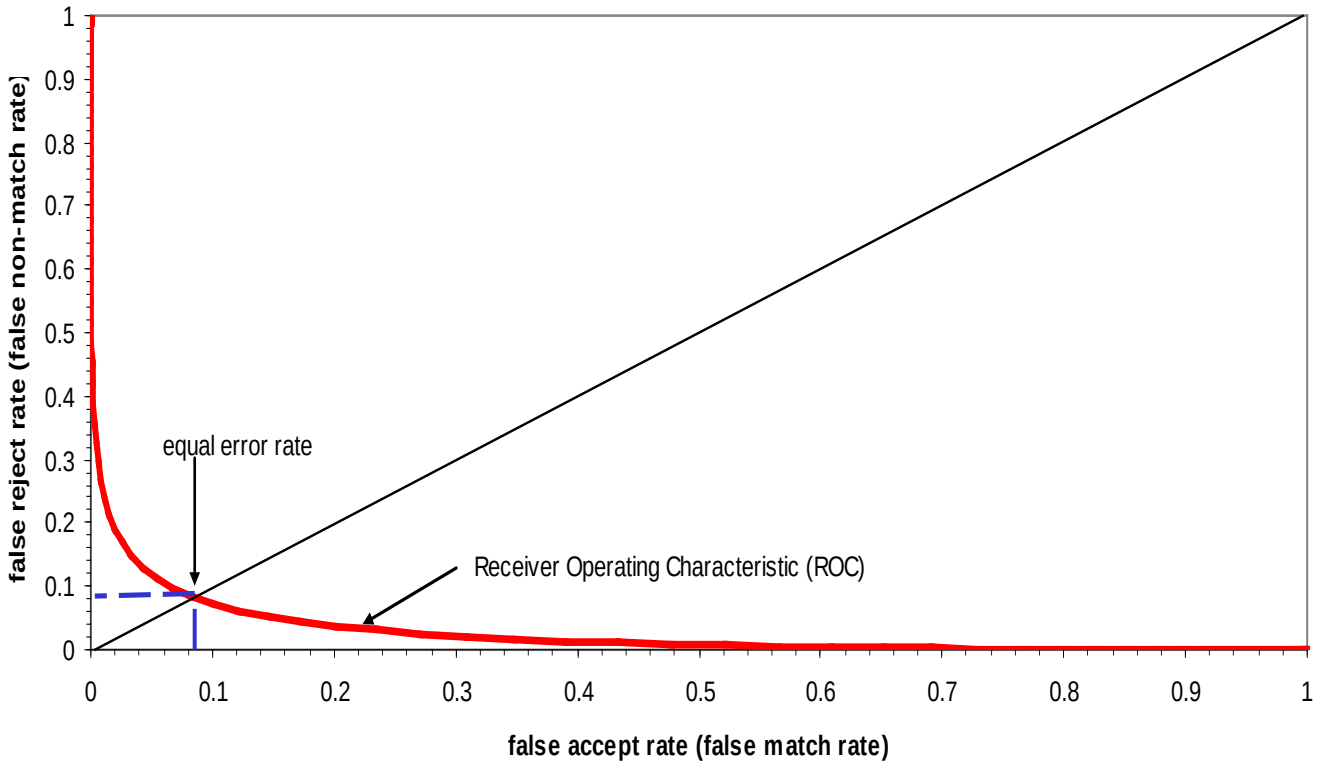
Characterizing Performance: Error Rate Curves

- FRR and FAR are used to generate error rate curves
  - The point that these two curves intersect is the Equal Error Rate (EER)
- EER curves are used to help determine the performance of biometric systems

Example: Error Rate Curves

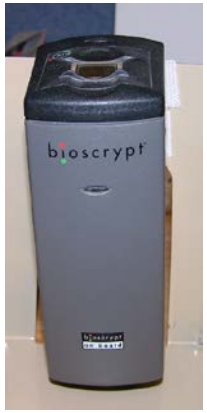


Receiver Operating Characteristic (ROC) Curve



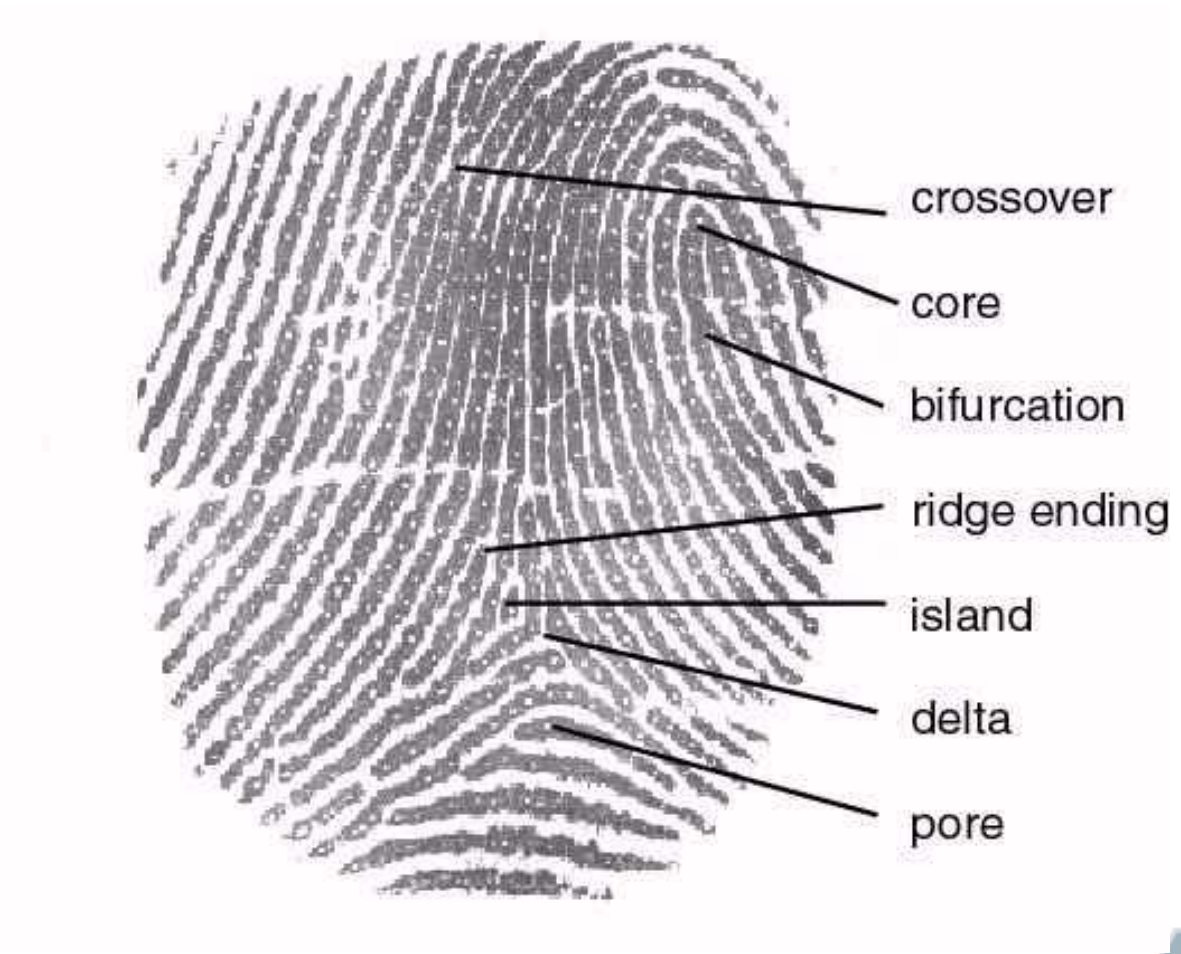
Fingerprint

- Most reliable means of identification
- Current methods used
  - Optical, capacitive, and ultra-sonic imaging
  - Solid state, also known as silicon or chip sensor
  - Ultra-sonic uses sound waves to capture image



Characteristics of Fingerprints

- **Finger-scan minutiae**



Fingerprint Templates

- Templates can range in size
  - 200 to over a 1,000 bytes
- The templates cannot be used to recreate an image of the fingerprint
- Vendor designed algorithms determine whether a presented finger matches a stored template

Fingerprint - Optical

- First technique to be commercially developed
  - Most widely used
- Uses a CCD device to capture an image
- Image is processed by a proprietary algorithm

Fingerprint - Optical Strengths

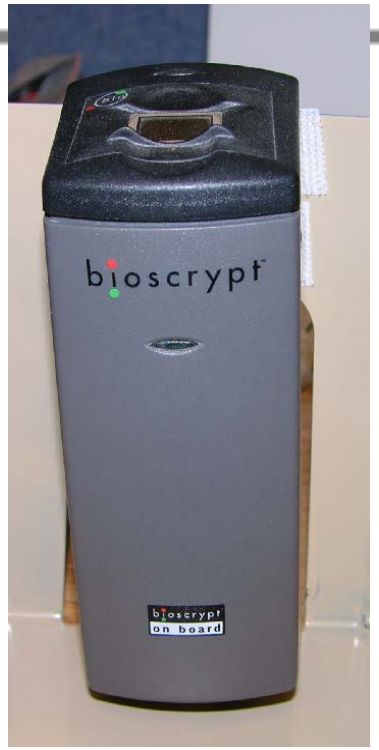
- Proven reliable over time
- Resistant to electrostatic discharge
- Fairly inexpensive
- Can provide up to 500 DPI resolution
  - A benchmark for high quality fingerprint images

Fingerprint - Optical Weaknesses

- The size of the platen is rather large
  - The area and depth must be sufficient to capture quality images
- A sporadic tendency to show latent prints as actual fingerprints
- Susceptibility to fake fingers

Fingerprint – Solid State

- Solid state fingerprint biometric devices
  - Also known as silicon or chip sensor
  - Based on DC capacitance
  - Converts capacitance into an 8-bit, gray-scale image
  - Emerging technology

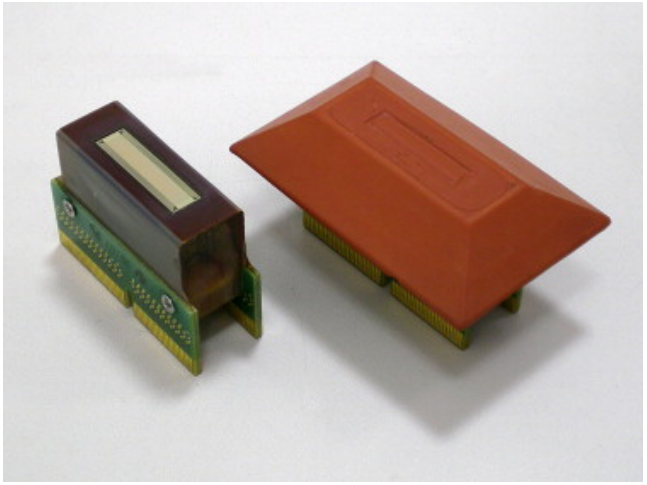


Fingerprint – Solid State *(cont'd)*

- Strengths
  - High image quality
  - Smaller size
  - Low power requirements
  - Does not hold latent prints
- Weaknesses
  - Durability is still subject to question
  - Some types have been to susceptible to electrostatic shock

Fingerprint - Ultrasound

- Similar to medical ultra-sound imaging
- Uses sound waves to capture image
- Measures impedance between the finger and platen

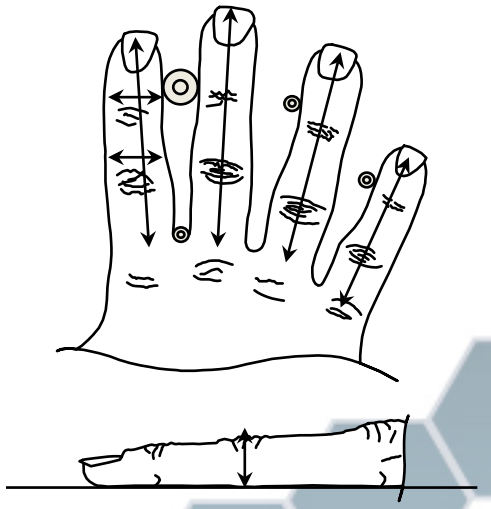


Fingerprint – Ultrasound *(cont'd)*

- Strengths
  - Less impacted by dirt and residue than silicon or optical devices
  - Less susceptible to latent prints
- Weaknesses
  - Mechanical scanning mechanism results in a larger unit than other techniques
  - Slower than optical methods

Hand Geometry

- Claimed identity is entered via the PIN pad or a card reader
- Hand is placed on reflective platen for silhouette imaging
- Unique ID features are the lengths and widths of four fingers
- Hand must have thickness



Hand Geometry - Strengths

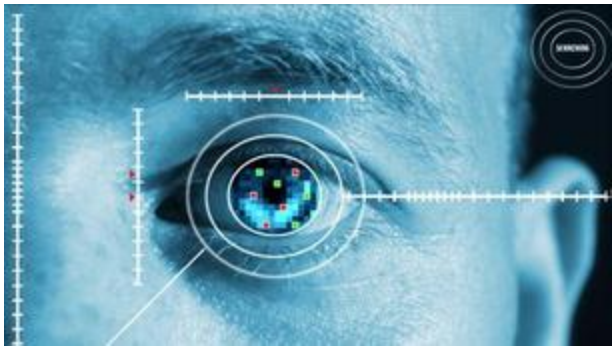
- Ability to operate in many environments
  - Can work outdoors and other places where many other biometric devices would not
- A mature technology that has been successfully deployed in many locations
- The technology is well accepted by most people in the public

Hand Geometry - Weaknesses

- Although fairly diverse, the size and shape of the human hand are not as unique as fingerprint or iris patterns
- In larger populations, it is almost certain that various individuals will have very similar hand dimensions
  - Has to be operated in verification mode for a high-security application

Iris

- Images the iris with a monochrome camera in both the visible and IR ranges
- Very fast acquisition and processing
- Looks for movement in the iris



Iris Recognition

- Iris features used for template:
  - Ridges
  - Freckles
  - Furrows
  - Striations
- Annular sectors are digitized using B&W video camera image to create unique 256-byte template

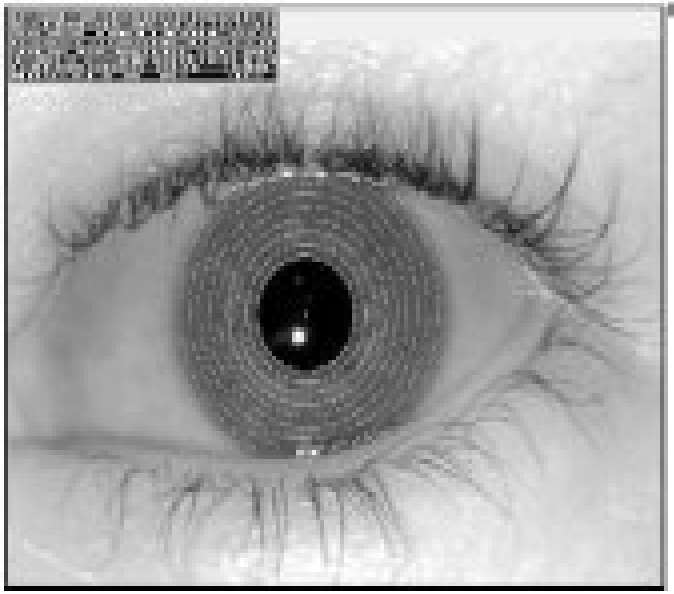


Photo Courtesy of IrisScan

Iris Recognition - Strengths

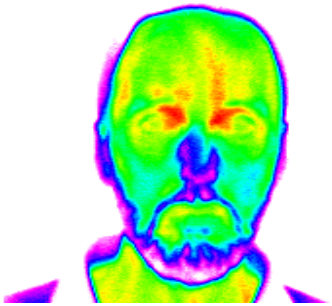
- Extremely low false accept rate
- Capable of operating in the recognition mode as well as verification mode
- No physical contact between individual and device
- Iris characteristic are very stable over lifetime
- Transaction times are fast
  - 4 to 15 seconds

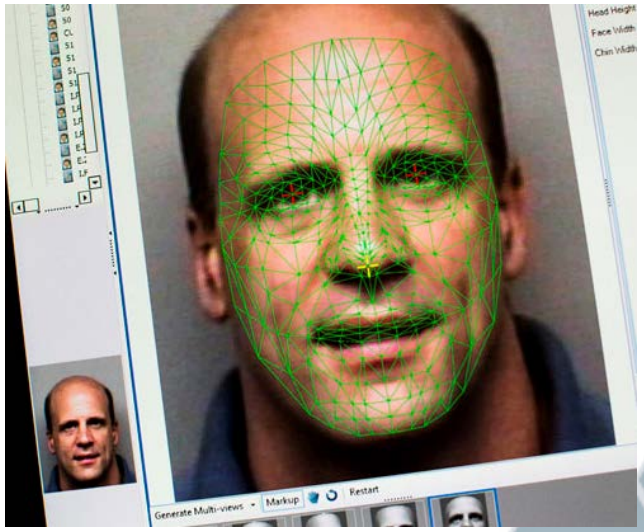
Iris Recognition - Weaknesses

- Acquisition of the image requires moderate training and attentiveness on part of the person being screened
- Moderately high false reject rate
- Lighting in the area has to be controlled
- Some irises are so dark it is difficult to capture sufficient details

Facial Recognition

- This method has appeal because of its similarity to the way humans identify one another
- Most systems use standard video cameras for image capture
- One company attempted to use facial thermograms





Facial Features

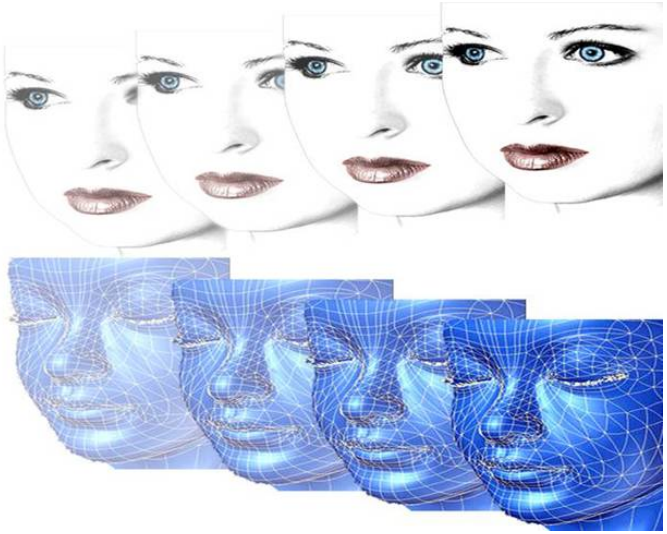
- Developers choose features that are least likely to change over time
  - Upper ridges of the eye sockets
  - Areas around the cheekbones
  - Corners of the mouth
  - Nose shape
  - The position of major features relative to each other

Templates

- Templates can range in size
  - 100 bytes to over 3000 bytes
- Numeric templates cannot be used to recreate original images

Three-Dimensional Facial Recognition

- One of the greatest obstacles to facial recognition is facial orientation
- Development of 3-D approaches include dual camera and laser scanning techniques



Facial Recognition - Strengths

- Does not require specialized hardware
- Can be used on a subject without the subject's cooperation
- Ability to enroll images from other sources
  - Mug shots, video captures
- Can be operated covertly

Facial Recognition - Weaknesses

- Environment affects matching accuracy
  - Users must be facing the acquisition camera straight on
  - The user's face must be lit evenly
- Changes in physiological characteristics that can adversely impact error rates
  - Changes in hairstyle, makeup, or facial hair
  - Wearing or removing eyeglasses
  - Hats and scarves

Facial Recognition – Weaknesses *(cont'd)*

- Potential privacy abuse due to non-cooperative enrollment and identification
  - Certain facial-scan deployments have met with public objections
    - In particular, the one aimed to catch criminals at the 2001 Super Bowl

Other Biometrics Technologies

- Voice
- Handwriting
- Finger geometry
- Keystroke (typing patterns)
- Ear shape
- Gait (walking patterns)
- Fingernail bed
- Body odor
- Etc.

Environmental Factors

- Environmental factors impacting biometric acquisition
  - Lighting
    - Artificial and natural
  - Dust and debris
  - Background noise
  - Electromagnetic noise

Personnel Characteristic Factors

- Personnel characteristic factors impacting biometric acquisition
  - Fingerprint
    - Cold, very dry, oily, cuts, scars
  - Face
    - Hair, glasses, lighting, clothing, camera, presentation
  - Hand
    - Jewelry, bandages, weight change
  - Eye
    - Glasses, head movement, injuries, surgery
  - Voice
    - Speaker volume, illness, repeatability

Biometric Evaluation

- Ease of integration
  - A factor of how many different systems support a specific technology
  - If the biometric has a flexible interface
- Performance
  - Expressed as error rates associated with the specific technology
- Cost
  - Initial purchase, installation, and maintenance
- Availability
  - Available stock and expected life of company

Biometric Evaluation *(cont'd)*

- Usability
  - User acceptance and difficulty of use
- Throughput
  - Number of transactions per unit of time
- Security
  - Susceptibility to defeat, both by imposter and physical attack
- Reliability
  - Mean time between failure

Benefits of Biometrics

- Benefits of biometrics used in conjunction with traditional authentication methods
- Increased security
  - Traditional authentication methods can be stolen, guessed, or duplicated
  - Biometrics cannot be guessed and are difficult to capture or duplicate
- Development of biometric devices using very unique personnel characteristics may result in a device where PINs and credentials are not needed

Combinations of Identity Verification Factors

- By combining all three factors used for identity, verification security can be increased

Factors Impacting Biometric Capture

Environment:

- Lighting—both artificial and natural
- Dust and debris
- Background noise
- Electromagnetic noise

Personnel characteristic:

- Fingerprint: cold, dry, oily, cuts
- Face: hair, glasses, light, clothing, camera, presentation
- Hand: jewelry, bandages, weight change
- Eye: glasses, head movement,
- Voice: speaker volume, illness

Levels of Entry Control

Level	Verification	Examples
1	One type	Credential **OR** PIN **OR** Biometric
2	Two Types	Credential **AND** PIN OR Credential **AND** Biometric OR Biometric **AND** PIN
3	Three Types	Credential **AND** PIN **AND** Biometric

Features of Biometric Systems

- Ease of Integration
  - A factor of how many different systems support a specific technology and if the biometric has an flexible system interface
- Verification times
  - 2 to 20 seconds
- Enrollment
  - 1% to 3% of population is incompatible
  - 30 seconds to 10 minutes required to enroll
- Cost
  - $1,000 to $5,000 per terminal

Personnel Entry Control Errors

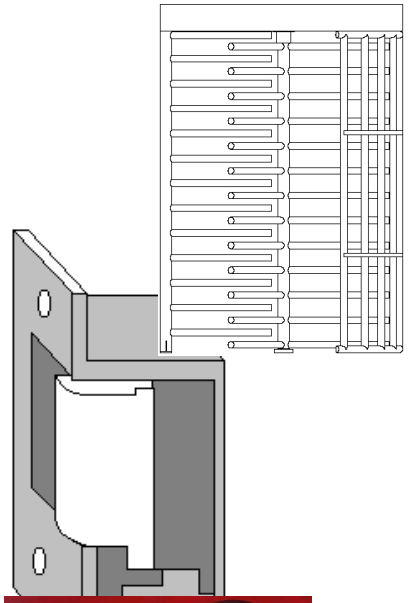
- Performance - Expressed as error rates associated with the specific technology
  - False rejection
    - Authorized persons are not allowed to enter
    - A small number may be an acceptable trade-off for high security situation
    - Easy to quantify
  - False acceptance
    - Unauthorized persons are allowed to enter
    - A small number may be an acceptable trade-off for low security situation
    - Difficult to quantify

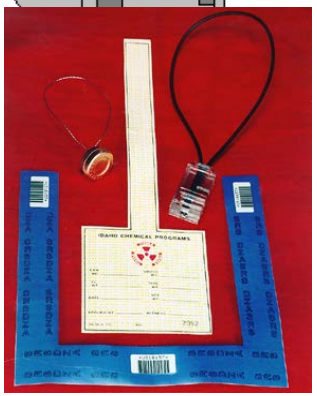
Features of a Good Entry Control System

- Integration with boundary
  - Cannot be bypassed
  - Block individuals until access authorization verified
  - Interfaces with the alarm system
- Integration with the guards/response force
  - Protects guard
  - Area is under surveillance
- Personnel integrate with system
  - Easy to use for entry and exit
  - Accommodates peak throughput (loads)
  - Accommodates special cases

Methods of Controlling Access

- Manual and electronic security systems use turnstiles, doors, locks, safes to control access to areas or information
- Electronic locks are usually used t interface physical barriers with electronic entry control systems
- Tags and seals (tamper indicating devices) are used to prevent undetected access to areas and containers





Integration with Other Aspects of Security

- Entry control and contraband detection is often interfaced with the physical barriers (delay features) to automatically grant or deny access to a security area
- Another area of close integration is between entry control and the alarm communications and display system
  - Entry control systems are often used to place security areas in access
  - Entry control systems are used to mask alarms during authorized entries

Subgroup 11
Entry Control Systems

Session Objectives

After the session, the participants will be able to do the following:

1. Select generic equipment for an effective entry control system to verify credentials.
2. Determine appropriate False accept and False reject error rates of positive personnel identification equipment depending on application.
3. Recommend environmental protection mechanisms for positive personnel identification devices.
4. Analyze a portal design and procedures.

Exercise 1 - Selection of Badge Equipment

Using the information from the lecture and slides, choose badge equipment that satisfies the requirements below.

Requirements:
1) **The reader must be able to be used outside in all weather.**
2) **The card must have a high resistance to counterfeiting, and ease of use is important.**

Selected Equipment: _____

Reasons**:** _____

_____

_____

Exercise 2 - Selection of Personnel Identification Equipment

Using the data in Table S-1, choose personnel identification equipment that satisfies the requirements below.

Requirements:

1) **The personnel identification equipment must be very user friendly.**

2) **The equipment must have a user throughput rate of at least 6 persons per minute.**

3) **The equipment will be used at an exterior fence gate.**

Selected Equipment: _____

Reasons: _____

_____

_____

What kind of environmental protection will be required?_____

_____

Table S-1. Personnel Identification Equipment

Technology	Verification Time (seconds)	False Reject Rate (FRR)	False Accept Rate (FAR)	User Acceptability	Adverse Conditions
Iris pattern	10**	medium	very low	high	reflections (e.g., glasses)
Face	4*	medium	medium	high	ambient light changes
Hand geometry	4*	low	low	high	direct sunlight on platen, dust/dirt
Fingerprint	4*	medium	very low	medium	dust/dirt, dry fingers
Voice	10*	medium	medium	high	high noise

* Includes time to enter a PIN or read a card.
** Recognition time (no PIN entered or card read).

Exercise 3 – Threshold Setting of Personnel Identification Equipment

Some positive personnel identification devices have the built-in option to change the balance of acceptance and false rejection; which is often called the threshold setting. This setting changes the acceptance precision of the device.

Consider the following applications for a biometric device with a 5% "Equal Error Rate Point". For the following situations determine what would be the best setting and the resultant False Accept and False Reject Errors.

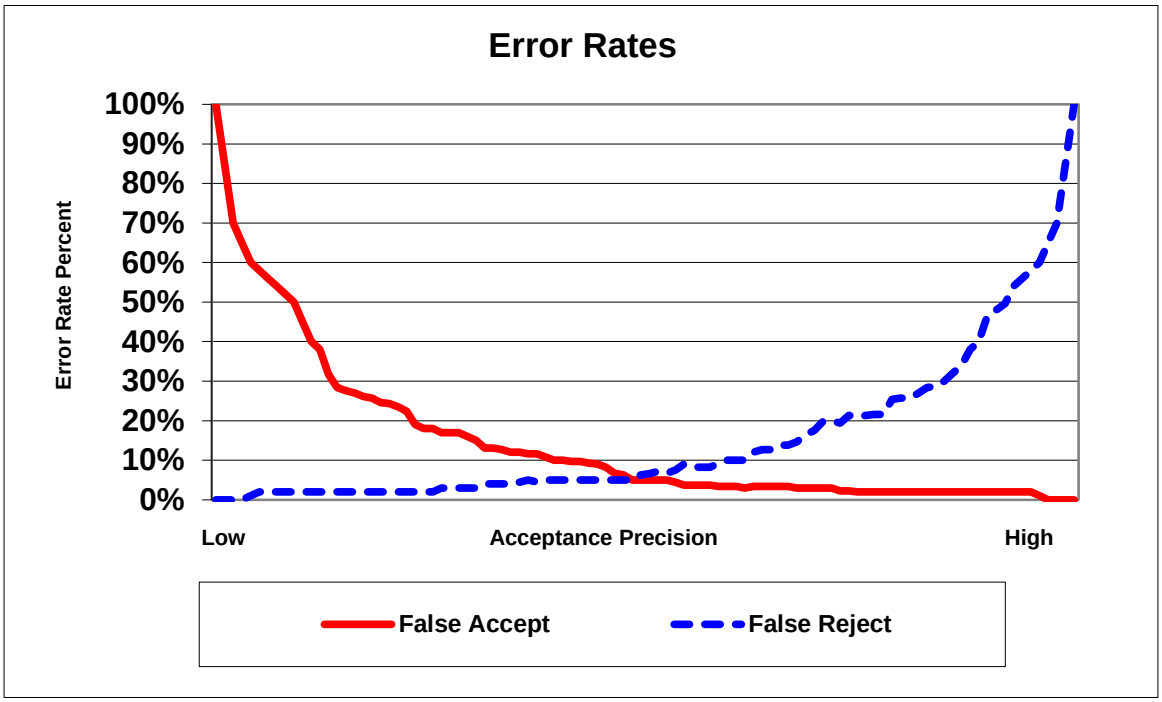


Figure 9S-1. False Accept and False Reject Error Rates

Situation 1 – Entry into a very secure plutonium vault.

False reject _____

False accept _____

Reasoning_____

_____

_____

Situation 2 – At the main gate of a very large reactor complex.

False reject _____

False accept _____

Reasoning_____

_____

_____

Situation 3 – At a PPS control console which allows putting detection equipment into access or secure mode.

False reject _____

False accept _____

Reasoning_____

_____

_____

Situation 4 – Entry into a warehouse which stores the spare PPS equipment.

False reject _____

False accept _____

Reasoning_____

_____

_____

Situation 5 – Entry into the accounting Paymaster's office

False reject _____

False accept _____

Reasoning_____

_____

_____

Situation 6 – Entry into the Reactor Control Room.

False reject _____

False accept _____

Reasoning_____

_____

_____

Exercise 4 – Environmental Protection for Entry Control Equipment

Indicate the kind of environmental protection you would recommend to counteract the "adverse conditions" indicated on the following table.

