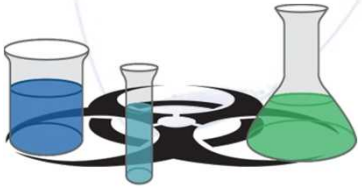
SAND2008-5663P

Physical Protection 101

Biothreats and Legitimate Bioscience Laboratories

Training Course
International Biological Threat Reduction
Sandia National Laboratories



SAND No.
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

International
BIOLOGICAL THREAT REDUCTION

Objectives

- To provide a basic introduction to physical protection system concepts and terminology
- To provide a definition for the characteristics of an effective physical protection system
- To introduce physical protection system methodologies and technologies
- To provide knowledge about the complexities of physical protection system implementation and evaluation

Physical Protection

- **The objective of physical protection is to protect objects/material and/or people from adversaries intent on performing adverse acts**
  - Unauthorized removal of objects or material
  - Sabotage
  - Bodily harm (facility staff and/or general population)
- **A system is a procedure or process for obtaining an objective**
- **A Physical Protection System follows three principles to met the physical protection objective**
  - Delay
  - Detection
  - Response

Physical Protection *is not*:

- **Safety**
- **Emergency response (fire, medical, clean-up)**

Security and safety are not the same but must work together

- **Personnel security (trustworthiness)**
- **Information/network security**

A comprehensive security system requires physical protection, personnel, and information/network security, these components interoperate

How much protection is enough?

A risk based approach help decision makers determine how much protection is enough, given…

- There will always be some level of risk
  - All attacks cannot be prevented
  - All consequences cannot be eliminated

International BIOLOGICAL THREAT REDUCTION

Defining System Requirements

- Regulatory Compliance
  - **Regulations specify which features must be present**
  - Simple, consistent, not subjective
- Expert Opinion
  - **Experience-based estimation of required features**
  - Subjective
  - Inconsistent (each subject matter expert will have a different opinion)
- Performance Analysis
  - **Analytical determination of system performance**
  - Complex; effectiveness must equal or exceed specified metric
  - Requires design experts and analytical techniques
  - Structured (consistency, non-subjectivity, repeatable results)
  - Directly related to physical protection objectives
  - Requires data
    - **Performance testing**
    - **Response exercises**

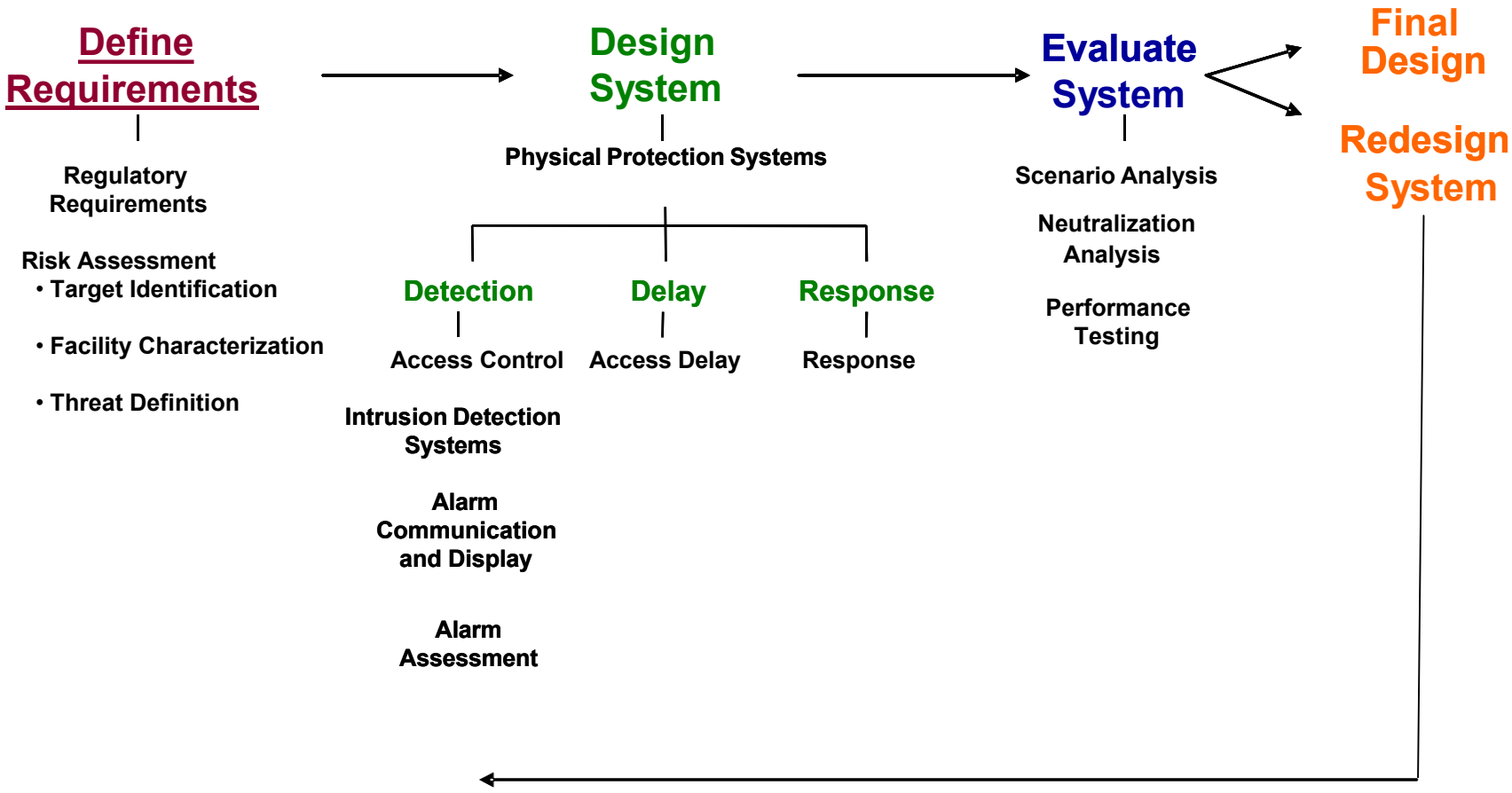
Advantages and Disadvantages

Design Approach	Advantages	Disadvantages
Expert Opinion	**Easiest to apply**	**Two experts disagree? Verify performance? Satisfy regulations?**
Compliance Based	**Easy to apply, Easy to measure, Meets State regulations**	**No assurance of desired performance**
Performance Based	**Identifies effectiveness, Validates performance**	**More difficult to apply, requires expertise**

Typical Approach to Specifying Requirements

- **Use all three methods**
  - Expert opinion on options
  - Compliance requirements where quantification is difficult
  - Performance requirements should be in as many areas as feasible
- **The combination leads to improved cost-effectiveness: right amount of security in right place**

Physical Protection System Design Scheme



International BIOLOGICAL THREAT REDUCTION

Regulatory Requirements

- **International Community**
  - Treaties and Conventions
  - IAEA
  - Multinational commercial and government organizations
  - UN1540

- **State**
  - Competent Authority (define DBT)
  - Other Regulatory Agencies
  - National Police and Law Enforcement Agencies
  - Intelligence Service
  - Military
  - State System for Accountancy and Control (SSAC)
  - National Response Agencies

Risk Assessment

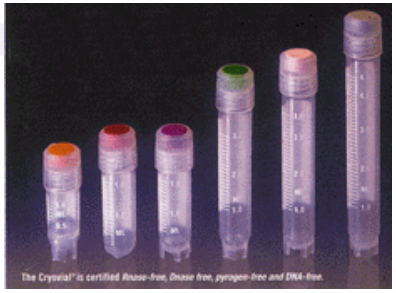
- **Target Identification**
  - What needs to be protected?
- **Facility Characterization**
  - What needs to be considered about the facility?
- **Threat Definition**
  - What is the threat to this asset and facility?

Risk Equation

$$R = C * L (P_0 * (1 – P_E))$$

- Risk is a function of the consequences and likelihood
- Consequences
  - Based upon the identified asset
- Likelihood is a function of the probability of attack (P_0) and the effectiveness of the physical protection system (P_E)
  - Probability of an attack
    - Based upon the threat definition
  - Physical protection system effectiveness
    - Based upon the facility characterization and the designed physical protection system

Asset Identification

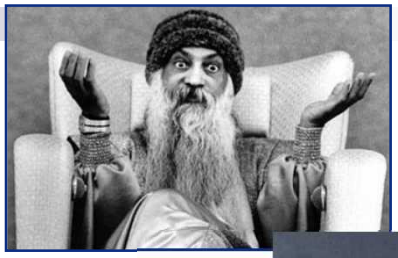


- **Each class of asset unique**
  - Each individual asset unique
- **An assessment required for each asset that is based upon physical security objective**
  - Protection of a specific material or object
    - **Material prosperities also must be included in assessment**
  - General protection of a facility
  - Protection of people at a facility
- **The asset properties drive the consequence component of the risk assessment**
  - Loss of life due to ‘release’ of asset
  - Loss of money due to loss of asset via theft or sabotage

Facility Characterization

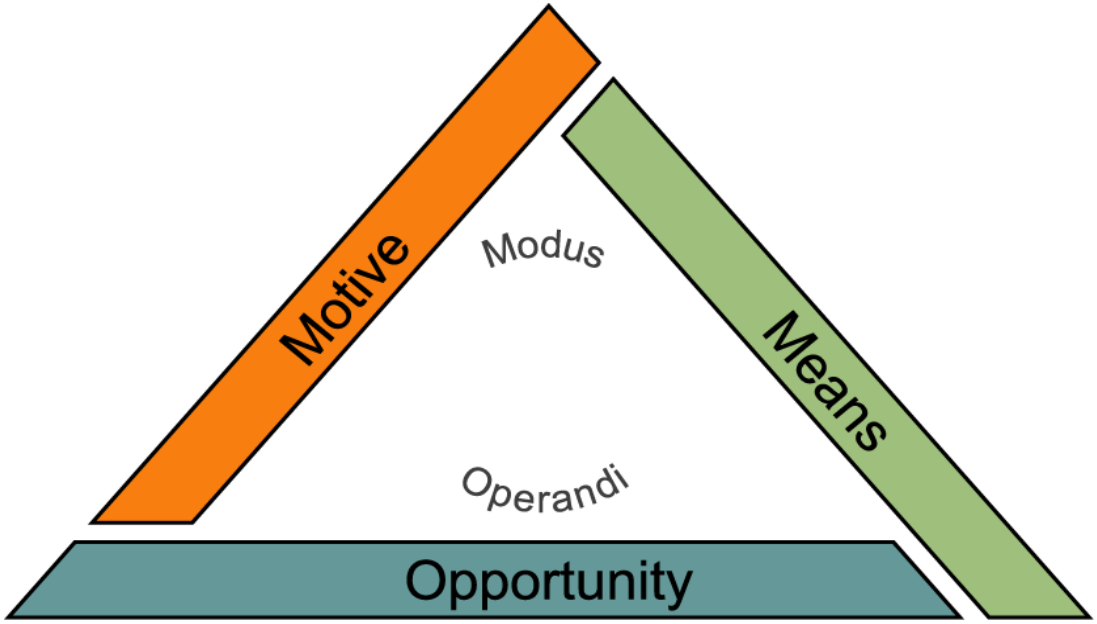
- Large or small facility
- Open campus or limited access area
- Long term storage area or requires daily access
- Location of facility including terrain properties
- Fixed location or protection of a moving asset

