SAND2011-0538P

Physical Protection Overview

Session Objectives

This session will provide answers to the following questions:

- What is a physical protection system?
- What constitutes a good physical protection system?
- How can cost and operational impacts of physical protection systems be minimized?

Physical Protection System

- An integrated set of personnel, procedures, and equipment intended to prevent the completion of a malicious act.
- Malicious acts of concern:
  - Unauthorized removal (theft) of nuclear material.
  - Sabotage of nuclear material or a nuclear facility that leads to release of radioactive substances or exposure to radiation.
- Focus of this presentation is on nuclear material and nuclear facilities, but the concepts apply to any assets requiring protection.

Four Physical Protection Objectives

- Protect against unauthorized removal of nuclear material in use and storage, and during transport;
- Ensure the implementation of rapid and comprehensive measures by the State to locate and recover missing or stolen nuclear material;
- Protect against sabotage of nuclear facilities and sabotage of nuclear material in use and storage and during transport; and
- Mitigate or minimize the radiological consequences of sabotage.

IAEA document GC(45)/INF/14, Sept 2001

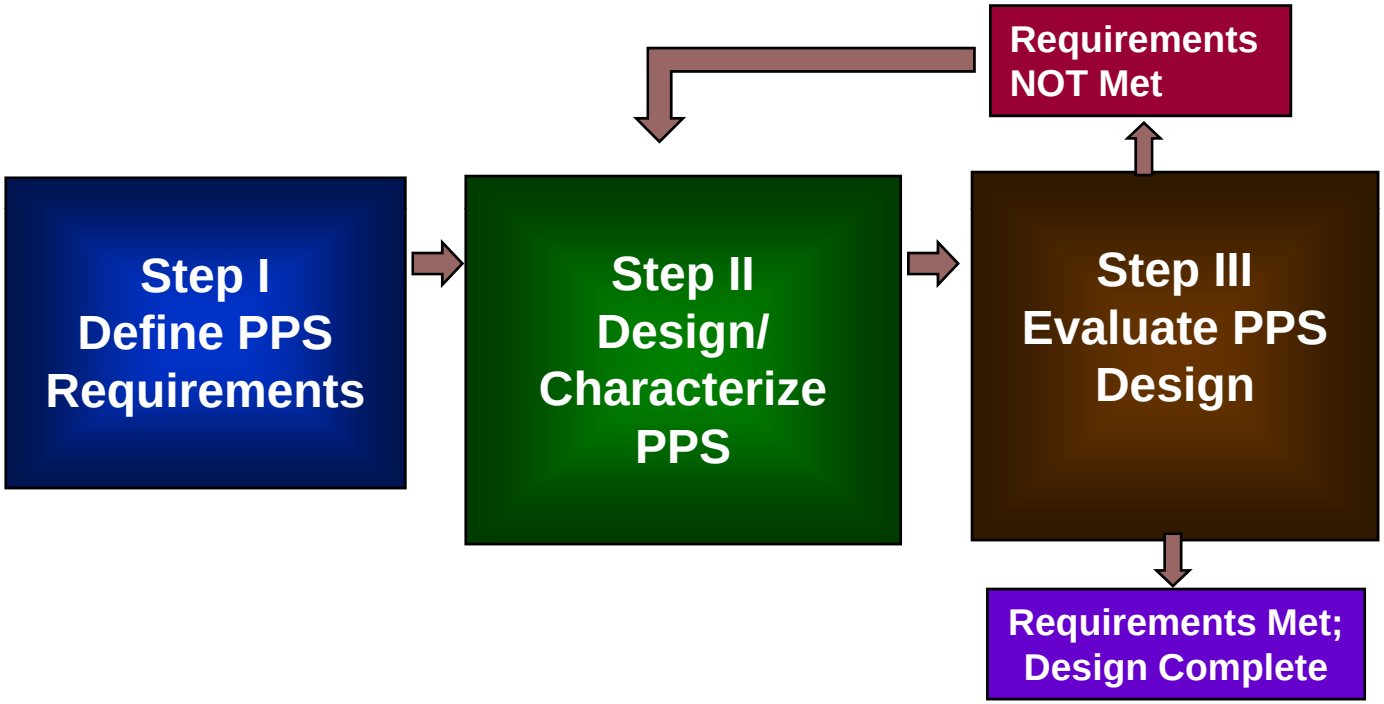
Some Fundamental Principles of Physical Protection*

- The prime responsibility for implementation of physical protection rests with the operators.
- Organizations should develop and maintain an effective security culture.
- Physical protection should be based on the current assessment of the threat.
- Requirements should be based on a graded approach that reflects the threat, attractiveness of the target, and potential consequences of malicious acts.
- Physical protection should include several layers that an adversary must overcome (Defense in Depth).

* From the *Convention on Physical Protection of Nuclear Material and Nuclear Facilities*