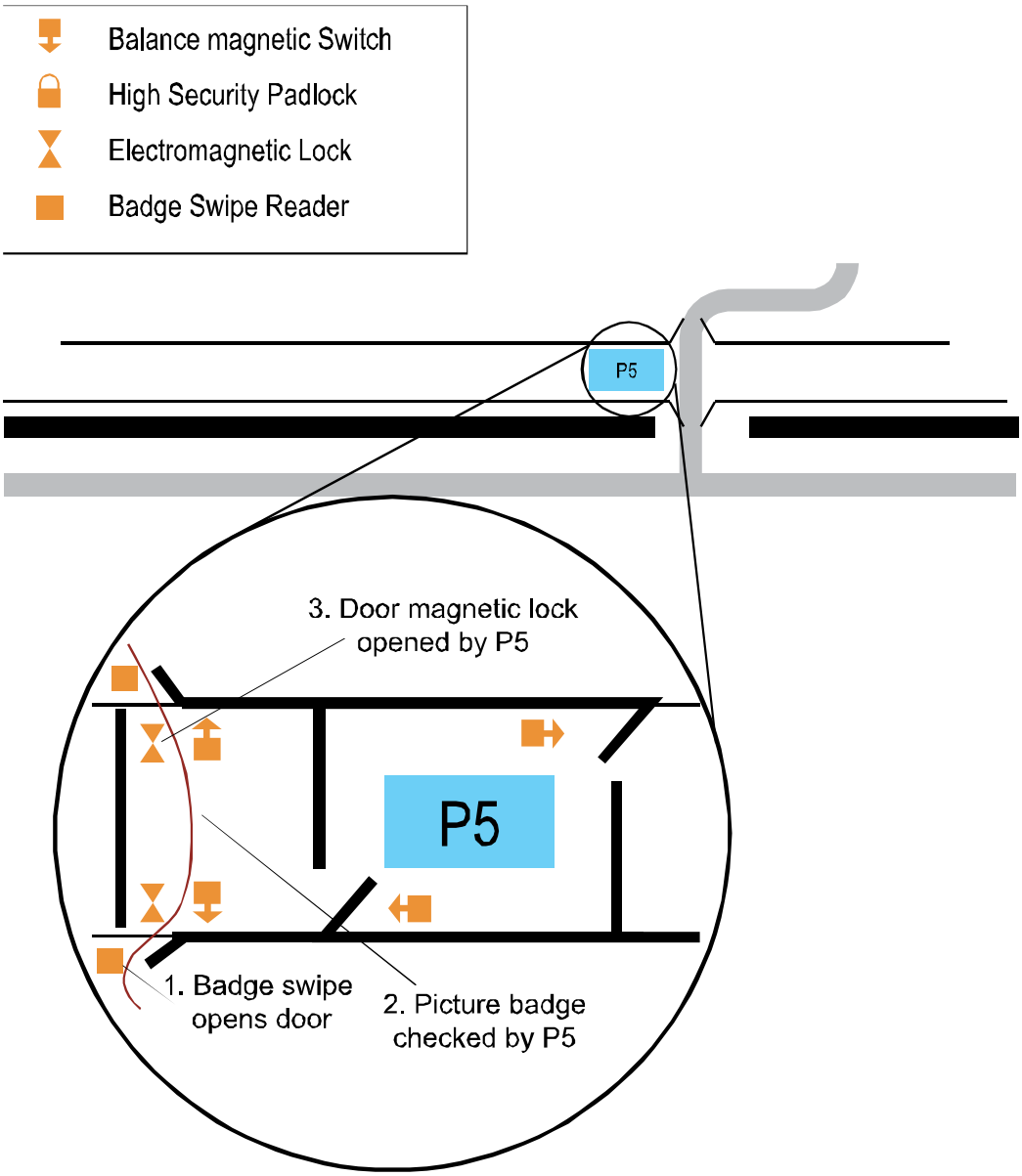
Technology	Adverse Conditions	Environmental Protection
Iris pattern	Reflection (e.g., glasses)	
Face	Ambient light changes	
Hand geometry	Direct sunlight on platen, dust/dirt	
Fingerprint	Dust/dirt, dry fingers	
Voice	High noise	

Exercise 5 – Personnel and Vehicle Portal

The diagram below shows a hypothetical vehicle and personnel portal permitting access to the PTR protected area. Some strengths of the vehicle control system are:

- Vehicle driver is separated from vehicle during vehicle search.
- Vehicle driver must go through personnel portal.

The procedures governing entry and exit from the P5 Personnel and Vehicle Portals are given in the hypothetical data book, section 7. Use this information to evaluate this entry control system, and write down any improvements that could be made to upgrade the system.



Improvements

1. _____

_____

2. _____

_____

3. _____

_____

4. _____

_____

Application Considerations

Discuss the following application considerations:

1) Controlled, free space should be provided for entering personnel.

2) A “back out” route should be provided for unsuccessful users.

3) Enrollment information should be kept under security control.

4) Security personnel should be able to observe entry control equipment (e.g., personnel or via CCTV).

5) Special requirements (e.g., fire lanes, break-out doors, etc.) should be considered when designing entry control system.

6) Alternate entry control procedures should be provided for people with special needs, such as the handicapped.

7) Measures should be taken to compensate for unreliability (e.g., power failures and equipment breakdowns), usually with parallel components.

8) In what situations would a protective force (guard) be used for entry control? What impact could this have on the physical protection system, the cost, etc.?

9) Why might the design be for portal doors that interlock so that only one door can be opened at one time?

10) What would be the combined False rejection error if we consider that entry depends on something you have, something you know, and something about you?

   a) Something you have – picture badge (guard verified)

   b) Something you know – 4 digit PIN

   c) Something about you – Hand geometry set to a 10% False rejection error rate

11) Why should portal doors, walls, and the roof provide the same delay as the perimeter or building walls in which they are installed?

Introduction to Contraband Detection

Learning Objectives

After completing this module, you should be able to:

- Define contraband
- State the purpose of contraband detection
- List the contraband objects and materials that are most often banned from security areas
- Introduce the concepts and techniques of contraband detection
- Discuss the tools used to detect common contraband objects and materials

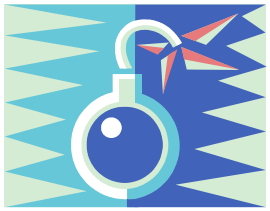
Contraband Detection

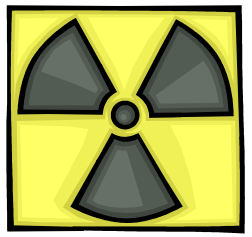
- Contraband detection systems seek to detect contraband by a variety of means in order to deny their introduction into a security area

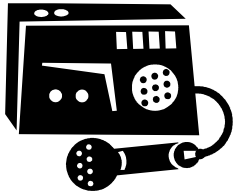
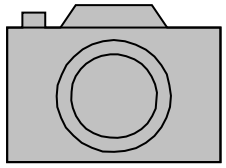
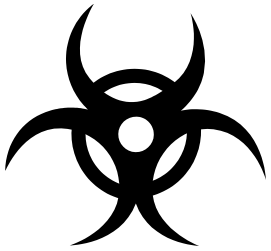
Contraband Defined

Contraband: any object or material that is prohibited in a security area

- Contraband is also any device or material that can be used by an adversary to gain an advantage in an attempt to commit an act detrimental to a facility




The Purpose of Contraband Detection

- The primary purpose of contraband detection is to detect the presence of contraband objects and materials for the purpose of preventing their entrance into a security area
- Contraband detection systems seek to detect contraband by a variety of means

Purposes of Contraband Detection Systems

Allow entry of
- Authorized material

Prevent entry of
- Weapons
- Explosives
- Other contraband

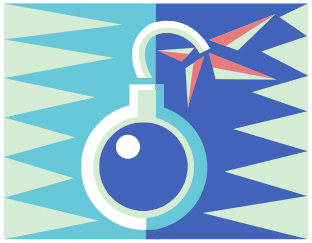
Allow exit of
- Authorized material

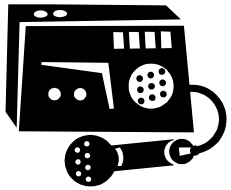
Prevent unauthorized exit (theft) of
- Special nuclear material

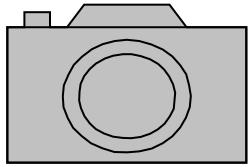
Contraband: *An item that is prohibited in an area.*

Contraband Objects

- Contraband objects can include:
  - Guns
  - Bombs
  - Tools
  - Recording devices
  - Cell phones
  - Cameras
  - Other

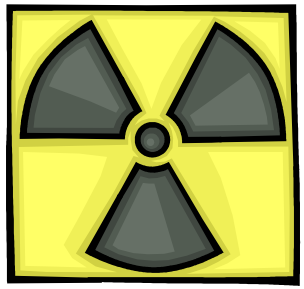



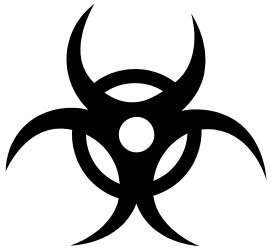





Contraband Materials

- **Materials that can be contraband, include:**
  - **Explosives**
  - **Drugs**
  - **Nuclear materials**
  - **Others may include:**
    - **Toxins**
    - **Bio-agents**
    - **Other dangerous materials**





Detection Techniques

- Manual search is a viable detection technique for low throughput situations
- Using electronic detection tools for machine assisted screening can greatly speed up the screening process
  - To some extent remains a manual process
- Fully automated detection is practical in some applications and for certain types of contraband
  - Nuisance alarm rates remain relatively high

Contraband Detection Devices

- Devices and tools used to detect contraband include:
  - Metal detectors
  - Explosives detectors
  - X-ray imagers
  - Canine

Manual Search

- Manual search may be highly effective
  - Typically takes too long for very high throughput
- Effectiveness depends heavily on
  - Good procedures
  - Application of the procedures
- Materials may not always be recognized due to form and camouflage
- More subject to human error

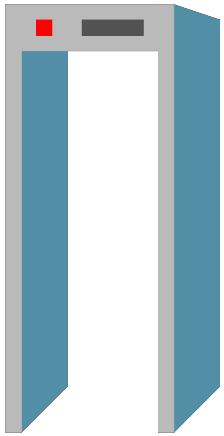
Machine-Assisted Screening

- Examples include airport passenger screening with X-ray and hand-held metal detectors
- Detection of contraband dependent on human interpretation of machine output
- Carry-on bag screening by X-ray machine does not typically involve automated detection
- Still subject to human error

Photo by Rapiscan

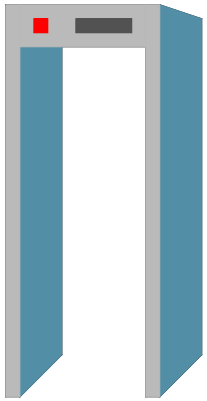
Automated Detection

- Some systems are fully automated
- Good examples are portal metal detectors, trace explosives detectors, and some bulk explosives detectors
- Relatively high nuisance alarm rate means secondary screening is frequent
- Secondary screening is often manual or a different machine assisted and therefore still subject to human error



Contraband Detection Tools - Metal

- Many tools available to help perform the contraband detection function
- Most common means of detecting metallic items on persons is the portal metal detector
- Detecting metallic items inside packages is typically performed using an X-ray package search imager



Magnetometers

- Magnetometers are passive devices
  - Measures the earth's static magnetic field
- Used because ferromagnetic materials in weapons disturb the earth's magnetic field
- Term is used incorrectly to refer to metal detectors
  - Differs from modern active metal detectors

Metal Detectors

- Metal detectors are active interrogation devices used to search for:
  - Metal
    - Ferromagnetic and non-ferromagnetic
  - Any conductive materials
- Metal detectors fall into two areas
  - Continuous wave
  - Pulse

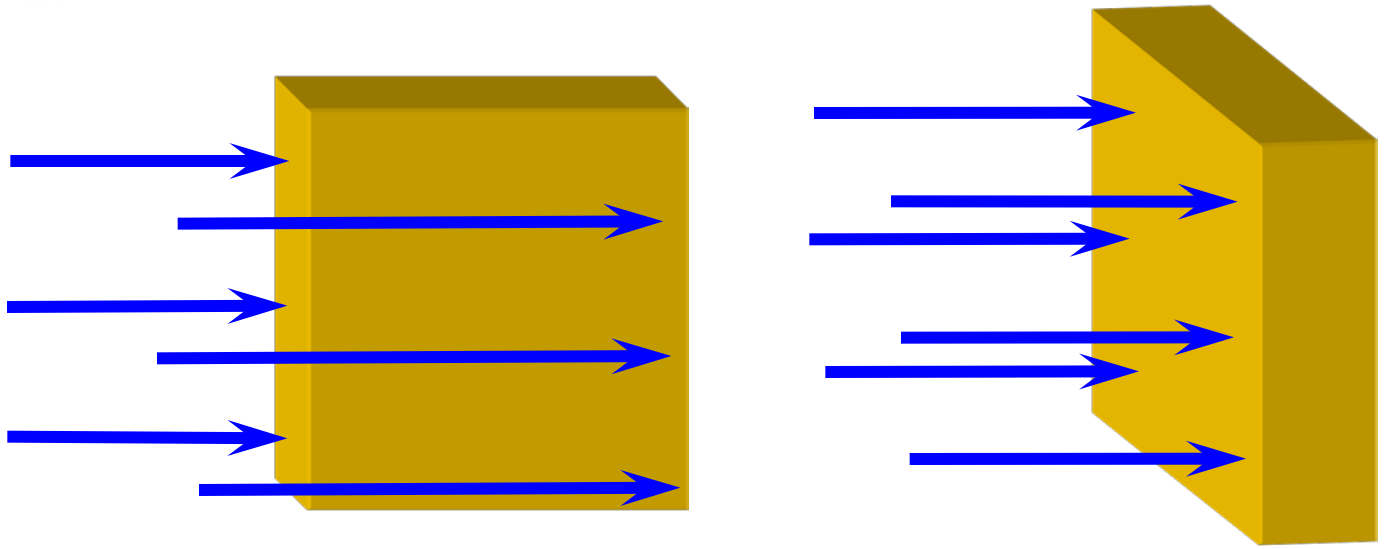
TIME FOR A BREAK

Faraday's / Lenz's Law

$$\varepsilon = -\frac{\partial \Phi_B}{\partial t}$$

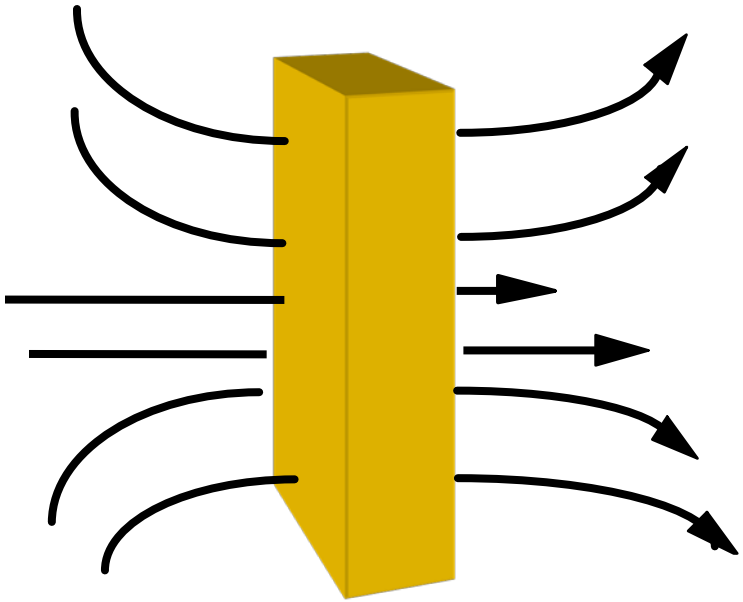
- Faraday's law states that a magnetic field changing with respect to changing time, will produce a voltage
- Lenz improved this by adding the negative sign to relate the direction of induced currents

Orientation



- The orientation of an object determines the maximum amount of magnetic flux striking the object

Ferromagnetic Materials



- Ferromagnetic materials distort the ambient magnetic field increasing the maximum magnetic flux striking the object

Ohm's Law

$$I = \frac{\varepsilon}{\rho L} = \frac{\varepsilon\sigma}{L}$$

- Ohm's law states that a voltage in a conductive medium will produce a current
- More commonly seen as $I = V/R$

Object Shape

- Two shapes of the same material have equal areas
  - The 9 sq. in. circle has a circumference of 10.63 in.
  - The 9 sq. in. (18x1/2 in.) rectangle has the perimeter of 37 in.
- The resistance of the rectangular path is three times higher than the circular path

Conductivity of Object

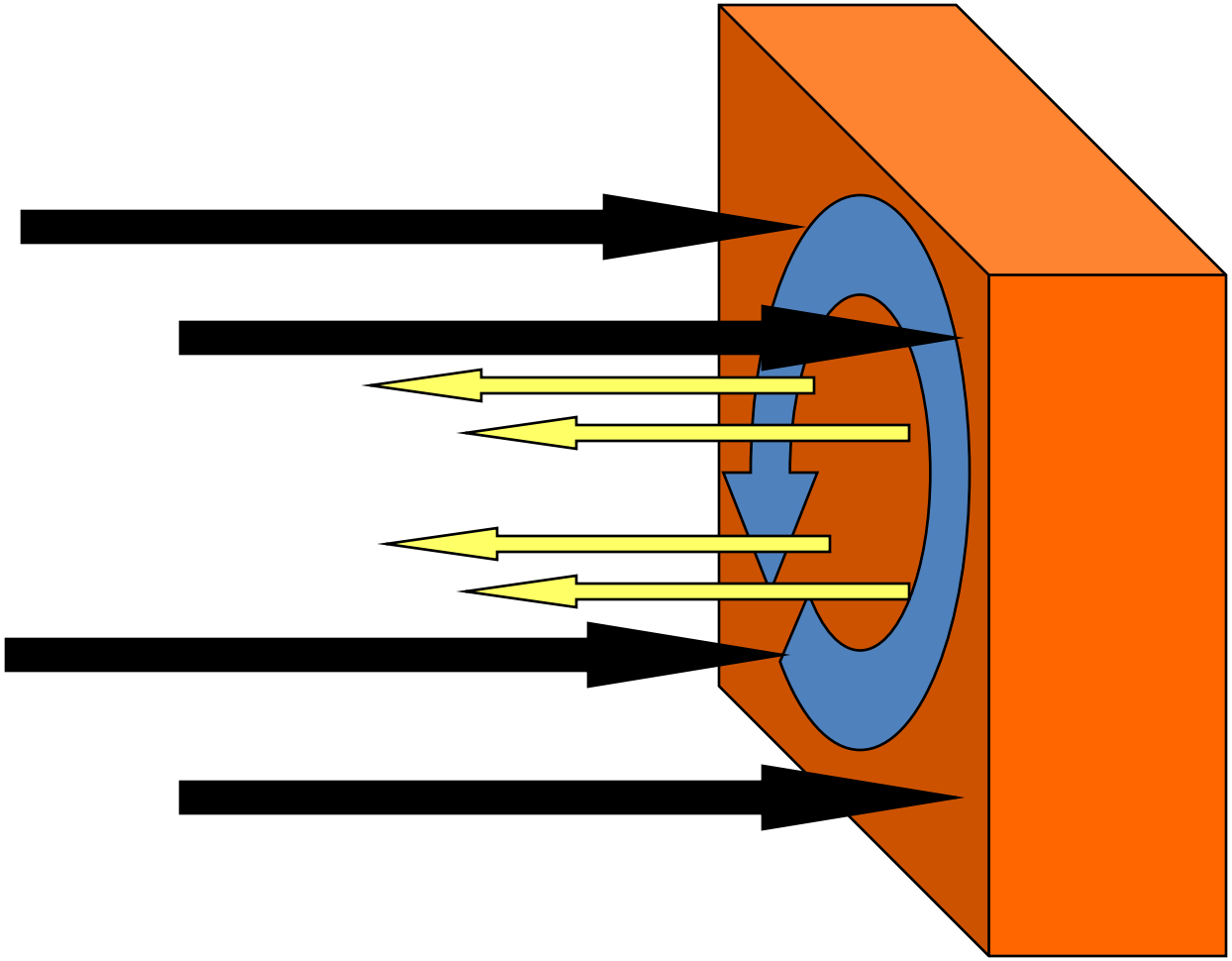
Copper

High Conductivity
Easy to Detect

Titanium

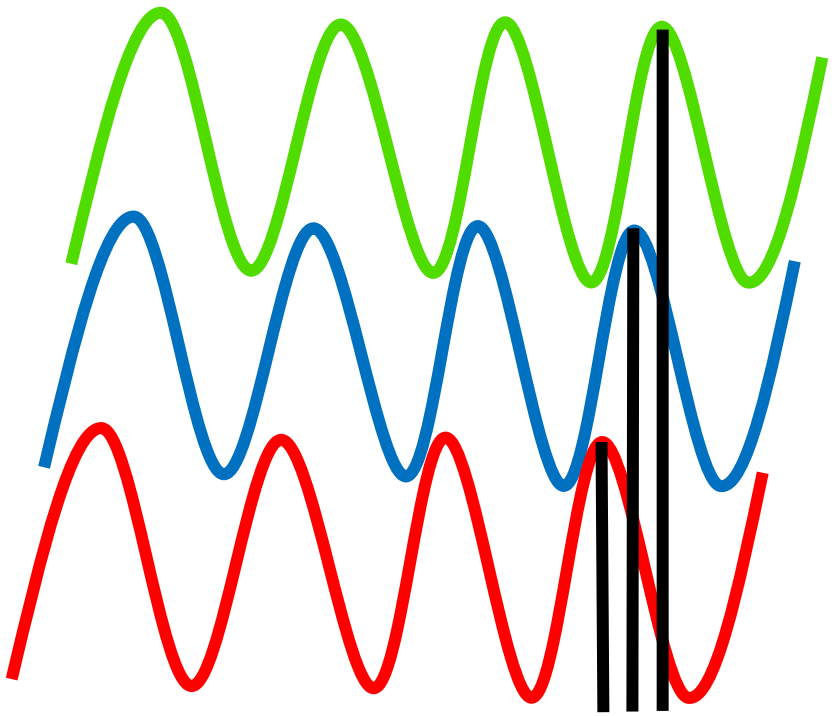
Low Conductivity
Hard to Detect

Eddy Currents



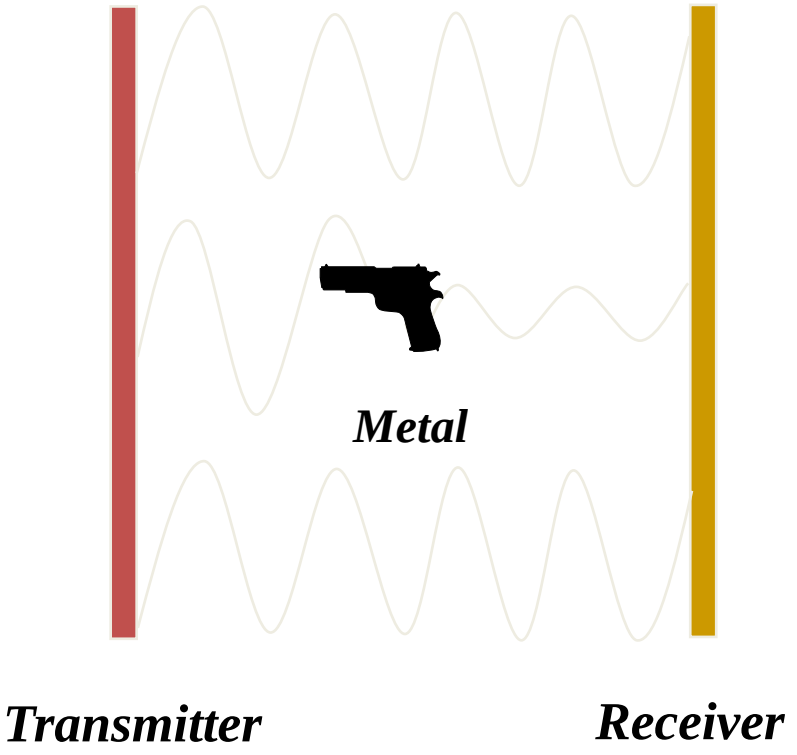
Response Phase

- Green signal is the transmitted signal
- The blue response signal represents the phase change introduced by a small inductance
  - Non-ferromagnetic response
- The red response signal represents increased phase change introduced by a larger inductance
  - Ferromagnetic response



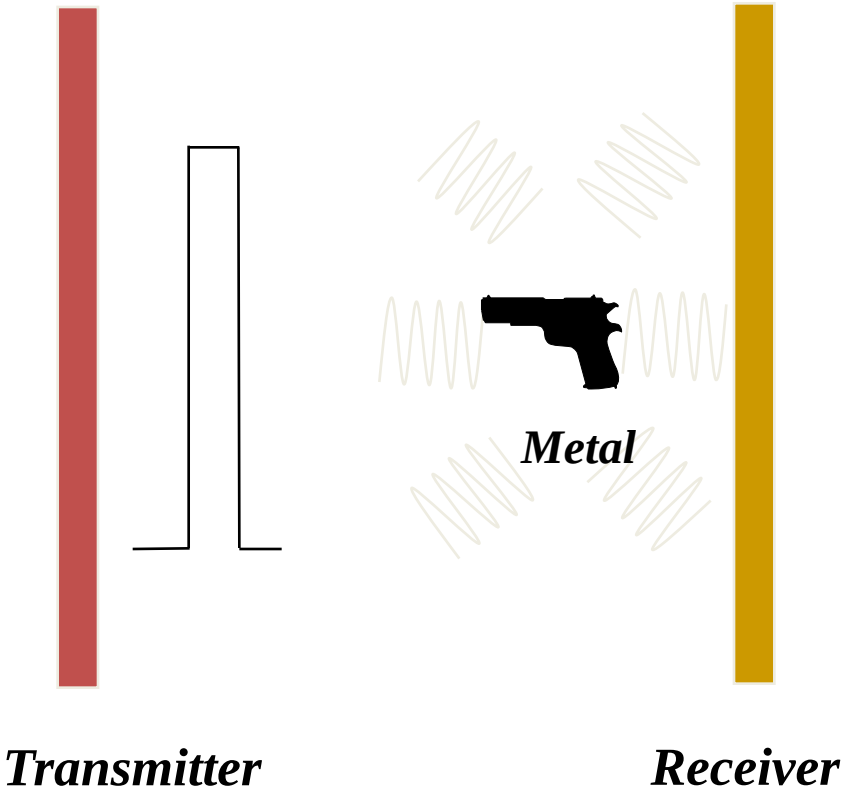
Continuous Wave Metal Detector Operation

- The transmitter generates a continuous time varying magnetic field
- The transmitted field induces an eddy current
- Since the magnetic field created by the eddy current opposes the transmitted field there are changes in the magnitude of the transmitted field as seen by the receiver

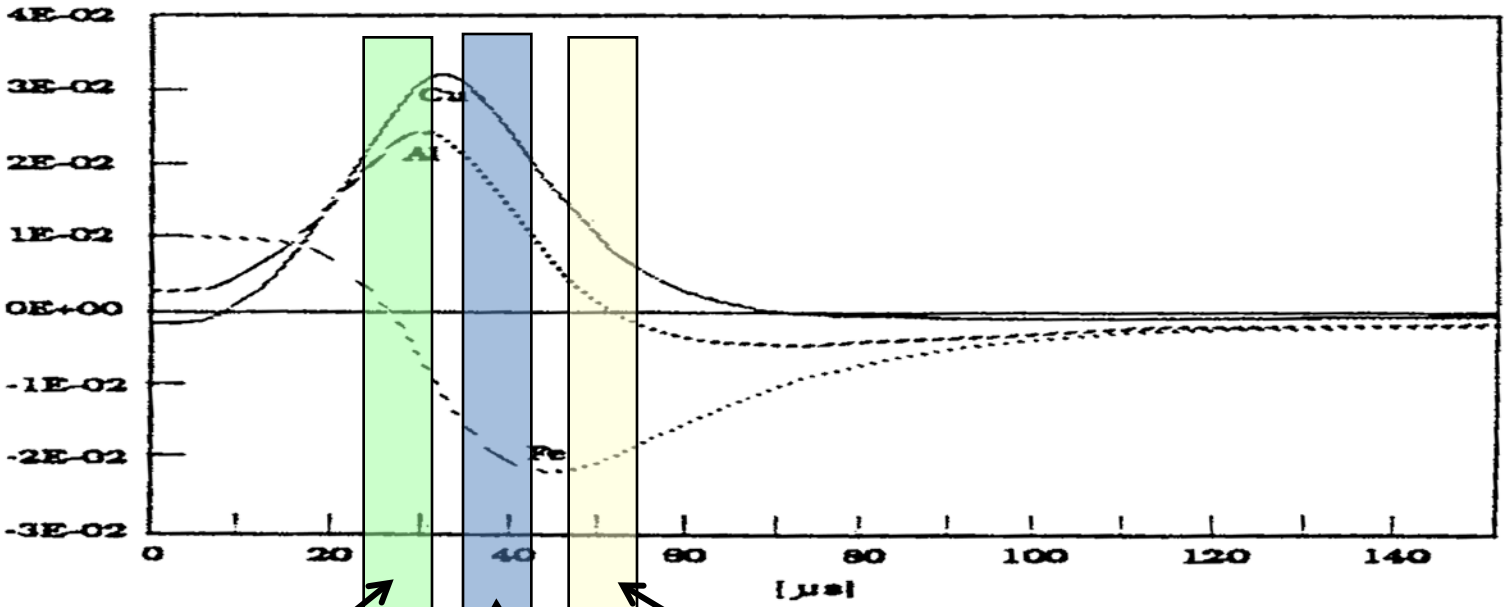


Pulsed Metal Detector Operation

- Short bursts of magnetic field are generated by the transmitter
- The burst induces eddy currents in metallic objects
- The receiver detects the rapidly decaying magnetic fields produced by the eddy currents



