



GLOBAL THREAT REDUCTION INITIATIVE

Working to reduce and protect vulnerable nuclear and radiological material located at civilian sites worldwide. SAND2013-5501P

Module D

Interior Sensors



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



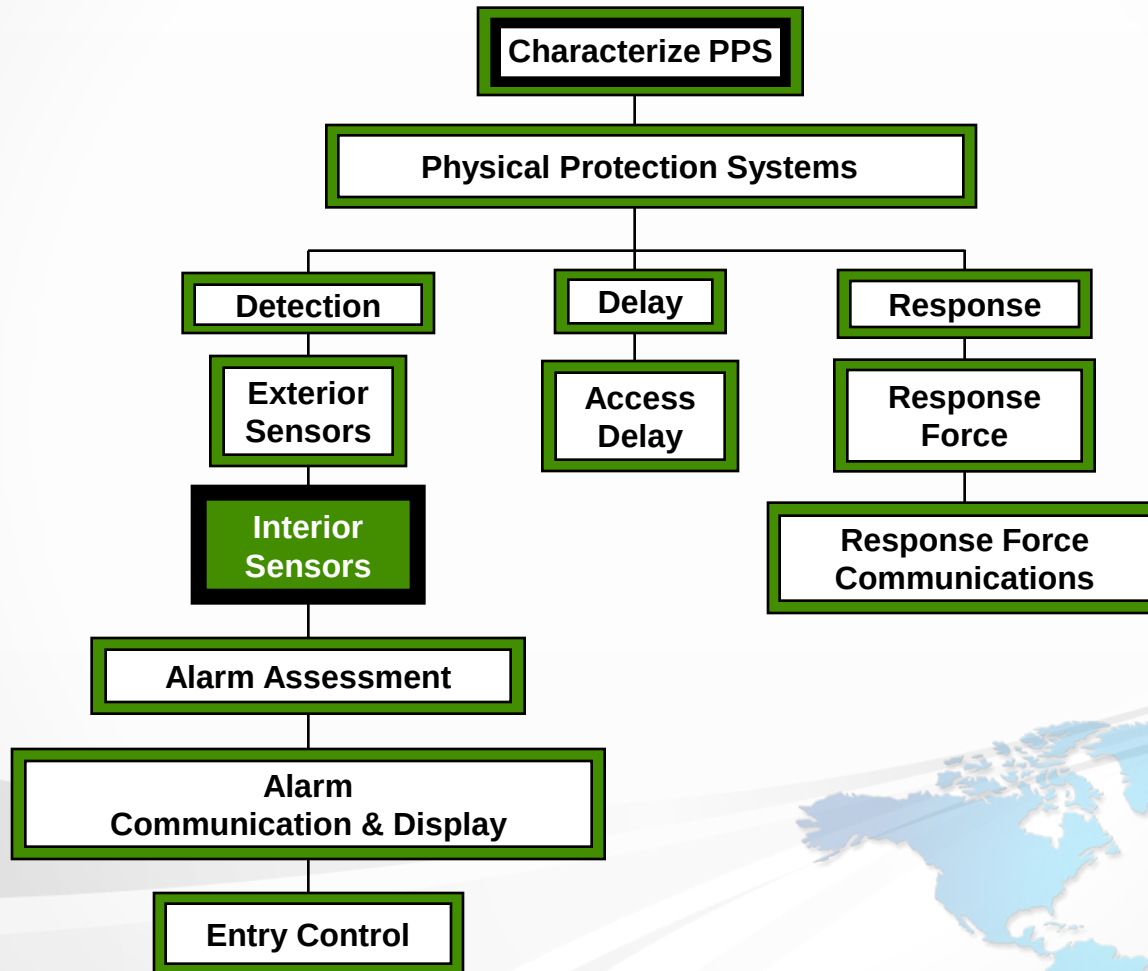


Module Objectives

- Explain some sensor fundamentals.
- Present some example sensors and their suitability for providing effective detection for given threat tactics and environmental conditions.
- Show how to evaluate and determine effective placement of intrusion sensors.
- Determine the advantages and methods of combining sensor systems.



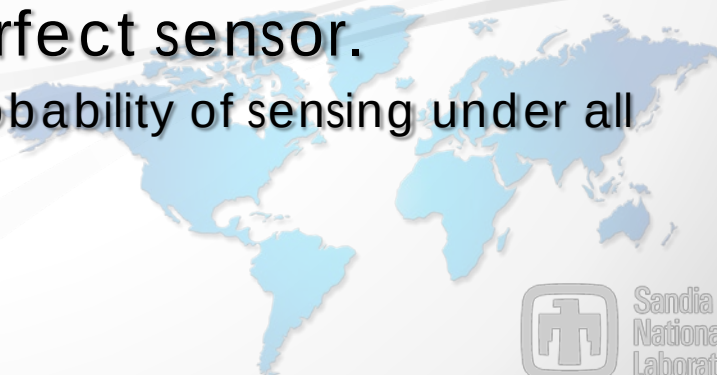
DEPO – Interior Sensors





Sensor Fundamentals

- Sensors are classified according to the way they operate.
- Performance Characteristics:
 - o Probability of sensing (P_s)
 - o Nuisance alarm rate (NAR)
 - o Vulnerability to defeat
 - o Maintenance required
- There is no such thing as a perfect sensor.
 - o Perfect sensor would have 100% probability of sensing under all situations and conditions





Sensor Classification

Sensor operation:

- Active vs. passive
- Covert vs. visible
- Volumetric vs. line detection
- Mode of application
 - Boundary penetration, interior motion, or proximity detection

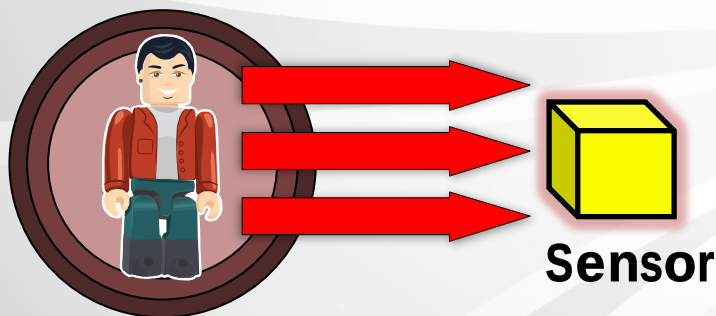




Classification: Passive vs. Active

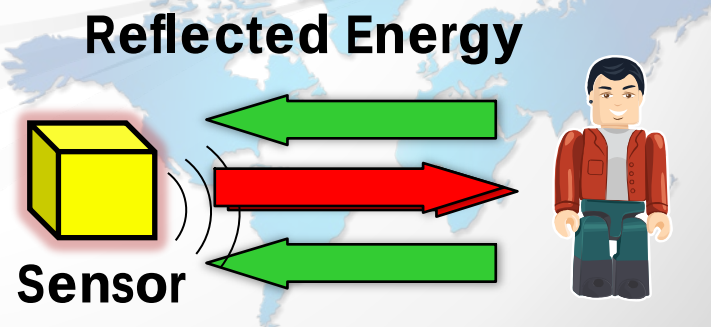
Passive

- o Receiver only
- o Detects using:
 - Vibration
 - Heat (infrared energy)
 - Sound
 - Capacitance
 - Pressure



Active

- o Transmitter and receiver
- o Types include:
 - Microwave / RF energy
 - Active infrared
 - Sonic / ultrasonic





Classification: Covert vs. Visible

Covert

- o Sensors hidden from view.
- o More difficult for intruder to detect.
- o More difficult & expensive to install and repair.

Visible

- o Sensors in plain view of intruder.
- o Simpler to install and repair.





Classification:

Volumetric vs. Line Detection

Volumetric

- Detection in a volume of space.
- The actual detection volume is usually not visible.

Line Detection

- Detection along a line.
- Detection zone easily identified.

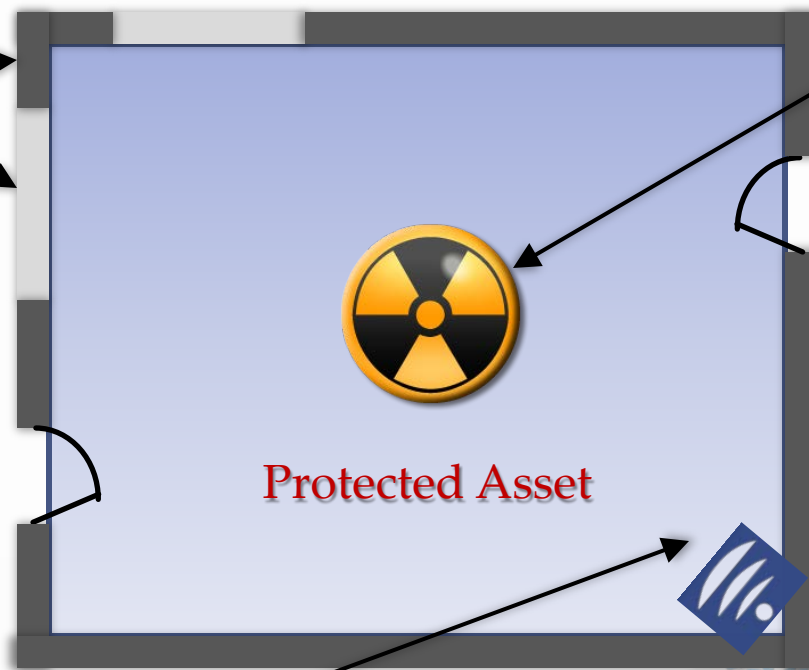




Classification: Mode of Application

Boundary

- Detection at doors, windows, walls, vents, floors, ceilings, etc.
- Detection zone easily identified.



Proximity

- Detection at an object.