Systems Engineering Process for PPS Design

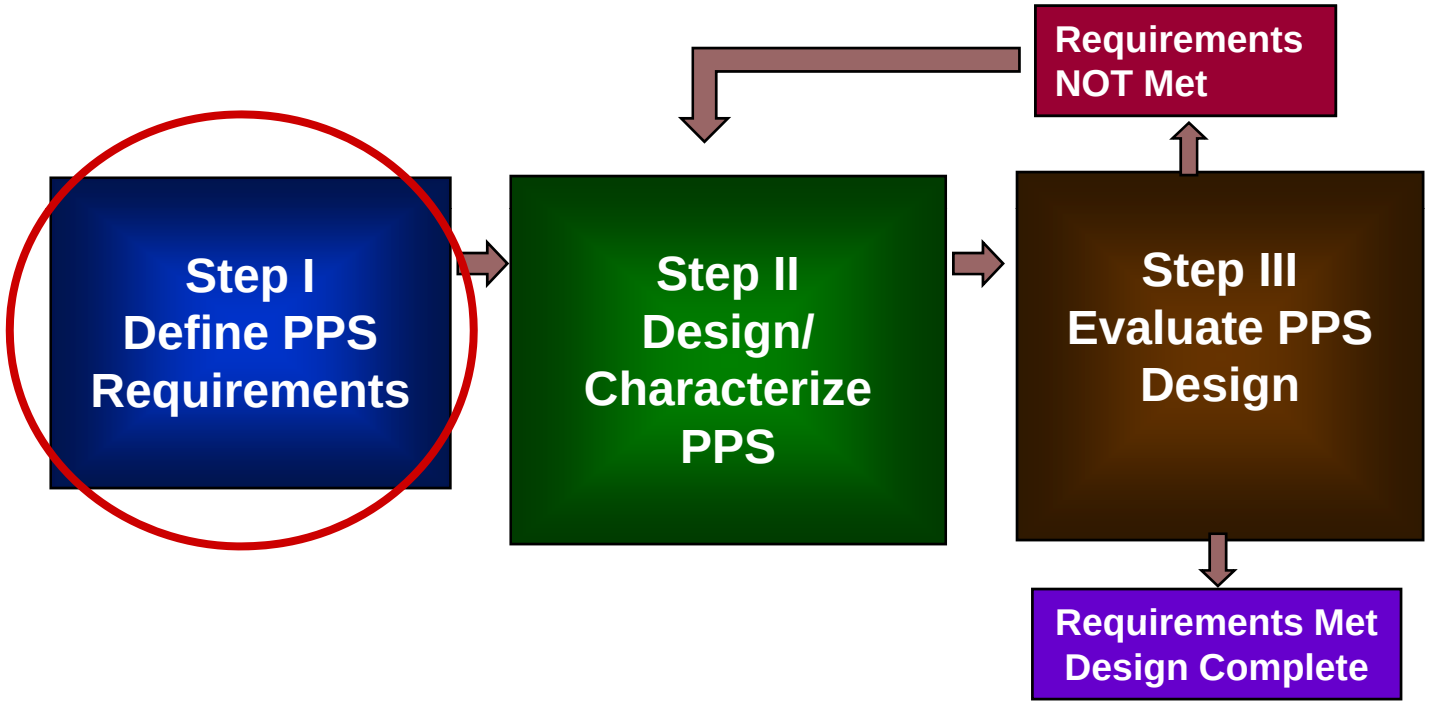
Three interdependent steps required:



Repeat process until requirements are met (iterative process)

Systems Engineering Process for PPS Design

Three interdependent steps required:



Repeat process until requirements are met (iterative process)

Three Essential Questions that define the requirements for a PPS

1. What assets must be protected to prevent undesired consequences?
2. What threat must be protected against?
3. What level of protection is adequate?

Some Undesired Consequences of Malicious Acts

- Damage to national security
- Successful terrorist attack
- Loss of control of nuclear material
- Loss of life as a result of hazardous material release
- Theft of material or information
- Interruption of critical utilities such as water, power, or communications
- Degraded business operations
- Loss of market position
- Workplace violence, extortion, blackmail
- Damage to reputation
- Legal liability

1. What must be protected?

- Nuclear materials
- Nuclear facilities
- Information
- Radioactive sources in the facilities
- People
- Environment

Targets—What are they?

- Theft Targets
  - Nuclear or radioactive materials
    - IAEA provides guidance on categorization of nuclear material and radioactive sources to determine the level of protection required
  - Information
  - People
- Sabotage Targets
  - Nuclear or radioactive materials
  - Process or support equipment needed to prevent unacceptable radiological consequences

2. What threats must be protected against?

- The regulatory authority should define the threat that the physical protection system (PPS) is expected to withstand.
- The defined threat specifies the adversary attributes and characteristics that the PPS must be designed to defend against.
- This is commonly referred to as the design basis threat (DBT).

Categories of Adversary

- Outsider Threat
  - Protestors, terrorists, criminals
- Insider Threat
  - Act alone or in collusion with external threat
  - May be passive or active
  - May be violent or nonviolent

Identify What Needs to be Known About the Threat

- Motivation
  - Ideological, Personal, Economic, Psychotic, or Other
- Intention
  - Theft or Sabotage
- Capabilities
  - Group Size
  - Weapons
  - Explosives
  - Tools
  - Transportation
  - Skills
  - Funding
  - Collusion with Insider
  - Support Structure