Threat Definition



- **Types of threats:**
  - Terrorists
  - Criminals
  - Extremists
- **Threats can be classified as:**
  - Outsiders: persons without authorized access to a facility
  - Insiders: persons with authorized access to a facility
- **Threat motivations**
  - Theft
  - Sabotage
  - Criminal
  - Financial

The Threat Triangle

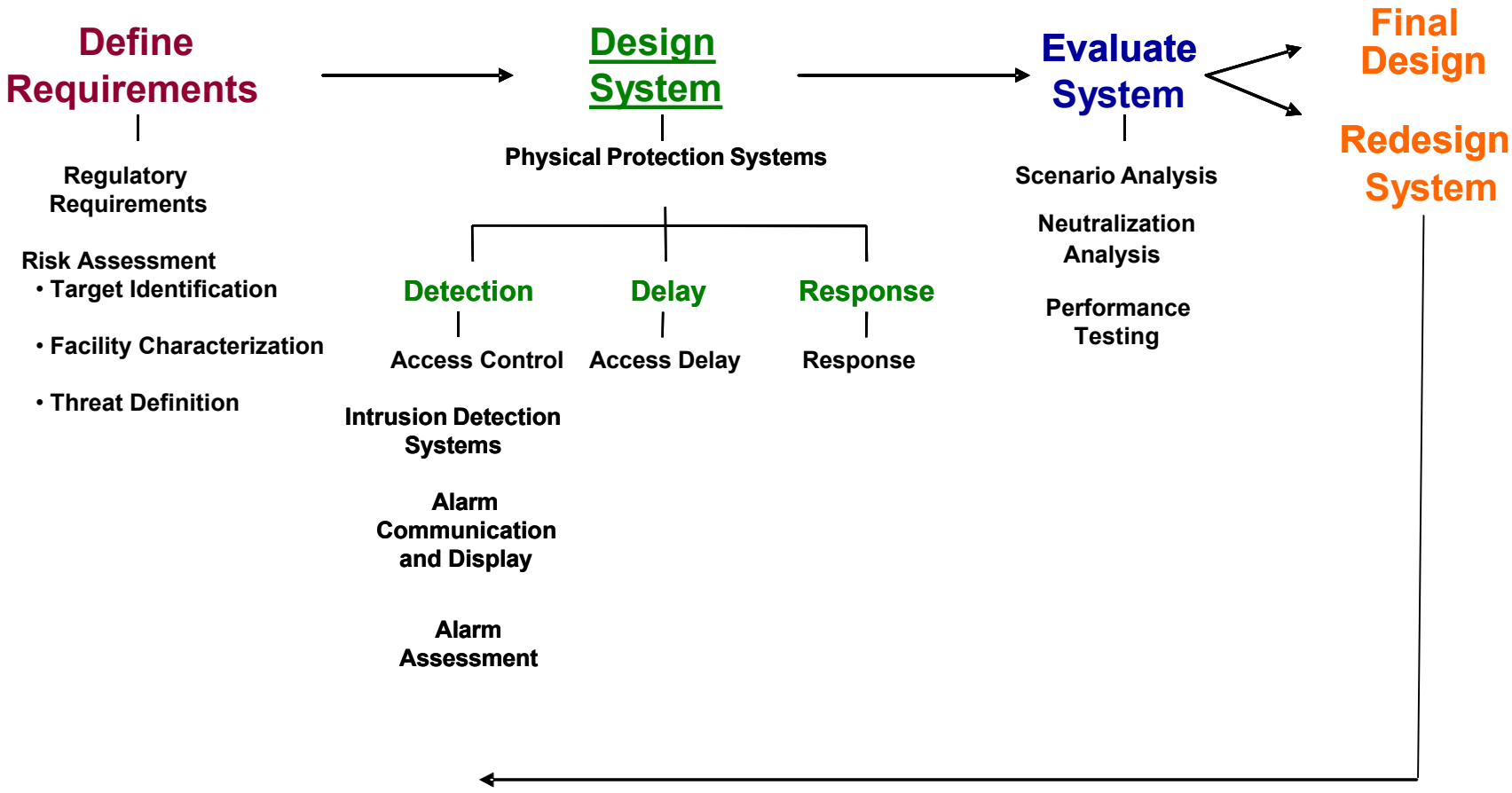


Motive + Means + Opportunity = Attempt

Means and Opportunity based upon the classification of threat

International BIOLOGICAL THREAT REDUCTION

Physical Protection System Design Scheme



International BIOLOGICAL THREAT REDUCTION

Physical Protection System Principles

- **Detection**
  - Determining that an unauthorized action has occurred or is occurring
  - Detection includes sensing the action, communicating the alarm to a control center, and assessing the alarm
- **Delay**
  - Slowing down an adversary's progress
- **Response**
  - The act of alerting, transporting, and staging a security force to interrupt and neutralize the adversary
  - Mitigation and recovery interface with the response function

Detection

Performance metric: Probability of detection

Design parameters:

- Time for communication
- Frequency of false alarms
- Vulnerability to defeat

- **Access Control**
- **Intrusion Detection**
- **Alarm Communication, Display and Assessment**

"Detection without Assessment is <u>not</u> Detection"

Access Controls

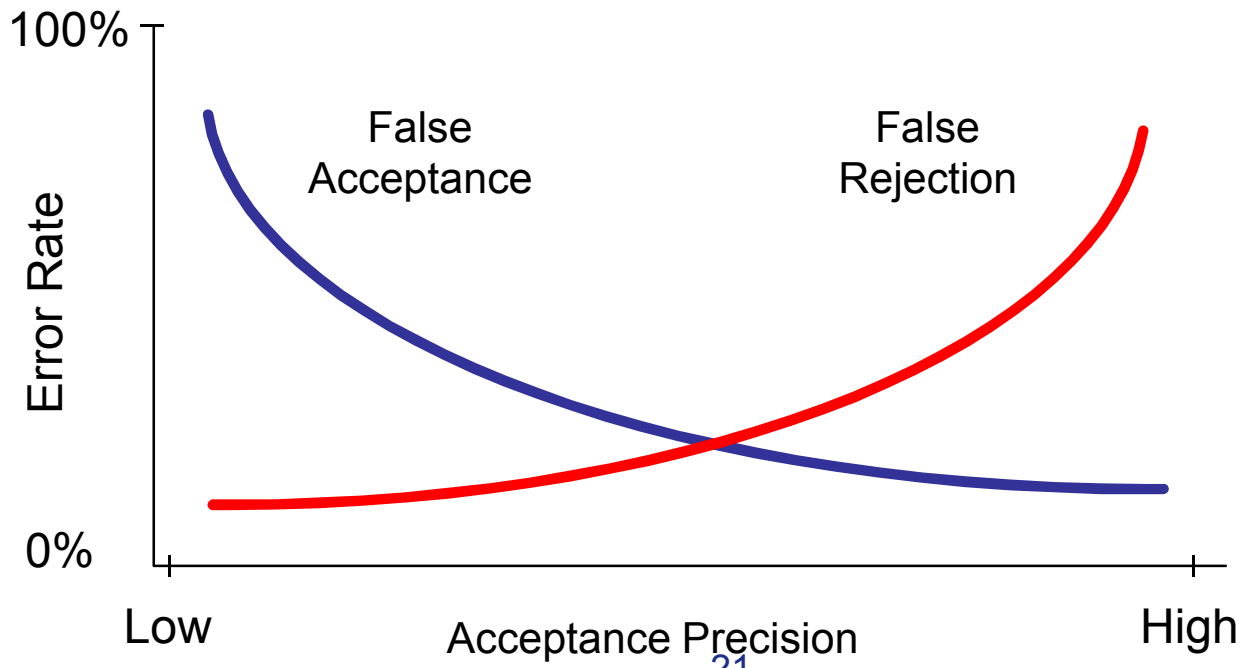
- **Allow entry of**
  - Authorized persons
- **Prevent entry of**
  - Unauthorized persons
- **Allow exit of**
  - Authorized persons

Basis of Access Controls

- **Something you have**
  - Key
  - Card
- **Something you know**
  - Personal Identification Number (PIN)
  - Password
- **Something you are**
  - Biometric feature (i.e., fingerprints)
- **Combining factors greatly increases security**
  - Combinations typically used for exclusion or limited access areas

Errors for Access Control

- **False rejection**
  - Authorized persons are not allowed to enter
  - Easy to quantify
- **False acceptance**
  - Unauthorized persons are allowed to enter
  - Difficult to quantify



International BIOLOGICAL THREAT REDUCTION

Considerations for Access Control

- **Access control systems**
  - Can be low or high tech
  - Give varying levels of assurance of person's identity
    - **Risk assessment!**
  - Have error rates and enrollment issues
    - **1-3% of the population is incompatible with any biometric device**
    - **Must have secondary method for those who cannot pass automated inspection**
  - Needs to accommodate peak loads / throughput
  - Should be designed for both entry and exit