Motion

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



Performance

Important Sensor Characteristics:

- **Probability of Detection, PD**

$$P_D = P_S \times P_A$$

PS is the probability of sensing

PA is the probability of assessment

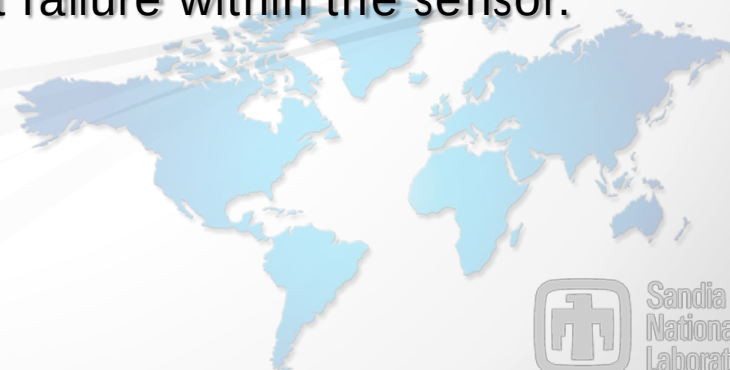
- Nuisance Alarm Rate (NAR)
- Vulnerability to Defeat





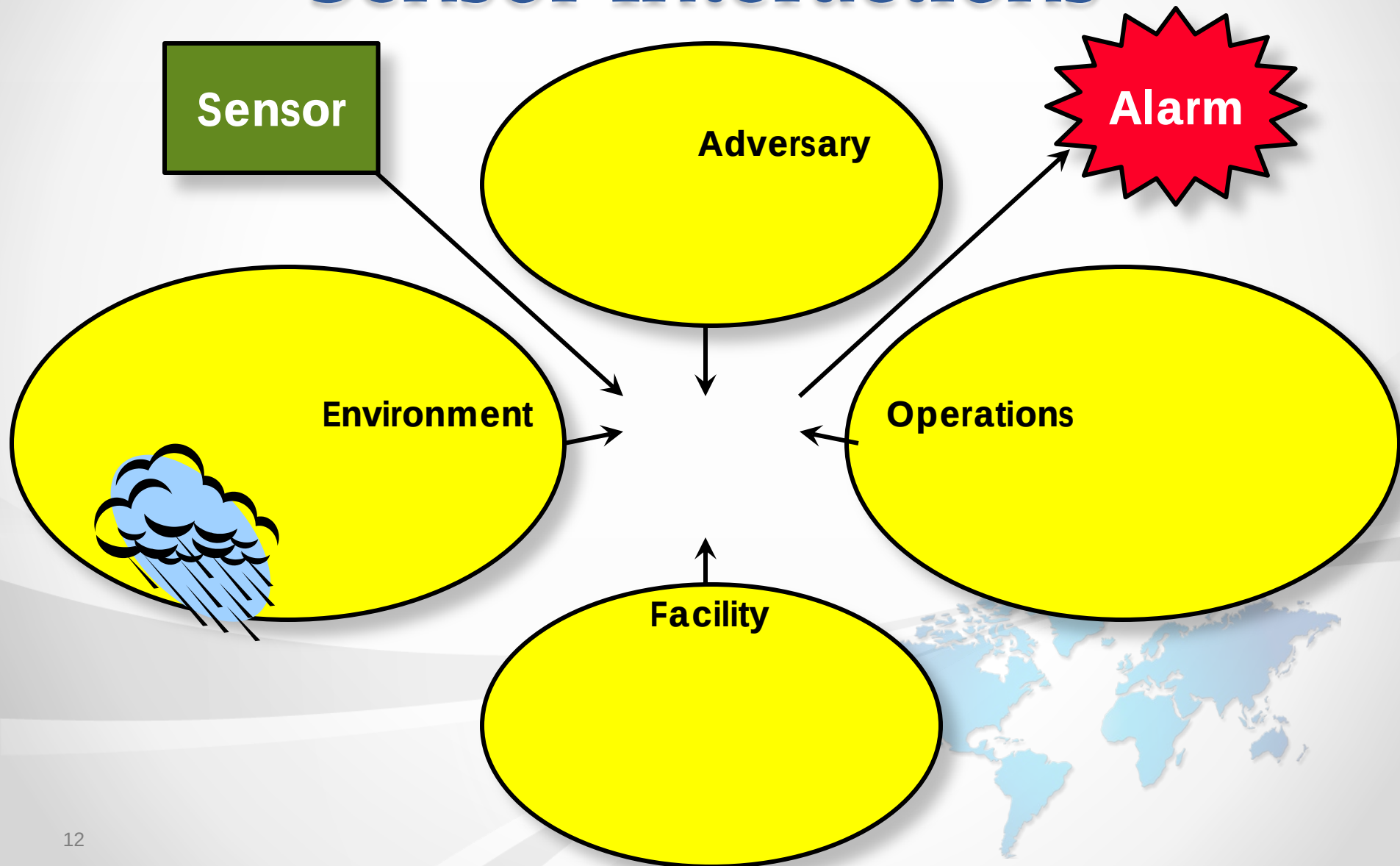
Sensor Performance – NAR & FAR

- Nuisance alarm rate (NAR)
 - Expected rate of alarms from an intrusion detection sensor which **can** be attributed to known causes, but is unrelated to intrusion attempts.
- False alarm rate (FAR)
 - Expected rate of alarms from an intrusion detection sensor which **cannot** be attributed to known causes.
 - Example: Electrical component failure within the sensor.





Sensor Interactions





Warning:

P_s is Dependent on Many Variables

- Probability of sensing for a sensor depends on:

- o Target direction, size, and speed
- o Sensor hardware
- o Installation conditions
- o Sensitivity settings
- o Environmental conditions
- o Maintained condition of sensor
- o Method of the intrusion and adversary capabilities
 - Walking, crawling, jumping, tunneling, etc.





Common Types of Interior Sensor Technologies

- Simple and Balanced Magnetic Switches (for doors)
- Glass Break
- Microwave
- Passive Infrared
- Video Motion Detection
- Others
 - Capacitive
 - Fiber Optic
 - Vibration
 - Ultrasonic
- Dual-Technology





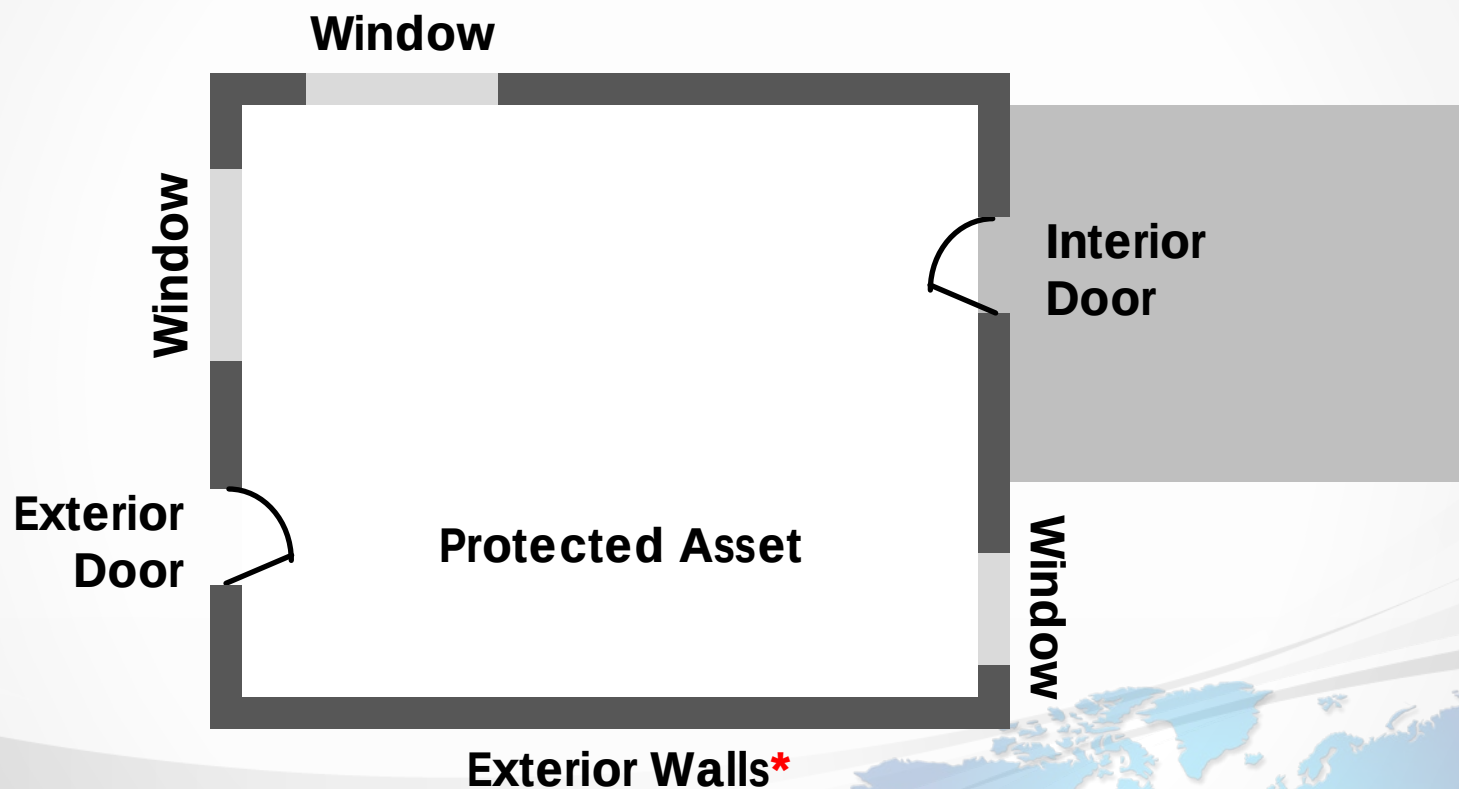
Boundary Penetration Sensors

- Magnetic switches (simple)
- Balanced magnetic switches (BMS)
- Glass break sensors
- Other





Boundary Penetration Areas



* Wall, roof, and floor protection sensors will **not** be covered in this presentation

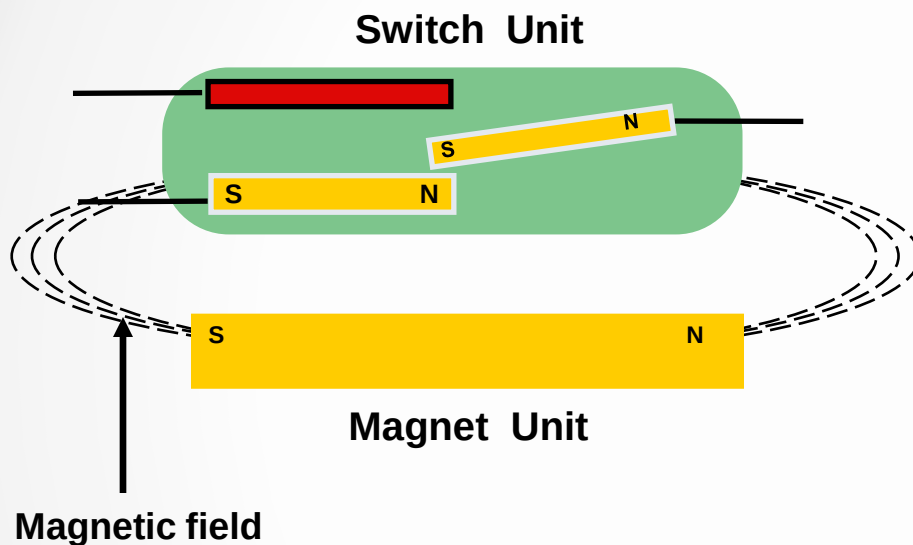


Magnetic Switches

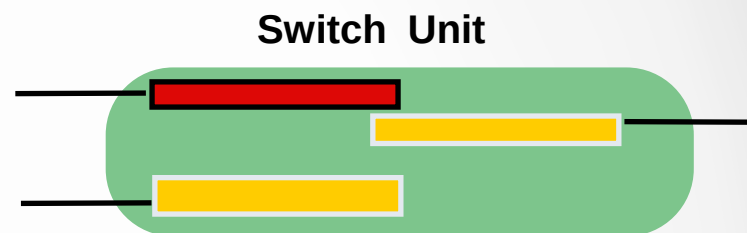




Simple Magnetic Switch



(Door Closed)



(Door Opened)