Eddy Current Decay Phases

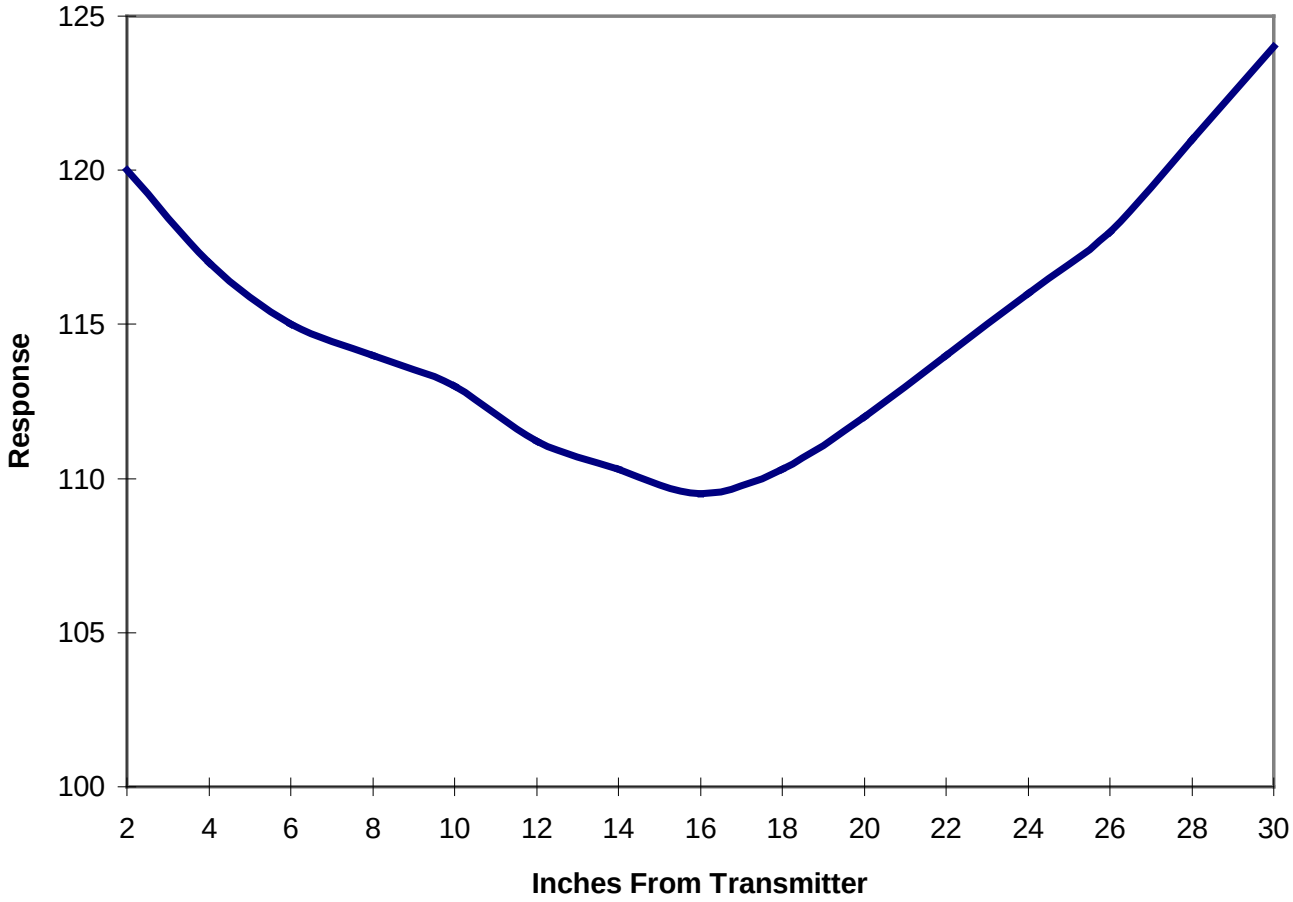


Non-Ferromagnetic Detection Window

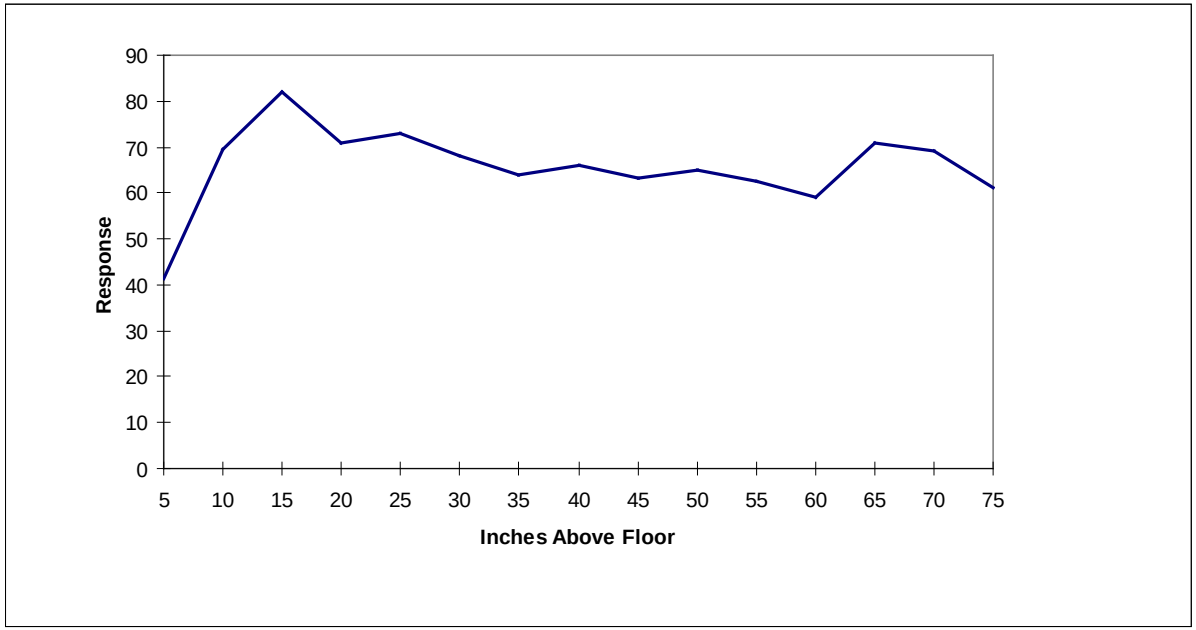
Balanced Detection Window

Ferromagnetic Detection Window

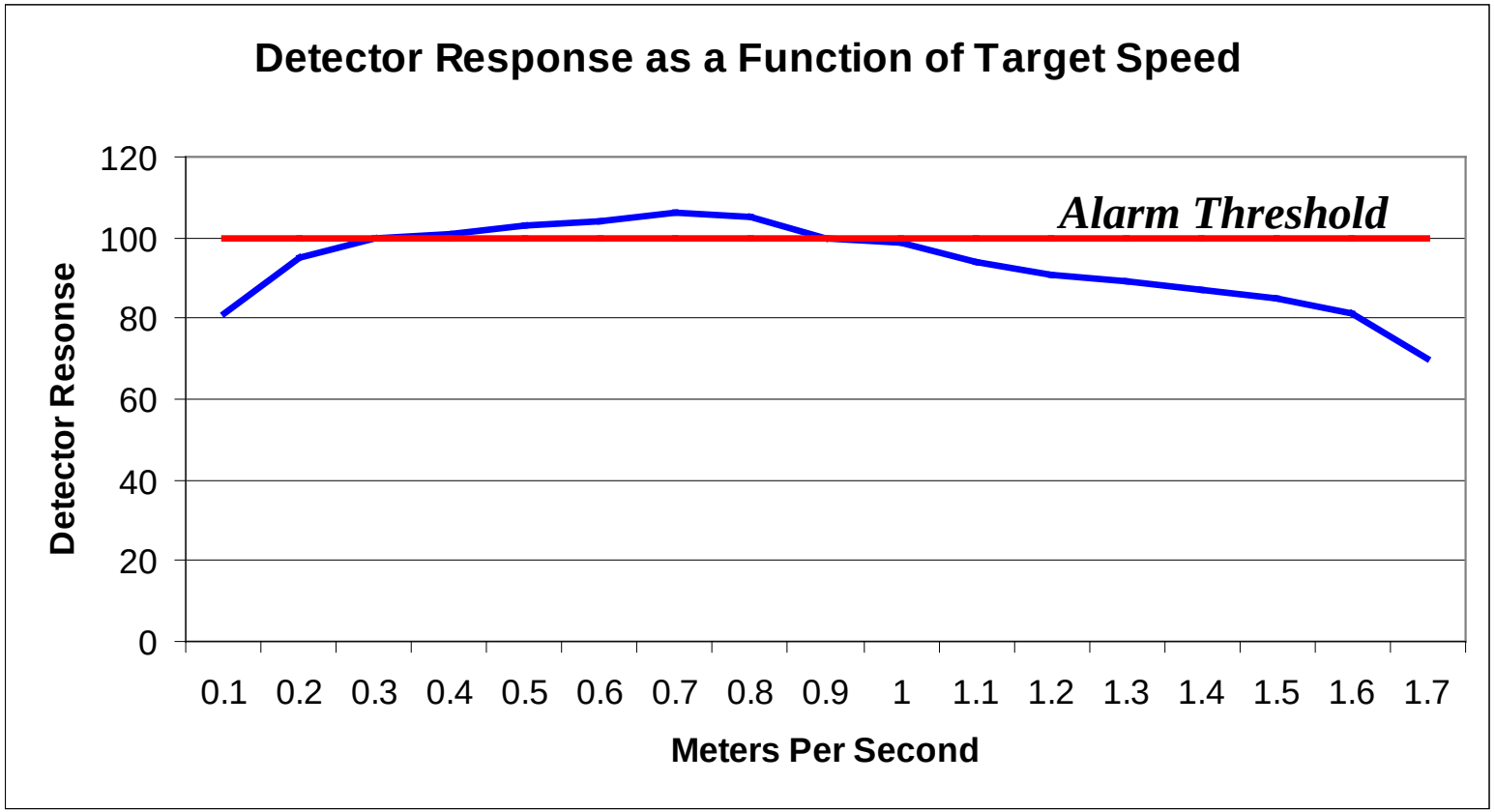
Example Sensitivity Profile



Example Vertical Sensitivity Profile



Impact of Target Speed on Detector Response



Portal vs. Hand-held Metal Detectors

- Portal metal detectors
  - Better for handling large throughput
    - Example: passengers in an airport
  - Take human error out of the screening process
- Hand-held metal detectors
  - Can detect much smaller metallic objects
  - Detection success is very dependent on procedures
  - Human error can be a cause for failure to detect an object when using hand-held
- Both will likely be used at a screening point

Factors Affecting Metal Detector Operation

- Environment
  - Metal doors
  - Equipment operating nearby (e.g., fork lifts)
  - Metal cabinets, electromagnetic sources (e.g., radio transmitters, fluorescent lights)
- Installation
  - Stability of the floor
  - Attachments to floor or walls
  - Near plumbing
- Control of access to settings

Test Criteria

- Metal detectors need to be tested for adequate detection of the worst case threat item
  - In the worst case orientation, and
  - At the worst case location in the detector
- Detectors need to be tested in the location where they are installed
- Detectors have to be tested periodically to ensure their performance has not changed since installation

Test Criteria *(cont'd)*

- Detectors need to be tested after changes like maintenance and the locations of metallic items in the environment
- Tests should be based on statistical criteria defined in regulations

Categories of Detection

- Two broad categories for detection of explosives:
  - Bulk
  - Trace

Contraband Detection Tools - Trace Explosives

- Detection of trace quantities of explosives on personnel can be performed by portal explosives detectors
- Detection of trace quantities of explosives on packages can be performed by desk-top or hand-held explosives detectors

Trace Detection

- Detection of microscopic amounts of vapor or particles of the material in question
- Note: An alarm does not always imply the presence of a bomb; contamination may be present without a bomb
- A primary screening technique
  - After an alarm, an alarm resolution procedure is needed

Typical Measuring Units

- Pressure:

  one part per million = 1 ppm

  one analyte molecule per every one million molecules in ambient air, or one millionth of one atmosphere

  one part per billion = 1 ppb

- Mass:

  one nanogram = 1 ng = 10^{-9} gram = one billionth of a gram

Types of Sample Collection

- Types of sample collection for trace detection
  - Swipe sampling
  - Vacuum sampling

Trace Sampling - Swiping

- Swipe Sampling: Wipe a sampling medium across the surface
  - Direct physical contact to pick up adsorbed particulates

Trace Sampling - Vacuuming

- Vacuum Sampling: Use a “dust buster”-type device to inhale a sample into a collection medium (e.g., cloth pad)
  - No direct physical contact
  - Collects vapor and / or airborne particulates
  - Usually less sensitive but less invasive than swipe sampling

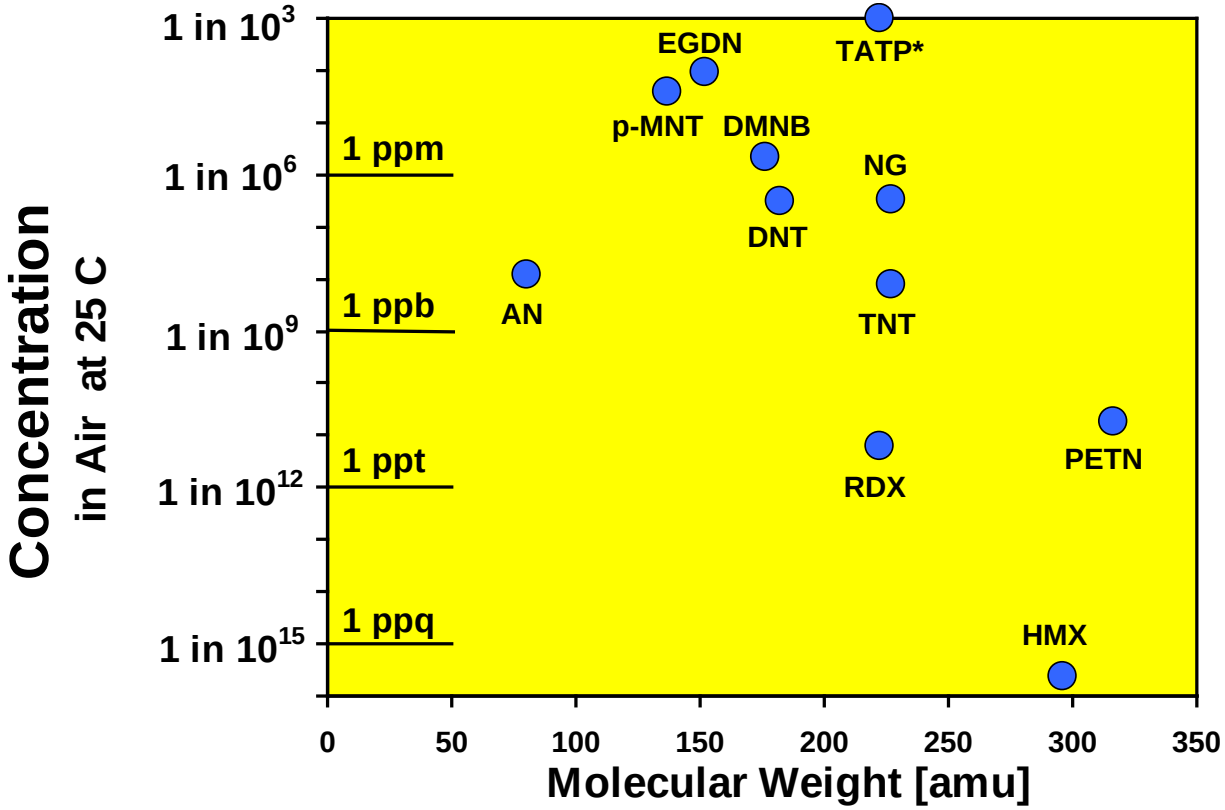
Swiping: Sources for Surface Contamination

- Handling explosives
  - One factor working in our (the screener's) favor is that explosives molecules are very sticky
  - Particulate contamination gets on a person's hands
  - Transfers to anything else that is touched
- A single fingerprint deposits ~100 micrograms (100,000 ng) of explosives

Swiping: Sources for Surface Contamination *(cont'd)*

- Deposited explosive mass decreases:
  - With subsequent fingerprints
  - If hands are washed
  - Through careful handling and use of gloves
- The amounts deposited are normally large compared to the detection limits
  - 1 ng or less for state-of-the-art trace chemical sensors

Vapor: How Much is in the Air?



The amount of vapor that will be available for vacuum sampling depends dramatically upon the type of explosive

Summary: Swipe vs. Vacuum Sampling

	Swipe	Vacuum
Sampling apparatus	Cloth swipe with or without wand	"Dust-buster" – type device
Direct physical contact with person or object sampled	Yes	No
Material collected	Adsorbed particles	Vapor and airborne particles
Invasiveness	Higher	Lower
Sensitivity	Usually higher	Usually lower
Key variables that influence amount of material collected	Handling history of explosive material	Type of explosive packaging / wrapping / container Temperature

Trace Chemical Sensors

- Definition: A trace chemical sensor is any chemical detector with the ability to detect and identify microscopic amounts of vapor or particulate contamination.
- Some sensors can detect almost any type of chemical compound
  - While others are more specialized.
- Modes of sampling: Most can accommodate both vacuum and swipe sampling.

Performance Criteria of Trace Chemical Sensors

- Two key performance criteria: Sensitivity and Specificity

1. Sensitivity—What is the smallest mass of a chemical substance that can be detected reliably?
2. Specificity—How good is the sensor at distinguishing compounds of interest (e.g., explosives) from other compounds that are not of interest?

False Positives

- Identification of an innocuous material as a threat compound is called a false positive
- Substantial numbers of false positives in screening applications will lead to operational difficulties and will reduce the usefulness of the sensor
  - Reduced throughput rate
  - Operators lose confidence in sensor
  - Less public acceptance of screening

Types of Trace Chemical Sensors

- Ion Mobility Spectrometer (IMS)—
  - Most widely used sensor for explosives detection
  - Emphasized in this module
- Chemiluminescence Detector
- Electron Capture Detector
- Mass Spectrometer
- Others

Ion Mobility Spectrometer

- IMS can refer either to the detection technique

  (Ion Mobility Spectrometry)

  or to the chemical sensor

  (Ion Mobility Spectrometer)

- Ion mobility spectrometry
  - The most widely exploited trace chemical detection technique for explosives
  - Used to detect other types of compounds, such as narcotics and chemical agents

Ionization in an IMS

- Many explosives form stable negative ions
  - Running an IMS in negative ion mode reduces the number of false positives from background environment
- Ionization source is normally radioactive, usually Ni-63
  - Americium and plasma sources are also used
- A gas in the ionization region produces reactant ions that aid in the ionization process
  - e.g., CH_2Cl_2 to produce Cl^-

Ionization in an IMS *(cont'd)*

- Stable ions collected at the detector plate can be
  - Ions of the parent analyte molecule,
  - A fragment of the parent, or
  - An adduct
- Drift times identify the material based on comparison to spectra of known samples

IMS Summary - Advantages

- High sensitivity
  - Detects one nanogram or less
- Fast
  - Known in < 10 seconds
- Relatively low cost
  - $20,000—$50,000
- Commercial development for many applications

IMS Summary - Disadvantages

- Most systems use a radioactive ionization source
  - May require some regulatory paperwork involved with ownership, use, and transport
- Specificity is adequate for most explosive detection applications
  - Not as good as in some other techniques such as mass spectrometry

Chemiluminescence Detectors

- Identify explosive molecules containing NO_2 (nitro) groups by decomposing the molecules, with conversion of the NO_2 groups to electronically excited NO (NO*) molecules
- Detection occurs via emission of light of characteristic wavelengths from the NO*
- Chemiluminescence by itself cannot distinguish one NO_2 - containing compound from another
- For specificity, separate compounds with a gas chromatograph before they enter the detector

Chemiluminescence Detectors Pros and Cons

Pros

High sensitivity

No radioactive source

Cons

Detects a narrower range of explosives than IMS

Usually costs more ($70K - $150K) than IMS

Less developed for field use

Electron Capture Detectors (ECDs)

- Identify the presence of explosives by exploiting the tendency of many explosives to form stable negative ions
- ECDs draw explosive vapor into a region with a standing current between a cathode and anode
- Electrons attach to the analyte molecules, resulting in a measurable reduction of this standing current

Electron Capture Detectors *(cont'd)*

- Pre-separation of analytes using a gas chromatograph achieves specificity
- Application:
  - In the past widely utilized for explosives detection
  - In recent year use has decreased, as use of IMS has increased

BREAK FOR LUNCH

Mass Spectrometers

- Mass spectrometry (MS) involves
  - Ionization of analyte molecules, and
  - Analysis of the motion of the ions in a magnetic field, thus determining their charge–to-mass ratio
- During the ionization process, several ions are formed in detectable amounts
  - In IMS, only one or two ions are detected
- Lots of information in a mass spectrum gives high specificity

Mass Spectrometers – Pros and Cons

Pros

Excellent specificity

Sensitivity can also be high

Cons

More experimentally complex than IMS—requires high vacuum

More expensive than IMS—typically $70K and up

Less adapted to field applications than IMS

Trace Detection Systems

- Definition:
  - A trace detection system is an integrated device that incorporates a means of sampling trace material and a trace chemical sensor
  - It may also contain a preconcentrator, a device that collects and concentrates trace material before it is delivered to a trace chemical sensor
- Trace detection systems are designed to be useful in one or more real-world applications

Applications of Trace Detection Systems

- Baggage screening
- Mail screening
- Personnel screening
- Screening hand-carried items, e.g., briefcases, laptops
- Vehicle screening
- Analysis of suspicious objects (suspected bombs)
- Other possibilities

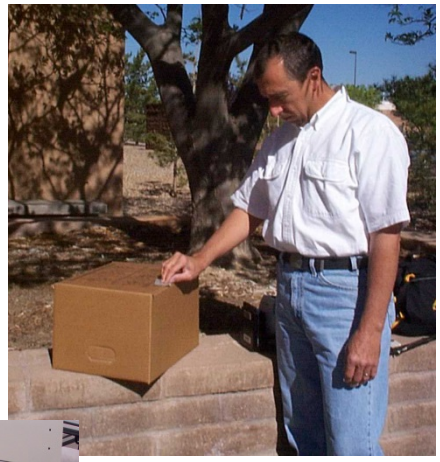
Screening hand-carried items

Screening vehicles

Proper Sampling Technique

- Effective sampling is critical to the success of any trace detection system
- The sampling may be either
  - Manual (e.g., collecting swipes by hand) or
  - Fully automated (e.g., air flow sampling used in portals)

Manual sample collection via swiping



Air nozzles in portal walls “puff” air over subject.

Vents draw in air.

Categorization of Trace Detection Systems

- Systems can be categorized by
  - The type of sensor that is used
  - The size and portability of the system
    - Handheld systems
    - Benchtop systems
    - Personnel portals
    - Other, less common types of systems

Handheld Detection System Characteristics

- Small and lightweight
- IMS systems costs - $20,000 to $40,000
- Usually designed mainly for vapor sampling
  - Swiping can be accommodated
- Suited to applications where mobility is important
  - For example, screening a suspected bomb that cannot be moved or touched

Examples of Handheld Detection Systems

GE IonTrack
VaporTracer

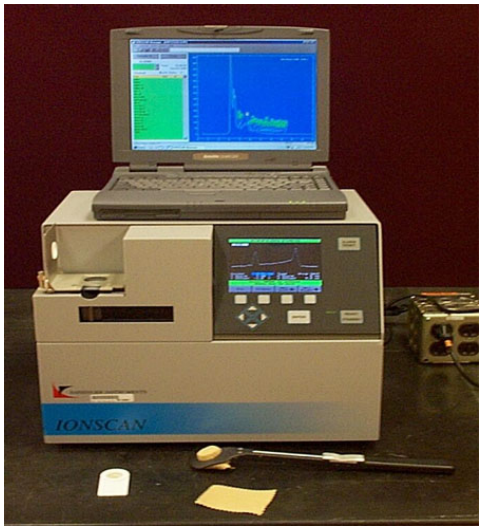
Smiths Detection
Sabre 4000

Scintrex
E-3500

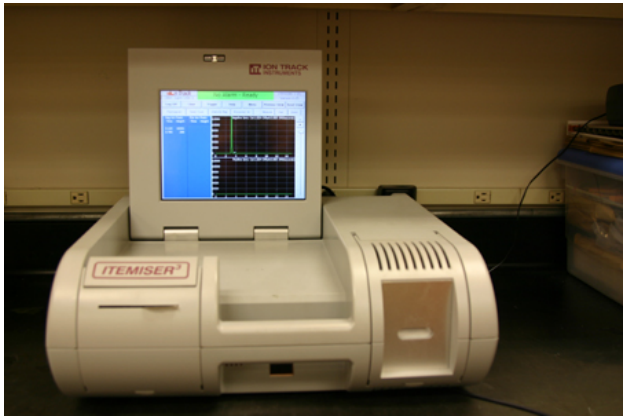
Benchtop System Characteristics

- Too large to be carried easily by a person
  - Typically weigh ~50 to 100 pounds
- Typical cost $40,000 to $75,000
- Designed mainly for swipe sampling
  - Can accommodate vacuum sampling
- Ideal for table top operation at fixed checkpoints
  - Particularly for screening hand-carried items

Examples of Benchtop Systems



Smiths Detection
IonScan 400B



GE IonTrack
Itemiser 3

ThermoDetection
EGIS II

Trace Detection Portals

- Specifically designed for personnel screening
  - Especially in high throughput situations such as airports
- Sample collection utilizes air flows and directed air puffs from nozzles
  - Dislodges particulates
- No physical contact with person screened
- Screening time on the order of 8 to 10 seconds per person
- Cost typically $100,000 to $150,000 per portal

Examples of Trace Detection Portals

Photo courtesy of Smiths Detection

Smiths Detection
Sentinel II
(IMS-based)

Photo courtesy of GE IonTrack

GE IonTrack
EntryScan
(IMS-based)

Syagen Prototype
(mass spectrometer-based)

Trace Detection: Canine

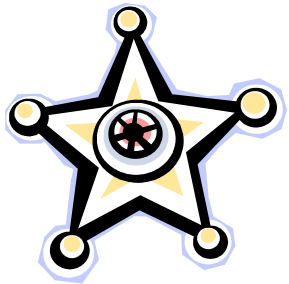
- Method of choice for search applications
  - high mobility and ability to follow scent to its source
- Very fast and sensitive under optimal conditions; can detect any explosive
- Problematic for
  - Long-term, repetitive applications *(dogs become tired)*
  - Screening people (fear of dogs)
- Low purchase cost (~$10,000), but substantial upkeep costs (intensive training)
- Dogs available from a variety of sources

Introduction to Canines

- Canines are a commonly used real-world detection system
  - US Forces have used dogs since WWI
  - Dog's nose is the best vapor sensor
- Canine and handler are a team and are trained as a team
  - Months of initial intensive training
  - Training happens several hours each week
  - Possible yearly certification
  - Switching handlers requires retraining of the team

Canine Breed Selection for Explosives Detection

- Where will the team be working? (i.e., the team's operational environment)
  - Law enforcement, military
  - Public sector
- Will the canine be cross-trained?
  - Dual-use: security, patrol, attack, etc.



Canine Breed for the Public Sector

Photo by Freddie Brasfield

- Labradors, Beagles, Chesapeake Bay Retrievers, and Golden Retrievers are preferred
  - Good social skills
  - Intelligent
  - Strong drive to retrieve
  - Willingness to please

Canine Breed for Military or Law Enforcement

- German Shepherd, Belgian Malinois and Dutch Shepherds are preferred, especially if the canines are cross-trained
  - Intense (very focused)
  - Very intelligent
  - Good work ethic
  - Fast and have a strong bite

Photo by Freddie Brasfield

Attributes of Canine Detection

- Canines have two attributes that man-made explosives detection technologies can not match:
  - They are highly mobile
    - Able to screen cargo, buildings, aircraft, vehicles, etc.
  - They have the ability to follow a scent to its source

General Notes on Canine Detection

In principle, a dog can be trained to detect any type of explosive material. Though, this does not mean that one dog can detect every type of explosive.