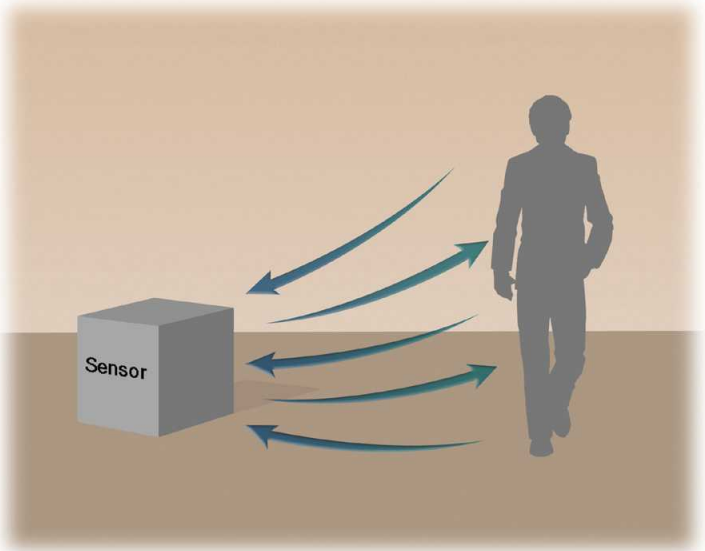
Intrusion Detection

- **Objective: Detect unauthorized access**

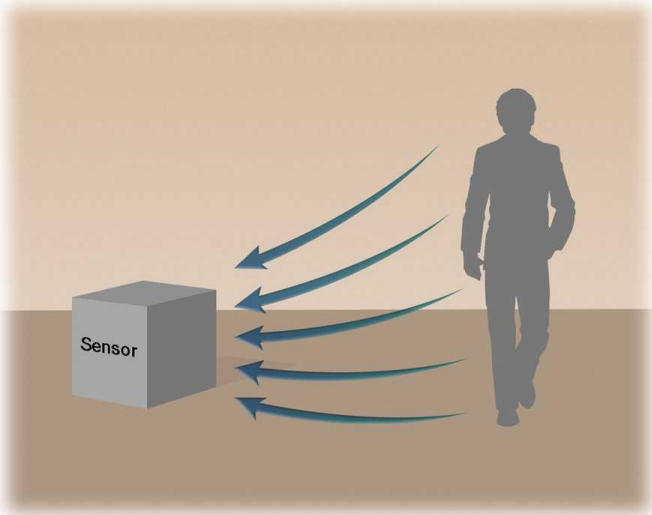
- **Many types of intrusion detection**
  - Personnel noticing unauthorized access attempt or unauthorized persons
  - Electronic sensors
    - **Active**
    - **Passive**
    - **Covert**
    - **Visible**
    - **Volumetric**
    - **Line detection**
    - **Line of sight**
    - **Terrain Following**

Concept of Active and Passive Sensors

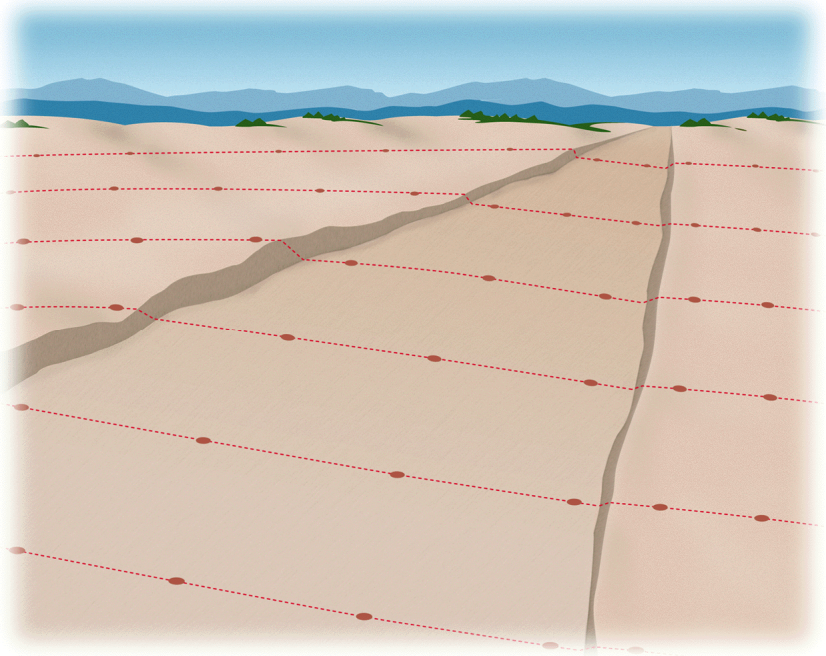
- **Active sensors emit energy and measure reflected response**



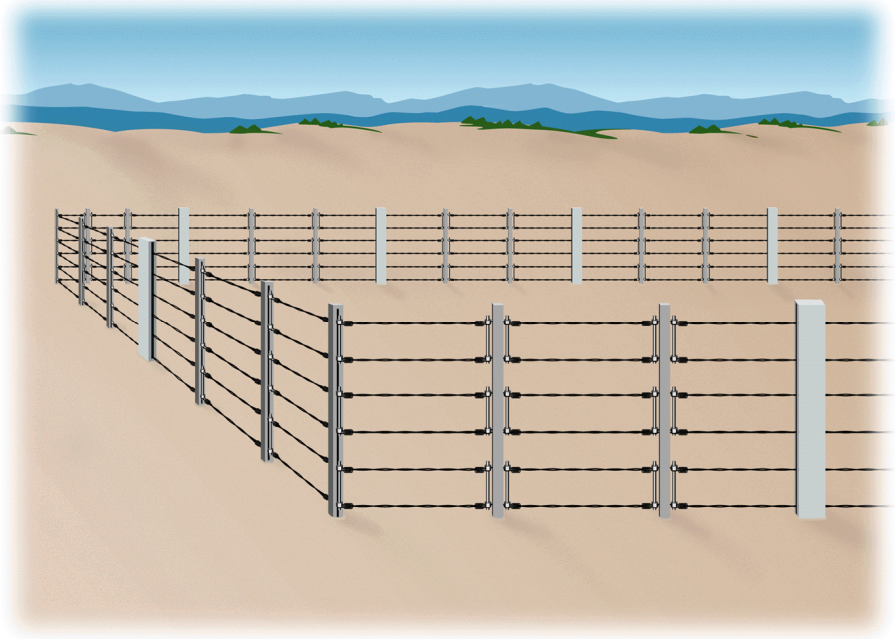
- **Passive sensors respond to energy emitted by external sources**



Covert or Visible Sensors



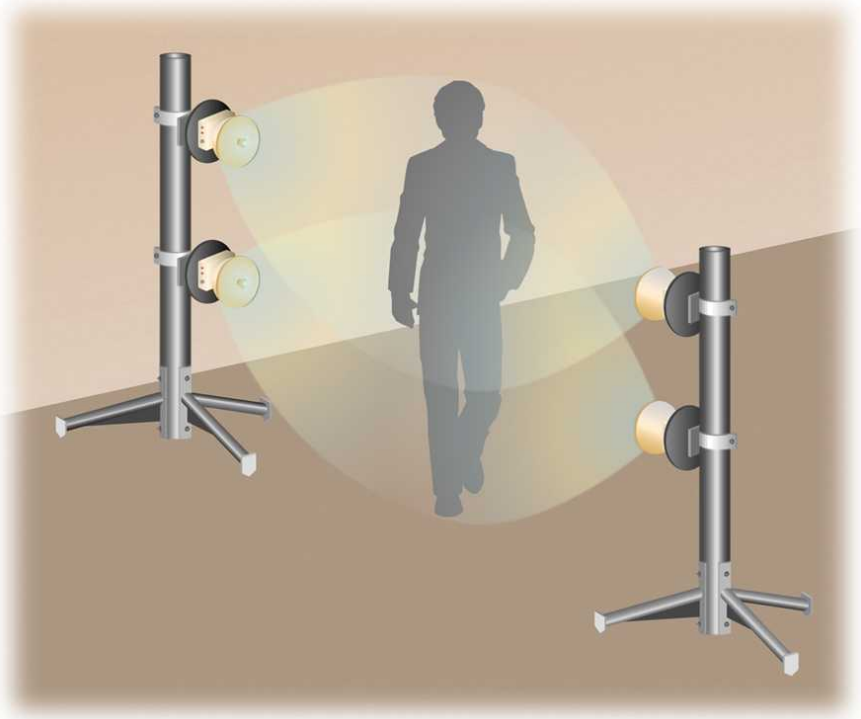
Covert
Hidden sensors



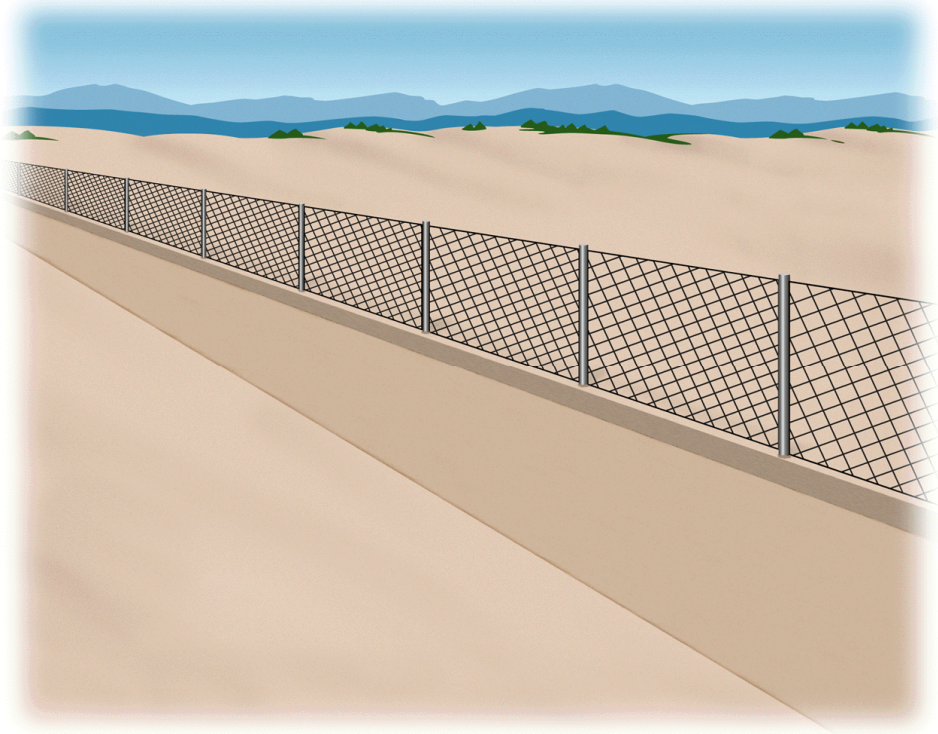
Visible
Sensors in plain view

International
BIOLOGICAL THREAT REDUCTION

Volumetric or Line Detection



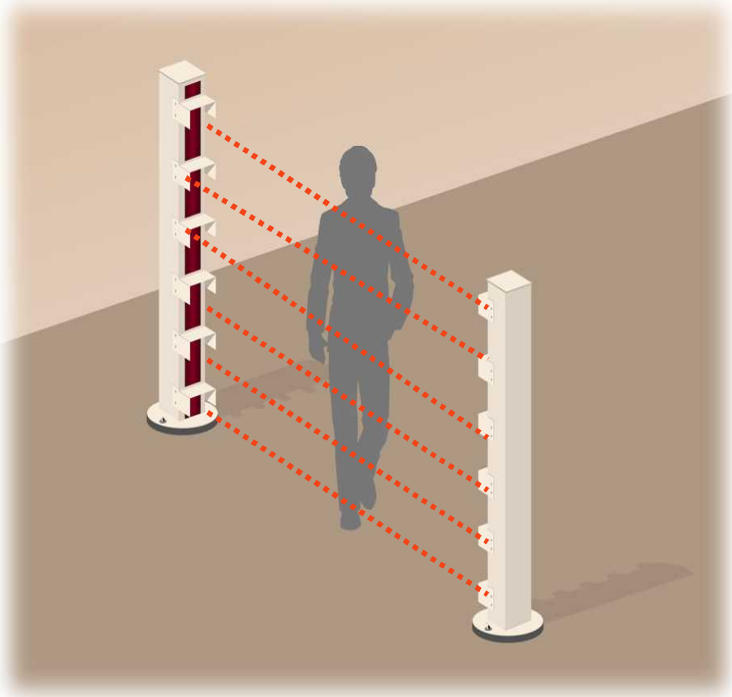
Volumetric
Detection in a volume of space