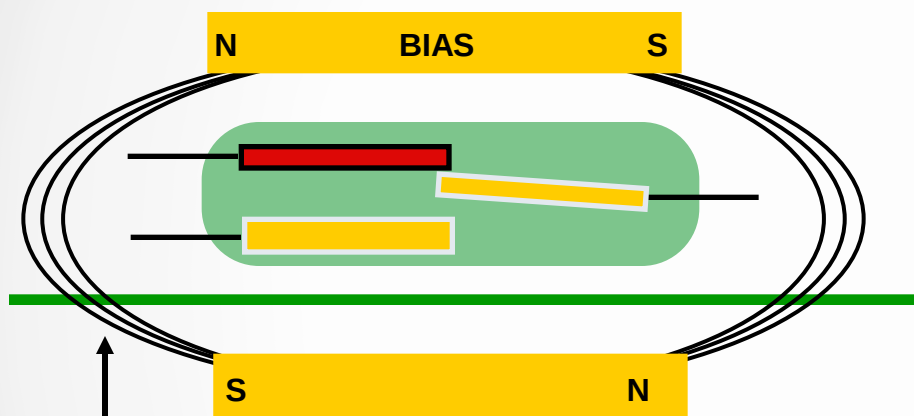
Non-Magnetic Contact = 





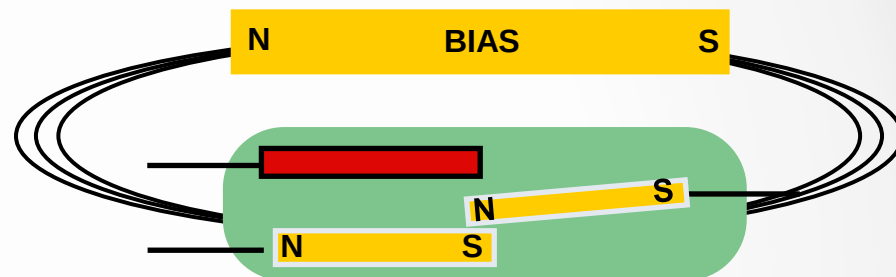
Balanced Magnetic Switch

Switch Unit



(Door Closed)

Switch Unit



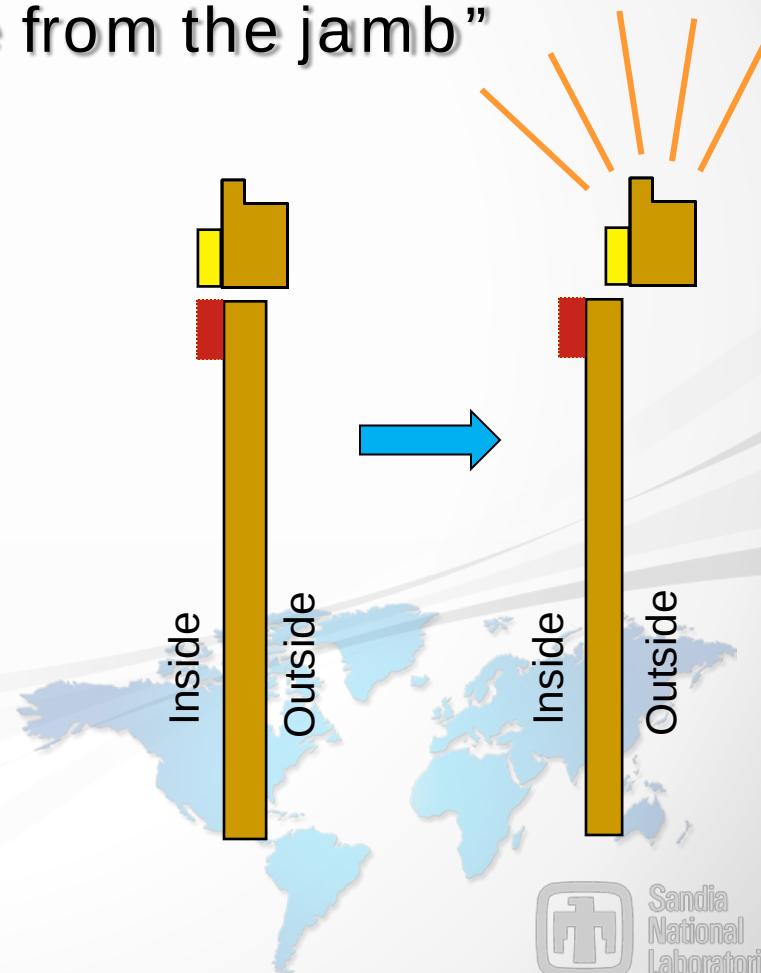
(Door Opened)

Non-Mag = 



Example Design Criteria

“A BMS shall initiate an alarm whenever the door is moved 1 inch or more from the jamb”





Glass Break Sensors

- Glass break sensors are generally less reliable than other interior sensors. Types available include
 - o Shock
 - o Frequency
 - o Shock/stress
 - o Passive audio





Interior Areas Can be Protected by Motion Sensors



Protected Asset



Interior Motion Sensors

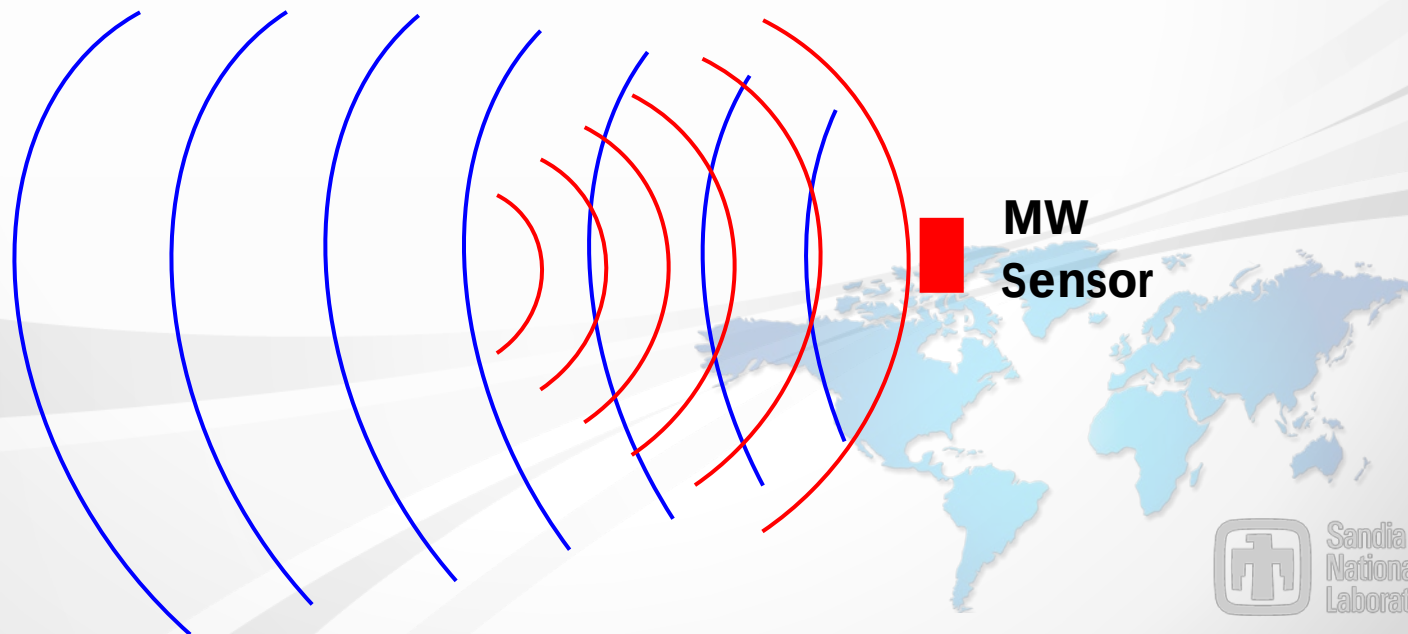
- Monostatic Microwave
- Passive Infrared
- Video Motion
- Dual-Technology





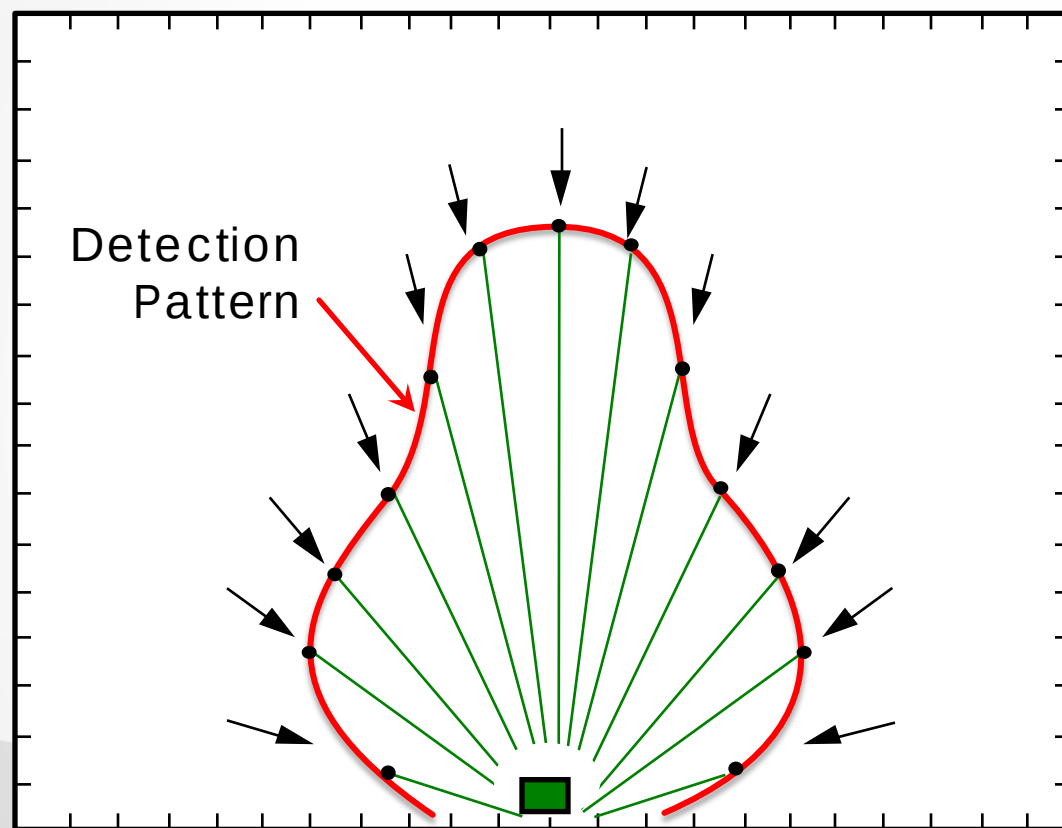
Monostatis Microwave: Basic Operation

- A pattern of microwave energy is transmitted and monitored by receiver
- Intruder's motion alters pattern / frequency
- Detection based on a Doppler frequency shift
 - Sufficient amplitude change and duration time to cause an alarm





A Typical Doppler Detection Pattern



**Top / Plan
View of Room**

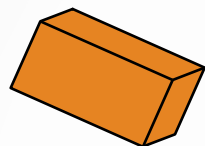
Microwave
Sensor Mounted
on Wall

Walls

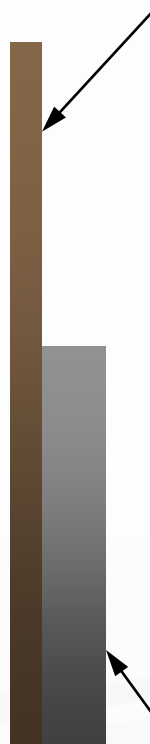


Microwave (Monostatic)