- Training on specific materials determines what a canine can detect
- Presently, canines are most often trained to detect 10 to 20 different explosives

Factors that Affect Canine Explosives Detection

- Canine's Training history
  - Dogs detect what they are trained to detect
- Detection Environment

Canine's Training History

- The intrinsic ability of the each individual dog to learn and retain odor knowledge
- Odor generalization
- Time spent training (canine / handler)
- Normal daily work schedule

What the Team Trains On

- The desired amount (or weight range) of explosives that the canine team is expected to detect
  - Should be related to the training amount
- The quality and purity of the training aids
  - Possible cross-contamination of training aids

Photo by Freddie Brasfield

Detection Environment

- Canines perform best under conditions that match their training conditions
  - Temperature effects on working canine
  - Wind
  - Humidity
  - Noise or visual distractions
  - Temperature effects on explosives

Advantages of Canine Detection

- Low purchase cost for the canine
- Mobility
- Follow scent to source
- Very sensitive
- Low nuisance alarm

Disadvantages of Canine Detection

- Biological system
  - Canines need to rest, eat, and sleep (not work 24/7)
  - Can suffer from burn-out
  - Has a working lifetime of 10 to 12 yrs
- Maintenance costs
  - Training costs
  - Housing and veterinarian costs
- Dedicated canine / handler team
  - Canine is only as good as the handler
  - Switching handlers requires retraining

Canine Explosives Detection Summary

- Require appropriate canine breeds for explosives detection
  - Typically are shepherd or retrieving canines
- Canine and handler form a team
- Extensive initial and maintenance training required for the canine team
- Two broad factors influence the canine's detection performance
  - Training
  - Detection environment

Contraband Detection Tools - Bulk Explosives

- Bulk quantities of explosives can be detected by X-ray based systems
  - Examples: dual energy, backscatter, and computed tomography
- They can also be detected using other systems
  - Examples: thermal neutron, pulsed fast neutron, and quadrapole resonance

Photo by Smiths-Heimann

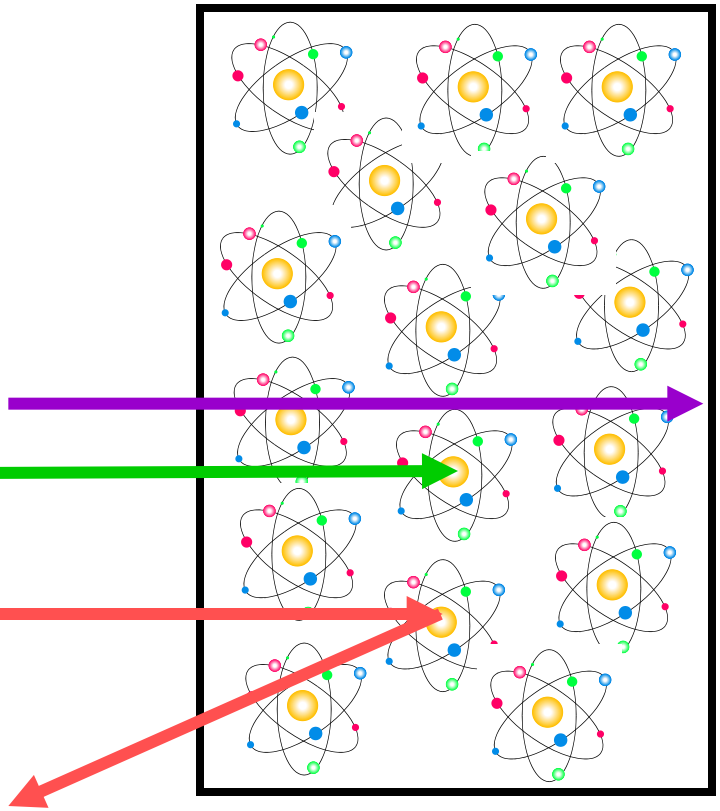
Photo by Ancore

Package Search Systems

- Purpose
  - Detect any contraband contained in packages (weapons, explosives and others)
- Method
  - Active detection using x-ray energy (photons)
    - Backscatter
    - Dual-energy
    - Computed Tomography (CT)

How X-Rays Interact with Matter

- When directed at a subject material, X-rays may:
  - Continue through material (transmission)
  - Be absorbed
  - Be redirected back (Compton backscatter)

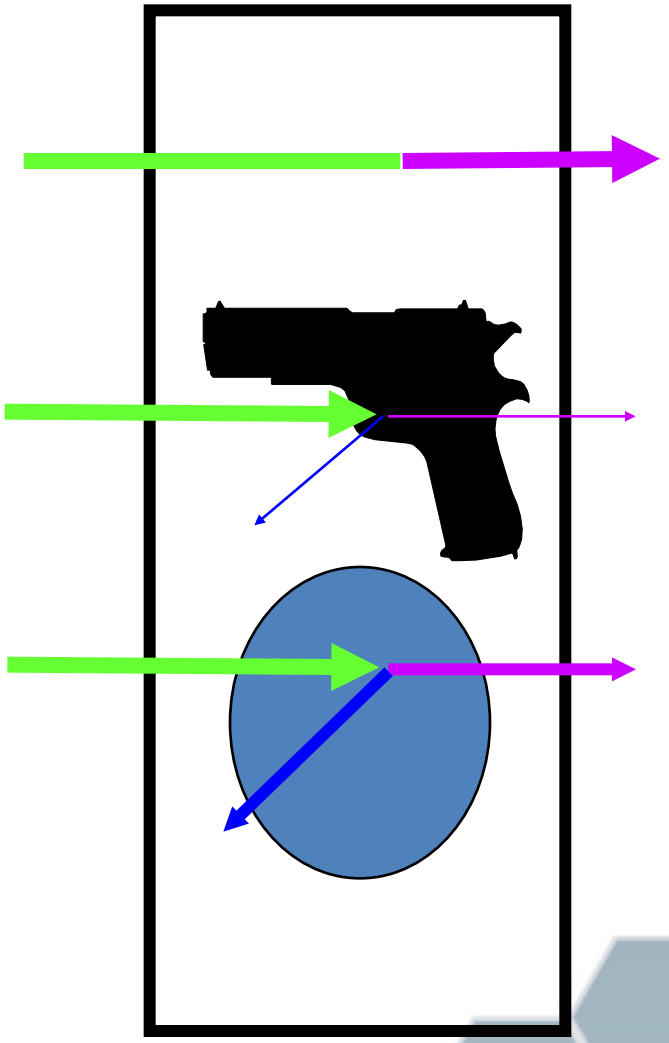


Background Information: Z (Effective Atomic Number)

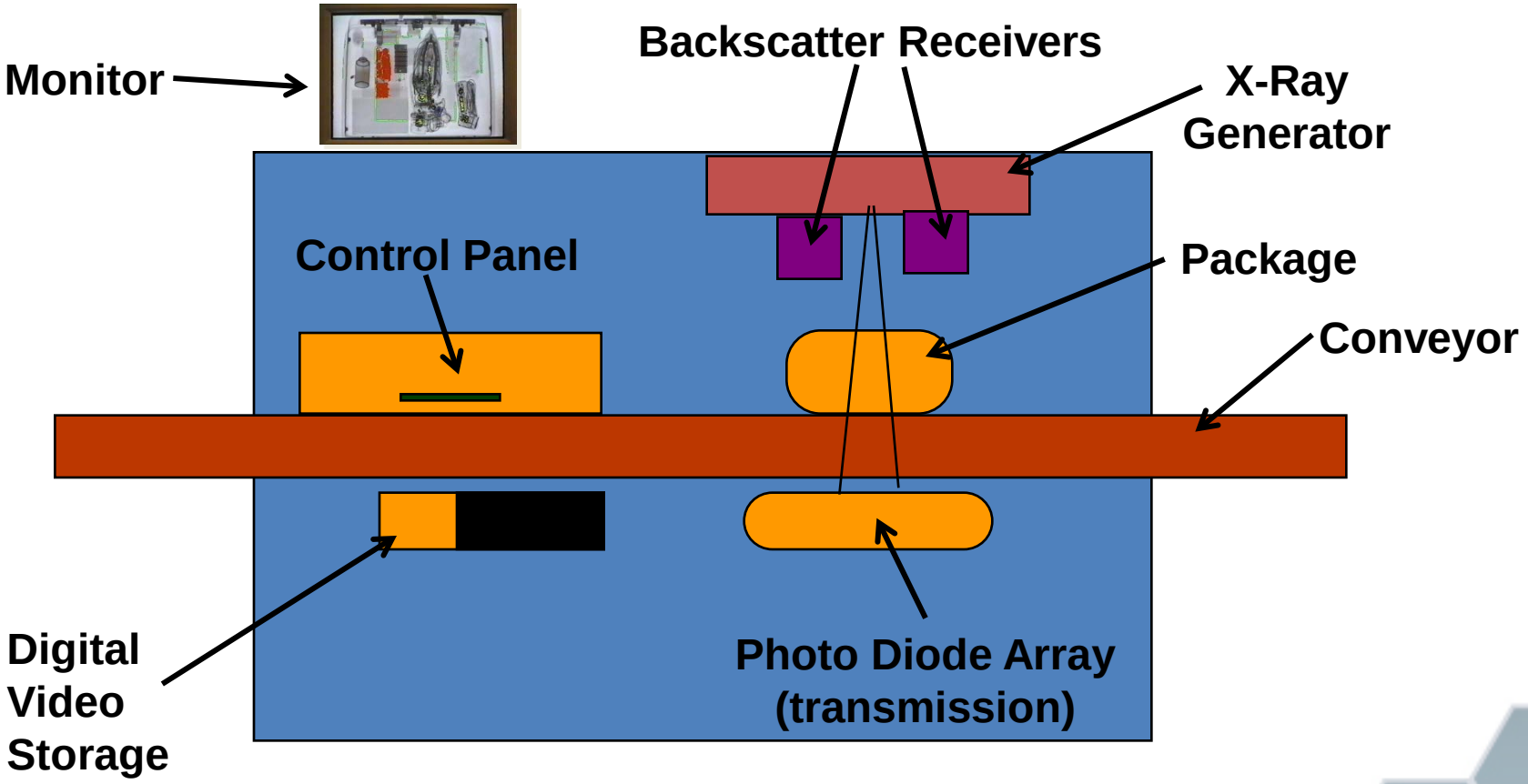
- Techniques used to image low - Z materials
  - Backscatter, dual energy, computer tomography (CT)
  - Low – Z materials composed of elements with low atomic number
  - Low – Z elements include hydrogen, oxygen, carbon
  - Up to aluminum, with Z number 26
- Examples of low – Z contraband
  - Drugs
  - Explosives
  - Some food stuffs

How X rays Interact with Packages

- X ray encounters:
  - Open volume
    - Very high probability of transmission, very low probability of absorption, very low probability of backscatter
  - High-density, high Z material
    - Low probability of transmission, high probability of absorption, low probability of backscatter
  - High-density, low Z material
    - Moderate probability of transmission, moderate probability of absorption, moderate probability of backscatter

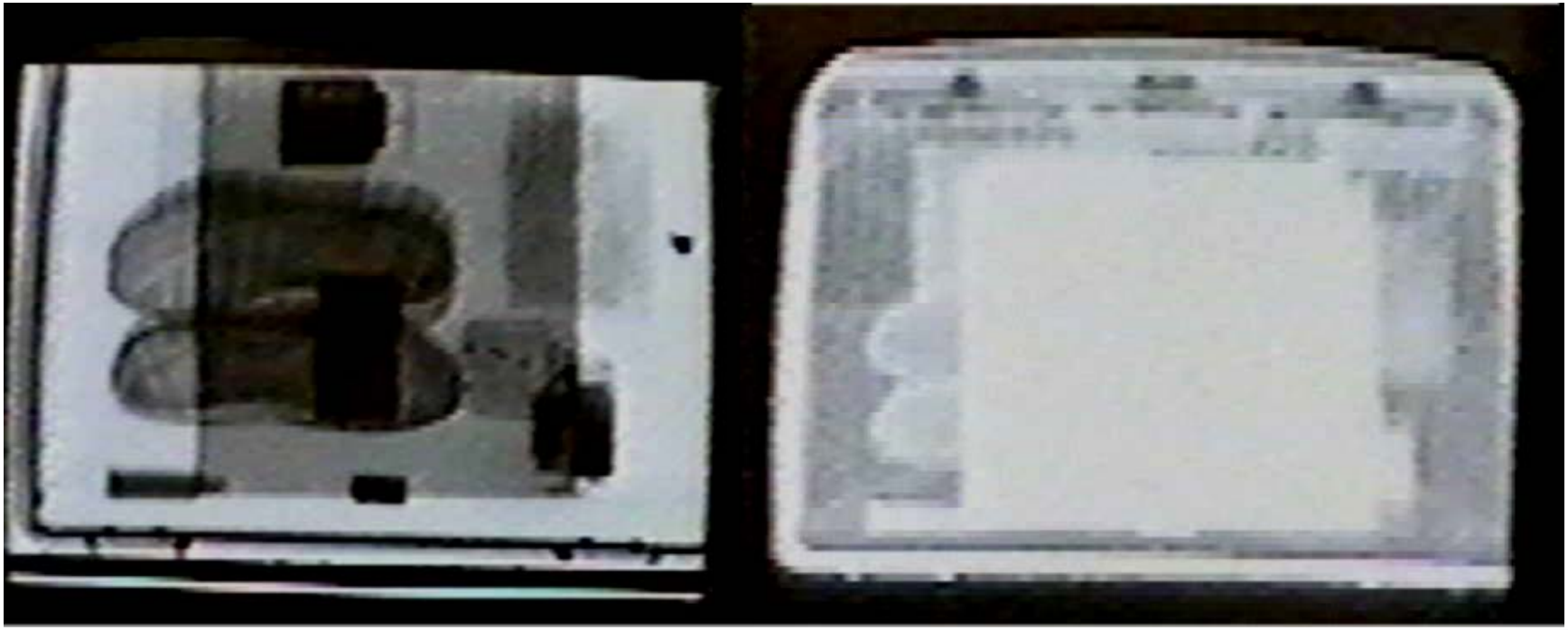


Generic X-Ray Package Search System Layout Transmission and Backscatter

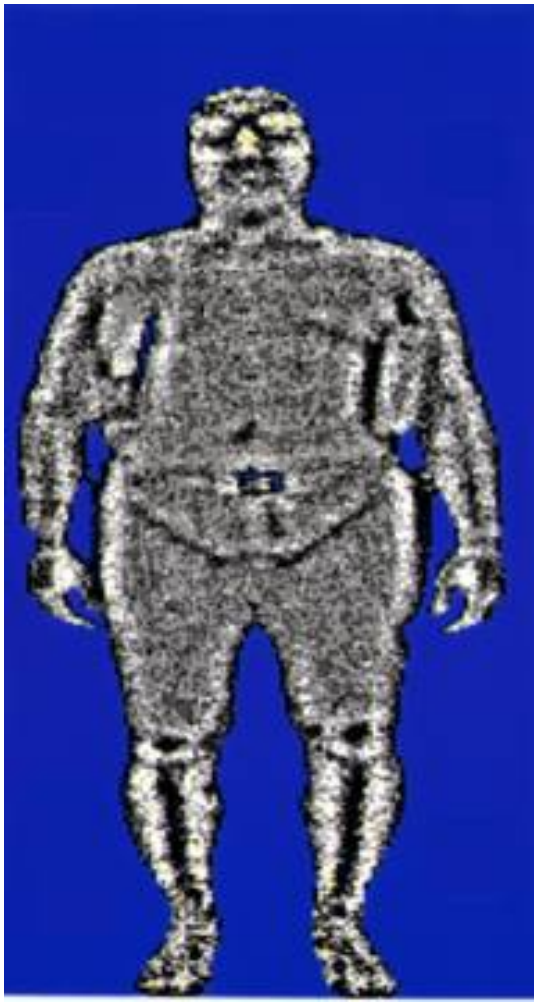


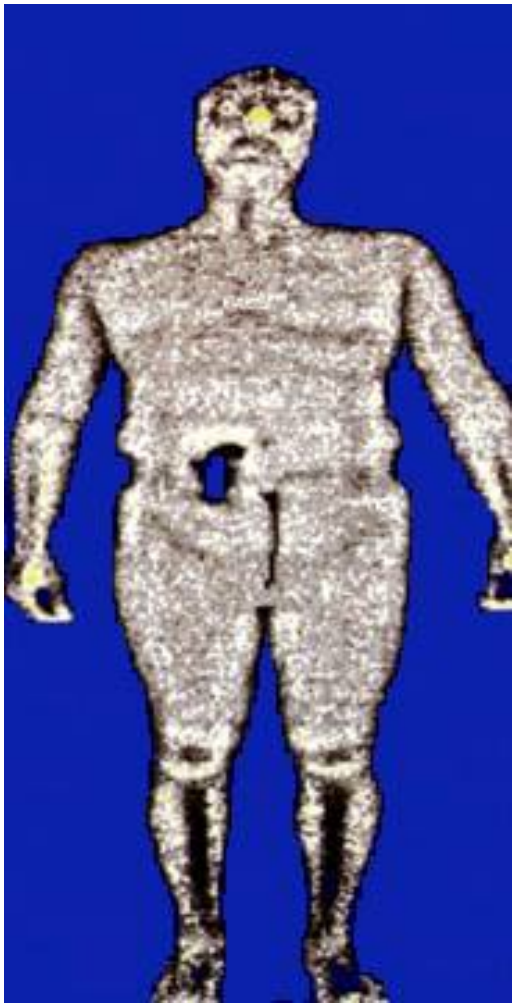
Backscatter Package Search

Transmission **Backscatter**



Backscatter X-ray Scan for Personnel





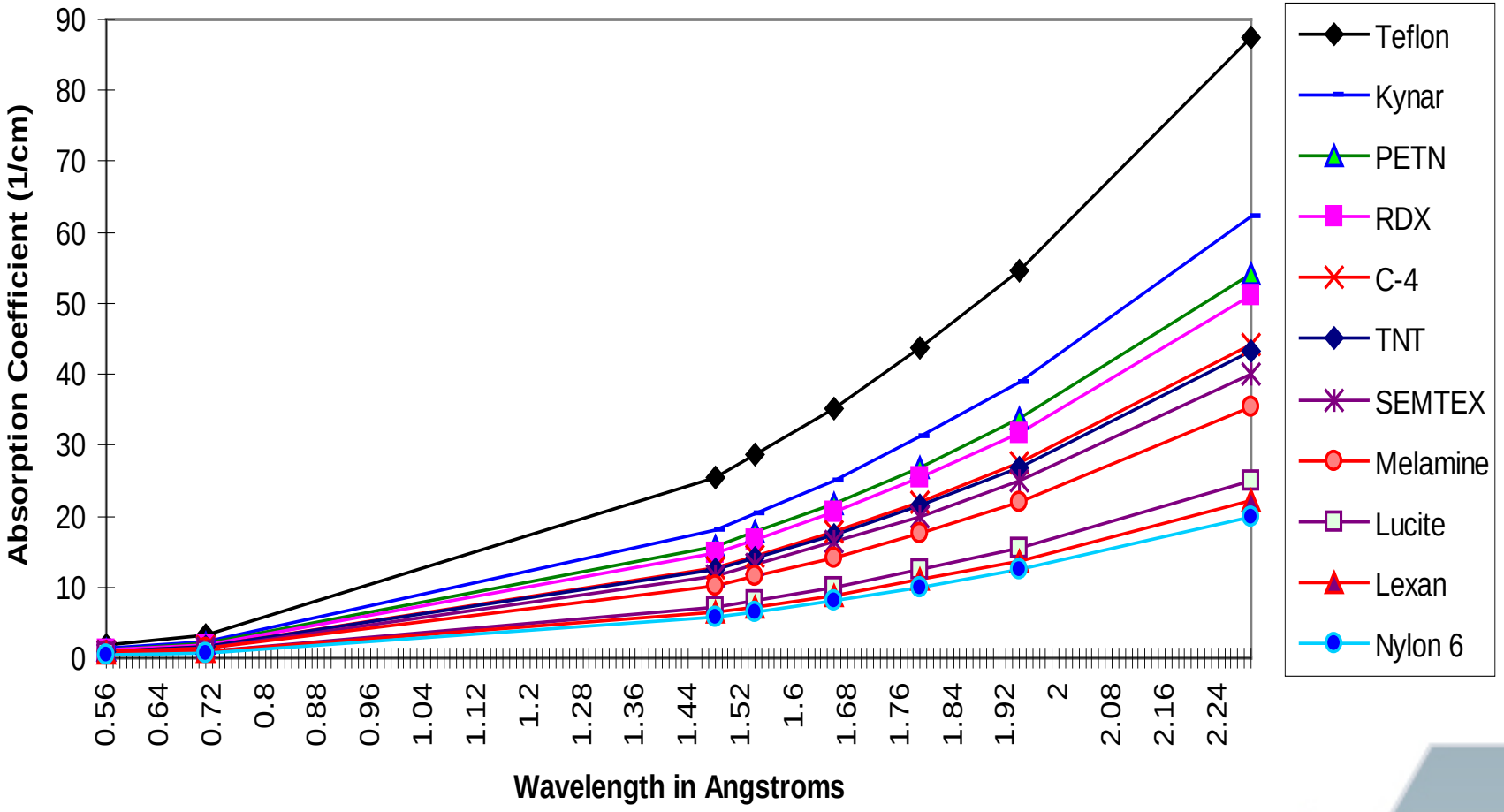
Backscatter System - Advantages

- Ease of use
- Speed of use
- Low – Z imaging
  - Differentiates between low and high Z materials
- Exposure to least radiation dose compared to other X-ray based systems

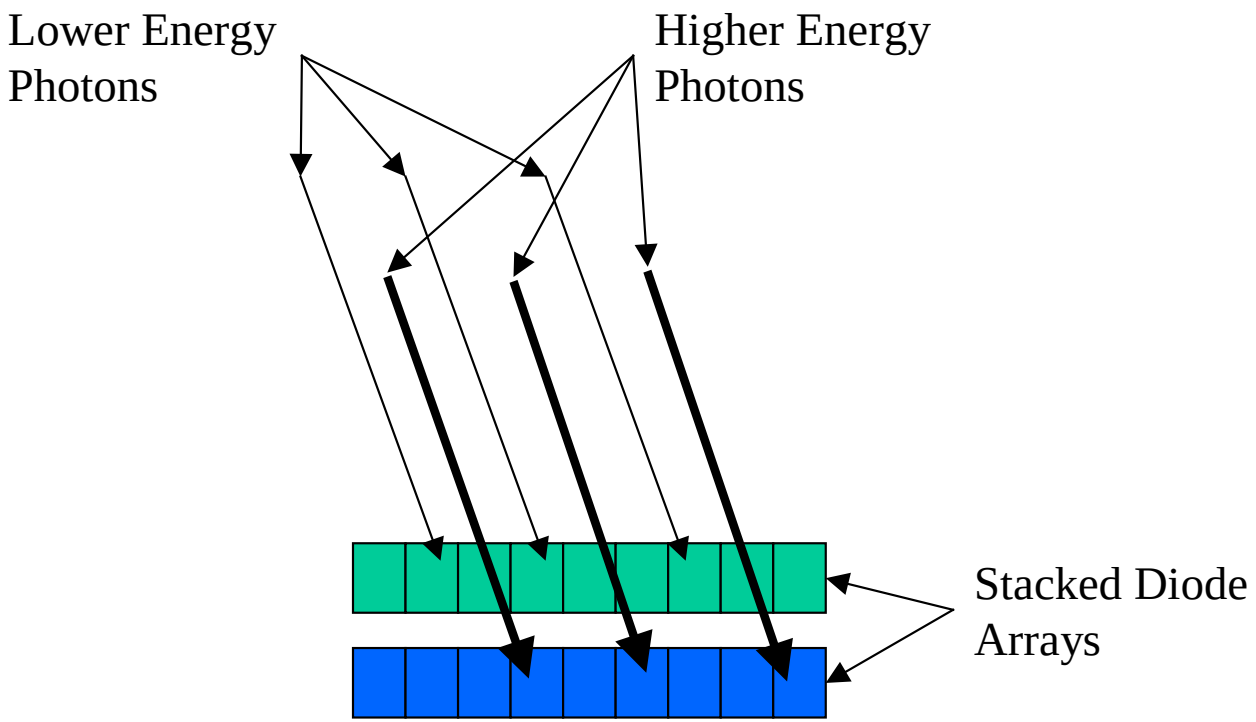
Backscatter System - Disadvantages

- Inability to distinguish between various low – Z materials
- Size
- Cost ($100K)
- Invasion of privacy (personnel)
- Perceived health risk (personnel)

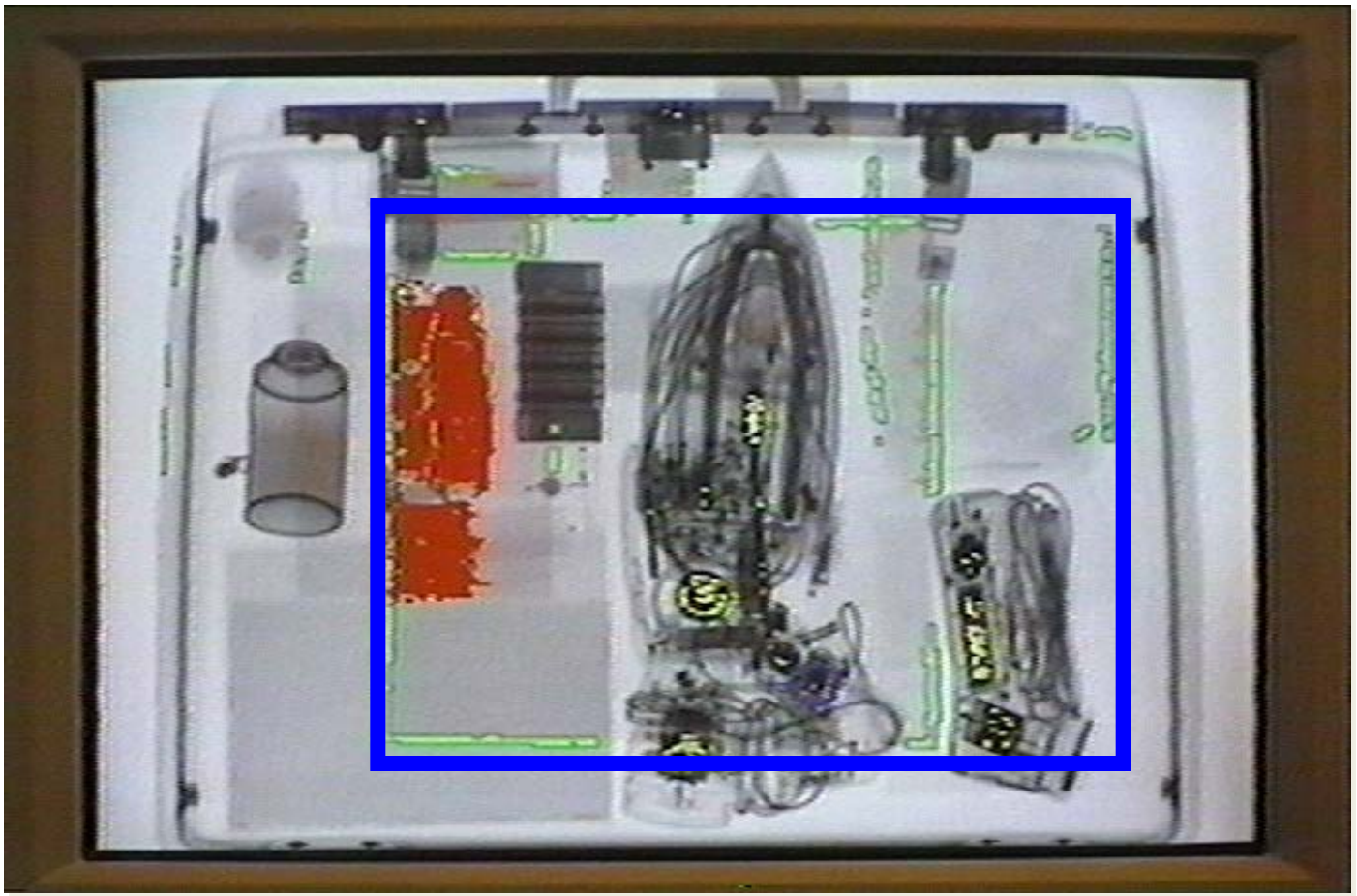
X-Ray Absorption Coefficients of Various Materials as a Function of X-Ray Wavelength



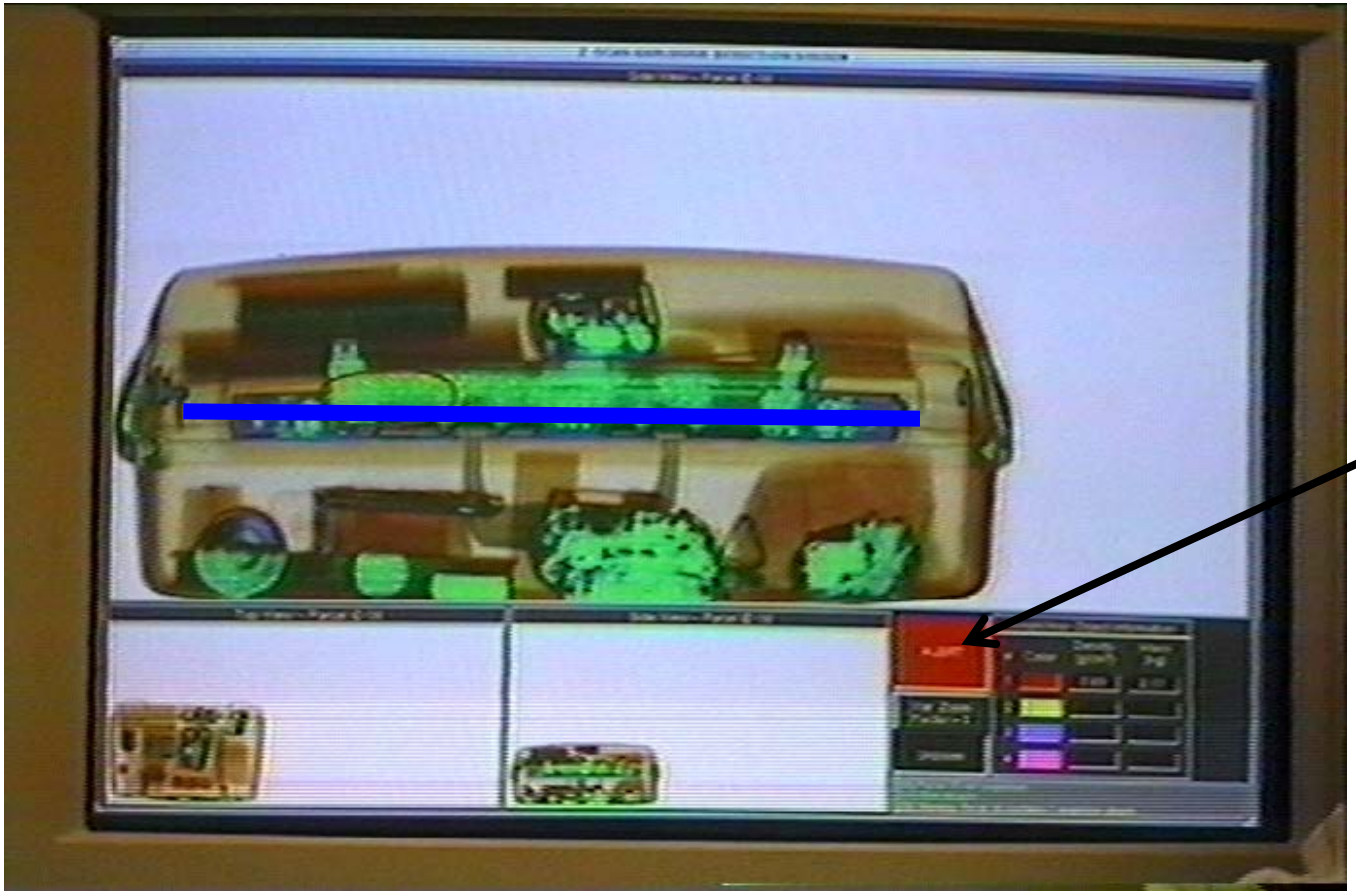
Stacked Array Method for Dual-Energy



Dual Energy Package Search



Dual Energy / Dual Look Angle

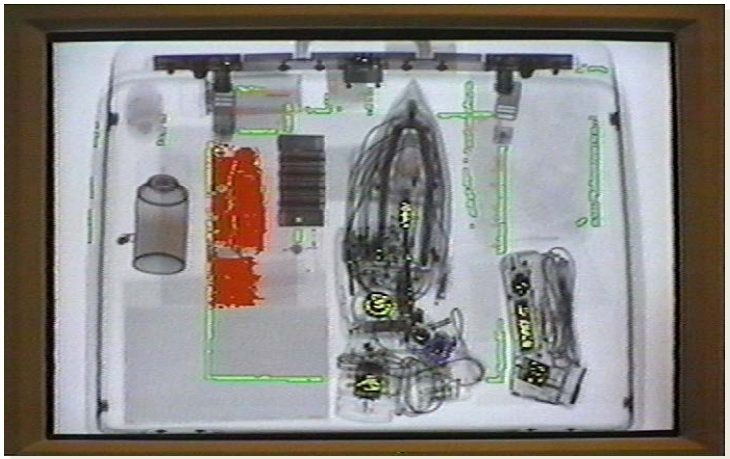


Dual Energy - Advantages

- Relative low cost
- Ease of usage
- Low maintenance
- Can be configured for automated alarm
- Film safe