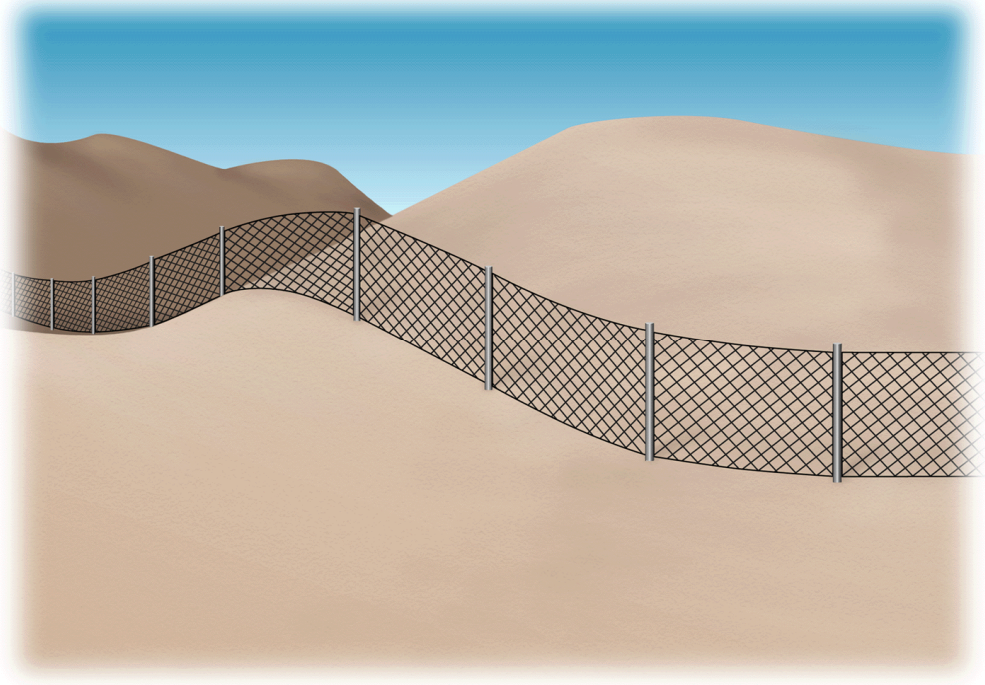


Line Detection
Detection along a line

International
BIOLOGICAL THREAT REDUCTION

Line-of-Sight or Terrain-Following



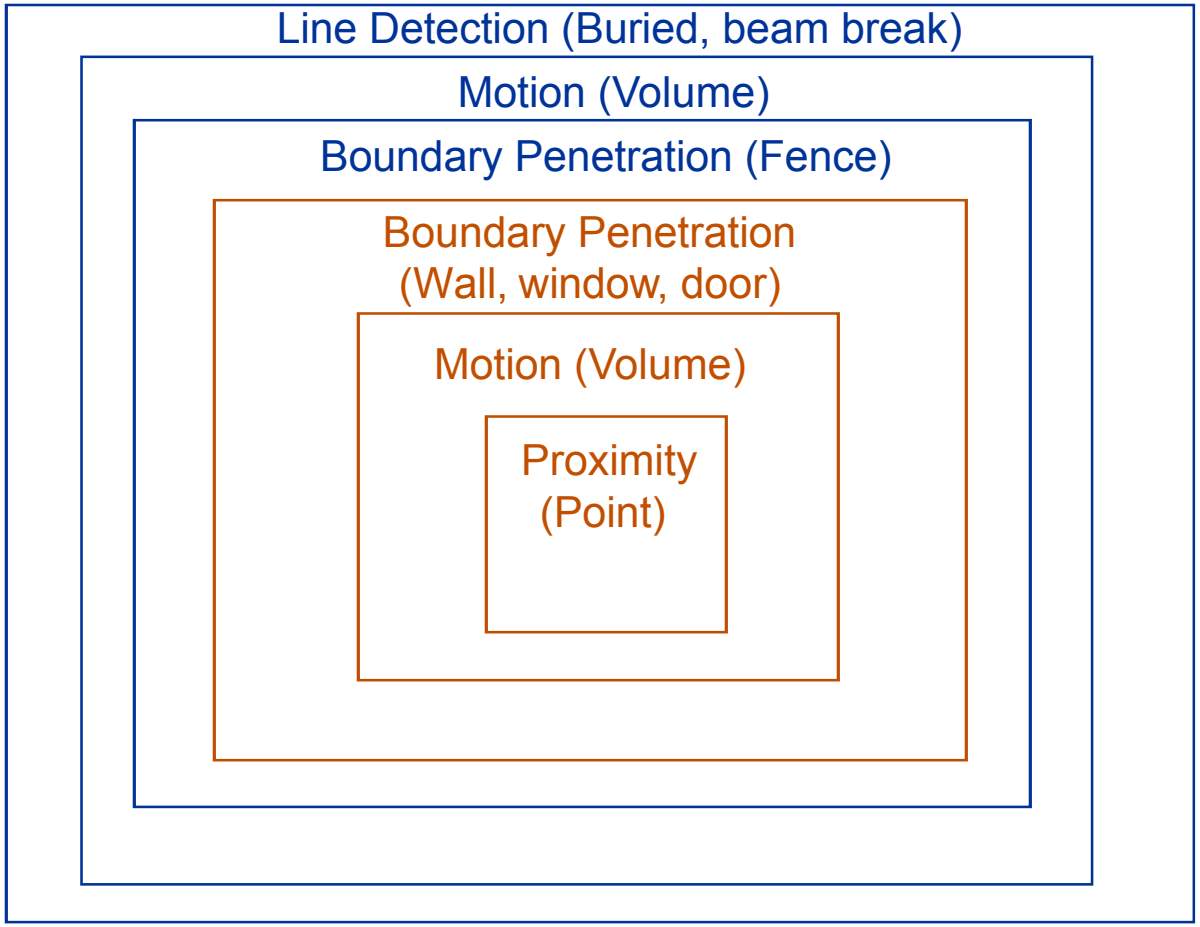


Line-of-Sight
Requires flat surface or short segments

Terrain Following
Able to follow natural contours

International
BIOLOGICAL THREAT REDUCTION

Graded Detection



Exterior Sensor Applications

Interior Sensor Applications

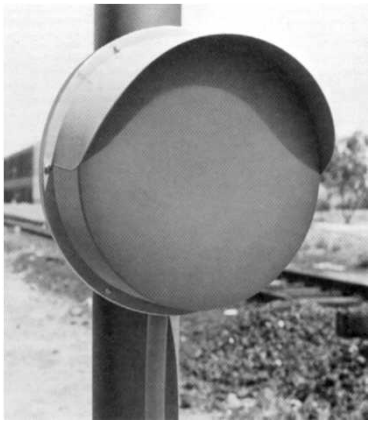
International
BIOLOGICAL THREAT REDUCTION

Categories of Exterior Area Sensors

- *Seismic sensors-* Respond to ground motion
- *Acoustic sensors-* Respond to sound waves
- *Magnetic sensors-* Respond to the presence of magnetic materials (iron based metals)
- *Passive infrared detectors-* Detect presence of object with a thermal signature different from the background
- *Active infrared detectors (break beams)-* Detect presence of an object which comes between an infrared beam and its detector
- *Fiber optic cables-* Detect deflections or damage to cable based on variations in transmitted light
- *Microwave (or radar) sensors-* Detect change in reflected or received microwave energy due to an object in its detection zone
- *Taut wire fence sensors-* Detect efforts to cut or deflect fence wires

Exterior Examples

- **Microwave Intrusion Detection (Volumetric)**

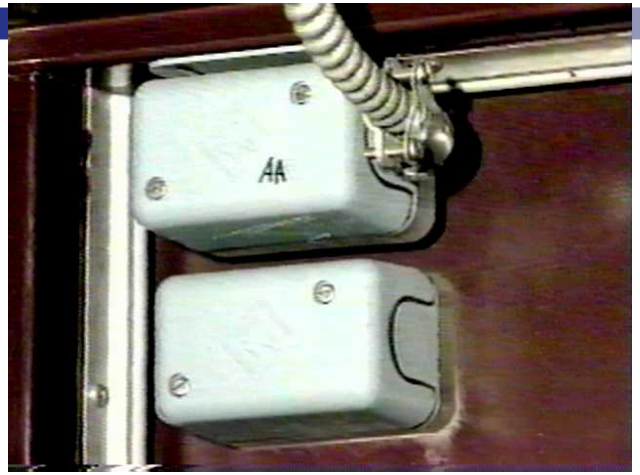


- **Fiber Optic Intrusion Detection (Line Detection)**

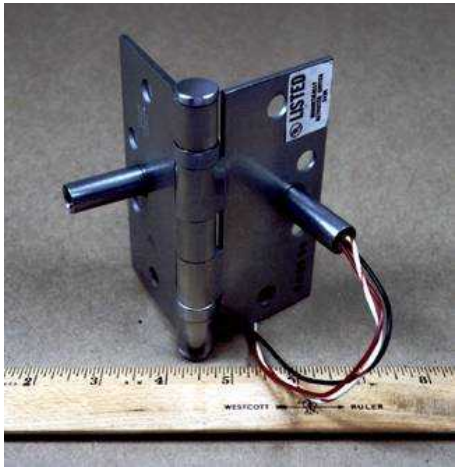
Categories of Interior Area Sensors

- *Active infrared detectors (break beams)-* **Detect presence of an object which comes between an infrared beam and its detector**
- *Magnetic switches -* **Detect the change of state between two magnets, typically used to detect if a door is open**
- *Microwave (or radar) sensors-* **Detect change in reflected or received microwave energy due to an object in its detection zone**
- *Ultrasonic or sonic sensors -* **Detect change in the reflected or received sonar signals from due to an object entering or departing the detection zone**
- *Passive infrared detectors-* **Detect presence of object with a thermal signature different from the background**
- *Video motion detection -* **Detects change of video scene**
- *Fiber Optic Seals -* **Detect tamper by activating alarm if fiber broken or bent**