3. What level of physical protection is adequate?

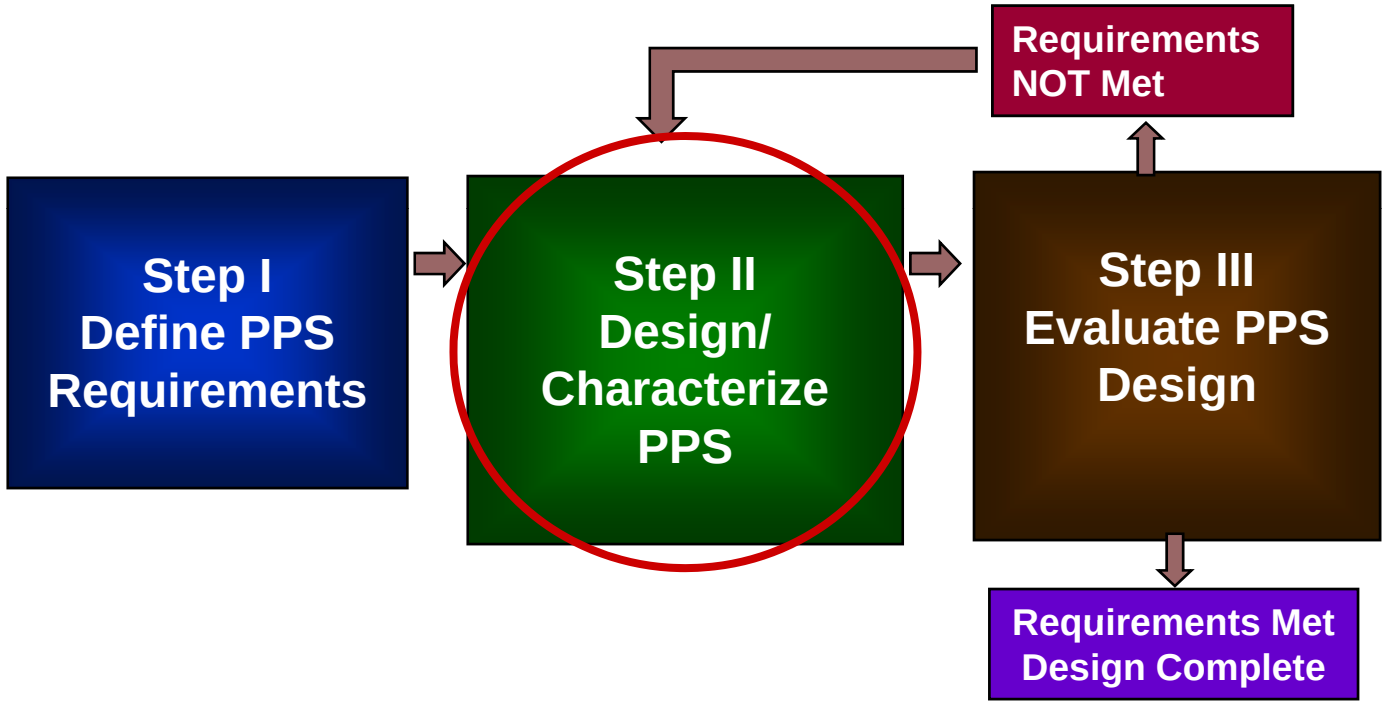
- Objective: reduce the risk associated with use of nuclear or other radioactive materials to an acceptable level
- Must strike a balance between risk, beneficial use, and costs
- The level of security should reflect the potential consequences of misuse of the material: higher potential consequences imply higher levels of security (i.e. graded approach)

INFCIRC/225/Rev.4 (corrected)

- Provides a set of recommendations on requirements for the physical protection of nuclear material in use and storage and during transport and of nuclear facilities.
- Provides a categorization of the different types of nuclear material.
- Links protection levels to categories of material.
- Currently under revision to address the current threat environment and ensure conformance to CPPNM.

Systems Engineering Process for PPS Design

Three interdependent steps required:



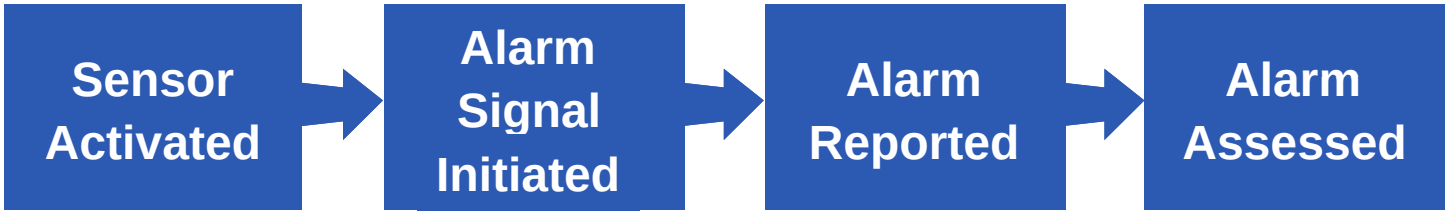
Repeat process until requirements are met (iterative process)

PPS Functions

PPS Functions

Detection	Delay	Response
• Intrusion Detection • Access Control • Contraband Detection • Alarm Assessment • Alarm Communication and Display	• Passive Barriers • Active Barriers	• Guards • Response Force

Detection



- Performance measures:
  - Time for communication and assessment
  - Frequency of nuisance alarms
  - Probability of detection
- A long time delay between sensor alarm and assessment lowers probability of detection
- People can provide both an alarm and assessment simultaneously

"An alarm without assessment is not detection."

Delay

Provide Obstacles to Increase Adversary Task Time

Physical Barriers

Guards/Response Forces

- Performance measure
  - Time to defeat obstacles
- Delay (to be effective) must occur after detection

Response

- Performance measures
  - Probability of communication to response force
  - Time to communicate
  - Probability of deployment to interruption location
  - Time to deploy
  - Response force effectiveness (neutralization)
- Part of the response may be the people who have detected the event