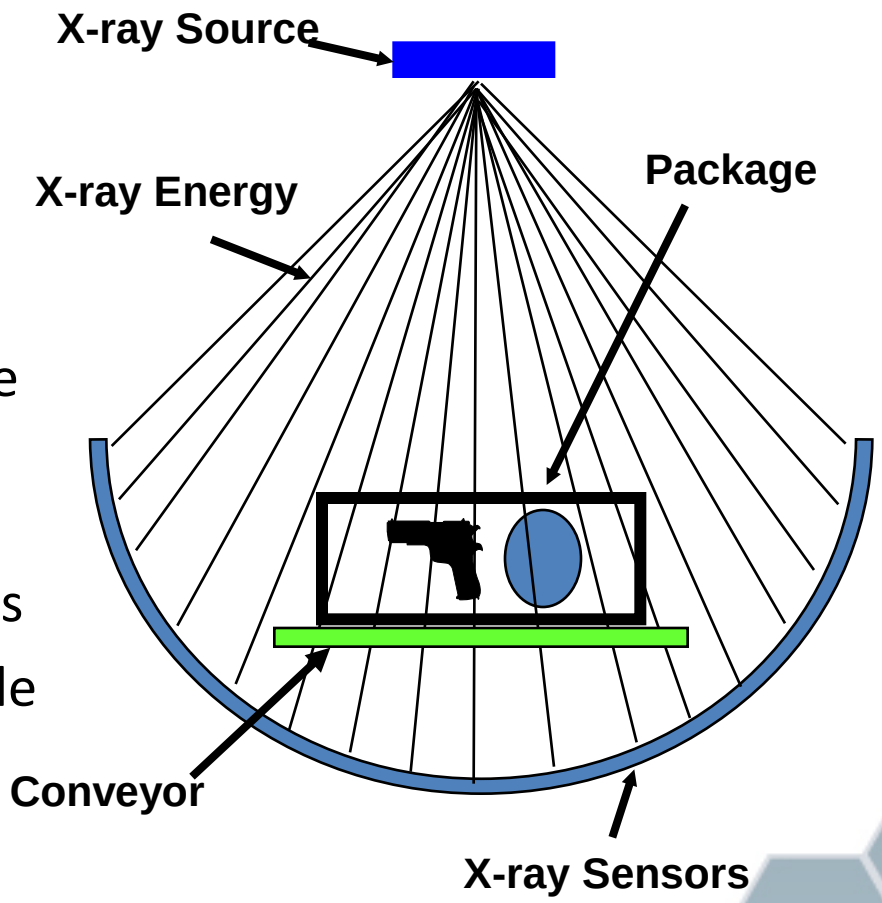
Dual Energy - Disadvantages

- Difficulty with analysis when material are stacked inside package
- Lower detection rate (compared to computed tomography)



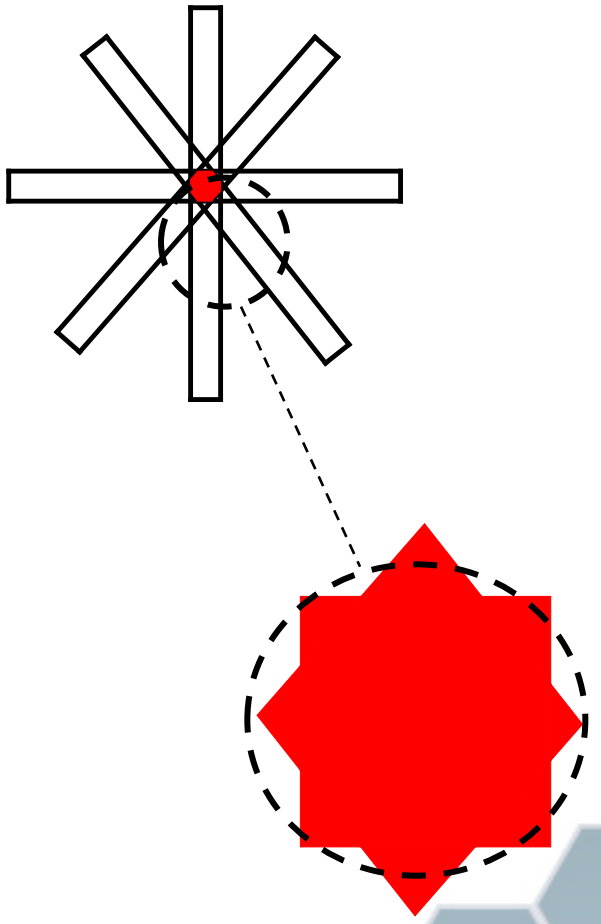
Computed Tomography (CT) Scanner

- The x-ray source and curved sensor array are attached to a spinning platform (gantry)
- The package is passed through the scanner on a conveyor
- As the scanner spins around, the package data are taken constantly
- Data represent many look angles
- Each revolution produces a single “slice”

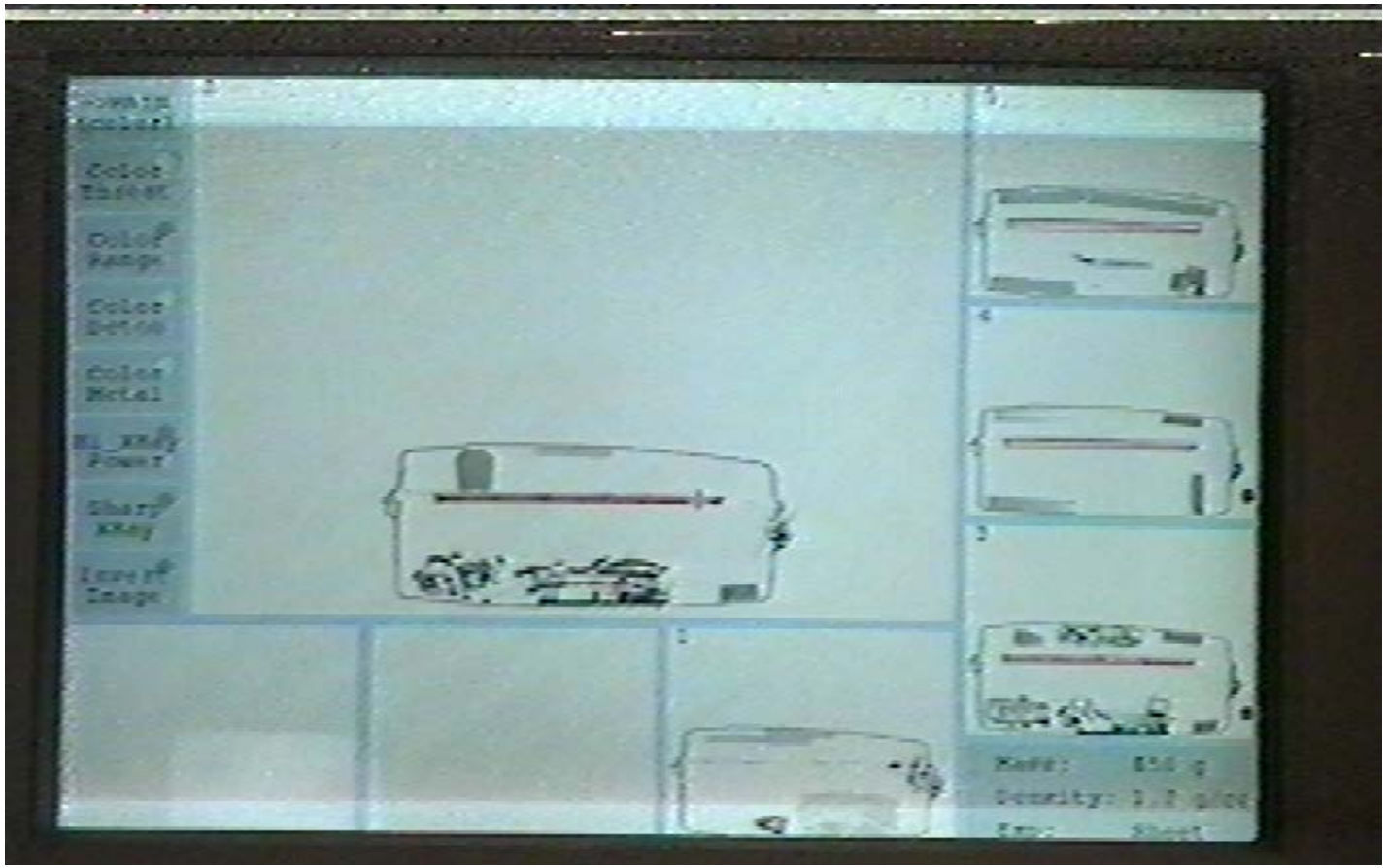


CT Reconstruction

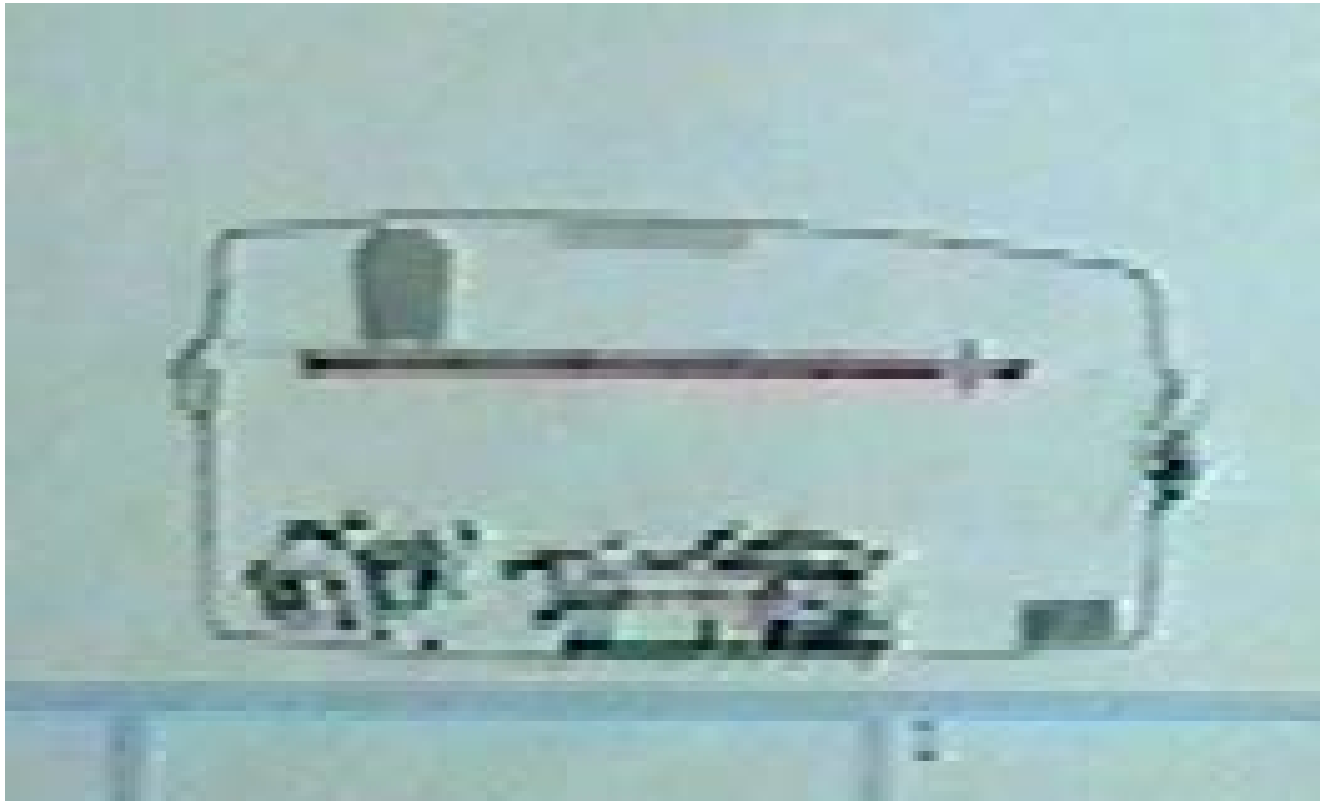
- The diagram at the right represents four look angles through a point in space
- The red area (the cross-section of the look angle beams) is called a voxel
- Density of each voxel is calculated
- Close-up of voxel shows artifacts



CT Alarm Screen Indicating Alarm



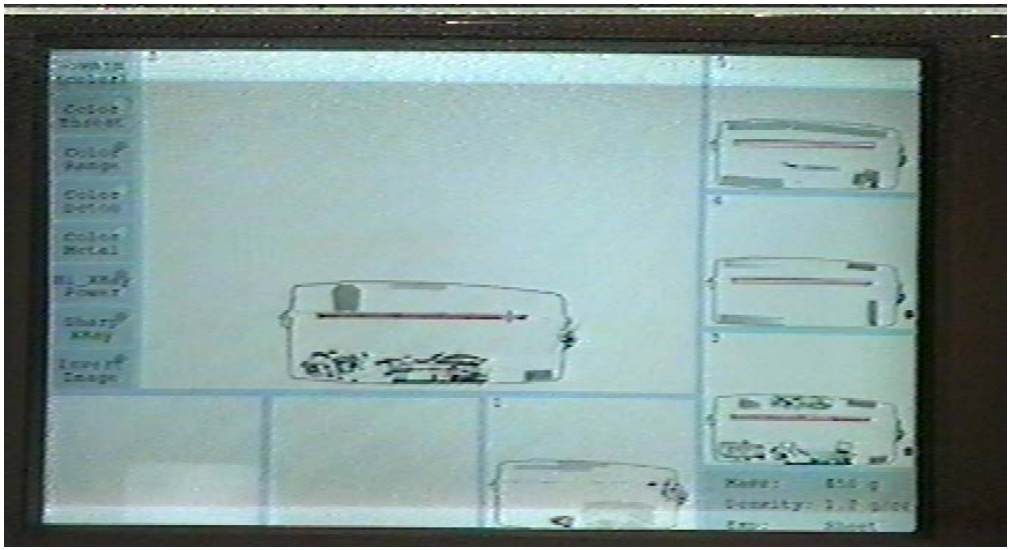
CT Detail of Image



Single Slice with Red Indicating Threat Material

CT Scanner - Advantages

- Best detection rate of all the X-ray systems



CT Scanner - Disadvantages

- Very expensive ($600K - $1M)
- Large size
- Not safe for photographic film
  - Higher X-ray dose
- Can accommodate packages up to the size of a large suitcase
- High maintenance cost

Complementary Systems

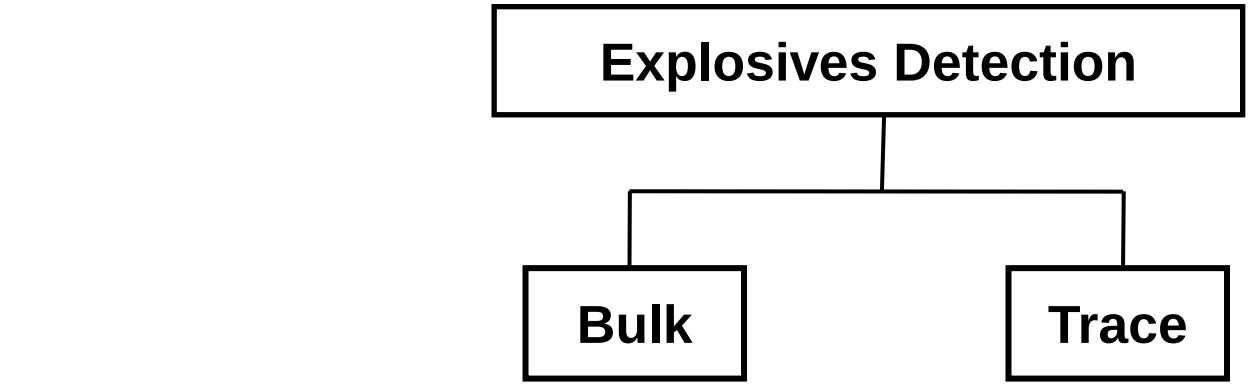
- No single bulk (or trace) system is the best system for all situations
- A combination of techniques in a single system or layered systems may be best approach for the detection of explosives
  - Increase detection rate and decrease nuisance alarms

Summary

- Techniques introduced included:
  - Backscatter
  - Dual-energy
  - Computed Tomography
- A good system integrates complementary techniques

Categories of Explosives Detection

Explosives detection has <u>two</u> broad categories: bulk and trace detection



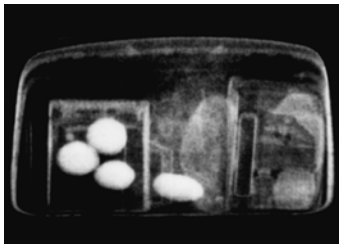
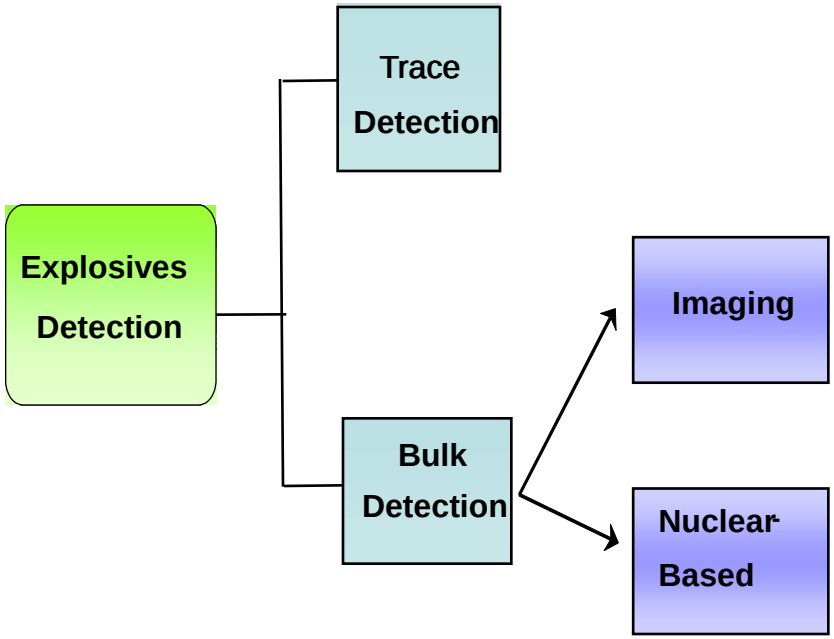


Photo by AS&E

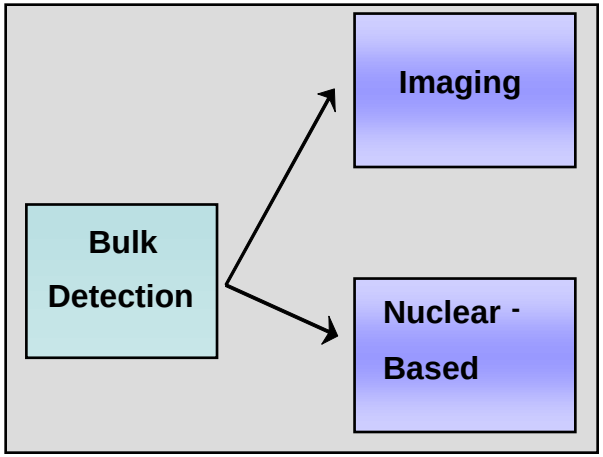
Two Categories of Bulk Explosives Detection

- Imaging Techniques
- Nuclear-based Techniques

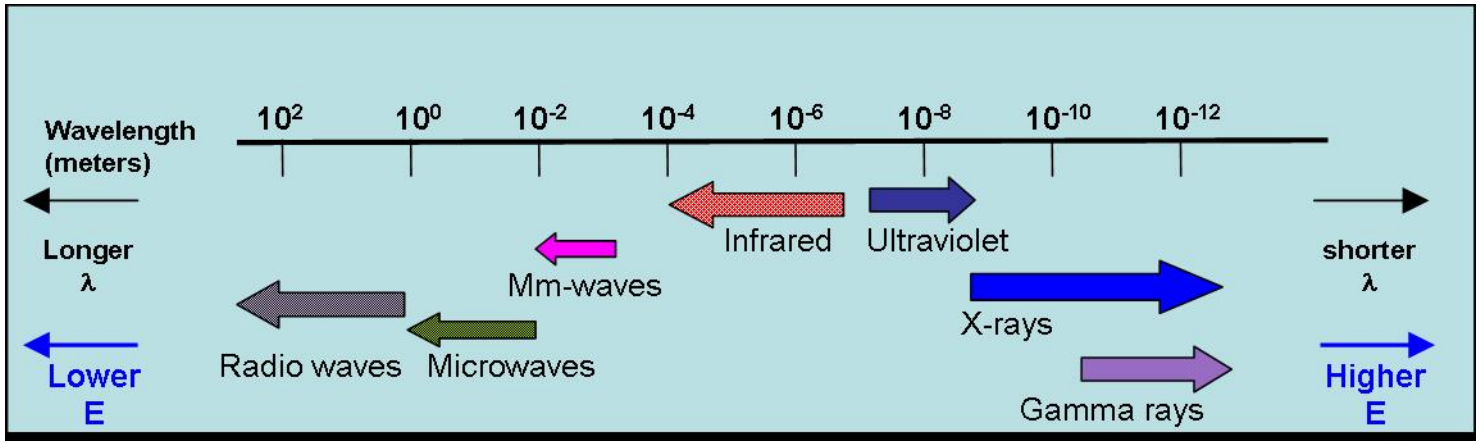


Imaging Techniques

- X-rays (covered in another module)
- Microwaves
- Millimeter waves (mm-wave)

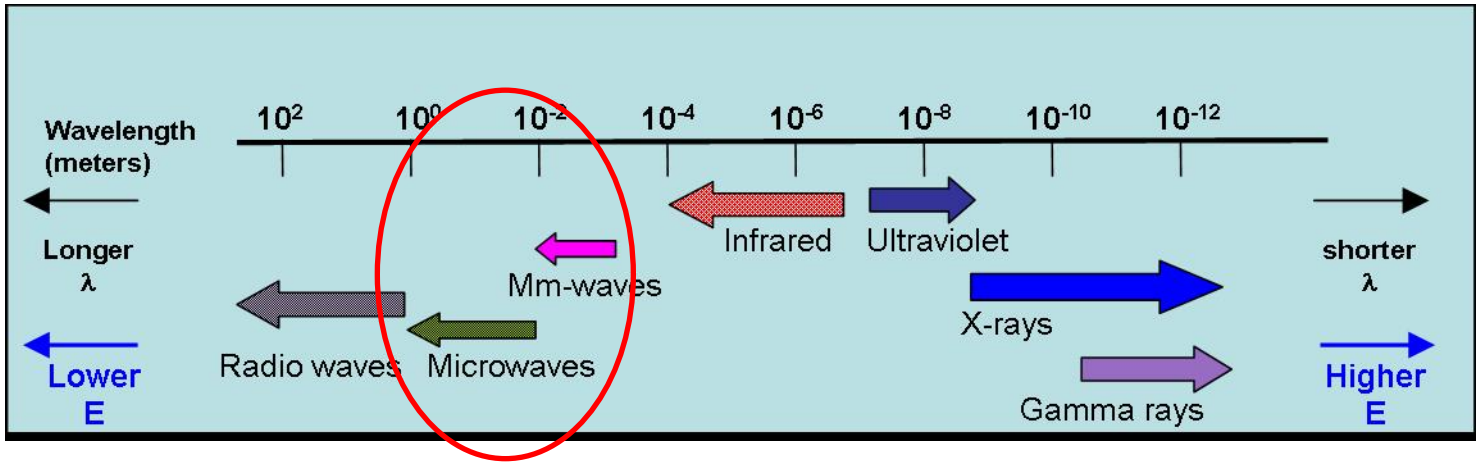


Electromagnetic Spectrum



Microwave Energy Technique

- Dielectrometry is an imaging technique that uses low energy microwaves to determine the dielectric constant of materials on the surface of an item of interest



Dielectrometer

- Dielectrometer is an anomaly detector
- Does not detect explosives directly
  - Objects typically categorized as metallic or dielectric
- No specific anatomic information displayed

Photo by Emit Technologies

Advantages of Dielectrometry

- Safe for humans
  - Non-ionizing and non-cumulative radiation
- Non-invasive and non-contact technique
- Maintains individual's privacy

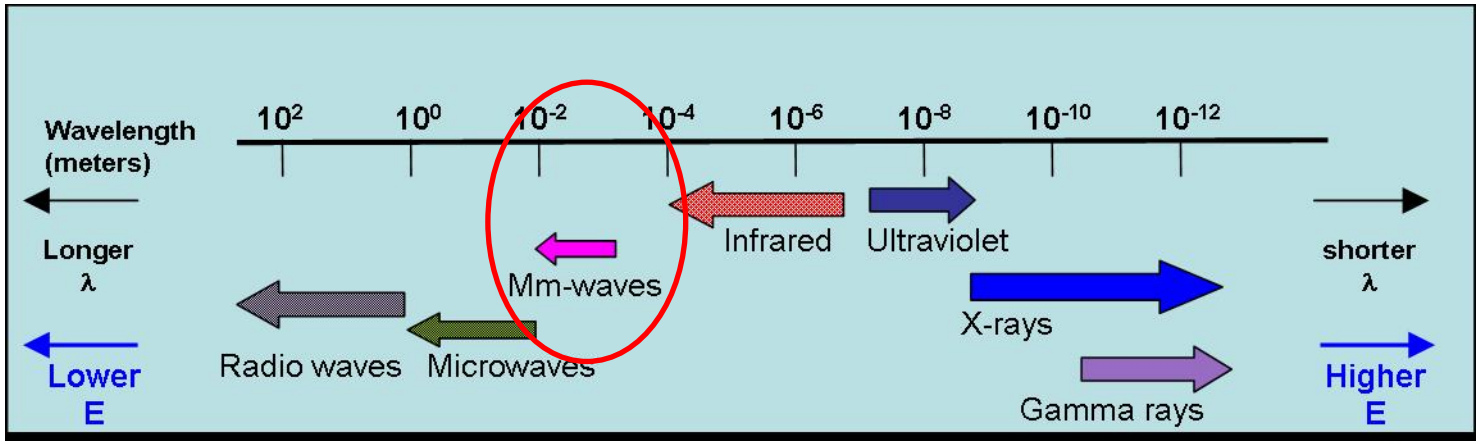
Disadvantages of Dielectrometry

- Anomaly detector
  - Not directly an explosives detector
- Moving parts and enclosure may frighten children and possibly adults (claustrophobics)

Photo by Emit Technologies

Millimeter Wave Techniques

- Passive Millimeter Wave: no interrogating energy and detection of the natural mm-wave emission
- Active Millimeter Wave: mm-wave energy interrogates the target and the emission (interaction) is detected

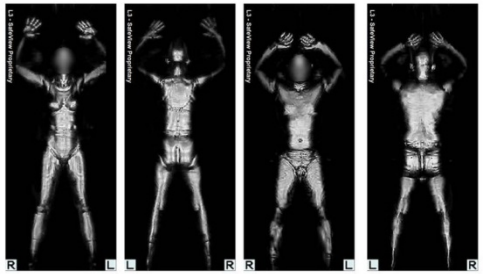


Advantages of Millimeter Wave

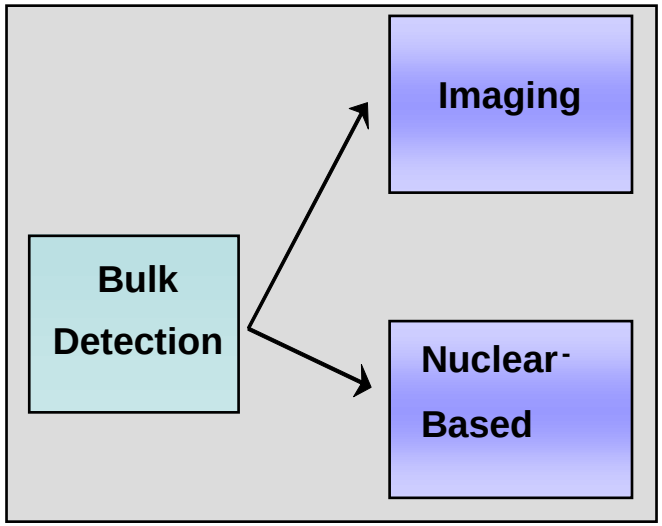
- Potentially can find plastic explosives
- Safe for humans
  - Millimeter wave is non-ionizing radiation
- Reveals objects hidden under clothing
- Many airports have changed software to display alert area on a generic figure. Less invasion of privacy

Disadvantages of Millimeter Wave

- Provides anatomical information
  - Potential for invasion of privacy
- Temperature sensitivity
  - Environmental effects
- Lacks specificity
  - Can't identify chemical composition
- Cost
  - Still being deployed at airports
  - About $170K USD



Nuclear - Based Techniques



- Use radiation to interact with atomic nuclei within the material
- Nuclei of the material emit characteristic radiation that predict the presence of explosives
- More material-specific than imaging techniques for explosives detection

Neutron or Nuclear - Based Technologies

- Thermal Neutron Activation (Analysis) or TNA™
- Fast Neutron Analysis or FNA
- Pulsed Fast Neutron Analysis or PFNA™
- Pulsed Fast and Thermal Neutron Analysis or PFTNA
- Nuclear Quadrupole Resonance or NQR

Comparison of Neutron Techniques

Technique	*Radiation source*	*Probing radiation*	*Detected radiation*	*Elements detected*
TNA	**^{252}Cf or ng[1]**	**Thermal neutrons (0.025 eV)**	**Neutron capture γ[4]**	**N, H**
FNA	**ng**	**Fast neutrons (8 MeV)**	**Scattered γ**	**O, C, (N), (H)**
PFNA	**ng**	**pulsed fast (ns[2]) neutrons**	**Scattered γ**	**O, C, N, H**
PFTNA	**ng**	**Pulsed fast (μs[3]) and thermal neutrons**	**Scattered γ and neutron capture**	**O, C, N, H**

ng[1]: neutron generator
ns[2]: nanosecond (1 x10^{-9} seconds)
μs[3]: microsecond (1 x 10^{-6} seconds)
γ[4]: gamma ray

Gozani; Nucl. Instr. and Method in Phys Res., 2004

TIME FOR A BREAK

Thermal Neutron Activation (TNA™)

Photo by Ancore

Photo by Ancore

- Method based on the nitrogen emission of a 10.8 MeV gamma ray (γ) when exposed to neutrons (n)
- Neutron flux (stream) from:
  - Radioactive isotope (^{252}Cf – Californium)
  - Electronic neutron generator