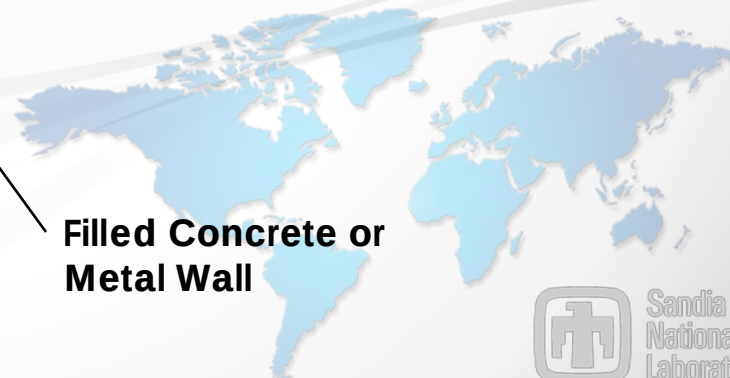
Transmitter/Receiver



Lightweight Construction Wall



**Filled Concrete or
Metal Wall**



Sandia
National
Laboratories



PIR Basic Operations

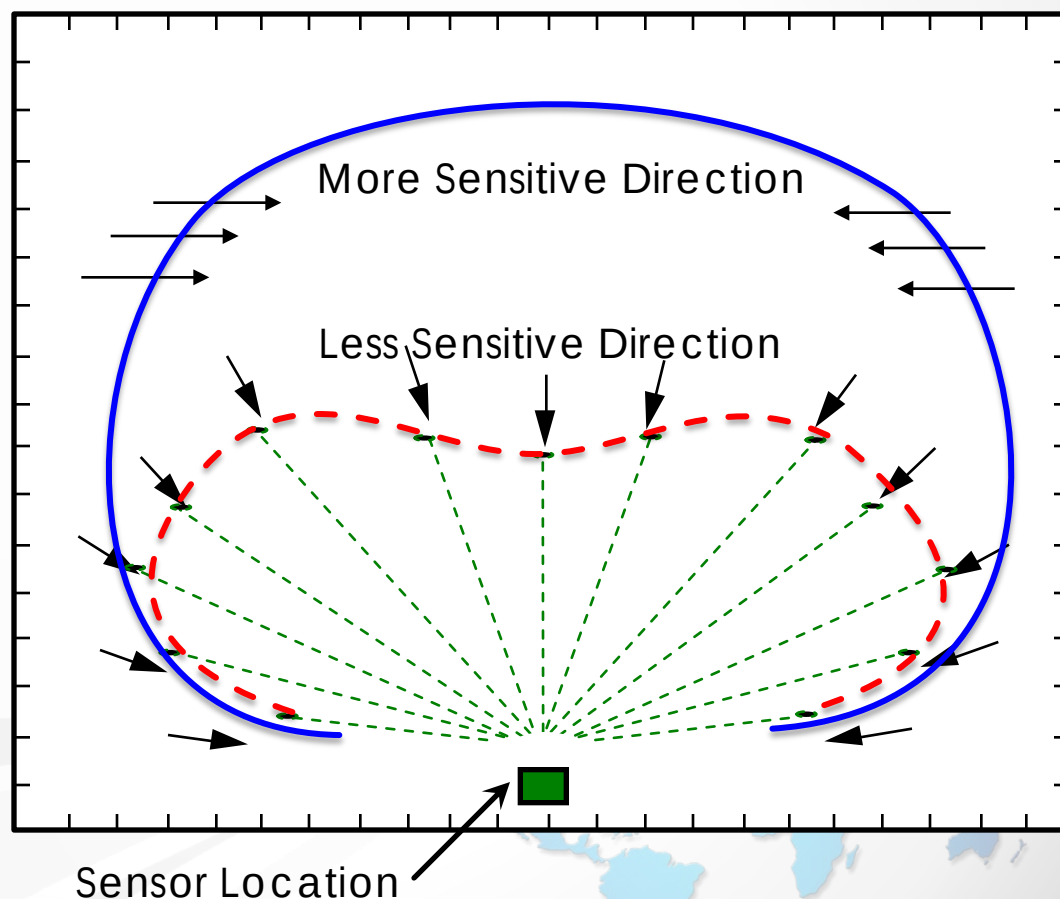
- The **Passive Infrared (PIR)** sensor is the most commonly used interior sensor
- The PIR receives infrared energy from objects in its “view”
- Ceilings, walls, floors, furniture, and all other objects emit infrared energy proportionate to their temperature
- Detection of motion is accomplished by measuring changes in received infrared energy





PIR Detection Pattern Example

(Walking rate for 1ft/sec)





Video Motion Detection

- Processes camera video signal
 - o Divides video scene into cells or zones
 - o Detects brightness/contrast changes in each cell
 - o Looks for logical movement
- Requires constant, controlled lighting





Dual Technology Sensors

- How a Dual Tech sensor works
 - o A Dual Tech sensors contain two different types of sensor technologies
 - o The unit **“AND”**s the two technologies so that both sensors must detect an alarm condition in order for a “valid” alarm signal to be sent to the central alarm monitoring system
- Alarm processing results
 - o Big reduction in NAR (GOOD)
 - o Small reduction in Pd (NOT so good)

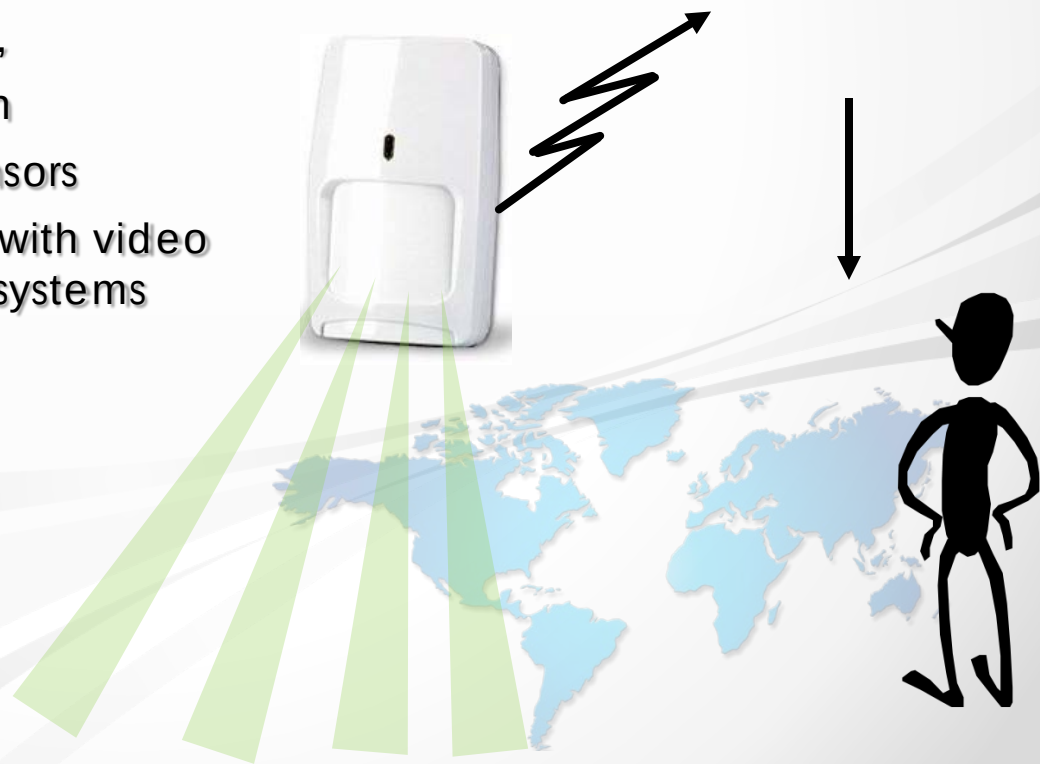
Both sensor technologies must detect motion in order to cause an alarm.



Interior Sensor Systems

- Preferred sensor **features and set-ups:**

- o Tamper-indicating
- o Self-testing
- o Properly installed
- o Where possible & desirable,
 - Use protection-in-depth
 - Use complimentary sensors
 - Sensors are integrated with video assessment and delay systems



Interior Sensor Selection Chart

32

Interior Sensor Summary

Features to look for:

- High P_s with low NAR
- Low vulnerability
- Fast communication system
- Good lighting & assessment system
- Balanced system approach
- No single point component failure
- Protection-in-depth
- Variety of technologies available
- Applications include detection of boundary penetration, motion, and proximity to target
- Performance measures determine suitability in given applications

Questions?



GLOBAL THREAT REDUCTION INITIATIVE

Working to reduce and protect vulnerable nuclear and radiological material located at civilian sites worldwide.

Module G

Entry Control



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.





Module Objectives

- Understand the functions of entry control technologies
- Understand the strengths and weaknesses of various types of equipment

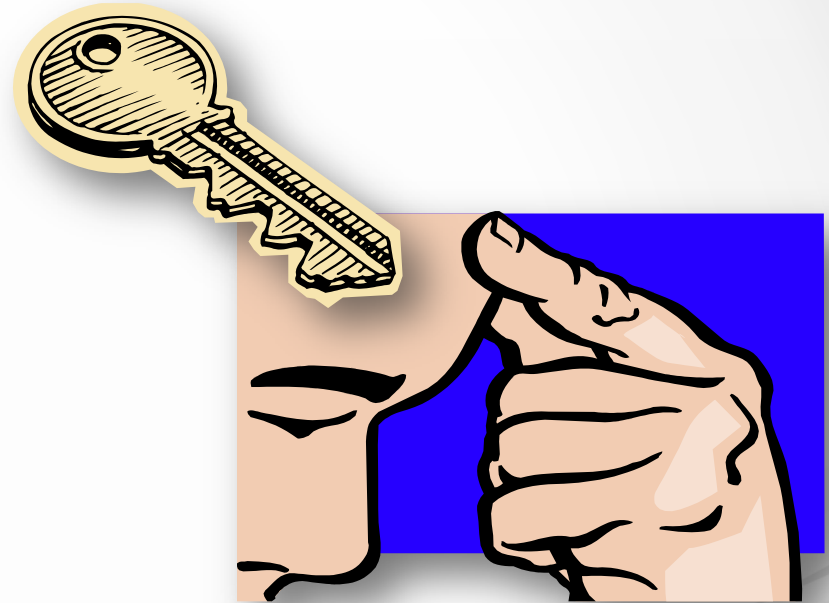


Purposes of Entry Control

ENTRY	Allow entry of • Authorized persons • Authorized material	Prevent entry of • Unauthorized persons • Weapons • Explosives • Other contraband
EXIT	Allow exit of • Authorized persons • Authorized material	Prevent exit of • Critical assets • High value assets

Basis of Personnel Entry Control

- Something you possess
 - o key
 - o Card
- Something you know
 - o PIN
 - o Password
- Something about you
 - o biometric feature