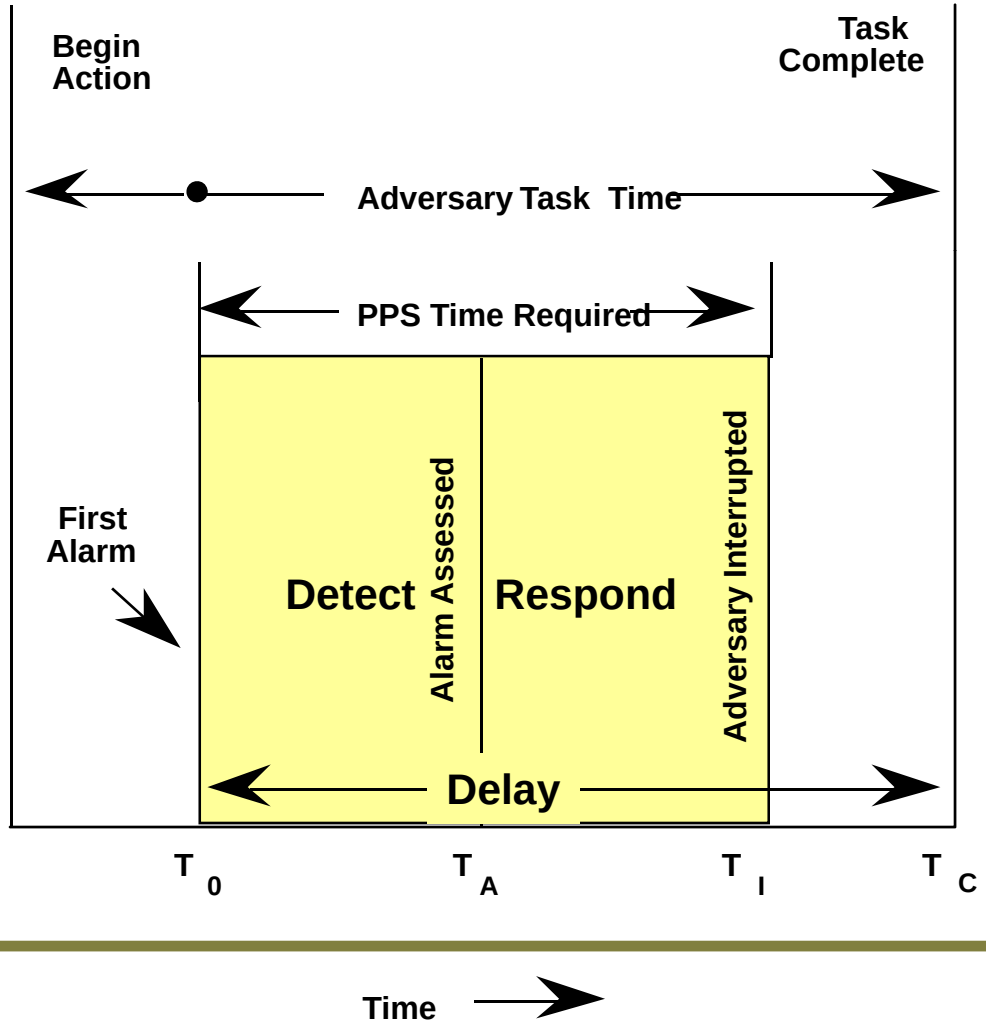
Relationship of PPS Functions

- System detection and response time must be less than adversary task completion time (timely detection)
- To increase the probability of system success
  - Detect intrusion earlier
  - Reduce assessment time
  - Increase adversary task completion time (add delay)
  - Reduce response time

Characteristics of an Effective Physical Protection System (PPS)

- Timely detection
- Balanced protection
- Protection-in-depth
- Minimum consequence of component failure

Timely Detection



T_0 = 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

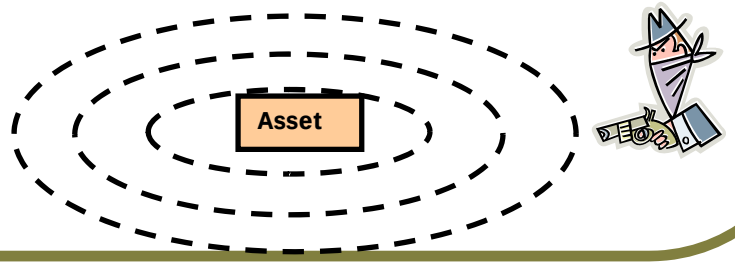
T_C = Adversary task completion time

Balanced Protection

- No matter how an adversary attempts to accomplish his goals, he should be confronted with effective elements of the PPS.
- A balanced PPS provides adequate protection against all adversaries along all possible paths.
- A balanced system addresses other considerations:
  - Cost
  - Safety
  - Structural integrity
  - Operational impacts, etc.

Protection-in-Depth

- Adversary must defeat or avoid a number of protection features 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
  - Require more time for adversary to access target