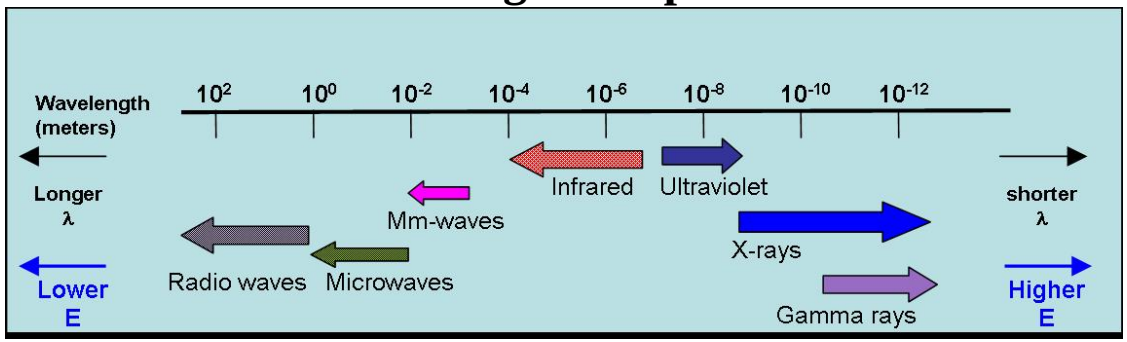
Thermal Neutron Activation (TNA^{TM})

- Nitrogen (^{14}N) absorbs a neutron (n) (neutron capture)
- Excited state (^{15}N*) formed and gamma (γ) ray is emitted

$$^{14}N + n \rightarrow {}^{15}N*$$

$$^{15}N* \rightarrow {}^{15}N + \gamma(10.8MeV)$$

Electromagnetic Spectrum



Advantages of TNA™

- Penetrating nature of neutrons and gamma rays
- High accuracy
- Low nuisance alarm rate

Photo by Ancore

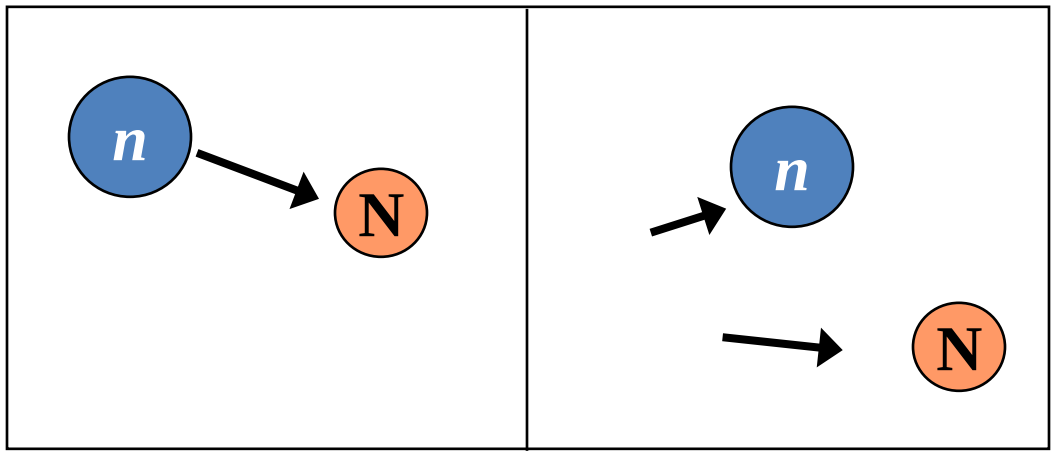
Disadvantages of TNA™

- Not safe for humans
  - Ionizing radiation
- Can't detect all kinds of explosives
- High cost

Photo by Ancore

Fast Neutron Activation (FNA)

- Measures the γ produced from inelastic scattering of continuous n stream
- Fast neutrons travel further and can be used on larger items



Pulsed Fast Neutron Activation (PFNA^{TM})

Photo by Ancore

- Very short (nanosecond) fast neutron (n) pulses
- Utilizes timing information from the neutron pulse and γ detection for 3-D location

Advantages of PFNA™

- Multi-element information obtained (N, O, C)
- Good neutron penetration and useful with very large cargo (transport containers)
- 3-D alarm location information

Disadvantages of PFNA™

- System complexity
  - Size
- High cost
- Not safe for humans
  - Ionizing radiation
- Slow throughput

Photo by Ancore

Pulsed Fast Thermal Neutron Activation (PFTNA)

- Microsecond pulsed fast neutrons with delay for thermal neutron (neutron capture from thermal n)

Photo by SAIC

Advantages of PFTNA

- Obtain information on multiple elements
  - PFNA detection process (O, C)
  - TNA detection process (N)
- Provides more elemental composition than other neutron detection approaches
- After equipment is in place, can have rapid assessment
- Cost - $100K

Disadvantages of PFTNA

- No exact location information
- System complexity
  - Requires training
- Not safe for humans
  - Ionizing radiation

Nuclear Quadrupole Resonance (NQR)

Photo by InVision

- RF spectroscopy method based on nitrogen (^{14}N) quadrupole detection
- Weak emitted RF signal
  - Characteristic energy based on the material and crystal structure

Advantages of NQR

- Safe for humans?
  - No ionizing radiation
- Specific nitrogen based explosive detection

Disadvantages of NQR

- RF signal is weak and can be masked or shielded
- Detects only explosives containing nitrogen
- Emitted RF is weak - detector must have close proximity

System Evaluation

- Right technology for right application
- Nuisance and False Alarm Rate (NAR/FAR) logs
- Alarm resolution procedures
- Detection rate (probability of detection)
- Throughput rate
- Installation / calibration / maintenance
- Performance testing
- Operator interface
- Operator interpretation
- Standards
- Etc.

Summary – Imaging Techniques

- Imaging Techniques (microwave, millimeter wave)
  - Produce image from some bulk property
  - Not direct detection of explosives
  - Safe for humans
    - Non-ionizing radiation
  - Applications are personnel screening and small packages

Photo by Emit Technologies

Nuclear Radiation Detection Systems

- Purpose
  - Detect theft of Special Nuclear Materials (SNM)
  - Discriminate SNM, Radiation Dispersal Devices (RDDs), and accidental contamination from natural, industrial, and medical radiation sources
- Principle of operation
  - Use detected gamma rays and/or neutrons to identify a threat
  - Small distance between the source and detector is important
- Components
  - Radiation detectors
  - Analysis software

Scintillating Gamma-Ray Detectors

- Plastic
  - Can be made very large – widely used for screening
  - Very inexpensive in comparison to other technologies
  - Poor selectivity – detects but does not classify radiation (many false alerts due to radiopharmaceuticals and legitimate industrial radioactive materials)
  - Poor sensitivity to higher energy gamma radiation
- Sodium Iodide (NaI)
  - Smaller but large enough to be usefully sensitive (up to $10 \times 5 \times 40$ cm or $4 \times 2 \times 16$ inch pieces are in common use)
  - Relatively affordable (< $2k each)
  - Good selectivity (can be used reliably for automated identification and classification of radiation sources)
  - Now being preferred for screening in most portal monitors

Solid State Gamma-Ray Detectors

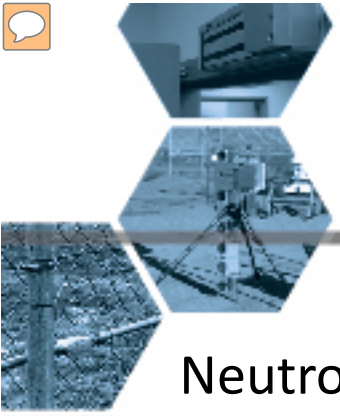
- Cadmium Zinc Telluride (not preferred by most analysts)
  - Does not require cryogenic cooling
  - Somewhat better selectivity (“resolution”) than scintillators such as sodium iodide
  - Very small (typically ~1 cm^3)– low sensitivity and poor efficiency at high energies
  - Not consistent in energy response or peak shape
- High-purity Germanium (often used for secondary analysis)
  - Most expensive – typically $30k - $120k
  - Medium size – typically 100 cm^3
  - Requires cryogenic cooling (typically liquid nitrogen)
  - Best selectivity by far ***– 30 times better than sodium iodide***

Gas Discharge Counters

- ^{3}He or BF_3 — Useful for detecting and locating neutron sources (pulses are in proportion to energy deposition and enable non-neutron noise rejection)

  Neutron capture, detect product ion:

  - $^{3}He + {}^{1}n \rightarrow {}^{3}H + {}^{1}p$, 0.76 MeV
  - $^{10}B + {}^{1}n \rightarrow {}^{7}Li + {}^{4}\alpha$, 2.3 – 2.7 MeV
- Geiger-Muller tubes — Generally used for gamma rays (simple, low-cost, all pulses are the same amplitude)
- Useful for surveying, locating sources, and measuring high dose rates
- Counters only provide a count rate — no energy information, nothing to distinguish “good” from “bad” sources



Neutrons and SNM Detection

Neutrons give some – but not reliable or specific – indication of SNM (specifically, plutonium)

- An increase of neutron count rate over the background rate can indicate Pu-239 (neutrons are primarily from spontaneous fission of an impurity of Pu-240)
- Many RIIDs also carry a neutron detector tube, usually based on He-3, which reacts with slow neutrons only
- However, neutrons are *not* a *specific* indicator of SNM
  - There are many innocent sources of neutrons such as soil density gauges, moisture sensors, and oil well loggers
  - A higher count rate can result simply from moving a RIID closer to a moderating source (heavy person, gasoline or water tank, …) which slows down more of the neutrons
  - False indication of neutrons also often results from energetic gamma rays interacting with the neutron detector material

Examples of Radioactive Isotope Identification Devices (RIID)

Ortec: Detective HPGe, ~$50k

Canberra: InSpector 1000, I2k DSP

SAIC: GR-130, GR-135, GR-460, Radsmart

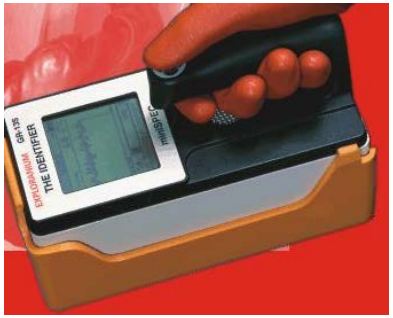
LANL: GN-2, GN-3, GN-5

Berkeley Nucleonics: SAM 935

Biocentric: Quantrad Ranger, Scout

ICx Radiation: IdentiFINDER

Many others



Photos: David Mercer, LANL

Example of a Sodium-Iodide Spectroscopic Portal Monitor in Use

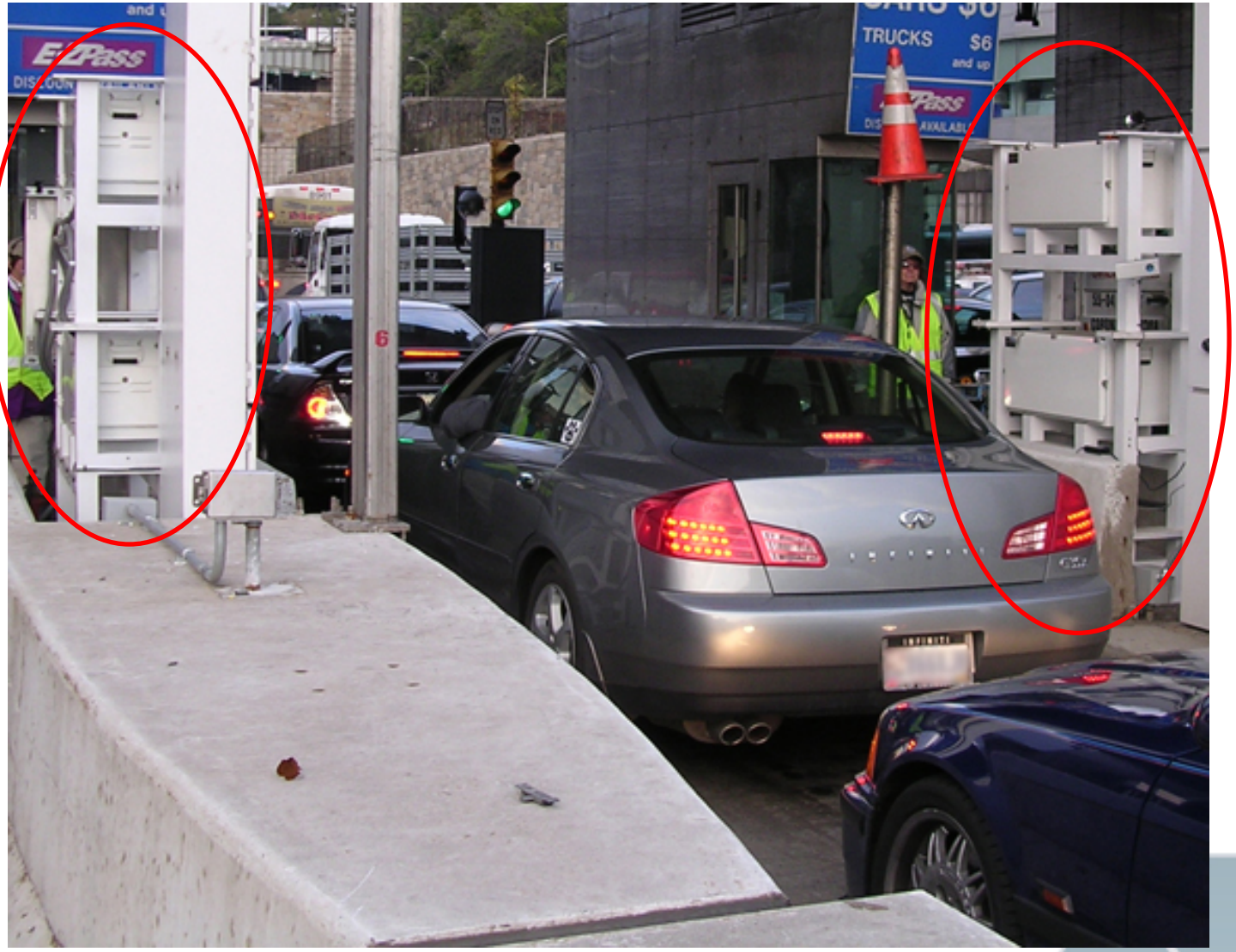


Photo: SNL

Second Line of Defense Project Scope

Typical Activities funded by DOE/NNSA:

- **Radiation detection equipment** and its installation
- Associated **cameras**, Optical Character Recognition (OCR), License Plate Recognition (LPR) technology, Global Positioning Satellite (GPS) and its installation, as appropriate
- **Computer equipment** and associated **communications systems** for Central Alarm Systems and as appropriate National Communication systems that link individual site systems to a central location
- Installation of **equipment** at Regional or National **training centers**
- **Training** in all aspects of system use and **maintenance** for multiple audiences
- Technical **support** assistance
- **Maintenance** and sustainability support

Pedestrian Crossing

Vehicle Inspection

Other Applications

Pedestrian monitor

Rail monitor

Vehicle monitors

Spectroscopic portal monitor

Mobile radiation detection system

Port vehicle monitoring

Straddle container monitoring

Contraband Detection Summary

- Contraband is any object or material prohibited from entry into a security area
- The purpose of contraband detection systems is to detect the presence of contraband on persons and packages in order to prevent the introduction into a security area
- There are three techniques used in contraband detection (1) manual, (2) machine assisted, and (3) automated
- There are a number of tools used for contraband detection

Subgroup 12
Contraband Detection

Subgroup Objectives

After the session, the participants will be able to do the following:

1. Select generic equipment for an effective system to detect contraband.

2. Select generic equipment to detect the following contraband:

    a. Firearms and tools
    b. Explosives
    c. Shielded radioactive material

Exercise 1 - Equipment Selection

Using the data in Table S-1, choose entry control equipment that satisfies the requirements below.

Scenario 1: Screen personnel for contraband dynamite and military grade TNT at two separate entrances of a controlled facility. Total budget for detection equipment cannot exceed $70,000.

Selected Equipment: _____

Reasons: _____

_____

Scenario 2: Inspect luggage at an airport boarding area for concealed C-4 plastic explosive using a vapor sampler. A minimum of 6 items per minute must be inspected to satisfy throughput requirements. Budget is not a major factor.

Selected Equipment: _____

Reasons: _____

_____

Table S–1. Summary of Commercial Trace Explosive Detectors

Instrument	***Smiths Detection Ionscan 400B***	***Smiths Sabre 4000[2]***	***GE MobileTrace[2]***
Detector Type	Ion Mobility Spectrometer	Ion Mobility Spectrometer	Ion Mobility Spectrometer
	Benchtop	Hand held	Hand held
Will detect:			
• Pistol Powder	Yes	Yes	Yes
• Dynamite	Yes	Yes	Yes
• Military TNT	Yes	Yes	Yes
• Semtex[1]	Yes	Yes	Yes
• C-4[1]	Yes	Yes	Yes
• DetaSheet[1]	Yes	Yes	Yes
Analysis Time (sec)	6-8	6-8	6-8
Training Required	Low	Low	Low
Maintenance Required	Low	Moderate	Moderate
Cost ($1000s)	40	28	40
Sensitivity	Very High	Moderate	Moderate

1 - Semtex, C-4, DetaSheet can be detected by swipe only (not by vapor).
2 - These detectors can collect and analyze samples from vapor or swipe collection. Swipe collection is more sensitive and reliable.

Exercise 2 - Equipment Selection

Choose metal detection for entry (weapons screening) equipment that satisfies the requirements below. Refer to Tables S-2 and S-3.

Requirements:

1) **Be able to detect spheres of steel, aluminum, and stainless steel at least 3 cm in diameter carried by a person.**
2) **Allow a minimum of 6 persons per minute to pass through portal.**
3) **Allow minimum sensitivity setting (to minimize false alarms).**
4) **Allow for good detection in all orientations.**

Selected Equipment: _____

Settings: _____

Reasons: _____

_____

_____

Exercise 3 - Equipment Selection

Choose metal detection for exit (CATEGORY 1 screening) equipment that satisfies the requirement below. Refer to Tables S-2 and S-3.

Requirement:	**Be able to detect a sphere of lead 3 cm in diameter carried by a person and is relatively insensitive to object orientation.**

Selected Equipment: _____

Settings: _____

Reasons: _____

_____

_____

Table S–2. Minimum Detectable Sizes of Metal Spheres

Detector	*Sensitivity Setting*	*Minimum Detectable Size (cm)*			
		Carbon Steel	*Aluminum*	*Stainless Steel*	*Lead*
–A–					
	High	2.5	2	2.5	3
Program 1	Medium	3	2.5	3	**
	Low	4	3	4	**
	High	2	2.5	3	**
Program 2	Medium	2.5	3	4.5	**
	Low	3	4	**	**
–B–					
	High	2.5	2	3	5
High Sensitivity Mode	Medium	3	2.5	**	**
	Low	4	3	**	**
	High	3	3	**	**
Discrimination Mode	Medium	4	3.5	**	**
	Low	4.5	4	**	**
–C–					
	High	3	3	4	5
Low Threat Mode	Medium	**	5	**	**
	Low	**	**	**	**
	High	2.5	2	2.5	3
High Threat Mode	Medium	3.5	4	4.5	5
	Low	5	5	**	**

* Samples presented at the center of the metal detector.
** Detector would not detect largest sphere.

Detector A is a programmable digital pulse detector.
Program 1 is optimized for nonferromagnetic metals.
Program 2 is optimized for ferromagnetic metals.

Detectors B and C are nonprogrammable pulse detectors.

Table S–3. Metal Detection Ratio of Most-Sensitive-Orientation to Least-Sensitive-Orientation*

Detector	*Carbon Steel*	*Aluminum*	*Stainless Steel*	*Lead*
–A–				
Program 1	3.2**	1.2	2.0	1.1
Program 2	1.8	1.3	1.9	1.1
–B–				
Both Modes	5.2	1.6	2.2	1.2
–C–				
Low Threat Mode	4.8	2.2	2.4	1.4
High Threat Mode	3.2	1.7	2.4	1.5

* All samples are 10-cm rods, 2.54 cm in diameter. See Figure 9S-1

** Ratio is the detector's response to the most sensitive orientation divided by the least sensitive orientation. Example: for Detector A running Program 1 the response of the detector to the most sensitive (vertical) orientation is 3.2 times greater than its response to the rod in the least sensitive (horizontal) orientation. See Figure 9S-1.

Utilizing the above information, why do detectors respond with greater detection to the two orientations?

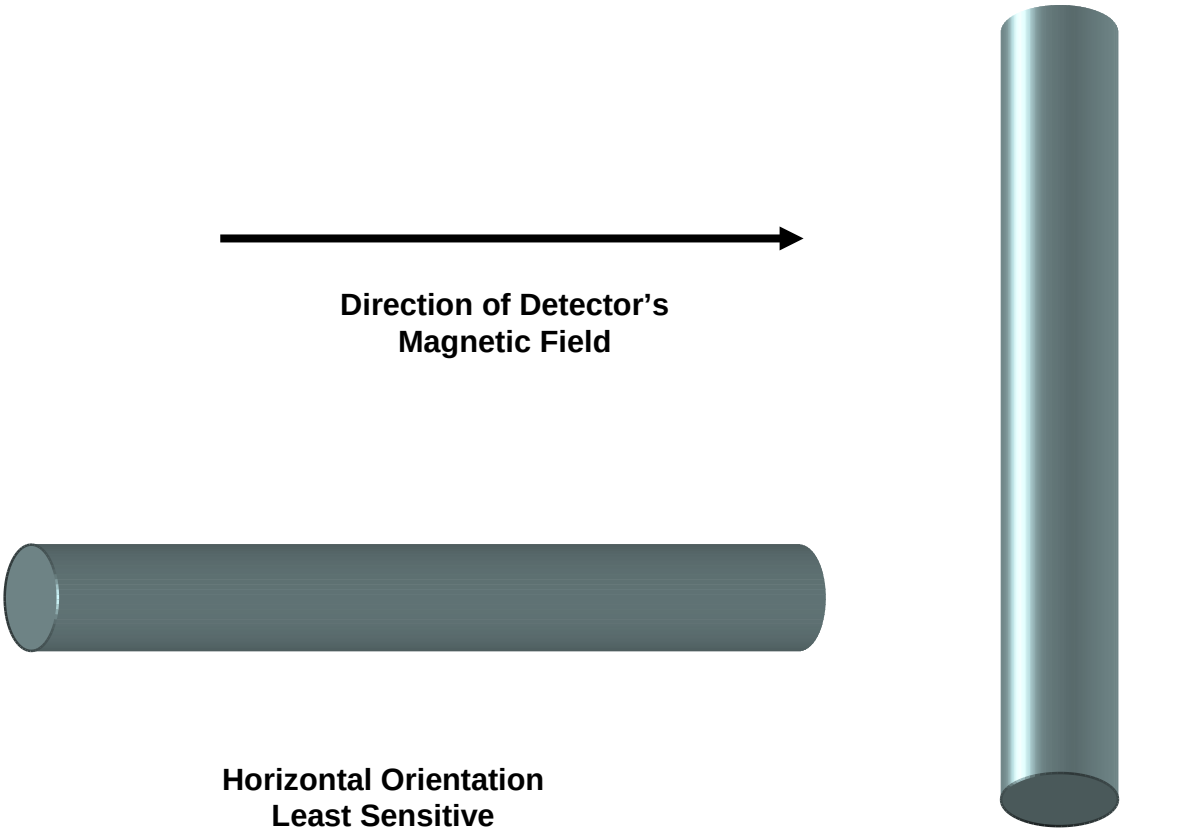


Figure S-1 Rod Orientations for Most Sensitive and Least Sensitive Orientations

Least Sensitive Detector Response Signal = 100
Most Sensitive Detector Response Signal = 320

Metal Detection Ratio of Most-Sensitive to Least-Sensitive

Orientation is 320/100 = 3.2

Application Considerations

Discuss the following application considerations:

1) Swinging metal doors may interfere with entry control devices (e.g., X-ray package search machine and CATEGORY 1 or metal detectors).

2) What problems would be created by a totally automated entry control system (including contraband detection equipment)?

3) What problems do you expect to encounter with an explosives detector system?

4) Why do we need a metal detector at the exit of the facility?

5) Does it matter whether the person is entering or exiting the facility? Should the same kinds of screening (weapons, explosives, CATEGORY 1) take place on entry and exit?

6) How much floor space will the contraband detection system require? How big does the screening room need to be?

7) Is the person performing the screening detection, delay, or response? What can be done to protect screeners?

Access Delay

Learning Objectives

After completing this module, you should be able to:

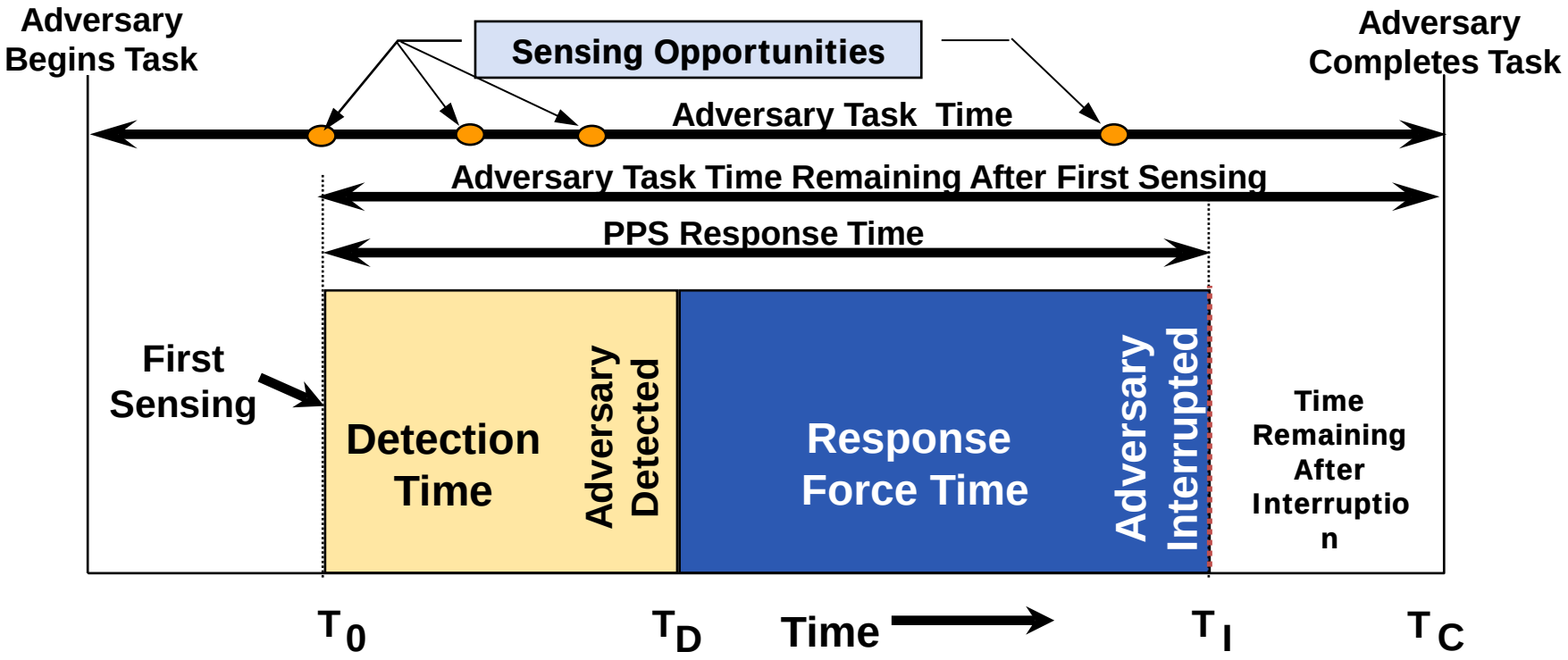
- Define access delay
- Identify the role of access delay systems
- List three characteristics of a good barrier system design
- Distinguish between passive and active delay
- Identify potential adversary tools and methods of attack against delay elements

Access Delay Definition

Access Delay: The elements designed to slow down an adversary, after they have been detected, by use of fixed barriers, dispensable barriers, or responders

- Delay is effective only after detection with assessment that initiates the response

Role of Access Delay



Role of Access Delay

- System detection and response time must be less than adversary task time after first alarm
- To increase system success probability
  - Detect intrusion earlier
  - Reduce assessment time
  - Reduce response time
  - **Increase adversary task time**

Module focus

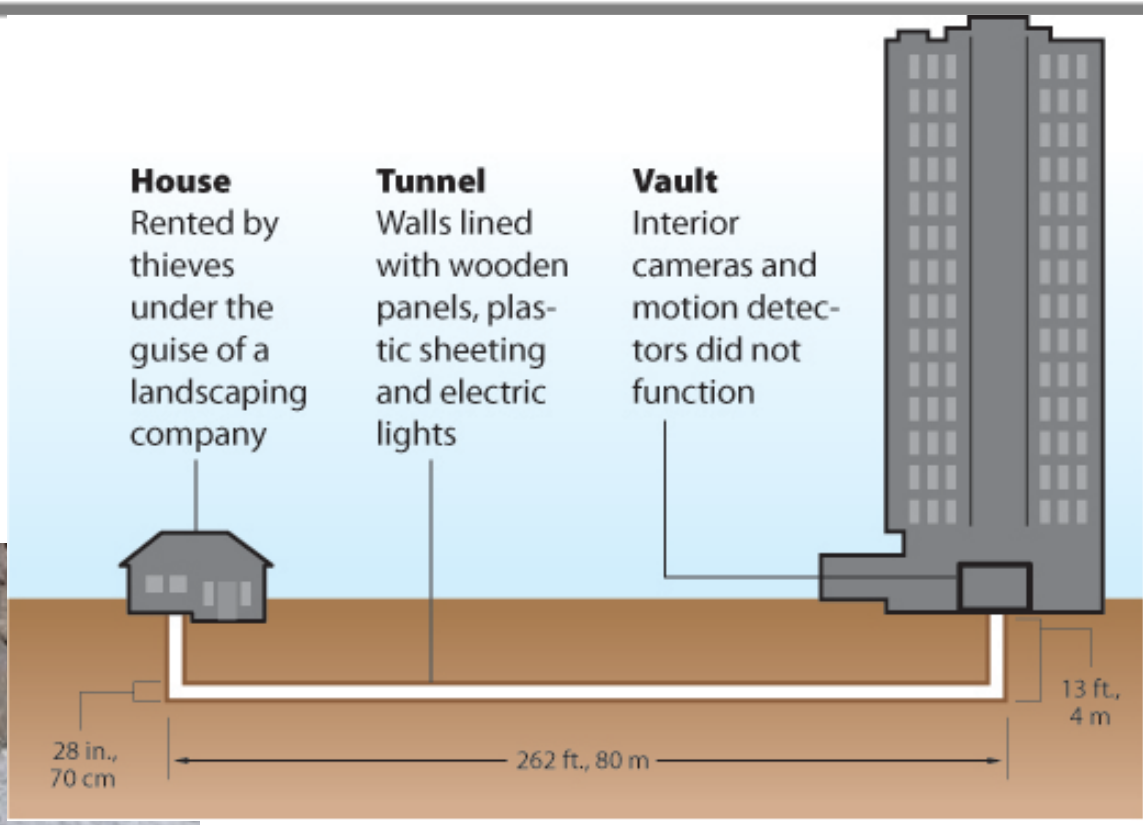
Access Delay Concepts

- Provide delay after detection (No credit for delay before detection)
- Long delay times are difficult and costly
- Need enough delay for response force to win
- Must accommodate operational requirements
- Balance delay, analyze all paths and all attacks
- Multiple different sequential barriers, with greatest delay at the target
- Force adversary to perform sequential operations
- Minimize adversary work area
- Create difficult working environment for adversary
- Intimate containment