**“Something you have, something you know,
And something you are.”**

Techniques of Personnel Entry Control



Personnel Entry Control

**Manual
(Police or Guards)**

**Photo
Badge**

**Automated
(Machines)**



Credential

**Memorized
Code (PIN)**

**Personal
Characteristic**



Personnel Entry Control Errors

False reject - Type I

- Authorized persons are not allowed to enter
- Easy to quantify

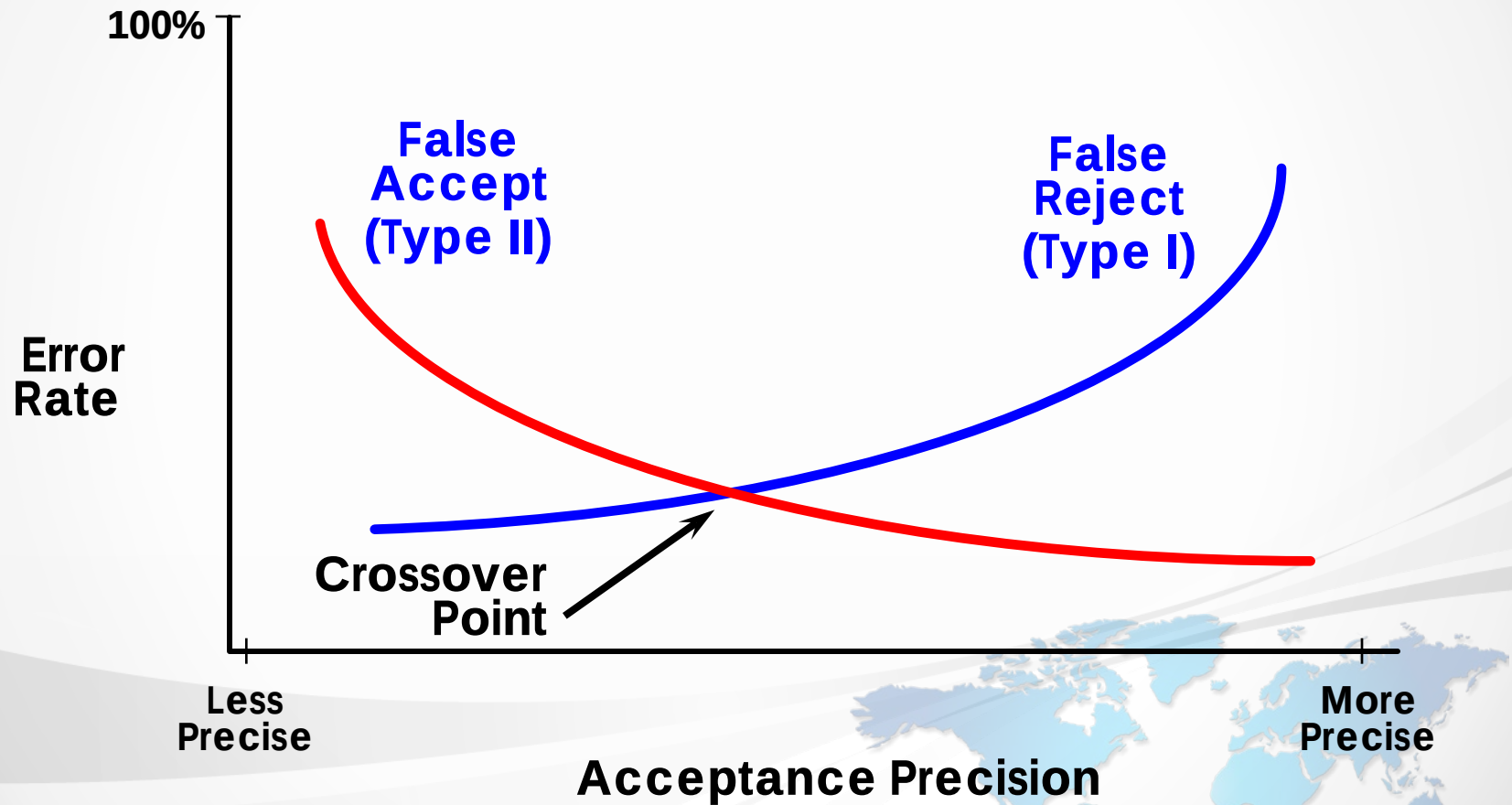


False accept - Type II

- Unauthorized persons are allowed to enter
- Difficult to quantify



Error Rates



Types of Credentials

- **Verified by protective force guards**
 - o Take-home photo badges
 - o Exchanged photo badges
 - o Electronically stored images
- **Verified by machine**
 - o Coded badges



Coded Badges

Positive Features

- Control access by location and time
- Record each access
- Have low false rejection rate
- Perform consistently

Negative Features

- Identify badge, not person
- Require maintenance
- May be defeated by counterfeit badge



Characteristics of Proximity Badges

- Potentially minimize operational impacts
 - o Hands-free operation
 - o Transparent to user
- Induction powered
 - o Resonant frequencies
 - o Coded RF transmitter
- Battery powered
 - o Magnetically initiated
 - o RF initiated



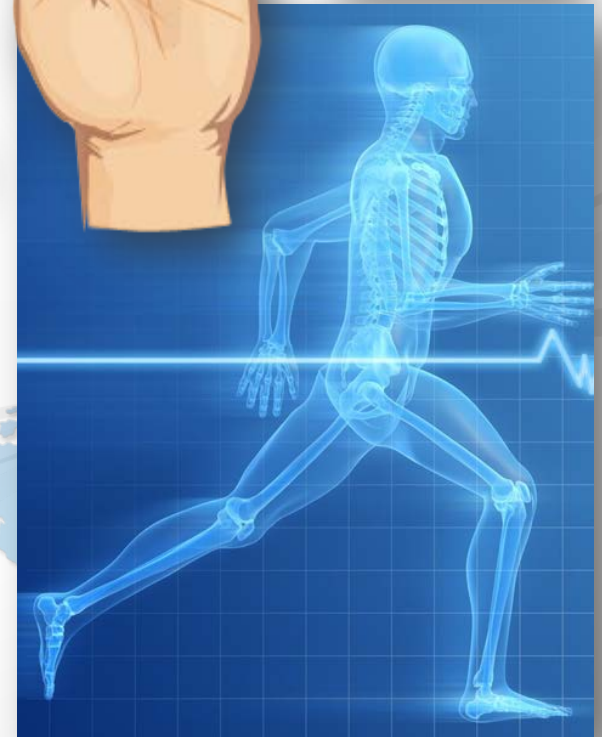
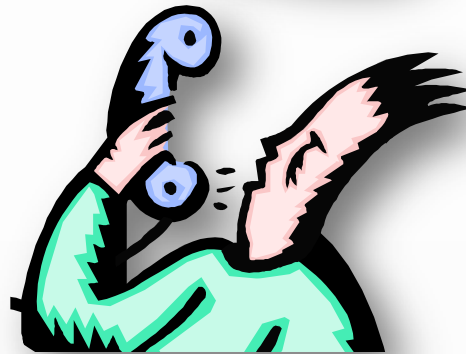
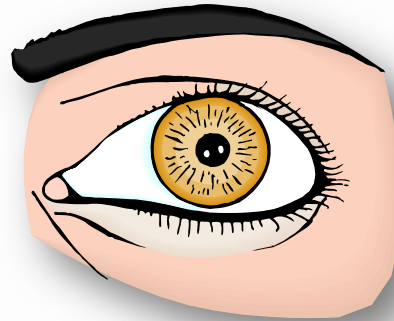
Ease of Counterfeiting Coded Badges

Proximity read	difficult
Direct read	
Magnetic stripe	easy to difficult
Bar code	easy
Magnetic spot	average
Wiegand wire	average
Optical	difficult
Capacitance	difficult
Smart card	difficult

Personal Identity Verification

May be based on:

- Fingerprint
- Handwriting
- Hand geometry
- Retinal pattern
- Iris Pattern
- Voice
- Other



Fingerprint Scanner



Handwriting Reader



Hand Geometry Scanner



Eye Retinal Scanner



Iris Scanner



GLOBAL THREAT REDUCTION INITIATIVE

Voice Recognition Device



Features of Personal Identity Verification Systems

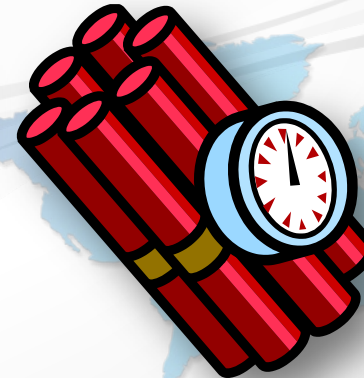
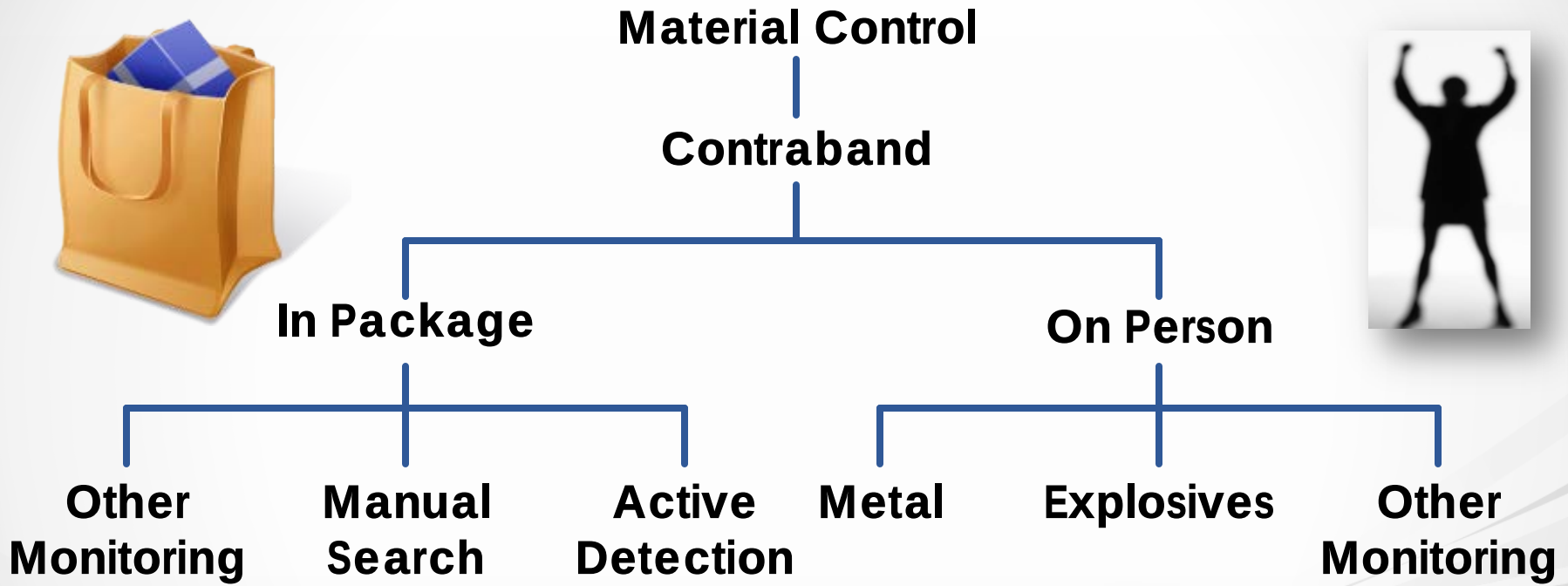
- **Verification times**
 - o 4 to 20 seconds
- **Enrollment**
 - o 1% to 3% of population is incompatible
 - o 20 seconds to 13 minutes required to enroll
- **Cost**
 - o \$1,000 to \$7,000 per terminal