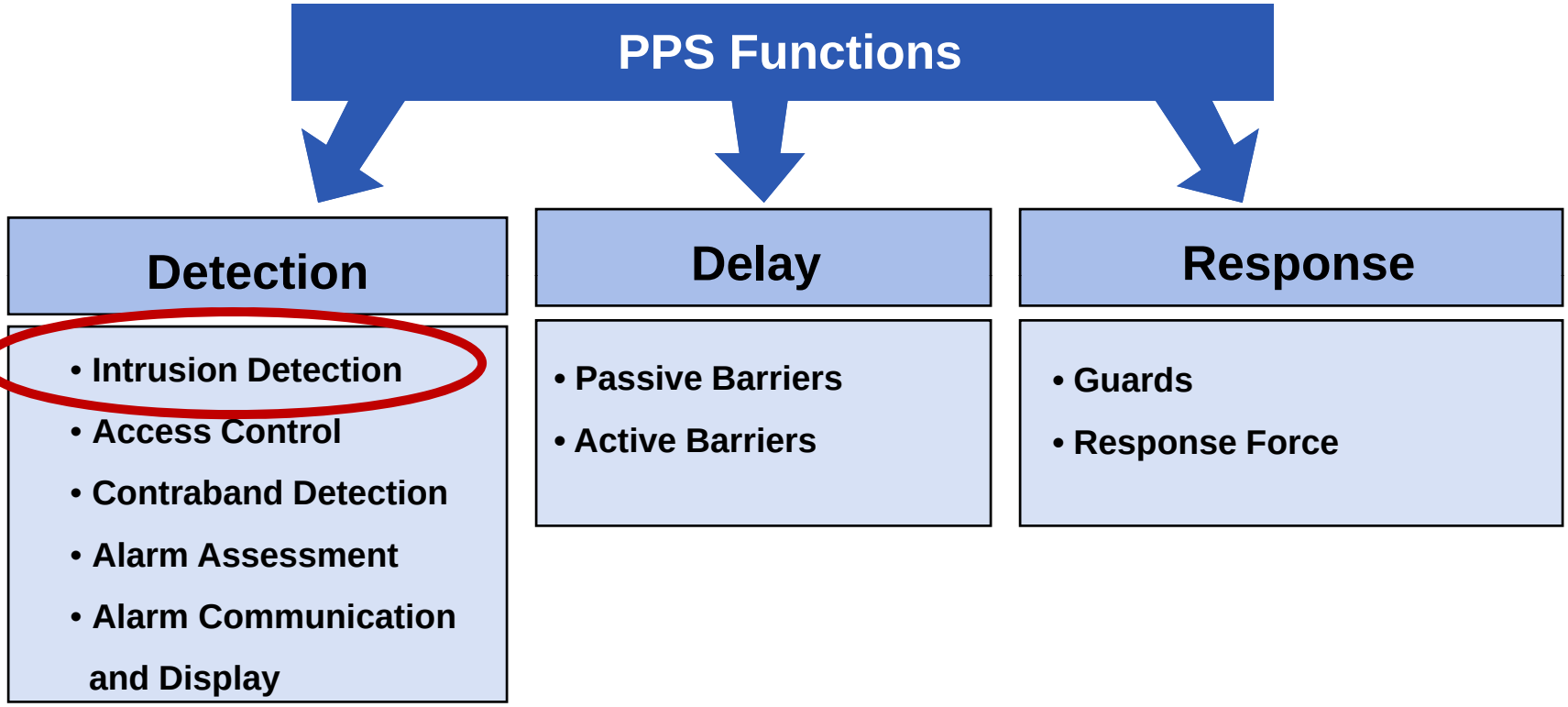


Minimum Consequence of Component Failure

- Compensatory measures must be provided so that the PPS continues to operate after a component fails
- Redundant equipment can take over the function of disabled equipment in some cases
  - e.g., backup power exists if primary power is lost
- Some failures require aid from sources external to the facility
  - e.g., National Guard is used to supplement security during times of higher alert status (i.e., replace sensors with manpower)

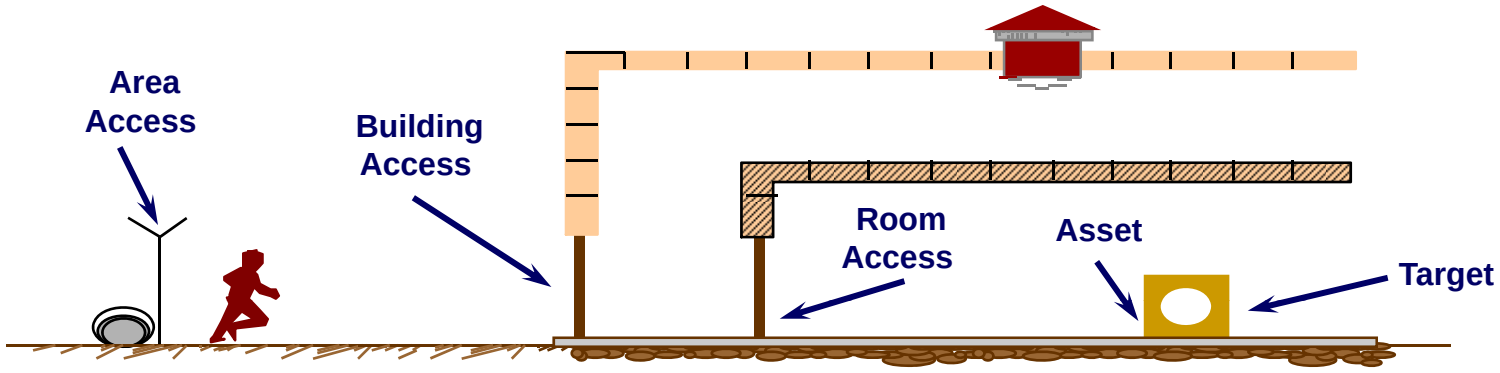
No single-point failures

Role of Intrusion Detection



- **Detection – a process that begins with sensing a potentially malicious or unauthorized act and completed with the assessment of the cause of the alarm**