Access Delay Concepts, *cont'd*

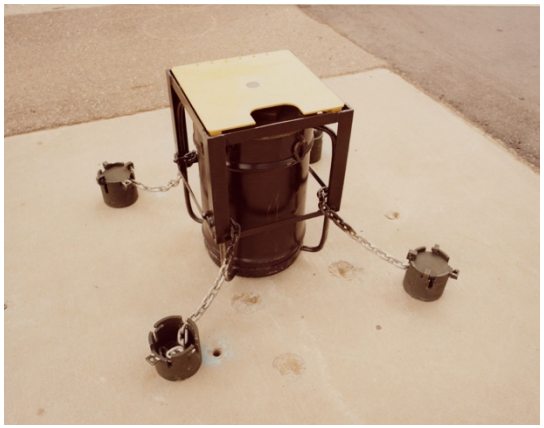
- Concealed delay features
- Synergistic (working together) delay features
- Combination of active and passive features
- Limit adversaries' use of vehicles
- Design a penalty into the parts
- Consider insider issues in the design, use 2-person control
- Optimize response force effectiveness
- Consider recapture issues in the design
- Robust design for changing threats
- Design for maximum credible threat
- Analyze and test against realistic adversary threat capability
- Any barrier can be breached given enough time

Recent Attack Example



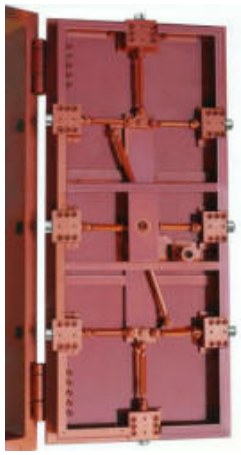
Characteristics of a Good Barrier System

- Provides delay immediately after detection
- Exhibits balanced design; no weak links
- Uses delay-in-depth



Passive vs. Active Delay (Examples)

- Passive delay examples
  - Physical fixed barriers – vehicle and personnel
  - Hardened walls, floors, and doors
- Active delay examples – requires electronics to activate
  - Dispensables
    - Obscurants
    - Irritants
    - Foams
  - Active barriers
    - Pop-up vehicle barriers



Three Elements of Access Delay

Fixed Barriers

- In place, fail secure
- Commercially available
- Weak against explosives
- Aesthetic limits

Dispensable Barriers

- Compact, rapidly deployed
- Maximize delay at target
- Somewhat threat independent
- Safety concerns

Response Force

- Flexible
- Sensitive to numbers
- Subject to compromise
- Continuous operational costs

Effective Access Delay Systems

Response Force as Delay Element

- Presence of guards / RF members increase task time (but not necessarily delay) for adversary using stealth or covert tactics
- Guards / RF members provide minimal delay to adversary, unless in nearby protected positions
- Superior adversary numbers, tactics, and equipment can overwhelm guards / RF members

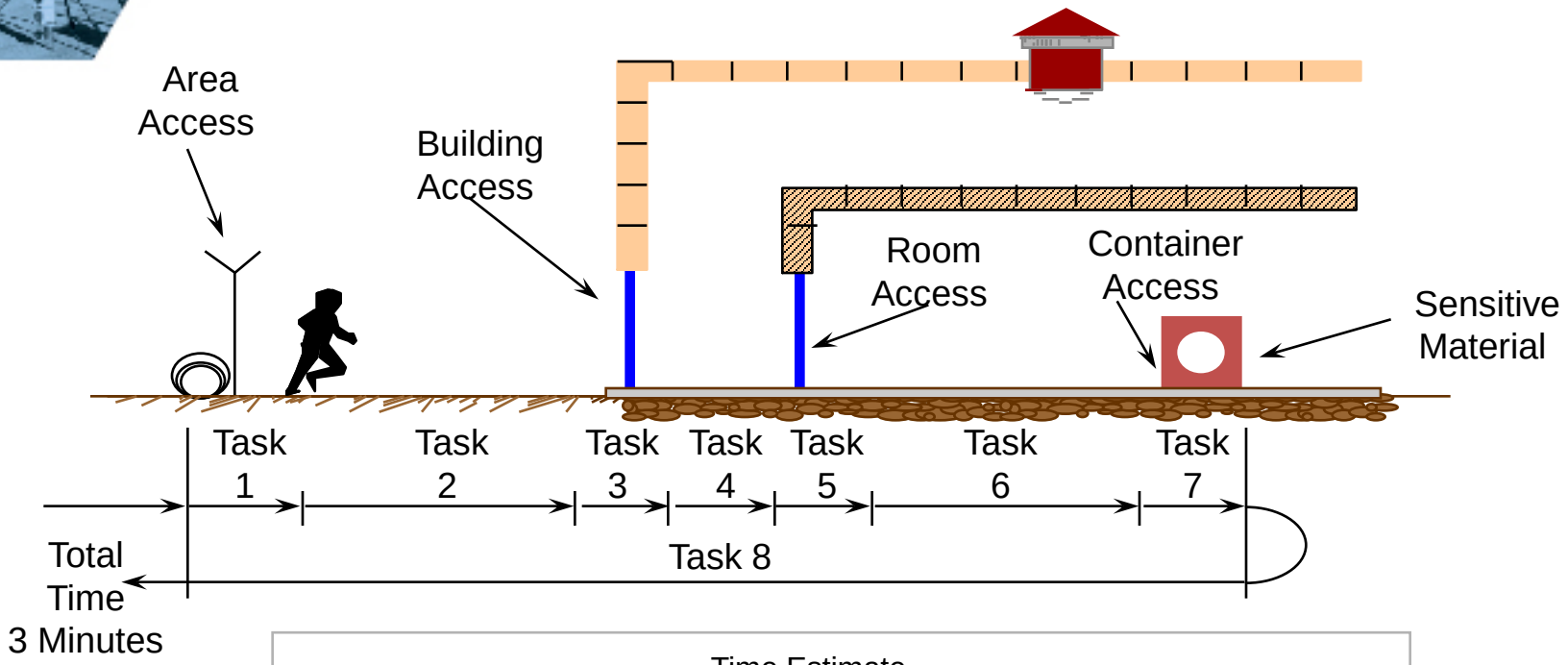
Aspects of Barrier Penetration

- **Penetration** — When an intruder can pass through, over, under, or around a barrier
- Penetration delay times depend on type of attack, adversary skills, location of the attack, and tools used
  - Delay values presented in this section are representative
- Multiple different barriers can extend penetration times

Some Possible Tools of an Adversary

Possible Tool of an Adversary

Example of Forcible Entry

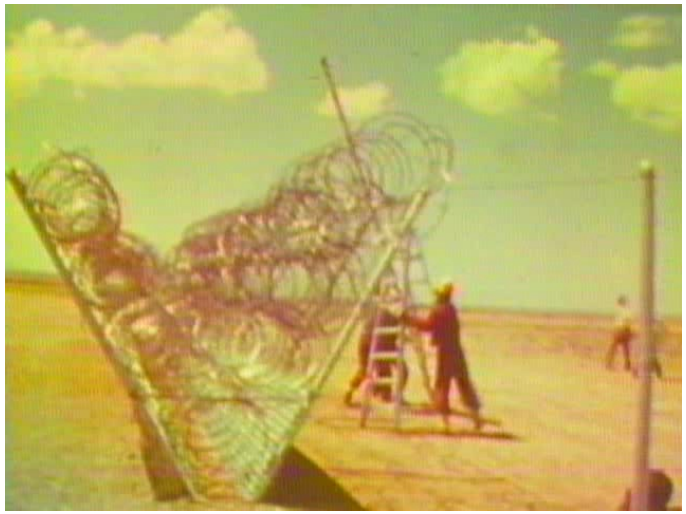


Time Estimate

Task	Mean Time (seconds)	Cumulative Time (seconds)	Task Description
1	12	12	Climb over fence
2	12	24	Run 76 m
3	48	72	Force door
4	24	96	Walk 45 m
5	12	108	Cut lock
6	06	114	Walk to container
7	12	126	Open container and gather material
8	54	180	Escape
	180		Total (approx. 3 minutes)

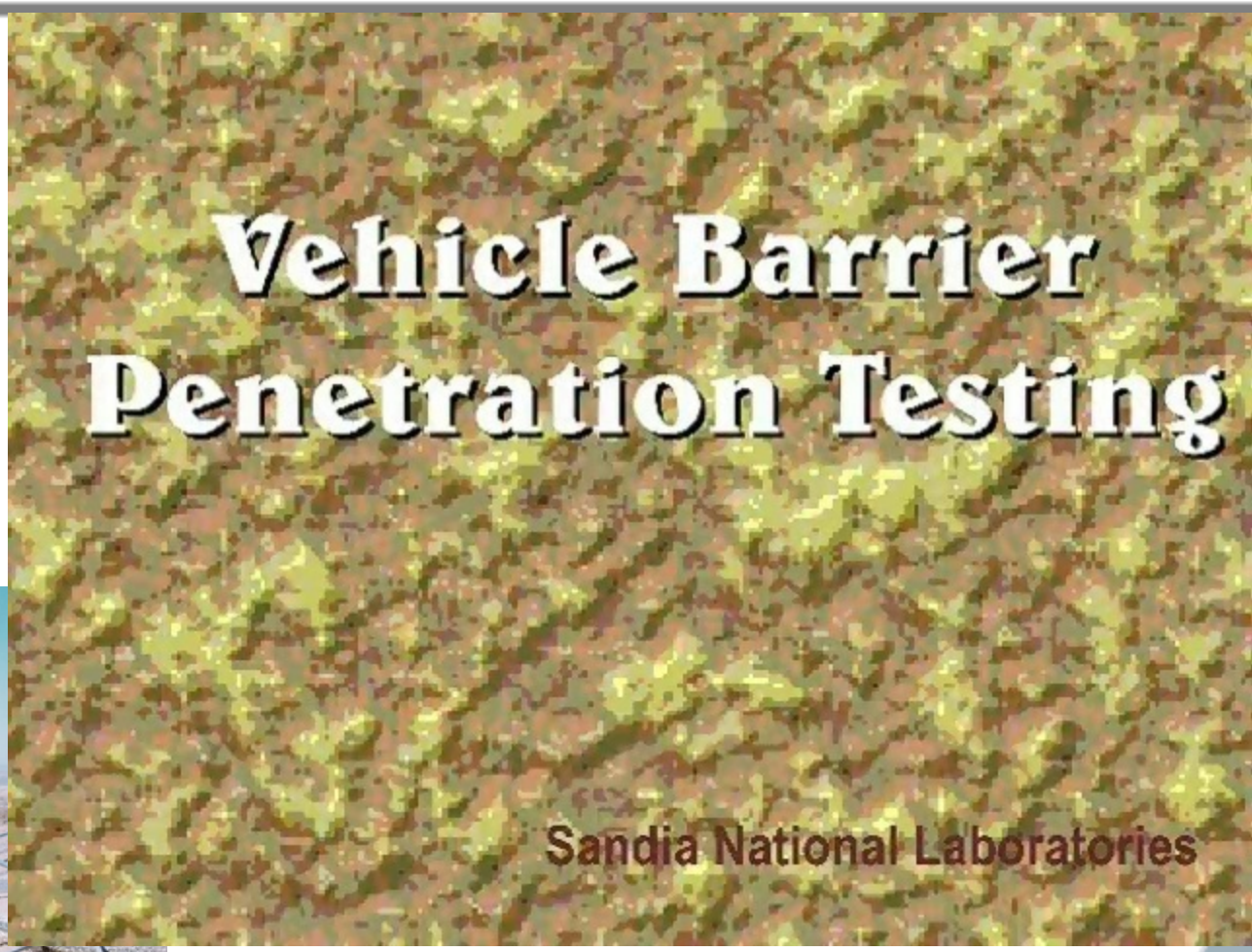
- Other Paths?
- Each Path Has Different Delay Times

Penetration of Fence Using Tools



VIDEO(3)

Fixed Barrier Penetration by Vehicle



VIDEO

Fixed Vehicle Barrier

- 61cm x 122cm steel box concrete /rebar filled
- Negative front slope angle to drive truck down
- 30.5 cm x 51cm x 1.6 m very deep posts in 91.5cm diameter low strength concrete

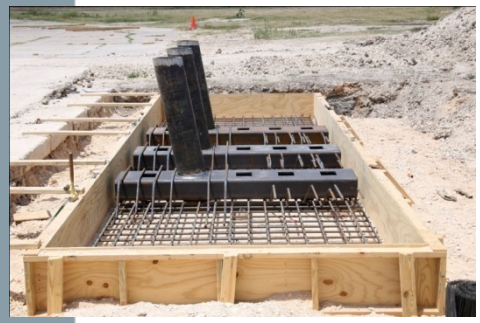
- 29.5 metric tons @ 80.5 kph
- Passed with negative penetration (front edge of the cargo bed was behind barrier at the conclusion of the test)

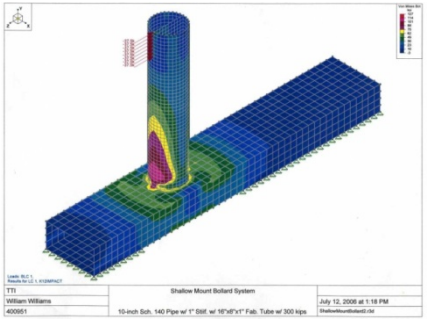
VIDEO

Fixed Vehicle Barriers - Bollards

- Shallow Mount Bollard, 10 degree angle
- Schedule 140 pipe (2.54cm wall) with 2.54cm thick vertical steel stiffener, concrete filled, welded to 20.3 x 30.5 x 1.3 cm box beams, 2 layers of rebar mat tying beams to concrete
- Rebar-filled concrete is 7.3m long x 2.4m wide x 0.46m deep

- 6.8 metric tons @ 80.5 kph
- Passed with negative penetration





VIDEO

Fixed Vehicle Barriers – Post & Beam Barrier

- 35.6cm square box beam 1.3cm wall with beam and posts the same material
- Posts on 4.9m span, 2.6m deep in unreinforced concrete footings

- 6.8 metric tons at 80.5 kph
- Passed with negative penetration

VIDEO

Moveable Vehicle Barrier

VIDEO

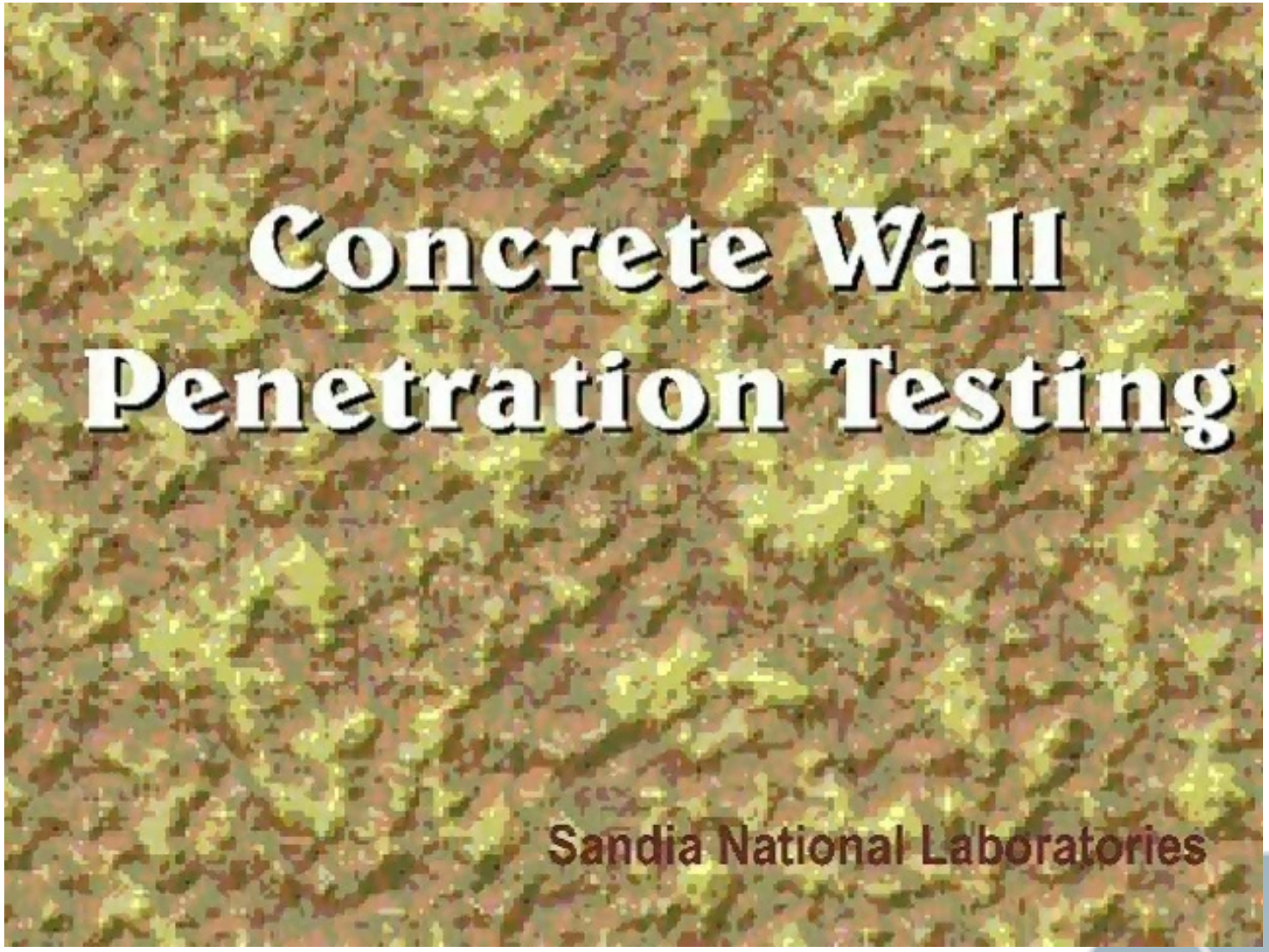
Structural Barriers

- Include walls, doors, windows, utility ports, roofs, and floors
- Conventional construction provides minimal delay against formidable threat
- Delay time depends on
  - Tools
  - Type of attack
- Barriers
  - Can detain an adversary at predictable locations
  - Multiple and complementary barriers are effective
  - Located close to assets are usually most cost effective

Structural Barriers

- Access delay features should be present 100% of the time, or take compensatory measures
- Example—This massive door only provides delay <u>when closed and locked</u>
- Balance delay for all attack paths. What about the walls?

Explosive Charge in Reinforced Concrete



VIDEO

Standard Steel Door Versus Steel Door Designed for Security

Standard Commercial Steel Door with Upgrades Added for Security:

- Drill Resistant Plate in front of panic hardware
- Z-strip to protect hinges
- Lexan Layer added to window
- Bar Grid over vent

Commercial Security Steel Door

- Forced Entry Resistant Rated
- Ballistic Resistant Rated
- Balances Delay of Walls, Roof & Other Structural Elements

Standard Versus Upgraded Vehicle Doors

Standard Commercial Rollup Door

Upgraded Vehicle Door

•Steel / Wood / Steel Sandwich for Upgraded Door Cross-Section
• Heavy Hinges
• Pry Strip
• Internal Locking Mechanisms
• Internal Z-strips to Mitigate Hinge Defeat
• Balances Delay of Walls, Roof & Other Structural Elements

TIME FOR A BREAK

Standard Versus Upgraded Turnstile Gates

- Four cross arms versus three
- Closer spacing of cross arms
- Stronger bars
- Heavily reinforced bottom & top anchor points
- Heavy sidewalls

Windows and Utility Ports

- Glazing materials for windows include
  - Standard glass
  - Wired glass
  - Tempered glass
  - Laminated glass
  - Ballistic glass
- Utility ports include
  - Electrical, mechanical, and service passageways
  - Heating, ventilating, and air conditioning systems

Penetration Attempt through Glass

Types of Roofs and Floors

- Wood sheathing with membrane
- Reinforced concrete beam and slab
- Metal roof
- Metal roof deck with insulation
- Metal roof deck with lightweight concrete
- Metal subdeck and reinforced concrete
- Prestressed concrete tee beam

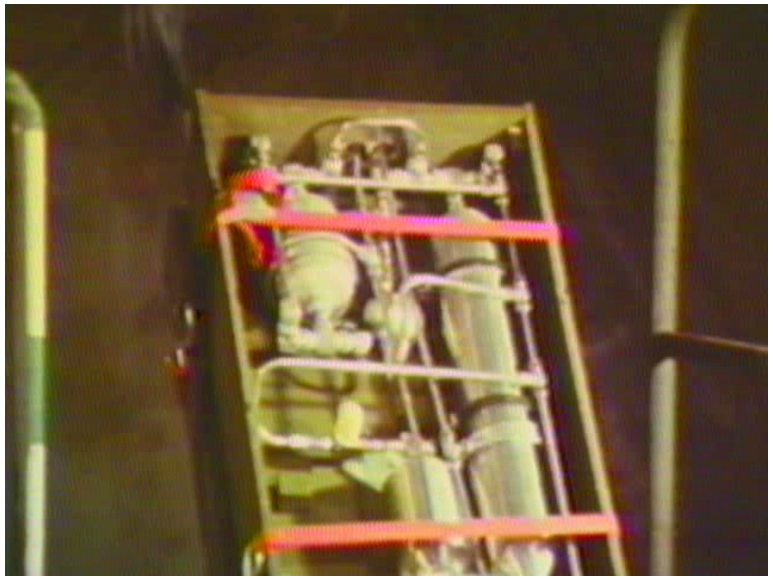
Penetration Attempt through Roof

Attributes of Dispensable Barriers

- Exert minimum impact on operations
- Afford volume protection
- Must provide adequate safety to personnel
- Operate independently of other barriers
- Should offer multiple activation options
- Have long storage life
- Provide maximum delay at target
- Can be cost effective
- Require a Command & Control System
- May require cleanup
- Have possibility of premature activation

Dispensable Materials

- Examples of material include:
  - Rigid polyurethane foam
  - Sticky thermoplastic foam
  - Stabilized aqueous foam
  - Cold smoke chemical obscurant
  - Low temperature pyrotechnic smoke
  - Fog
  - Various entanglement devices



VIDEO

Rigid Polyurethane Foam

Sticky Thermoplastic Foam

VIDEO

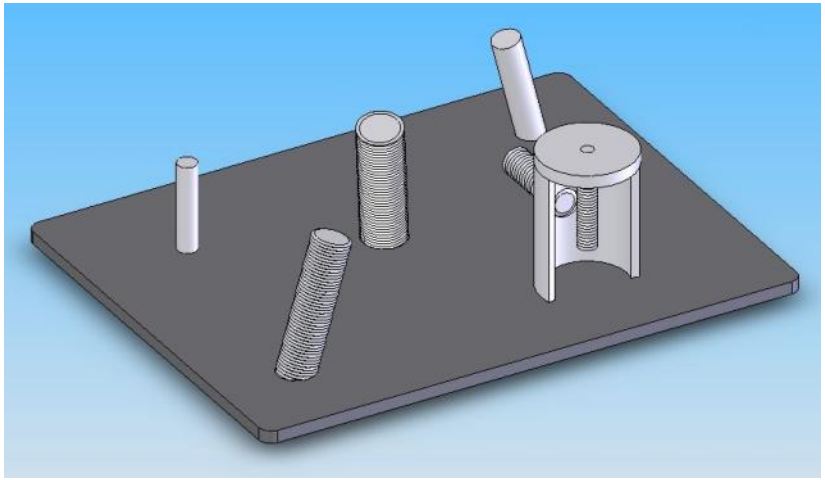
Fixed & Portable Aqueous Foam Dispensers

VIDEO

Pyrotechnic Obscurants

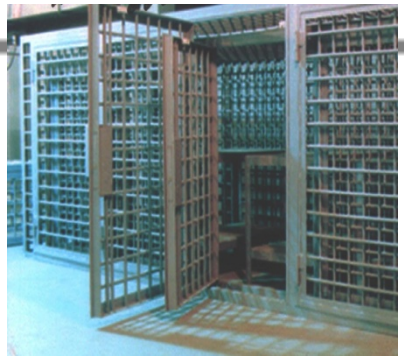
VIDEO

Performance Testing, Synergy, etc.



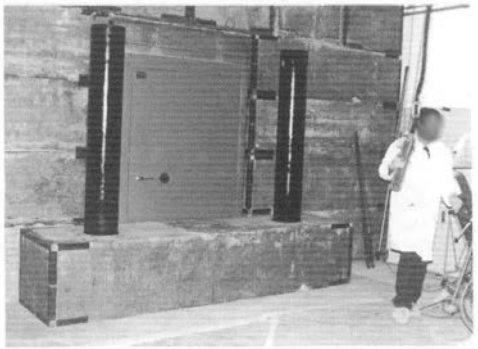
Delay Element Placement

- Delay should:
  - Immediately follow detection
  - Be maximized at the target for cost effectiveness
    - Fixed barriers with dispensables close to target can be effective use of resources
  - Include multiple different barrier layers requiring the adversary to
    - Use different skills
    - Plan better
    - Require a variety of tools to defeat



Access Delay Elements - Equipment

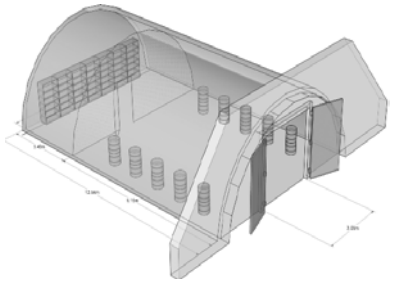
- Fences and gates
- Doors (exterior, vehicle, vault, etc.), door locking mechanisms
- Turnstiles, entry control point (ECP) barriers,
- Vehicle barriers
- Bullet resistant materials,
  armor (body, surface, container)
- Modular vaults



Access Delay Elements – Equipment *(cont'd)*

- Dispensable and deployable barriers
  - Obscurants, foams, irritants, command and control systems, etc.
- Tie-downs and restraints
- Non-lethal technologies
  - Acoustic whistles, flash bang grenades, etc.

Access Delay Elements – Upgrades/ Retrofits



- Storage bunkers
- Windows, grilles, utility ports
  - Ducts, air shafts, tunnels, crawl spaces, sewers, drains, water inlets, conveyor openings, trap doors, skylights, roof access hatches, filter banks, chimneys, roof vents, manholes, exhaust fans, electrical/ mechanical passageways, etc.
- Roofs, floors
- Walls
- Vaults
  - Above-ground, below-grade, in-ground, etc.

Access Delay Elements – Upgrades/ Retrofits *(cont'd)*

- Helicopter deterrents
- Methods for:
  - Balancing building surface delays
  - Increasing AD within existing vaults or very close to targets
  - Providing delay-in-depth
  - Providing multiple and different delays
  - Enhancing the synergy of potential delay upgrades
  - etc.

Access Delay Elements – New Construction

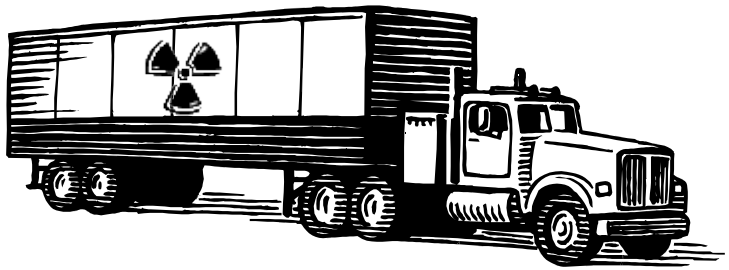
- Designing to meet access delay concepts for storage bunkers and underground facilities
  - Overburden
  - Personnel and vehicle entryways or tunnel ramps
  - Facility entry security doors
  - Facility air / power/ other service penetrations, emergency egress, etc.

Access Delay Elements – Transportation Security

- Material transporter exterior, interior, and at target item delays
  - Active and passive delays
  - Tie-downs
  - etc.

Access Delay for Transportation Security

- Is critical for nuclear material transportation security systems
- Allows for optimization of escort guard and responder tactics
- Is the number one defense against sabotage of nuclear material transportation systems



Access Delay for Transportation Security *(cont'd)*

- Provides critical time for convoy operators and responders to make informed, extremely difficult decisions
  - e.g., how to react to aggressive protestors versus a potentially higher threat
- Performance testing of access delay technologies is often required for both fixed facility and transportation systems

Design for Access Delay: Conceptual Guidelines - Design

- Design most delay close to target
- Design a balanced system
  - No weak links
- Design for easy assembly / disassembly by authorized personnel
- Design for difficult disassembly by adversaries
- Design large parts for confined volumes

Designing for Access Delay: Conceptual Guidelines - Installation

- Install delay only after detection
- Use multiple or combinations of barriers to provide delay-in-depth
- Use activated deterrents with passive barriers to complement design

Designing for Access Delay: Conceptual Guidelines - Adversary

- Force adversaries to use different tools
  - Hand, power, thermal, explosive, etc.
- Force adversaries to use different skills
  - Tools, equipment / clothing, dangerous operations, eye / hand coordination, etc.
- Force use of explosives
  - Force adversaries to retreat / exit for each high explosive event

Designing for Access Delay: Conceptual Guidelines - Other

- Neutralization or poisoning of target item
- Lethal delay for last choice options
- Conduct realistic adversary testing (performance testing) of delay barriers

Access Delay Summary

- Access delay features should be present 100% of the time
  - Otherwise compensatory measures should be implemented
- Building and barrier designs should be balanced to provide equal delay times
- Conventional fences, doors, walls provide minimal delay
- Vehicle delay is important to limit adversary tools

Access Delay Summary *(cont'd)*

- Explosives can defeat delay elements but cause collateral damage
- Various barriers have different delay times depending on
  - Their location
  - The attack
  - Tools
  - Adversary skill
  - Hole size
  - etc.