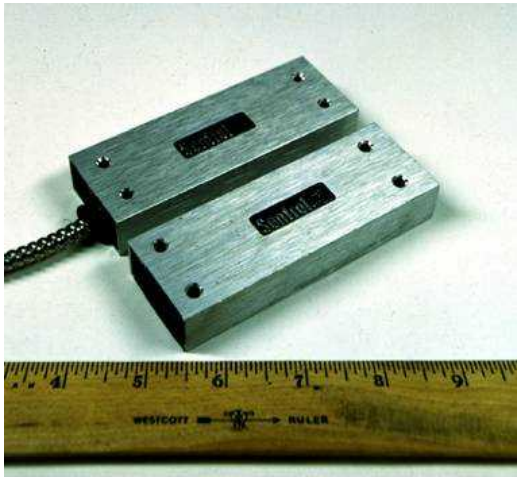
Magnetic Switches



Balanced magnetic switch

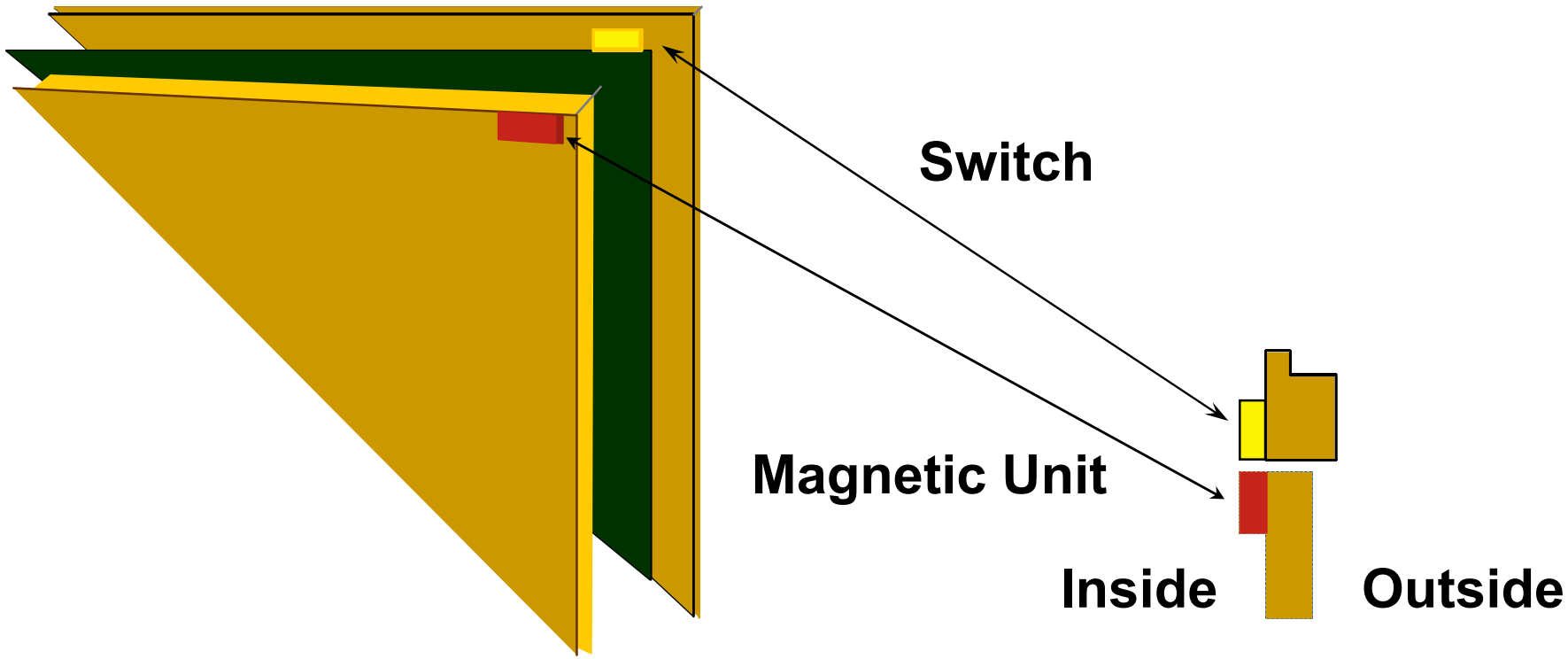


Covert magnetic switch



Complex balanced magnetic switch

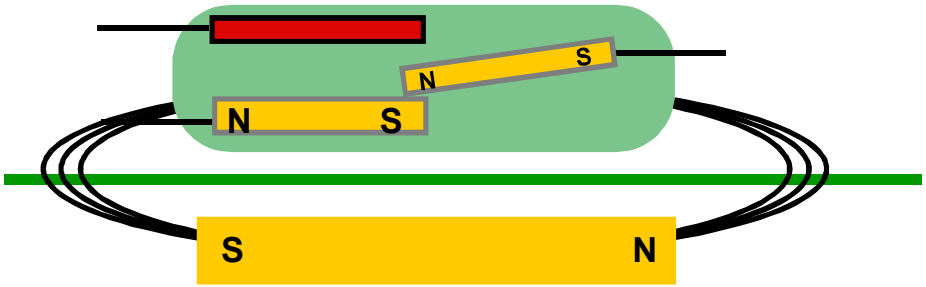
Magnetic Switch



Magnetic Reed Switch

Non-Mag =

Switch Unit



Magnet Unit

(Door Closed)

Switch Unit

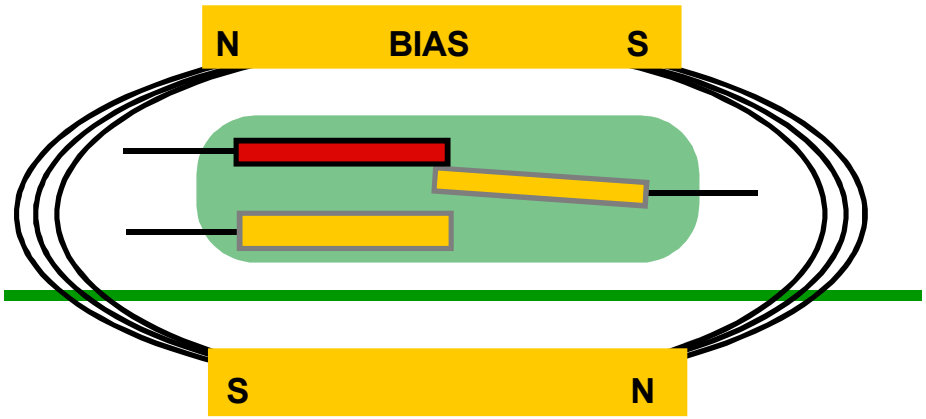
(Door Opened)

International BIOLOGICAL THREAT REDUCTION

Balanced Magnetic Switch (BMS)

Non-Mag =

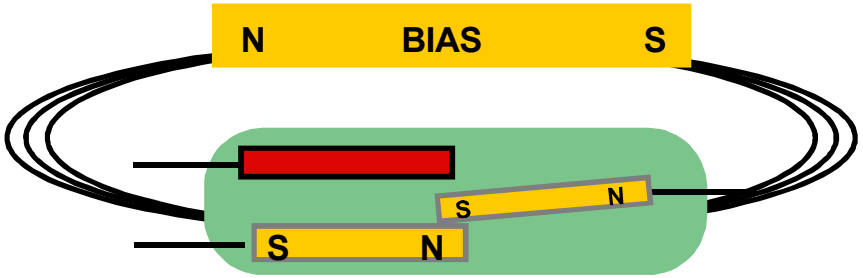
Switch Unit



Magnet Unit
(On Door)

(Door Closed)

Switch Unit



(Door Opened)

International
BIOLOGICAL THREAT REDUCTION

Tamper Indication

- **Tamper indication is used to monitor the integrity and identity of objects including monitoring equipment**

- **Mechanical**
  - Surface coatings
    - **Tamper indicating paint**
    - **Powder coating**
  - Physical feature
    - **Typically design and application specific**
    - **Custom penetrations**
    - **Labyrinth feature**
    - **Non-removable hinge pins**
    - **Concealed hinges**

- **Electrical**
  - Switch to sense opening and/or closing
  - Sensor based
  - Membrane technology
  - Volumetric applications
    - **Surface penetration**
    - **Multi-layer capacitive**
    - **Wire mesh continuity**
    - **Multi-layer conductive ink technology**

Data Authentication

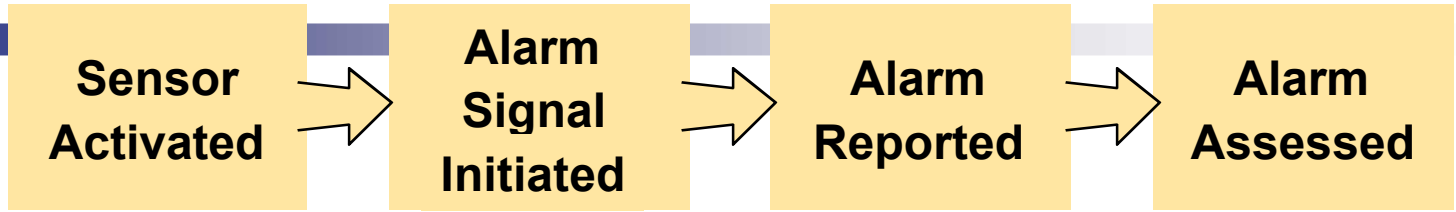
- **Why authenticate?**
  - Prevent spoofing
  - Prevent substitution of sensors
  - Prevent replay old data

- **Tamper indication of sensors required**
- **Digital signatures with data ideal**

Features of a Good Intrusion Detection System

- High probability of detection
- Low nuisance alarm rate
- Uses protection-in-depth
- Detects tampering
- Vulnerability to defeat is low
- Able to self-test
- Is properly installed: no loose mountings, wiring in conduit, proper location for sensors

Alarm Communication, Display and Assessment



- **Designer must decide:**
  - What information should be presented to the operator?
  - How should the information be presented?
  - How does the operator interact with the system?
  - How should the equipment be arranged at the operator's workstation?

- **Alarms must be communicated and displayed**

- **Alarms must be assessed before response is dispatched**
  - Can be direct (guards) or remote (video)
  - Determine cause of each sensor alarm
    - **Valid or nuisance alarm**
  - Requires adequate lighting
    - **Deters opportunistic adversaries**


BONG!
BONG!
BONG!
WHAAAAAAAAAAA
?