Types of Sensors



Extended Range

Exterior Sensors

Interior Sensors

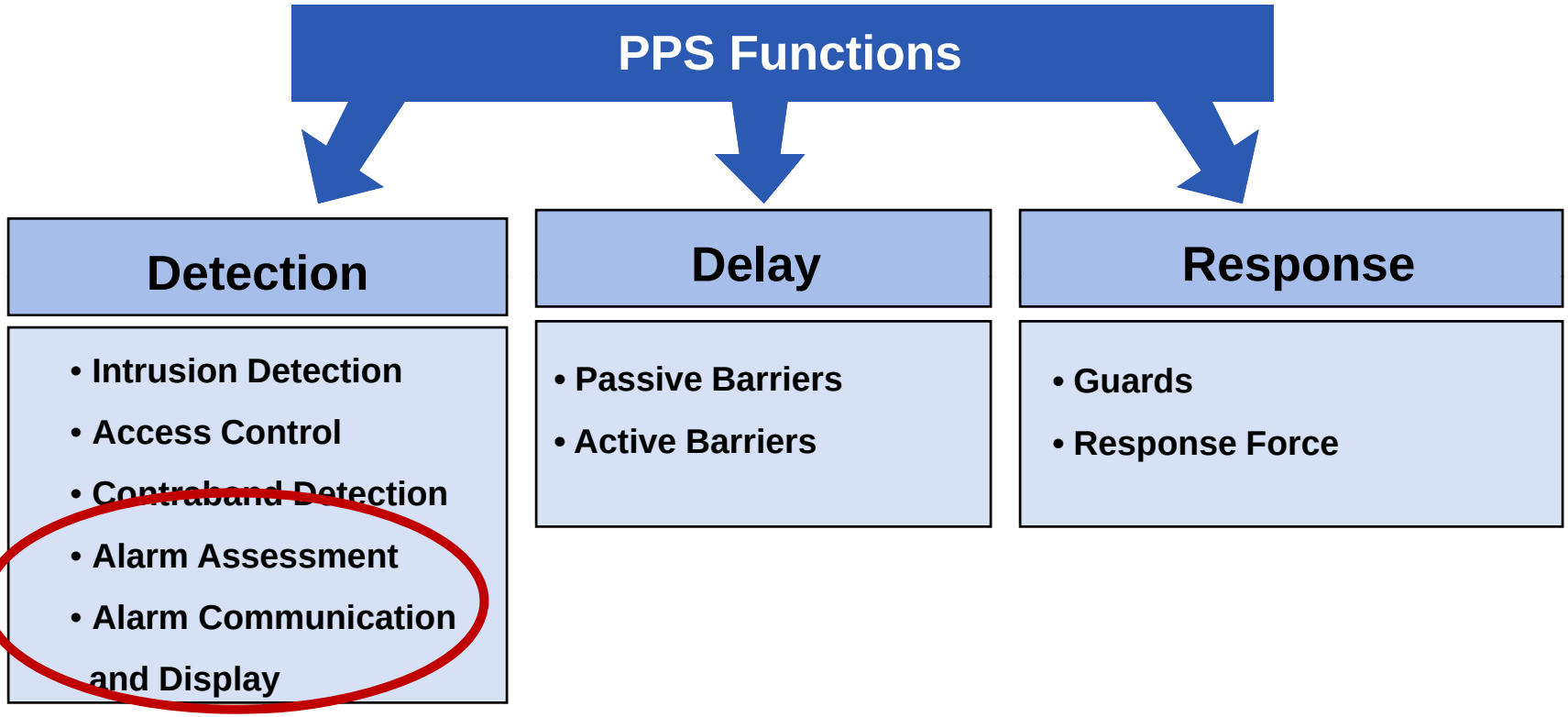
Vulnerability to Defeat

- Adversary Tactics
  - Bypass: avoiding the detection volume of the sensor by crawling, jumping, tunneling, or bridging
  - Spoofing: tricking the sensor into not reporting an alarm
- Given proper knowledge, tools, and time, every sensor can be individually defeated

Characteristics of a Good Intrusion Detection System Design

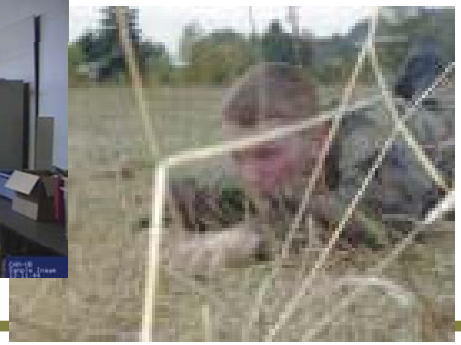
- Design to highest probability of detection with a minimum of nuisance alarms
- Design to minimize vulnerability to defeat
  - Integration with the barrier system
  - Continuous line of detection with overlapping detection zones
  - Protection of system and system components
  - Use of complementary and different types of sensors
  - Sensor selection for physical and industrial environment
- Integrate with Alarm Assessment System

Alarm Assessment, Communication, and Display



Purpose of Alarm Assessment

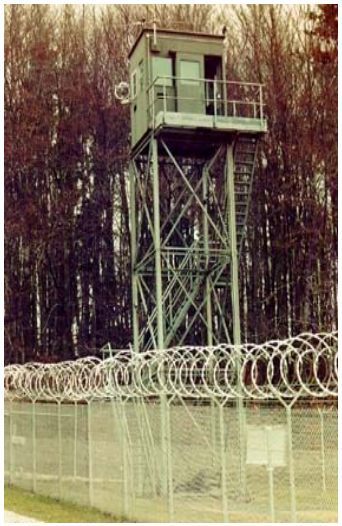
- Determine the cause of each sensor alarm
  - Intrusion Alarm – threat
  - Nuisance Alarm – other assessed causes
  - False Alarm – undetermined causes
  - Scheduled Alarm – maintenance or test
- Provide details for response
  - Who
  - What
  - Where
  - How Many



Methods of Alarm Assessment

Guard/Response Force

Elevated towers or dispatched patrols



Disadvantage: Delay between alarm and eyes on area for assessment

Video System Display

Central Alarm Station: Stationary Cameras or Extended Range Imager

Disadvantages: cost of infrastructure and maintenance; Response Force assessment may still be required

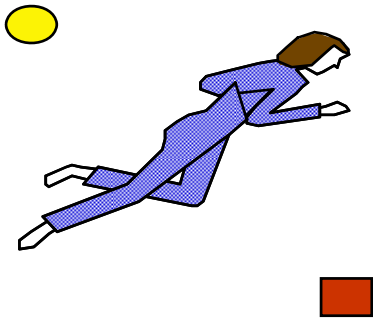
Is there a potential threat in perimeter?