Purposes of Material Control Systems

ENTRY	Allow entry of • Authorized persons • Authorized material	Prevent entry of • Weapons • Explosives • Other contraband
EXIT	Allow exit of • Authorized persons • Authorized material	Prevent unauthorized exit of • Critical assets

Components of Material Control

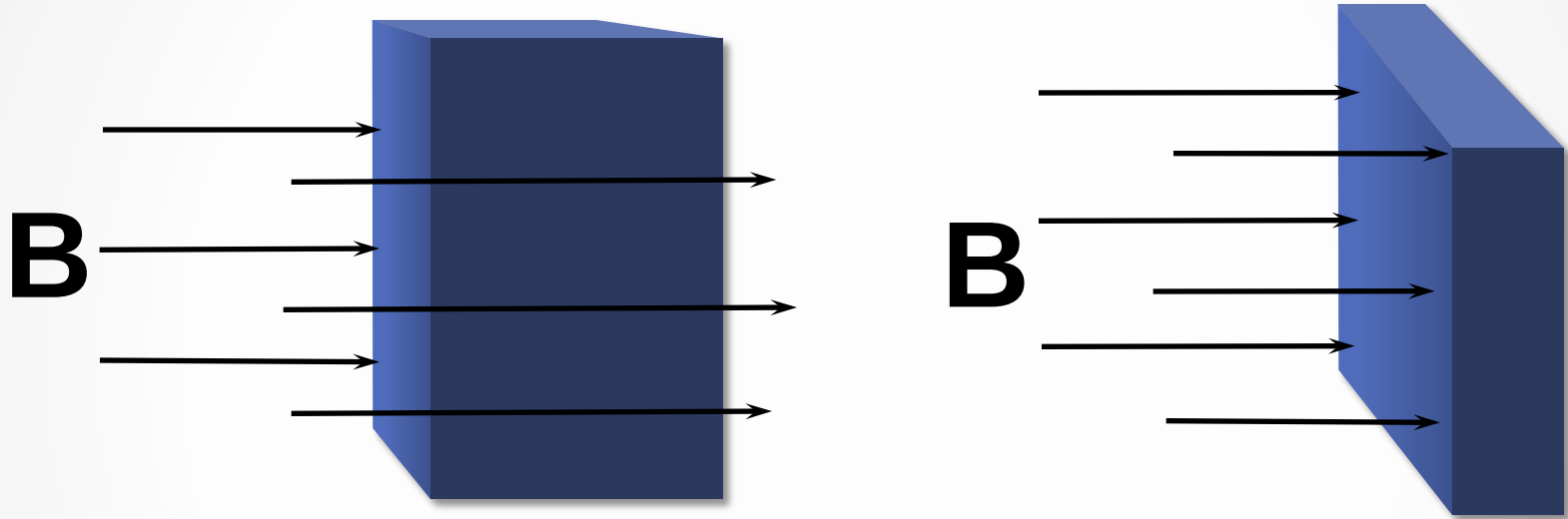


Metal Detection

- Factors that affect sensitivity
 - o Orientation
 - o Ferromagnetic materials
 - o Shape
- Types of detectors
 - o Continuous wave
 - o Pulsed field
- Installation and use

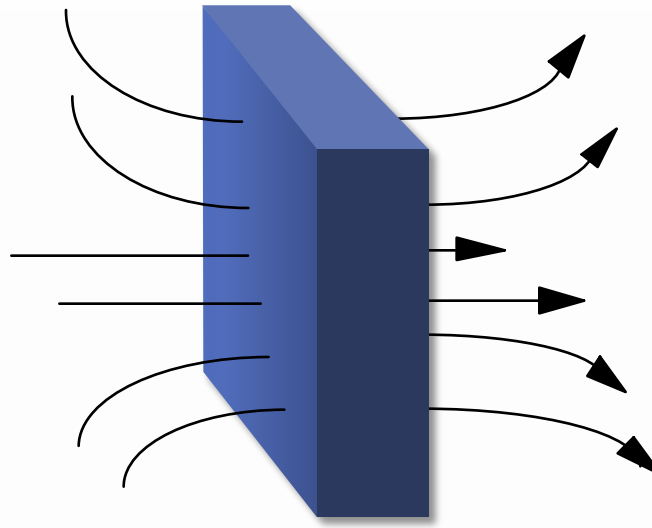


Orientation



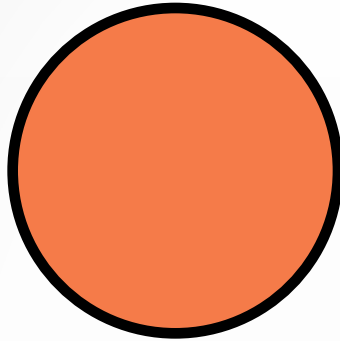
The orientation of an object can change the cross-sectional area that is normal to the magnetic lines of flux

Ferromagnetic Materials



- By providing a path of lower reluctance than the surrounding medium, ferromagnetic materials distort the magnetic field
- By intensifying the magnetic field within their volume, ferromagnetic materials have a higher induced voltage than other materials

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. (9x1 in.) rectangle has the perimeter of 20 in.
- The resistance of the rectangular path is almost

The resistance of the rectangular path is almost twice as high as the circular path. The result is that the circle is easier to detect.

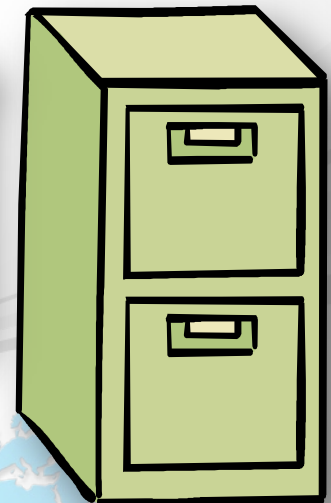
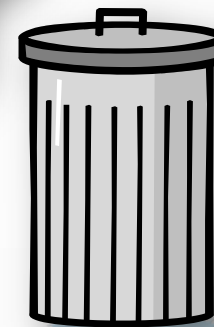
GLOBAL THREAT REDUCTION INITIATIVE

Factors Affecting Metal Detector Operation

- Environment

- Metal doors
- Metal cabinets
- Equipment operating nearby (example: fork lifts)
- Electromagnetic sources (example: radio transmitters, fluorescent lights)

- Type of metal
- Size and shape of object
- Orientation of metal object
- Location of metal object

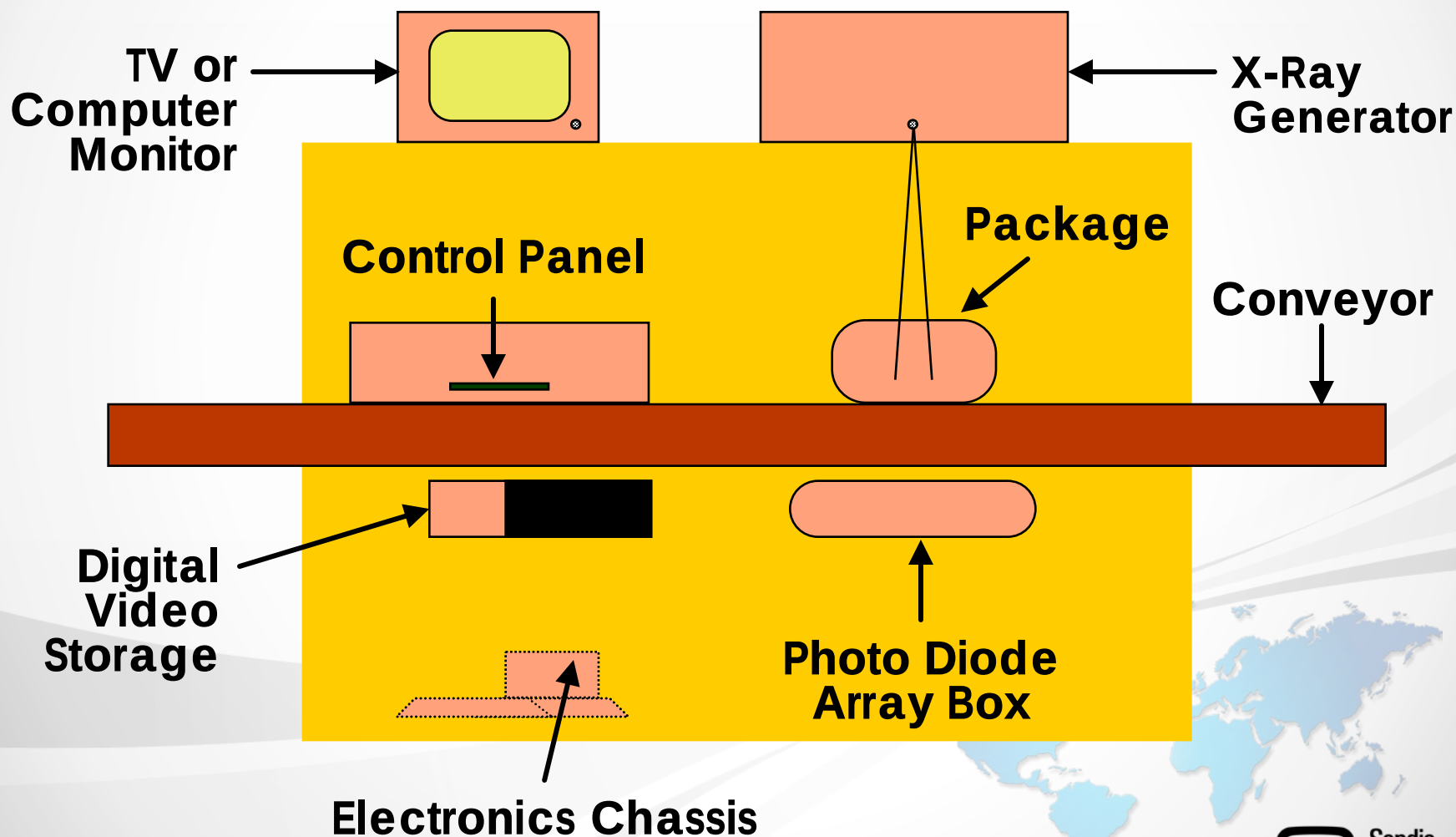


Package Search Systems

- Purpose
 - Detect any contraband contained in packages
- Method
 - Protective force guards manually search packages
 - Active detection uses X-ray, multiple energy X-ray, gamma ray, and neutron activation



X-Ray Package Search System



Bulk Detection Systems

- X-ray
 - o transmission and backscatter
 - o single energy and dual energy
 - o CT scan
- Nuclear Techniques
 - o thermal neutron activation(TNA)
 - o neutron resonance absorption
- Nuclear Magnetic Resonance (NMR)
- Microwave (personnel)
- Low Dose X-Ray (personnel)



GLOBAL THREAT REDUCTION INITIATIVE

Backscatter



GLOBAL THREAT REDUCTION INITIATIVE

Dual Energy



GLOBAL THREAT REDUCTION INITIATIVE

Personnel Backscatter X-ray Scan



Features of a Good Entry Control System

- Cannot be bypassed
- Allows observation by protective force guard
- Protects the guard
- Blocks passage until access and material control are done



Features of a Good Entry Control System (cont.)