Alarm Assessment

Direct observation by guards

- Can be campus police or other on-site security
- Takes time and can put guard in danger
- Can provide immediate response
- Can only tolerate low rate of nuisance alarms
- Labor intensive

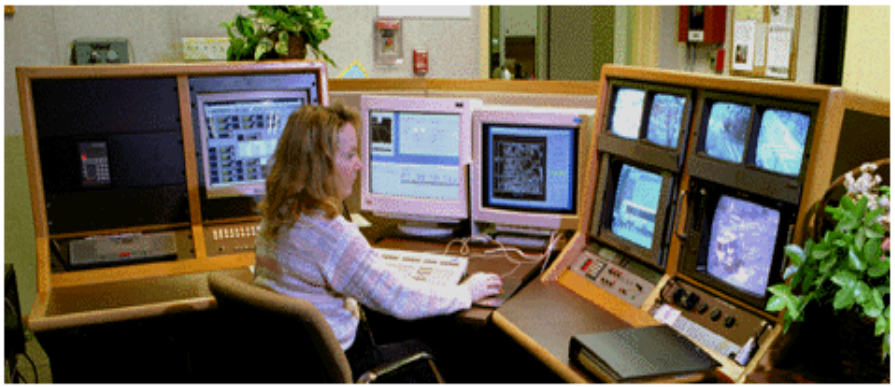
Remote assessment by video

- Video is immediate and focused
- Video is displayed to an alarm station operator for assessment
- Assessment of an alarm can occur almost immediately
  - Pre-event and post-event recording possible
- Later audit and review
- Efficient use of people
- Requires video infrastructure
- Can have high initial expense
- Maintenance can be expensive

Video Assessment vs. Video Surveillance

- **Assessment**
  - Alarm information triggered by sensor activation and directed to a human to determine if unauthorized access has occurred in a sensored area
  - Cameras located at sensor locations – e.g. pointed at doors

- **Surveillance**
  - Continuous use of a human as a intrusion detector to monitor several restricted areas that are NOT sensored by intrusion technologies
  - Systems often have many cameras
  - Someone must watch all video screens all the time
    - **Personnel can only watch a few screens for a limited amount of time before fatigue**



Lighting Requirements

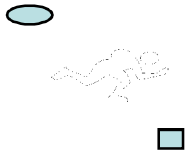
- **Minimum intensity**
  - 15 lux for color cameras
  - 10 lux for black & white cameras
- **Uniform illumination**
  - 6:1 light-to-dark ratio, maximum
  - 4:1 design goal
- **Extent of coverage**
  - 70% of field of view, minimum

Levels of Resolution

Detection

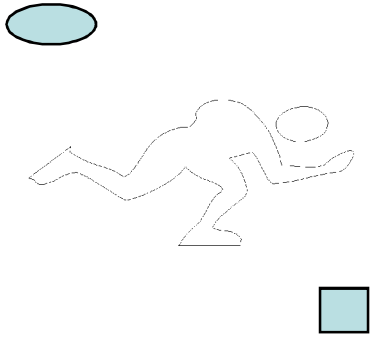
Determine Presence of Object

Classification



Determine Class of Object

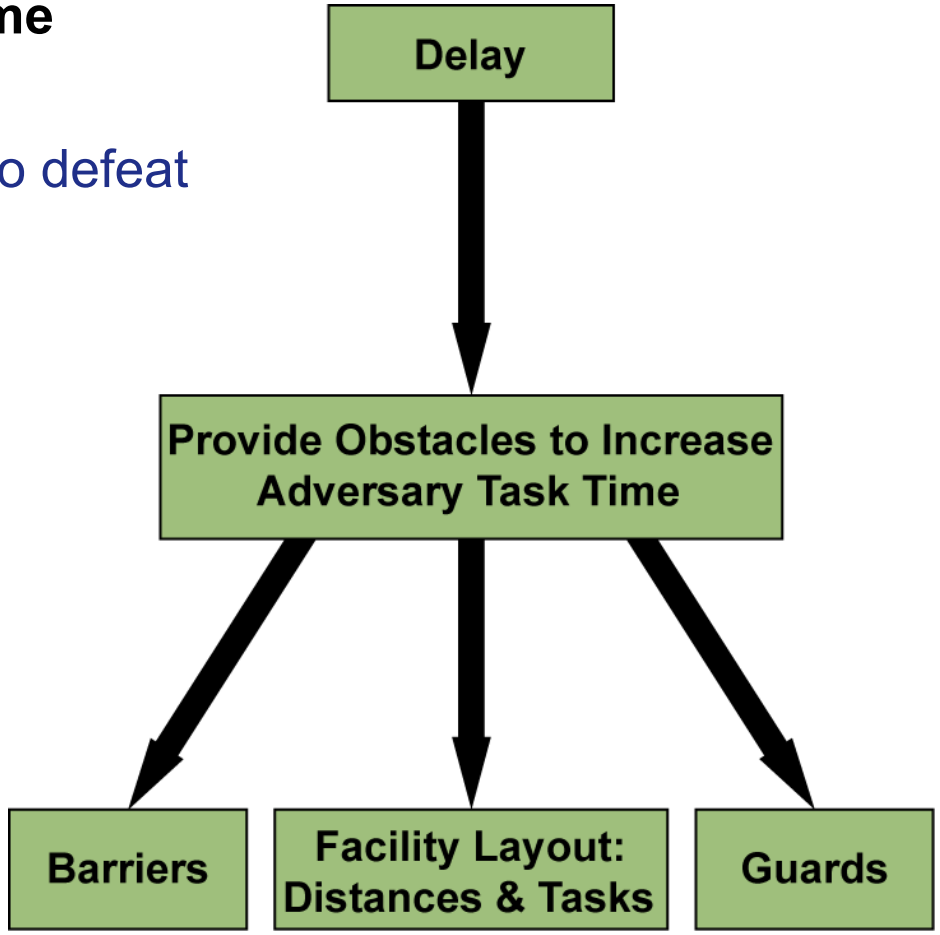
Identification



Determine Identity of Object

Delay

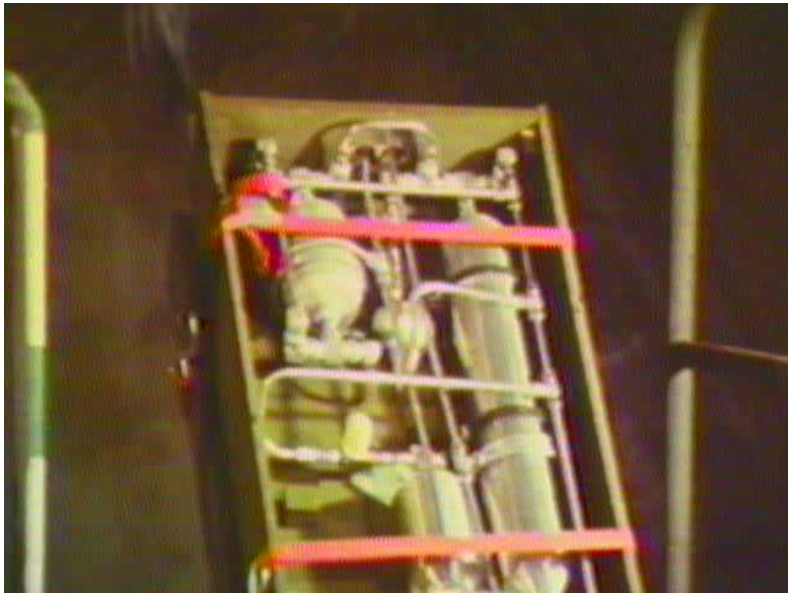
- **Performance metric: defeat time**
- **Design parameters:**
  - Tools/capabilities required to defeat
  - Complexity to defeat
  - Impact on operations



Fixed Barrier Penetration by Vehicle

Activated Barriers

- **Examples of material include:**
  - **Stabilized aqueous foam**
  - **Smoke obscurants**
  - **Low-temperature pyrotechnic smoke**
  - **Sticky thermoplastic foam**
  - **Various entanglement devices**



Guards

- **Can delay the intruders during access control, after detection, during alarm assessment, or after interruption**

Response

- **Performance metric: probability of neutralization**
- **Design parameters**
  - Probability of communication to response force
  - Time to communicate
  - Probability of deployment to adversary location
  - Time to deploy to appropriate location

Response Initiation

- **Who is authorized to initiate the response?**
  - The alarm assessor
  - A commanding officer
  - An outside organization
  - What is the chain of command?
- **What is decision criteria?**
- **What mechanism is to be used for communication?**
  - Telephone
  - Radio
  - Siren
- **Constraints on Response**
  - Legal authority
  - Rules of engagement
  - Strategy and tactics

Response Force

- **On-site guard force**
  - Can serve intrusion detection and alarm assessment roles in mechanically-based physical security systems
  - Supports electronic systems:
    - **Monitors Alarm Communication & Display (AC&D) system**
    - **Assesses electronic alarms at alarm console or at alarm location**
  - Patrols perimeter and buildings
  - Summons and directs local law enforcement

- **Local law enforcement (police)**
  - Reinforces on-site guard force
    - **Responds according to plan when summoned**
    - **Equipped and authorized to confront adversary**

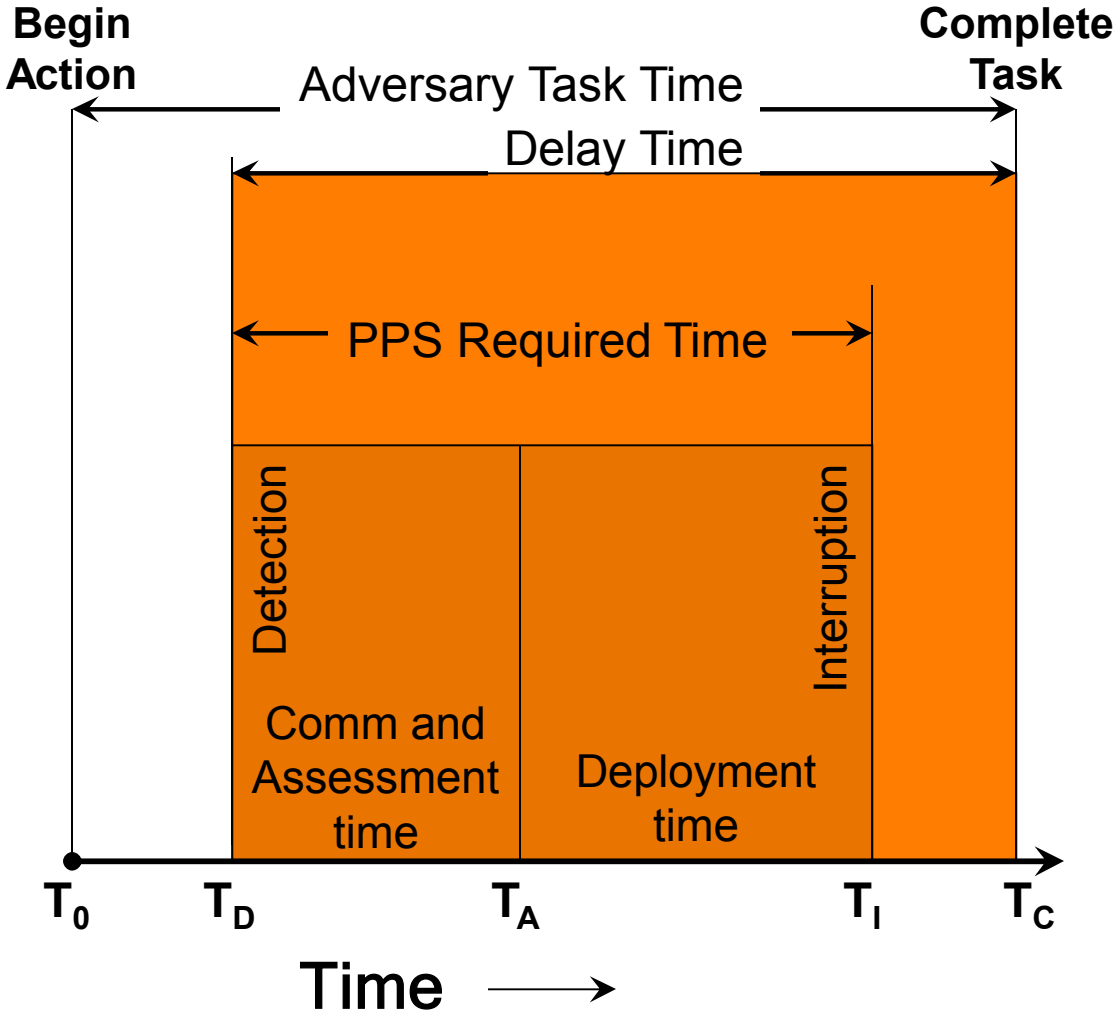
Response Force Requirements

- **Qualification and training**
  - Enforcement responsibilities and skills
  - Equipment familiarity and training
  - Familiarity with facility features and operations
  - Knowledge of restricted area access and biosafety