Is there a potential threat in perimeter?

Is there a potential threat in perimeter?

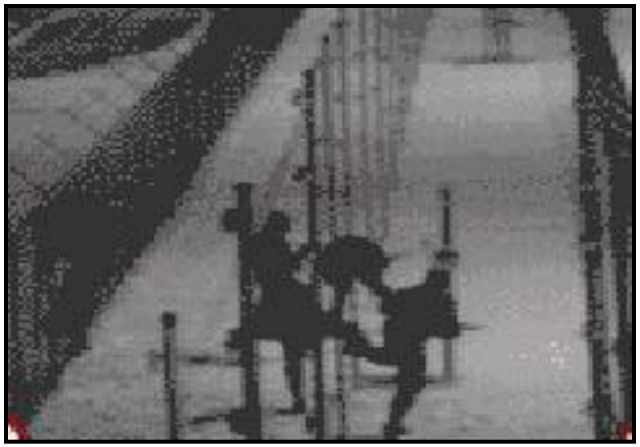
Resolution

- Resolution is the degree to which you can see fine details in viewed image
- What you see depends on camera resolution, size of the object, contrast, and motion of the object.

Sensing	Classification	Identification
		
Determine Presence of Object	**Determine Nuisance or Real Alarms**	**Determine Identity of Object**

Video Assessment

- **Video Assessment** – alarm-initiated video of a sensor detection zone at the time of an intrusion alarm



- Video assessment is integral to the Alarm Communication and Display (AC&D) system

Surveillance

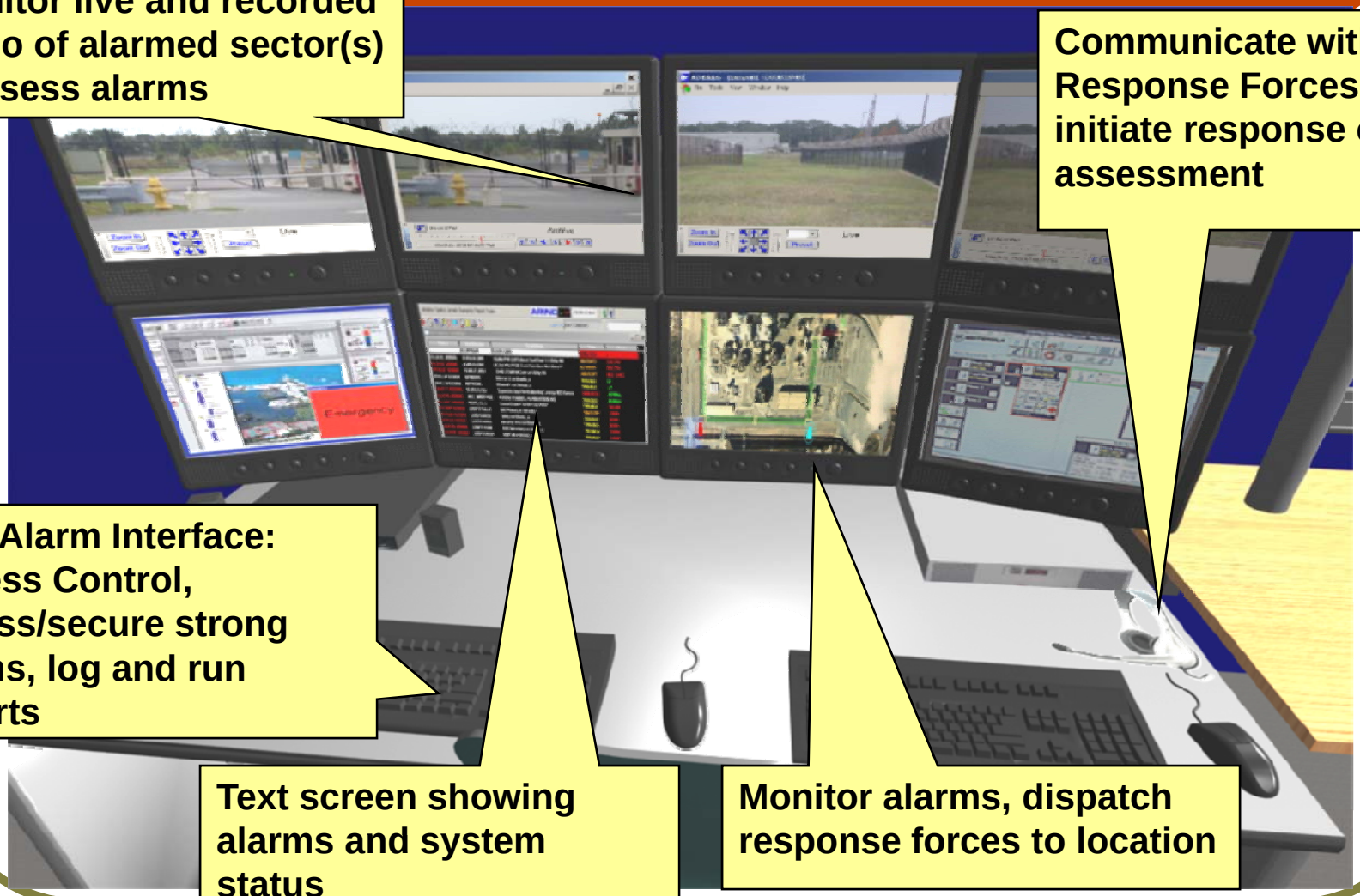
- **Surveillance** – continuous video monitoring of activity in an area without benefit of an intrusion sensor to direct attention to a specific event or area

- Surveillance is also integral to the Alarm Communication and Display (AC&D) system