- Provides secondary inspection for those who cannot pass automated inspection
- Accommodates peak loads
- Performs access and material control
- Is under surveillance by central alarm station
- Is designed for both entry and exit



Q&A





GLOBAL THREAT REDUCTION INITIATIVE

Working to reduce and protect vulnerable nuclear and radiological material located at civilian sites worldwide.

Module J

Response



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.





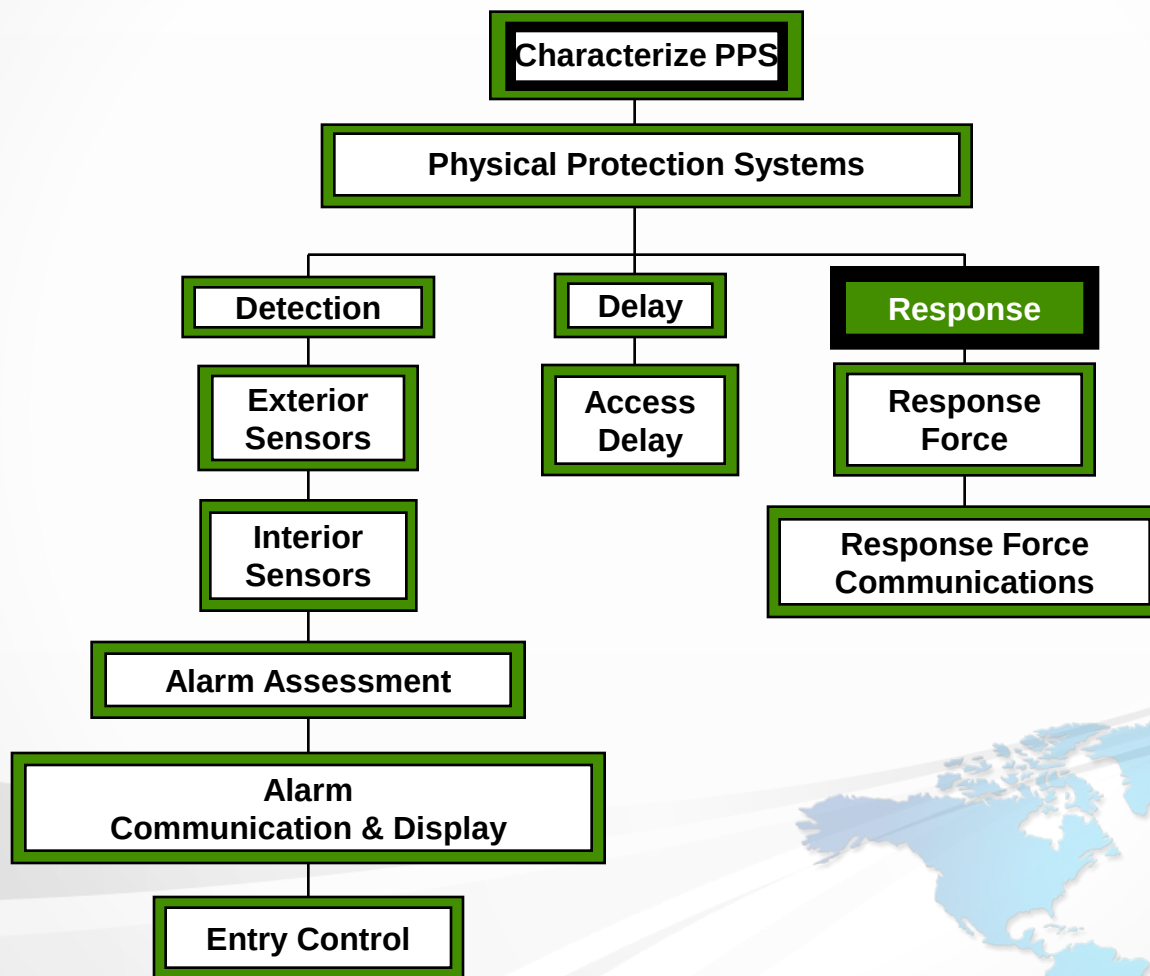
Module Objectives

- Know the basic concepts and principles of response force deployment in a physical security protection environment.
- Understand the role of the response force in overall physical security protection.
- Understand the difference between response force interruption and adversary neutralization.





DEPO - Response



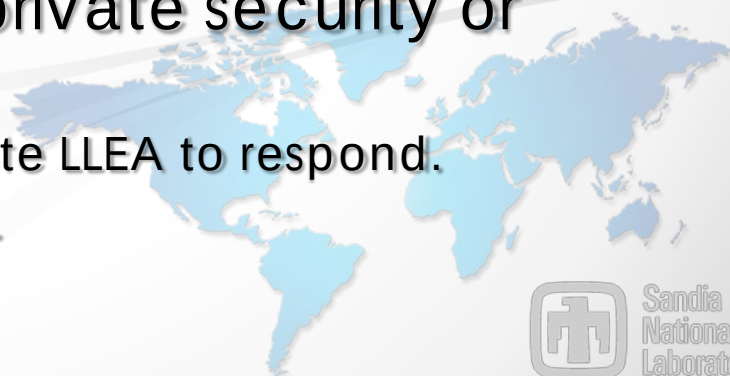
Type of Response Forces

- **Site Security**
 - o Armed Law Enforcement
 - o Private Security
- **Local Law Enforcement Agencies (LLEA)**
 - o Independent from the site
 - o Region, City
- **National Level**
 - o State Police
 - o Military



Legal Basis of Operations

- National, Local, and City
 - National law provides legal authority.
- Legal authority may include authority for:
 - Use of force.
 - Protect lives or prevent great bodily harm.
 - Prevent theft or sabotage of nuclear materials.
 - Carrying weapons and making warrantless arrests.
- Authority may be limited for private security or institution employees.
 - May need an agreement with off-site LLEA to respond.
 - Use of force based on national law.



Role of the Response Force

- Role will be driven by:
 - Type of material being protected
 - Sabotage or theft
 - Denial or containment
 - Recovery and/or recapture
 - Legal basis for authority
 - Level and type of training
- Alarm response and containment.
- Building entry and recapture/recovery.
- Sites rely on LLEA for at least some aspects of the response.



Response Functions

- The primary functions of Response are:
 - Deterrence
 - Delay
 - Interruption
 - Neutralization
- Effective response is achieved by:
 - Receiving & communicating alarms
 - Correct & timely alarm assessment
 - Communicating alarms to responders
 - Adequate deployment to the alarm
- Effective event or threat mitigation may be achieved by:
 - Arrest / Use of Authorized Force



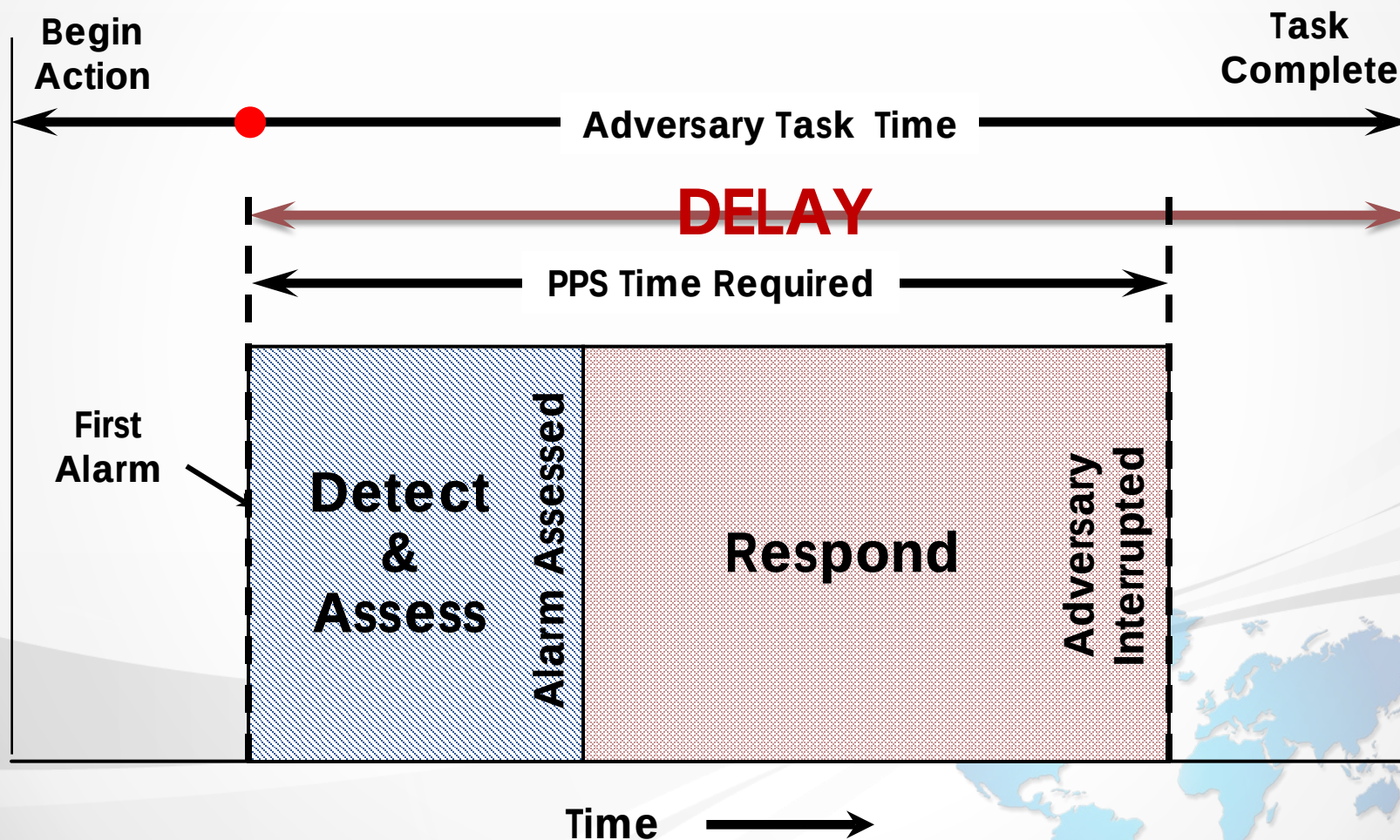
Deterrence

- Security Force and LLEA patrols should be:
 - o Highly visible
 - o Frequent
 - o Random and unpredictable
 - o Present a professional image





Interruption



Characteristics of Effective Interruption

- Tactics are trained to and performance tested.
- Deployment is timely.
- Deployment is sufficient in numbers of responders – should have overwhelming superiority.
- Reliable communications and communication protocols.
- Accurate assessment of alarms and the event in question
- Tactically sound deployment to the correct location.

This requires Planning, Training, and Performance Testing.