- **Guard Force Post Orders**
  - List specific duties and limits of authority
  - Procedures for response to specific alarm conditions
  - Emergency response procedures
  - Notification list

- **Memorandum of understanding with local law enforcement**
  - Specific instructions and agreements
  - On-site training and orientation

Relationship of Detection, Delay, and Response



T_0 = Adversary action begins

T_D = First alarm occurs

T_A = The time at which the alarm is assessed to be valid

T_I = The time at which the response force interrupts adversary actions

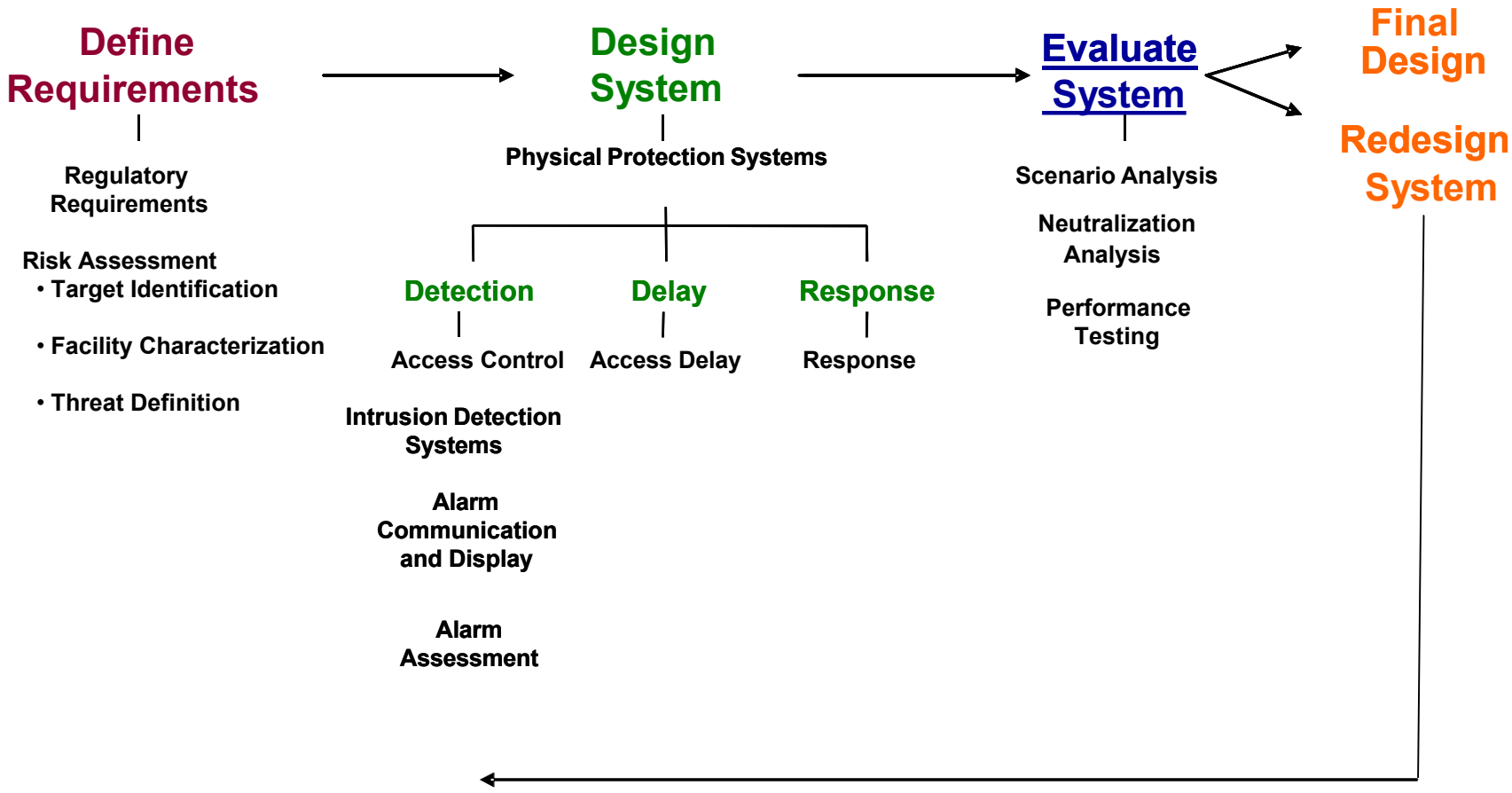
T_C = Adversary task completion time

Relationship of Detection, Delay, and Response

- **Detection without assessment is not detection**
- **Detection must be timely**
- **Delay must follow detection**
- **Detection + Assessment + Response < Delay***

(*only count delay time **after** detection)

Physical Protection System Design Scheme



International BIOLOGICAL THREAT REDUCTION

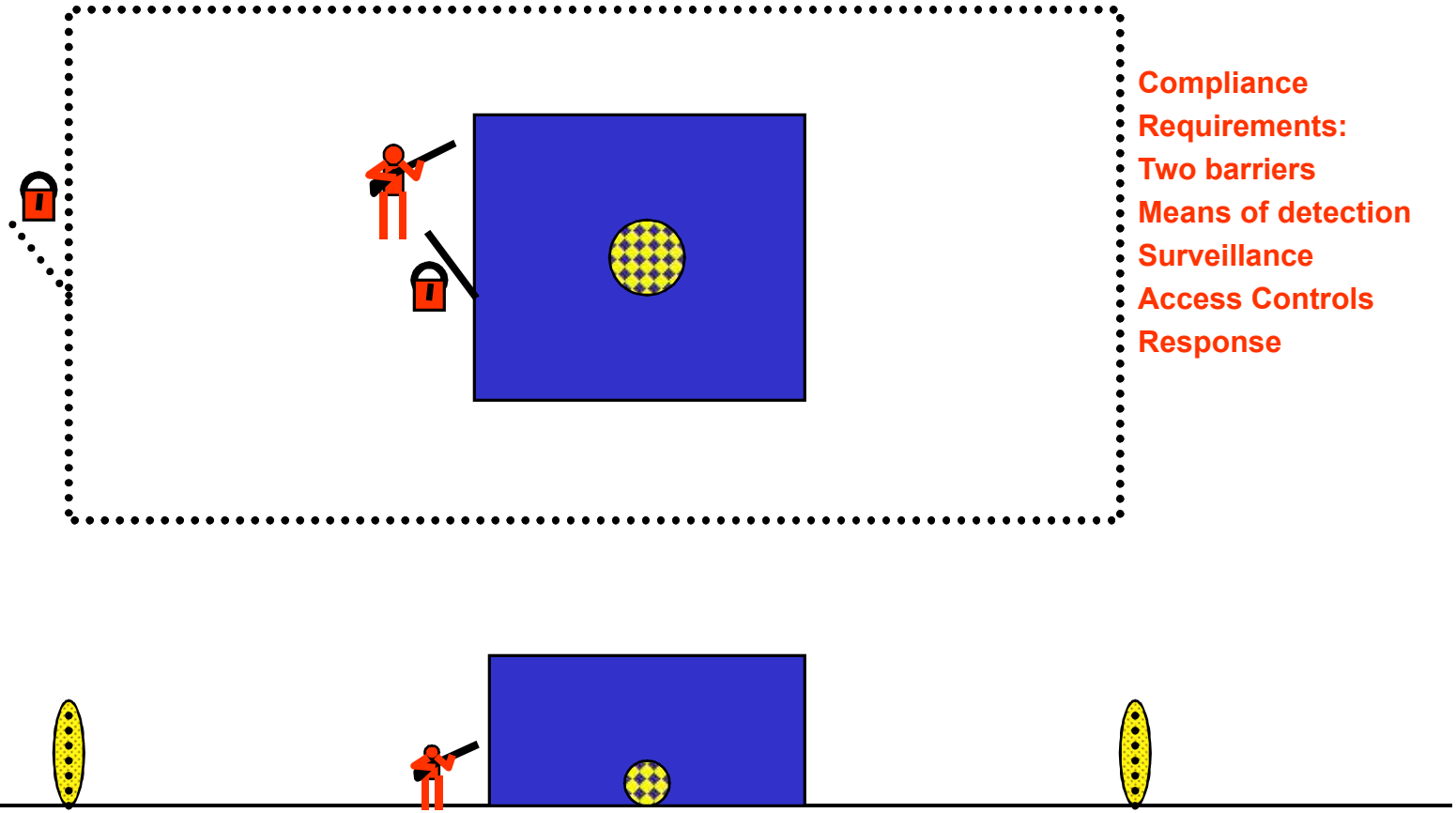
System Evaluation

- **Objective of physical protection system**
  - Prevent adversary from achieving undesirable event

- **Objective of physical protection system evaluation**
  - Provide assurance that physical protection system meets objective
    - **System performance based on the risk assessment including the assessed threat**
    - **Identify system deficiencies**
    - **Help select system improvements**
    - **Permit cost-benefit comparisons for different upgrades**

  - Evaluation requires a **METHOD** and a **METRIC**

Scenario Analysis - Example Facility



Compliance Requirements:
Two barriers
Means of detection
Surveillance
Access Controls
Response

Example System Evaluation

Scenario	Expert Opinion	Compliance	Performance
One adversary No equipment		Yes	
One adversary Pistol, fake badge		Yes	
Two adversaries Heavy bar		Yes	
Two adversaries Pistols, ladder		Yes	