Delay Summary

- Role of access delay system
  - Immediately slow down an adversary after detection by use of fixed barriers, dispensable / active barriers, and/or responders
- Distinguish between passive and active delay
  - Passive are physical fixed barriers
  - Active are dispensable or activated barriers
- Three characteristics of a good barrier system
  - Immediately provides delay after detection
  - Exhibits balanced design; no weak links
  - Uses delay-in-depth
- Delay times depend on type of attack, adversary skills, location of the attack, and tools used

Exercise
Access Delay

Session Objectives

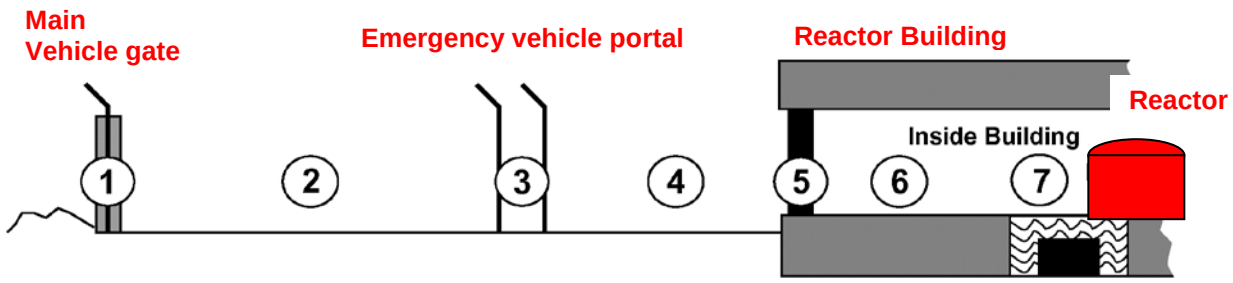
After this session, the participants will be able to do the following:

1. Use the example representative data to determine delay times for given paths and penetration equipment.
2. Recognize where to add barriers that will effectively increase delay time for the adversary.
3. Recognize the importance of documenting the sources or assumptions made in determining delay times used in analyses.
4. Recognize the importance of delay following detection.

Exercise 1 - Computing Delay Time

Two highly motivated people equipped with a truck, a 1.0-kg explosive charge, and a 45-kg explosive charge intend to sabotage the reactor. The adversaries intend to:

1. Crash a truck through the outer main vehicle gate.
2. Drive to the emergency vehicle portal.
3. Penetrate both gates of the vehicle portal with the truck.
4. Drive to the reactor building shipping door.
5. Penetrate the shipping door with 1.0 kg of explosives.
6. Run to the reactor with more explosives.
7. Set a 45-kg explosive charge and detonate it.



Barrier Number	Type	Specification
1	Main Gate	2.4-m x 4-m wide padlocked, chain-link gate on metal pipe (construction and maintenance gate)
2	Distance	1-km road
3	Vehicle portal	Two 2.4 m x 4 m wide, manually operated, chain-link gates on metal pipe (11 m apart)
4	Distance	115-m paved surface
5	Reactor shipping door	10cm thick wooden door with metal sheeting
6	Distance to reactor	30 m to reactor
7	Task Time	Time to place explosives and detonate

		Task Time (minutes)		
Barrier	**Task Description**	**Min.**	**Mean**	**Max.**
1	Crash truck through outer gate	**0.05**	**0.1**	**0.15**
2	Drive vehicle 1 km to emergency vehicle portal of reactor		**1.0**	
3	Penetrate both gates of vehicle portal with truck	**0.1**	**0.2**	**0.3**
4	Drive 115 m to reactor building shipping door		**0.13**	
5	Penetrate reactor building shipping door with 1.0-kg explosive charge	**1.25**	**2.10**	**2.80**
6	Run 30 m to reactor with explosives		**0.13**	
7	Set a 45-kg explosive charge on reactor and detonate		**0.65**	

1) What would be the total time required if the reactor building shipping door were unlocked and open during certain working hours?

Time:_____

2) What precautions would you suggest if the reactor building shipping door needed to be open for extended periods?

_____

_____

3) If you could add a vehicle barrier, where would you place it and how would it affect the total time?

_____

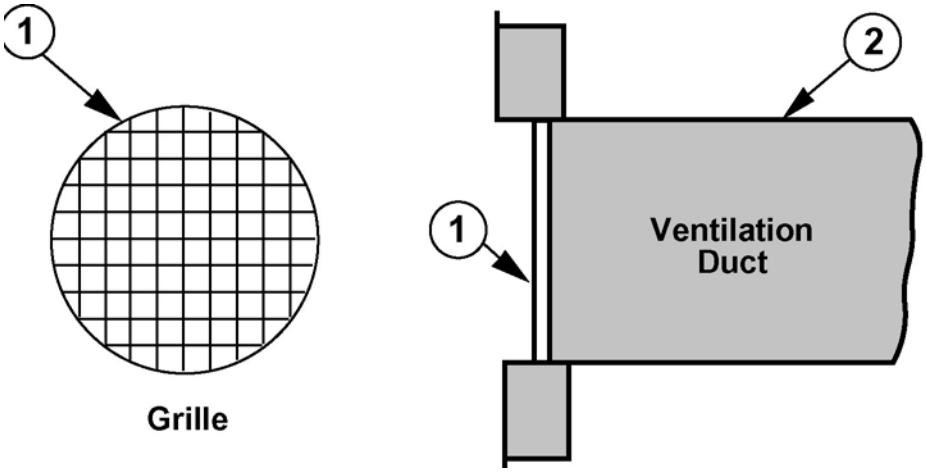
_____

_____

Exercise 2 - Computing Task Time

One highly motivated person equipped with 1-m bolt cutters and a portable oxyacetylene cutting torch intends to covertly penetrate a coolant security grille and ductwork to enter the building.

1. penetrate the security grille with bolt cutters
2. climb into the duct and then penetrate the ductwork with an oxyacetylene cutting torch



Barrier Number	Type	Specification	Task Time
1	**Security grille at end of air intake duct**	**No. 4 (13mm) reinforcement bar spaced 15 cm on center, horizontally and vertically, and welded to steel frame**	**1 cut takes ~20 sec**
2	**Air intake duct**	**1-m diameter mild steel, ,0.3 cm thick**	**Cutting rate ~ 0.6 cm / sec**

Exercise 2 - Worksheet

1 How many cuts would be recommended to create a man size hole (for a 29-cm x 29-cm man-sized opening) _____

2 How long would it take to make the cuts to the No. 4 (13 mm) rebar with bolt cutters to penetrate security grille _____

3 How long would it take to cut a square (30 cm x 30 cm) opening in ductwork (for man-sized opening) with oxyacetylene cutting torch to penetrate ductwork; length to be cut: 110 cm _____

Exercise 3

1. Would an adversary always choose the fastest penetration method? What situations would lead an adversary toward making a slower penetration effort?

2. Why are a variety of hand tools considered to be used for some barriers but only very limited penetration equipment for the more substantial barriers?

3. What are some of the ways that a perimeter fence line can be upgraded to increase the delay time for vehicle penetration?

4. Where is the best placement for a vehicle barrier in a double-fence system?

5. What are some of the ways that a perimeter fence line can be upgraded to increase the delay time for adversaries on foot?

6. Why is it important to ensure that the floor, ceiling, and walls of a room provide the same amount of delay?

7. Why is it important to use multiple barriers and different barriers?

8. What are some of the advantages and disadvantages of using explosives as a means to gain access to CATEGORY 1 material?

9. Why do you think we say that dispensable barriers near the target can be a very "cost effective" delay mechanism?

Response

Learning Objectives

After completing this module, you should be able to:

- State the differences between guard forces and response forces
- Discuss the two types of response to mitigate an adversary threat
- Discuss the components of Protection Planning
- Be aware of Response Force Equipment, Command, Control, and Communications
- Discuss the two categories of Performance Measures

Response Force Definitions

***Guard forces*:** A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals during transport, controlling access and/or providing initial response

Response forces: Persons, on-site or off-site who are armed and appropriately equipped and trained to counter an attempted *unauthorized removal* of nuclear material or an act of *sabotage*

Legal Basis for Guards and Response Force

- Arrest authority and use of force by guards and response force officers typically has a basis in law
- Some countries such as the United States allow the use of deadly force (neutralization) by non-police or military response forces
  - Section 161k of the Atomic Energy Act of 1954 authorizes DOE and its contractors to use appropriate force to protect its facilities
  - US state laws govern the use of weapons by guards at NRC-licensed facilities

Legal Basis for Guards and Response Forces

- Use of force does not always imply deadly force.
  - A ***Force Continuum*** may be established that direct response forces to use the minimum amount of force necessary to: control the situation, make an arrest, or perform other actions to stop the action of adversaries and prevent a malevolent act
  - ***Rules of Engagement*** define when a Response Force can use weapons against adversaries

Use of Force

- Response force personnel should have the ability to apply sufficient force to stop an adversary's actions, which may include the use of deadly force
  - Should have a legal basis
  - Should be clearly documented
  - Should be used to develop Rules of Engagement

Rules of Engagement (Examples)

- Adversaries on foot or in vehicles may be engaged with weapons fire when they have displayed hostile intent:
  - Attacked guard posts
  - Bypassed entry control systems (e.g., run gate)
  - Bypassed barriers (e.g., climb over PIDAS fence, crash vehicle through perimeter gates)
- Adversaries in helicopters may be engaged with weapons fire if they:
  - Attempt to land within the restricted area *and* are seen carrying weapons

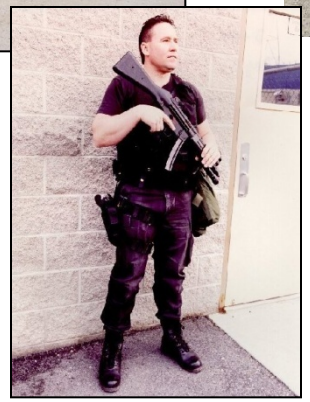
Force Continuum

- Not all force must be deadly force
- Policies based on legal authority should be developed describing the types of force authorized to be used by Guard and Response Forces
- Within the US, the legal framework defines a concept termed a Force Continuum, which describes the use of an authorized escalating amount of force, based on the actions of an adversary
  - It requires use of the minimum amount of force necessary to control the situation, make an arrest, or perform other actions to stop the action of adversaries and prevent a malicious act.

Force Continuum *(cont'd)*

Presence → verbal → use of hands → less lethal → deadly force

Impact Weapons



Tasers

Chemicals

Protection Planning Concepts

- Thorough protection planning is critical in ensuring an organized and effective response to a security incident
- This includes:
  - Identifying and prioritizing potential targets
  - Determining if targets are theft or sabotage targets along with appropriate protection strategy
  - Identifying optimal response force configuration
  - Determining probable adversary actions
  - Establishing pre-determined response plans
  - Developing realistic scenario-based training programs

Types of Response

- Two types of response used to counter an attempted *unauthorized removal* of nuclear material or an act of *sabotage*
  - ***Interruption*** – The successful arrival of the response force at an appropriate location to stop the adversary
    - Communication
    - Timely Deployment of the Response Force
    - Tactical requirements / training (survivability)

Right time

Right place

  - ***Neutralization*** – When the response force kills, captures, or causes the adversary to flee before the adversary is able to complete their task
    - Appropriate Use of Force
    - Proper use of weapons and equipment

Response Force Strategies

Containment : preventing adversaries from leaving the site with an asset

Denial: preventing adversaries from getting to an asset

Recapture: taking over by force a critical location on the site occupied by adversaries

Pursuit and Recovery (Contingency): attempting to recover an asset removed from the site by adversaries

Protest Strategy: preventing significant impact to the mission of a facility caused by demonstrators or protestors

Defense in Depth

- Security managers must ensure that the protection system provides integrated, in-depth protection of site security assets so that they cannot be easily overcome
  - The system should be organized in depth and contain mutually supporting elements coordinated to prevent gaps in responsibilities and performance
  - The protective force is the dynamic link between each of the elements and ensures their integration
  - Response plans should be developed to ensure that potential weaknesses in the physical security system are covered by protective force personnel

Tactical Planning

- Tactical planning involves using all the information described previously and developing comprehensive incident response plans
  - Describes specific actions the Response Force will take under various circumstances to prevent adversaries defined in the DBT from successfully completing a malicious act
  - Used as the basis for developing procedures and for developing training and performance testing programs

Interaction with Outside Agencies

- If the facility is utilizing outside or off-site agencies, protection requirements need to be carefully documented and rehearsed.
  - Written agreements or understandings
  - Key issues for consideration:
    - role of support agencies
    - agreements should be specific (number of responders, response time, locations of road blocks, etc.)
    - integrated communications with support agencies
    - off-site operations
  - Joint training exercises and validations

Outside Agency / Local Law Enforcement

- Benefits of utilizing outside agencies / local law enforcement
  - Reduces cost for part-time or contingent support
  - Resolves many jurisdictional issues
  - Allows increased pursuit capabilities
- Challenges
  - Difficulty ensuring performance
  - Difficulty attaining dedicated resources
  - Mandatory response times
  - Requires response training for external personnel
  - Classified information considerations
  - Integrated secure communications
  - Difficulty coordinating / conducting joint training exercise

Response Force Survivability

- Response force survivability considerations
  - Based on DBT capability
  - Site-specific
- Excessive attrition of response force will reduce effectiveness – consider:
  - Hardened posts
  - Fighting positions
  - Armored vehicles (Survivability and Equipment)

Hardened Posts

Fighting Positions

Armored Vehicles

Response Force Equipment

- Wide variety of types and models of equipment
- Consider DBT when determining what equipment is necessary
- Consider response equipment as a system, not as individual pieces of gear
- Response equipment
- Breaching equipment

Response Equipment (1 of 3)

Primary Weapon System

Backup Weapon System

Special duty weapons

Response Equipment (2 of 3)

- Body armor and helmet
  - Level of protection
- Gas masks
  - Readily available
  - Type of filter
- Chemical biological suits
  - Type of protection
  - Time to prepare

Response Equipment (3 of 3)

- Intermediate force weapons
  - Hand-to-hand combat
  - Impact and chemical weapons
- Night vision devices
  - Individual issue or team issue
  - Weapon, helmet, vehicle mount
- Miscellaneous equipment
  - Flashlights
  - Handcuffs
  - Load-bearing vest

Breaching Equipment

- Response force must be able to make entry into facility that has been barricaded by an adversary

Command and Control, and Communications

Command: Exercise of authority (Decision making) by response force leaders

Control: Direction by response force leaders over assigned personnel to accomplish the mission

Communications: Allow real time communication between the central alarm station, tactical leaders and response force in the field and allows tactical leaders to direct the actions of the response based on adversary actions

Communications Systems

- Vital to command and control
- A robust communication system uses multiple systems to ensure functionality is not lost
- Most common is simple radio frequency communication system
  - Most systems are conventional, narrow-band frequency modulation, clear-voice systems
  - Typical radios operate on any one of several frequencies or channels
  - Approximate range is 2 to 5 Km

Simple Radio Frequency Systems

- Advantages
  - Simplicity / Ease of operation
  - Efficiency
  - Low Cost
- Disadvantages
  - Short range of hand-held systems
  - Gaps in communication coverage
  - Susceptible to Adversary:
    - Eavesdropping
    - Deception
    - Intentional Interference (Jamming)

Other Communication Systems

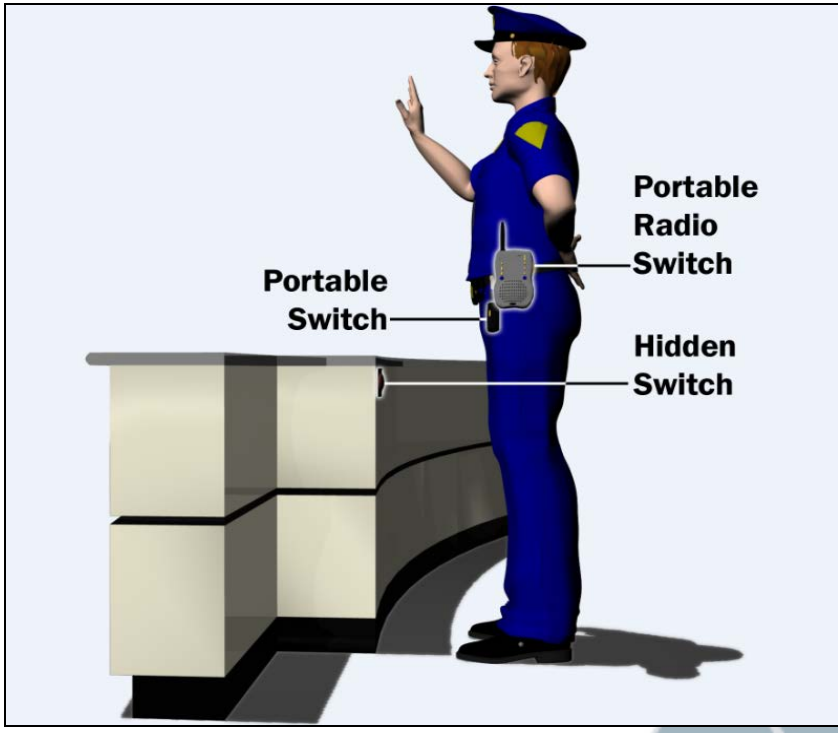
- Secure Radio Systems
  - Spread Spectrum System
  - Encrypted Radio System
- Paging Systems
- Cell Phones
- Land Lines
- Intercom Systems
- Sirens
- Flashing lights
- Public address system

Keys to Effective Communications

- Plan, train, and rehearse tactical operations without primary communications systems
- Develop contingency communication plans
- Maximize network effectiveness
  - Increase output, antennas, batteries, cabling
- Switch to encrypted mode in security emergencies
- Utilize authentication protocol for suspect transmissions

Means of Signaling Duress

- Constraint by threat or coercion
- Covert signal capability
- Covert response



Guard and Response Force Training

- Training is a critical part of the response force program
- Training should include all contingency missions
- Training should ensure appropriate response force times (RFTs)
- Complex, dynamic response requirements require sustained, dynamic training
- Training should be scenario-based and in a realistic environment
- Training schedule should be designed based on training needs analysis

Guard and Response Force Performance Methodology

- A combination of performance testing is used to evaluate the performance of the guard and response force
- Broken into two categories
  - Sub-System Performance Testing
    - Provided different types of tests to performance test individual components of the guard and response force functions
    - Testing individual components of the whole system
  - Whole System Performance Testing
    - Testing the sections of the whole system (sensors, RFTs, etc.)
    - Two performance measure criteria are evaluated
      - Interruption
      - Neutralization
    - ***Force on Force Testing***: A full scale field simulation of an attack on a site involving onsite guards and response forces

Example Response Force Time

- If a contingency plan requires a responder to arrive at a certain location within a certain time, there needs to be mechanism in place to determine if the time can be realistically achieved.
- The goal to this exercise is for you to understand how to collect data points along a response path and evaluate the data for upgrades to response time. In this exercise, you will time tasks for a response path in your classroom, and to implement and evaluate upgrades

Example Response Force Time

- There will be:
  - One response force person
  - One timer
  - One communicator
- The Picture-In-Time is that the responder is sitting in a chair with shoes removed, response backpack and simulated weapon are in storage locations in opposite corners of the room. Response force personnel has key-card to the facility (room) in pocket.

Example Response Force Time

- Communicate Response
  - Communication to respond and location for response
  - Responder communication that responding with confirmation of location
- Prepare to Respond
  - Put shoes on
  - Grab and completely don the backpack from the corner of the room
  - Grab the simulated weapon from the other corner of the room
- Respond
  - Walk around the table once
  - Exit room closing door on exit
  - Enter room with key-card
  - Touch the telephone.

Example Response Force Time

Task	Description	Time (sec)	Note any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Example Response Force Time

- Document the total response time (Task 3):
- Minimum: _____sec Maximum: _____sec Average: _____sec
- Determine upgrades that could improve response time:

Summary

- Guards and response forces have different response functions and authority, which should be based on a legal framework
- Interruption and Neutralization are types of responses to mitigate an adversary threat
- Response strategies are based on the target (theft or sabotage) and include containment, denial, recapture and Pursuit/Recovery
- Response force measures of performance in broken into two categories (Sub-System and Whole-System Performance Testing)

Summary

Workshop Objectives

- Review of the design and evaluation process outline (DEPO)
- Define the elements of a physical protection system
- Develop an understanding of the fundamental principles of the different elements

PPS Functions

- Detection
  - Exterior intrusion detection
  - Interior intrusion detection
  - Assessment
  - Alarm communication and display
  - Entry control
- Delay
- Response

Sensor Summary

- Sensors are classified as:
  - Passive or active; covert or visible; line of sight or terrain following; volumetric or line detection; and by application
- Exterior technology includes:
  - Buried line sensors, fence-associated sensors, freestanding sensors
- Interior technology includes:
  - Boundary penetration, interior motion, and proximity

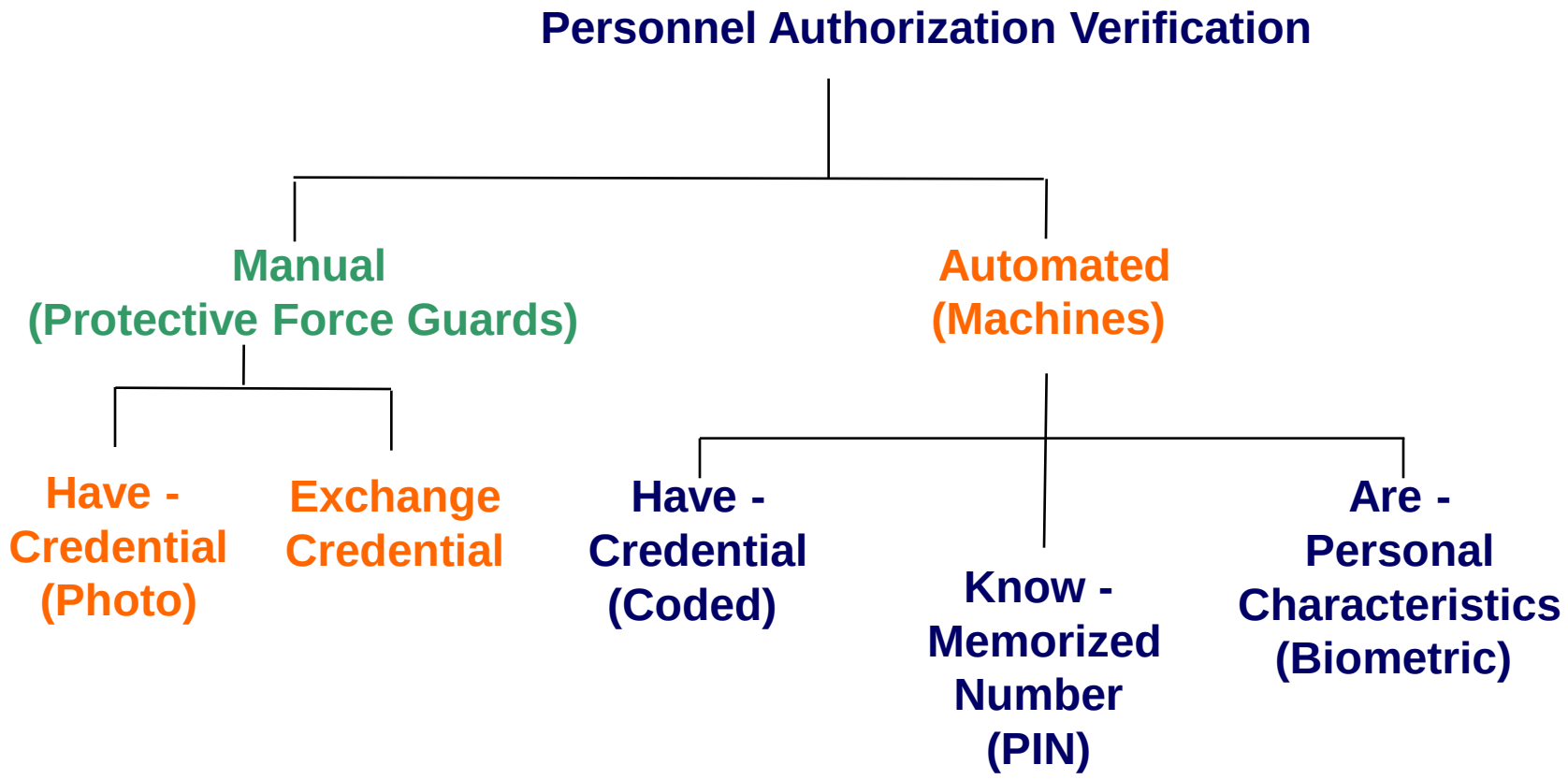
Sensor Summary *cont'd*

- Performance characteristics include:
  - P_D, nuisance alarm rate, vulnerability to defeat
- Designers should consider design goals, effects of physical environmental conditions, and interaction of system with a balanced PPS.
- Probability of Detection (P_D), Vulnerability to Defeat, and Types of alarms are important performance characteristics of intrusion detection sensors.

Entry Control

- A perimeter security system is to provide a boundary around each protection area to prevent or detect unauthorized penetrations
- Entry control is to allow authorized persons and materials to move in and out through that boundary in a balanced secure way
- The System must:
  - Allow entry of authorized persons
  - Prevent entry of unauthorized persons
  - Allow exit of authorized persons

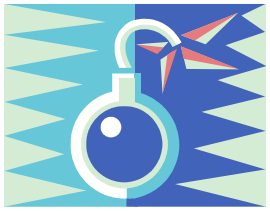
Types of Personnel Entry Control

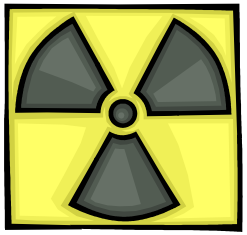


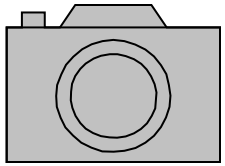
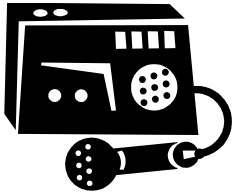
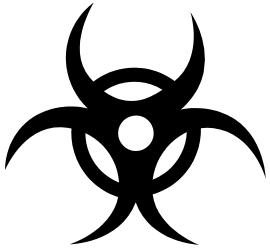
Contraband Defined

Contraband: any object or material that is prohibited in a security area

- Contraband is also any device or material that can be used by an adversary to gain an advantage in an attempt to commit an act detrimental to a facility




Purposes of Contraband Detection Systems

Allow entry of • Authorized material	Prevent entry of • Weapons • Explosives • Other contraband
Allow exit of • Authorized material	Prevent unauthorized exit (theft) of • Special nuclear material (Category 1)

Contraband: *An item that is prohibited in an area.*

Contraband Summary

- Contraband is an item you prohibit in an area
  - weapons, tools, explosives, controlled material (Category 1)
- Techniques covered included:
  - Manual search (everything)
  - Metal detection (weapons, tools)
  - Package x-ray inspection (weapons, tools, explosives)
  - Explosives detection
  - Radiation detection (Category 1)
- A good system integrates complementary techniques
  - e.g., metal detection (for shielding) + radiation detection
- The DBT lists the types and amounts of weapons, tools, explosives you need to consider

Alarm Assessment Summary

- Alarm assessment completes the detection process by determining the cause of a sensor alarm
- Assessment may be performed using response force/ guards or video alarm assessment
- Response force assessment components include sufficient trained personnel in appropriate locations, sufficient lighting, and effective communication
- Video assessment components include camera, lens, lighting, and video control system
- Video assessment system must provide complete coverage and display of sensored areas at all times

Delay Summary

- Role of access delay system
  - Immediately slow down an adversary after detection by use of fixed barriers, dispensable / active barriers, and/or responders
- Distinguish between passive and active delay
  - Passive are physical fixed barriers
  - Active are dispensable or activated barriers
- Three characteristics of a good barrier system
  - Immediately provides delay after detection
  - Exhibits balanced design; no weak links
  - Uses delay-in-depth
- Delay times depend on type of attack, adversary skills, location of the attack, and tools used

Response Force Summary

- Guards and response forces have different response functions and authority, which should be based on a legal framework
- Interruption and Neutralization are types of responses to mitigate an adversary threat
- Response strategies are based on the target (theft or sabotage) and include containment, denial, recapture and Pursuit/Recovery
- Response force measures of performance in broken into two categories (Sub-System and Whole-System Performance Testing)

Workshop Objectives

- Review of the design and evaluation process outline (DEPO)
- Define the elements of a physical protection system
- Develop an understanding of the fundamental principles of the different elements

Summary

Questions ??

&

Thank You

ROK Sensors in Use

In the small test field, the following sensors are installed:

- Peridect Sensor Vibration sensor mounted on fence (climbing, cutting, lifting off) piezoelectric sensor
- Magnetic field sensor – Dream Tech – complete miniature magnetometer
- Securit sensor IR and microwave stacked sensor down the middle of the iso zone
- Fiber optic mesh on fence ? operational?
- Duretec sensor – appears to be a bi-static IR volumetric sensor
- Exterior PIR – mono-static

Traditional CCTV including PTZ
Laser CCTV
Megapixel CCTV

For INSA, the following sensors are proposed in Sector 1:
Performance testing and practical exercises

- Magnetic Sensor
- Active IR sensor
- Microwave sensor
- Peridect sensor
- Dual technology sensor
- Heat detector
- Fiber optic sensor mat
- Fiber optic sensor net
- Fiber optic fence sensor/cable
- Microwave Sensor
- IPID
    - infrared

moveable streetlamp
moveable CCTV on pole

For Sector 2
State of the art equipment and technology for testing

Moveable streetlamp
LED lamp
Thermal imaging camera
High pixel IP camera
HD-SDI camera
Laser camera
Mega pixel camera
Ubiquitous imbedded equipment

For Sector 3
Security inspection equipment and entry control/contraband detection

Streetlamp
Vehicle delay
Intake
Steel wire
Blocks
Bollards
x-ray scanner
container scanner
Rexton test SUV
Heat detector
Under vehicle surveillance system
CCTV
Vehicle Sally port
Fence drain

For Sector 4
Durability and reliability testing, performance tests, practical exercises, FoF

Streetlamp
CCTV
Magnetic sensor
Active IR
IPID

Interior

- Glass break
- Heat sensor
- Infrared sensor
- Mock up structure
- Shock sensor
- BMS
- Full HD speed dome camera

Workshop on Elements of a Physical Protection System

Instructor Guide

Module Number:

Key Learning Points

Examples

Materials

Items to Prepare

Exercise Number:

Key Learning Points

Examples

Materials

Items to Prepare