Neutralization

- Effective neutralization depends on:
 - o Rules of engagement
 - o Effective plans
 - o Good communication
 - o Training and exercises
- Effective neutralization includes:
 - o Numbers, weapons, training
 - o Deployment tactics
 - o Engagement
 - o After action procedures
- Difficult to measure estimate effectiveness.
- Success depends on:
 - o Right people
 - o Right place
 - o Right time
 - o Right equipment





Working with an LLEA

- LLEA Role:
 - o Develop the written agreement, memorandum of understanding, signed policy, etc.
 - o Work within approved procedures, policies, and practices.
- Determine the effectiveness of the off-site response force.
 - o Periodic meetings or briefings between the Site and LLEA.
 - o Tours, walk-downs.
 - o Target Folders.
 - o Site familiarity and accessibility.



Knowing Your LLEA's Capabilities

- How does the facility communicate an alarm to site security or LLEA?
 - Hotline, Telephone (emergency #), Radio
- What is the alarm assessment and communication time?
- What is the response time?
 - On-site personnel
 - LLEA personnel
- How will site response forces communicate with LLEA?
 - Radios, cell phones, dispatcher?



Validating Response Capabilities

To ensure that the response system is effective, capabilities can be demonstrated by the following:

- Review MOU, policies, and procedures.
- Training records.
- Performance test communications systems.
- Performance test response times under realistic conditions:
 - Snap shot in time: Who will respond and from where?
 - Natural events & weather conditions.
 - Day & night conditions.
- Joint security and LLEA performance tests with all responders.
- Verify assumptions regarding response responsibilities.



Response Summary

- Types of Response Forces
- Interaction with LLEA
 - Roles and responsibilities
- Response Functions
 - Deterrence
 - Interruption
 - Neutralization
- Effective & timely communications critical



Video: Response Examples

The right people, right place, right time,
and right equipment...



Questions?



GLOBAL THREAT REDUCTION INITIATIVE

Working to reduce and protect vulnerable nuclear and radiological material located at civilian sites worldwide.

Module L

Information Security



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Objectives

- Define information security.
- Understand the what types of information are sensitive.
- Understand what types of security measures are applied to information.



Types of Information

Written



Visual



Electronic



Verbal



Types of Information

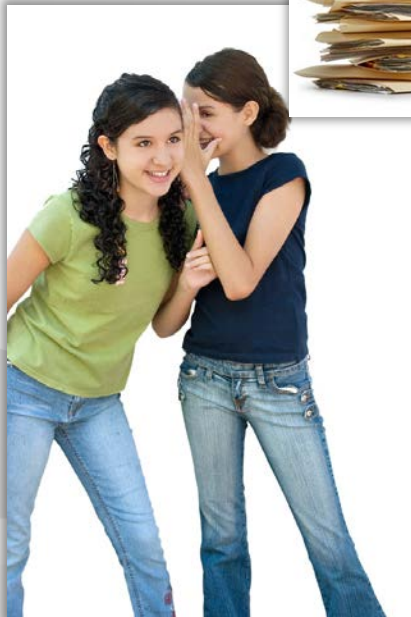
Information can be:

- Written and stored in paper, photographs, maps, schematics.
- Electronic, including communications, files, or images.
- Verbal such as conversations, briefings, and recorded audio and video.
- Visual such as a device or facility.



GLOBAL THREAT REDUCTION INITIATIVE

Information Storage and Communication



Adversary Scenario

To gain access to, corrupt, or deny access to:

- Stored information or information manipulation processes.
- Communicated information.



Information Security

- Information security is:
 - o Protection of information from
 - Disclosure
 - Corruption
 - Inaccessibility
 - o Graded to the severity of consequence.
- Information security assures information:
 - o Confidentiality
 - o Integrity
 - o Availability



Information Sensitivity

What makes information sensitive?

Sensitive information is information that facilitates a malicious act.

- Unauthorized access
- Denial of authorized access
- Authorized access to corrupted information

Degree of sensitivity is same as degree of value to adversary.

Sensitive Information

Examples of sensitive information for security:

- Target information
 - Location, device design, source activity
- Physical Protection information
 - Security components, security procedures and plans
- Vulnerability information
 - Consequence severity, weakness of device
- Access information/schedules/procedures
 - Maintenance schedules, procedures, transport routes

Sensitivity Based on Risk

Low

Loss of information, availability of information, or reliability of information could be expected to have limited benefit to adversary (little change in security risk), but could encourage attempt.

Moderate

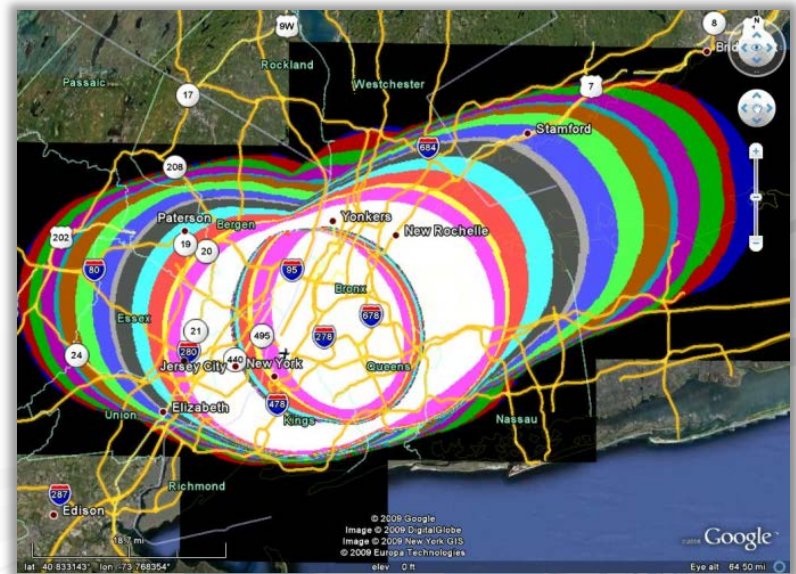
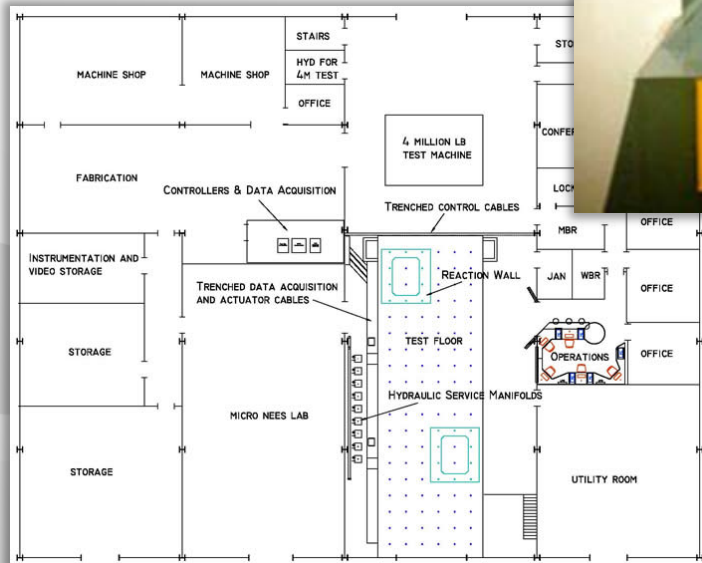
Loss of information, availability of information, or reliability of information could be expected to benefit to adversary (large change in security risk for limited scenarios).

High

Loss of information, availability of information, or reliability of information could be expected to greatly benefit to adversary (significant change in security risk or several scenarios).

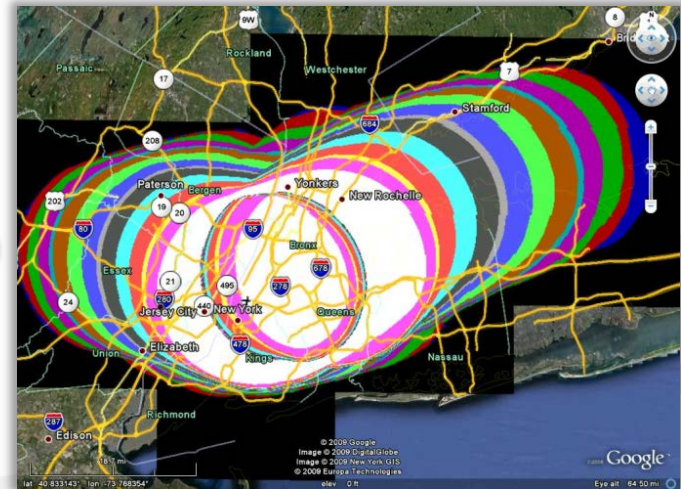
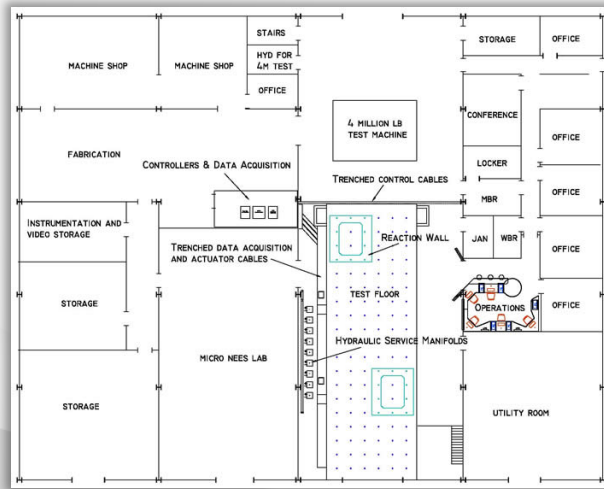
Information Sensitivity

Information without Context **may not be** sensitive.



Information Sensitivity

Information without Context **may be** sensitive



Security Measures

- Administrative Measures

- o Procedures
- o Surveillance
- o Penalties

- Technical measures

- o Locks/barriers
- o Cameras
- o Sensors
- o Tamper indicating devices



Security Measures

- Graded Approach
 - o Highest Value to Adversary
 - Alone could lead to successful adversary act
 - o High Value to Adversary
 - Alone could increase likelihood of success of adversary
 - o Important to Adversary
 - In concert with other information, could lead to successful adversary act



Security of Information

Required security for information can be expressed from a combined look at its sensitivity:

= {(confidentiality impact), (integrity impact),
(availability impact)}

Each impact can be low, medium, or high.



Security Measures (example)

Highest Value to Adversary (High)

- Two layers of administrative and technical measures to yield high confidence that data integrity, confidentiality, and availability is ensured—surveillance, locks, robust passwords, network isolation, video and sensors.

High Value to Adversary (Moderate)

- One layer of administrative and technical measures to provide some confidence that attempts to access , disrupt, or deny data is discouraged and perpetrators caught—administrative access logs, locks, sensors and video recording.

Important to Adversary (Low)

- Administrative measures to discourage malicious acts, and evidence gathered to prosecute (access tracking). Minimal technical measures (hi security locks, robust passwords, firewalls).

Summary

- Information comes in many forms.
- Information security addresses information confidentiality (loss), integrity (accuracy), and availability (access)
- Sensitivity of information is related to severity of consequence if lost.
- Graded approach applied to security including administrative and technical measures.



Questions?