Path analysis and scenarios necessary for performance

Neutralization Analysis

Definition of Probability of Neutralization

- Probability of neutralization (P_N) calculated based upon simulation, numerical methods, opinion or trials

$$P_N = N_{wins} / N_{engagements}$$

- All engagements have the same initial conditions
- Two possible outcomes per engagement: win or loss

Factors Affecting Probability of Neutralization

Factors	Examples
Numbers	
Weapons suite	None, baton, HG, SG, SMG, SAR, FAR, LMG, HMG, SNP
Area kill	Mortar, LAW, grenades, mines, IEDs
Ammo limits	Rounds/magazine, number of magazines
Training	None, basic, SWAT, military
Tactics	None, simple, advanced, military
Body armor	None, Level I, Level II, Level III
Posture	Stand, kneel, prone
Exposure	0% - 100%
Movement	Stopped, very slow, slow, medium, fast, very fast, riding
Vehicles	Soft, armored, weaponized
Range	

Neutralization Analysis Methods

- **Expert opinion**
- **Simple numerical methods**
  - Data Tables
  - Tabletop analysis
  - Markov chains
  - Monte Carlo Simulation
- **Complex computer simulations**
  - Computerized war games example
- **Simulated physical engagements**
  - Force-on-Force (FOF)
- **Actual engagements**

Neutralization of Direct or Indirect Attacks Against System

- **Direct attacks on physical protection system:**
  - Adversary actions confined to path
  - Minimize detection: force, stealth, or deceit
  - Minimize delay: force or stealth
  - Reduce assessment time, communication time

- **Indirect attacks**
  - Adversary attacks infrastructure or response
  - Infrastructure
    - **CAS, power supplies, communications, or otherwise disabling sensors or cameras or other equipment**
  - Response time
    - **Diversion, vehicle bomb, ambush**

Performance Analysis Steps

- **Characterize the system**
  - Collect data on facility and physical protection system
  - Features check
- **Analyze paths**
  - Path analysis for most vulnerable paths
- **Test against developed scenarios**
  - Credible adversary capabilities and tactics
  - Engagements and Neutralizations
- **Compute effectiveness and validate**
  - Expert opinion review
  - Component and system tests
  - Response exercises

Identify Upgrades after Conducting Analysis

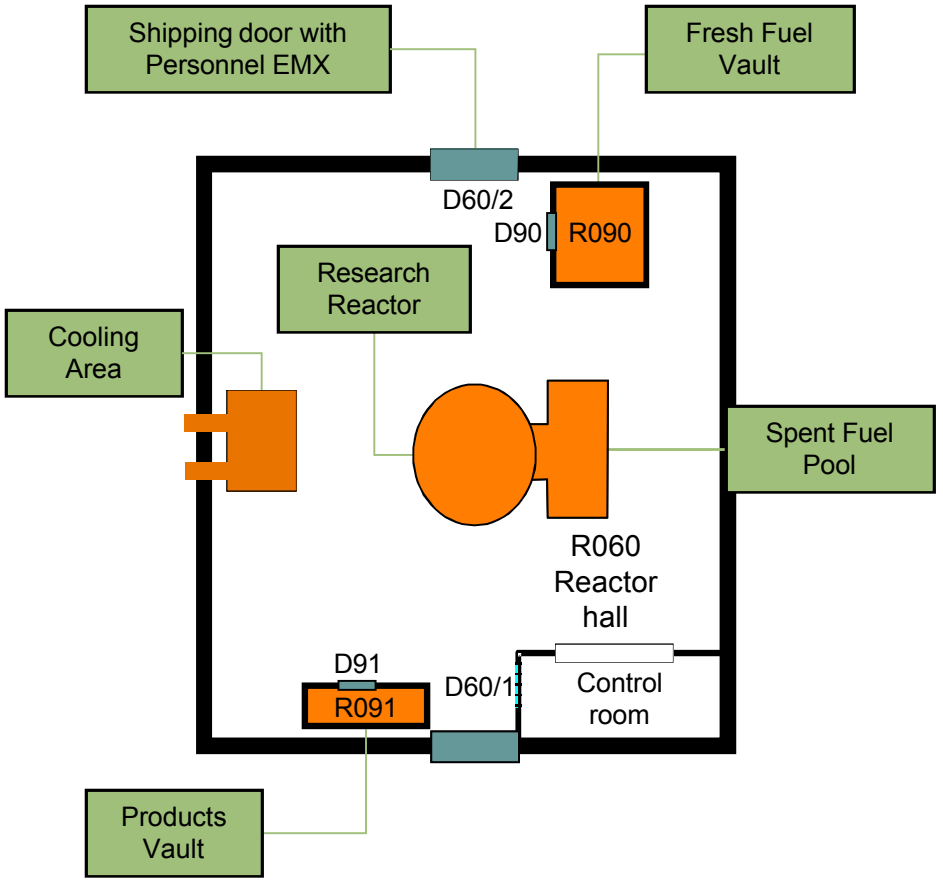
- **Improvements may be needed after initial evaluation.**
  - Use analysis to identify improvements:
    - **Better detection early in path**
    - **Increased delay late in path**
    - **Faster response**
    - **Response force survivability**
      - Improve numbers, weapons, tactics
  - Evaluate system with the improvements
    - **Increased effectiveness?**
    - **Acceptable metric?**
    - **Cost-effective?**

Summary Characteristics of an Effective System

- Balanced protection
- Protection-in-depth
- System reliability
- Minimum consequence of component failure
- Effectiveness against threat

Balanced Physical Protection System

- **Layers**
  - Equivalent detection and delay throughout the layer
    - **Example: door and walls have equivalent intrusion detection**
  - No “holes” in protection
    - **Example: window in concrete wall**



International BIOLOGICAL THREAT REDUCTION

Protection-in-Depth

- **Multiple concentric layers**
  - Adversary must defeat multiple protective measures in sequence

- **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

System Reliability

- **Goal is to have a system that never fails BUT:**
  - Electronics “wears out”
  - Procedures are not always followed
  - The environment changes

- **System reliability can be enhanced by:**
  - Design
  - Redundant equipment
  - Effective training
  - Rapid effective contingency measures

Minimize Consequences associated with Component Failure

- **Does risk warrant redundant equipment, such as**
  - Multiple complementary sensors
  - Central Alarm System and Secondary Alarm Stations
- **Contingency and incident response plans**
  - Spare parts
  - Compensatory measures
  - Agreement with local law enforcement
- **Fail-safe and fail-secure**

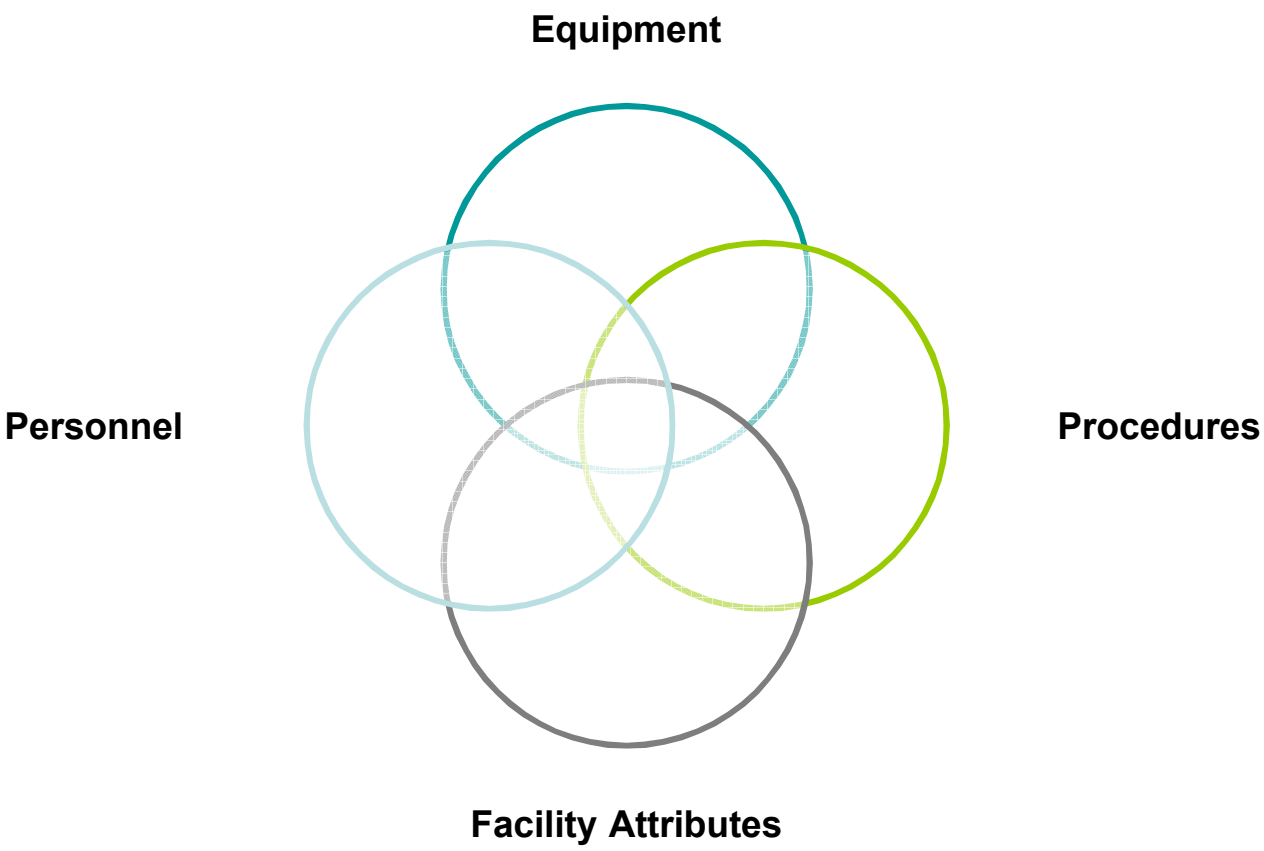
Performance Testing and Maintenance

- **Performance against threats**
- **Create security performance test plan and procedures**
- **Schedule periodic testing of hardware and policy implementation**
- **Periodic testing of response force procedures**
- **Document test results**
- **Take corrective action**
  - Schedule maintenance and repair of hardware
  - Corrective training and policy adjustments as appropriate for policy implementation failures
  - Corrective training and exercises for guard force

Other Security Considerations

- **Administrators have full control**
  - The ultimate insider
- **Protect the system using procedures**
  - Two person control
  - Configuration management
  - Password control
- **Restrict operator privileges**
- **Provide physical protection for equipment**
- **Backup equipment and procedures must be provided to maintain security**
- **Emergency power and uninterruptible power supply required for computers**

Physical Protection Systems



International BIOLOGICAL THREAT REDUCTION