Features of a Good Alarm Monitoring Station (AMS)

- Provides overall status of site “Security System”
  - Alarm annunciation – audible and visual, location
  - Video displays are linked to alarm outputs
- Provides effective communication between AMS and Protective Forces
- Interfaces with Access Control
- Robust and reliable system
- Has protection measures for system components and information
- Designed for ergonomics
  - Number of alarm monitoring station operators
  - Information management
    - Presents information quickly and effectively
    - Logs information

Operator functions of AC&D



Monitor live and recorded video of alarmed sector(s) – assess alarms

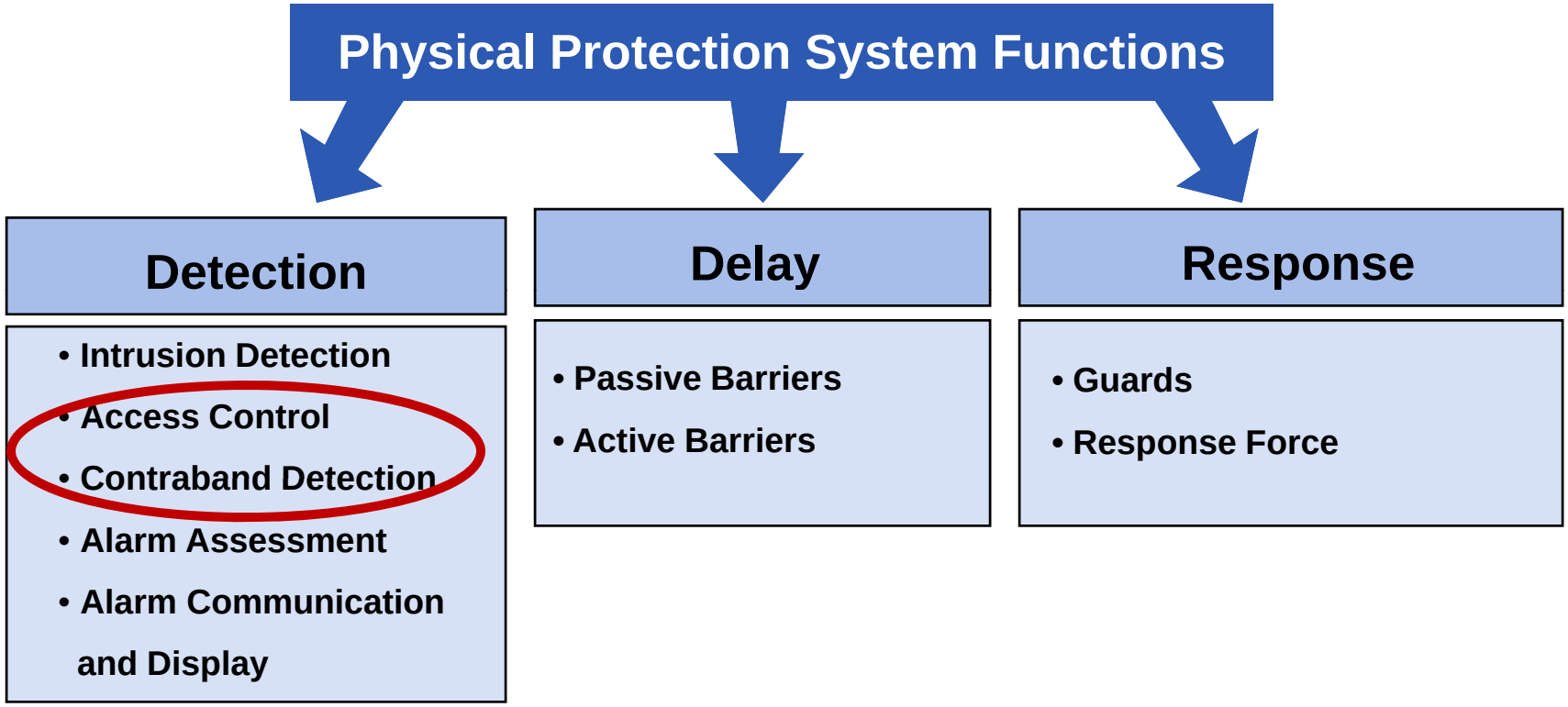
Communicate with Response Forces: initiate response or assessment

Non-Alarm Interface: Access Control, access/secure strong rooms, log and run reports

Text screen showing alarms and system status

Monitor alarms, dispatch response forces to location

Access Control/Contraband Detection



- Access Control and Contraband Detection are elements of the PPS function of Detection.

Role of Access Control/Contraband Detection

- A perimeter intrusion detection system provides a boundary around each protection layer to prevent or detect unauthorized penetrations.
- Access control/contraband detection systems
  - Allow authorized persons, items, packages and vehicles to move in and out through that boundary.
  - Prevent entry of unauthorized persons, items, packages, and vehicles.
  - Prevent exit of protected assets (such as nuclear material)

Access Control/Contraband Detction

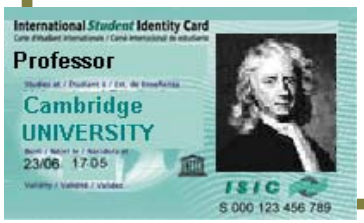
Access Control Personnel Verification Types

Personnel Authorization Verification

Manual (Protective Force Guards)

Automated (Machines)

Have - Credential (Photo)



Have - Credential (Coded)

Know - Memorized Number (PIN)

Are - Personal Characteristics (Biometric)

Levels of Access Control

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

Areas with the potential for higher consequences have higher levels of access control.

Contraband Detection Inspection

People

Walk-through Systems

Things

Package Inspection

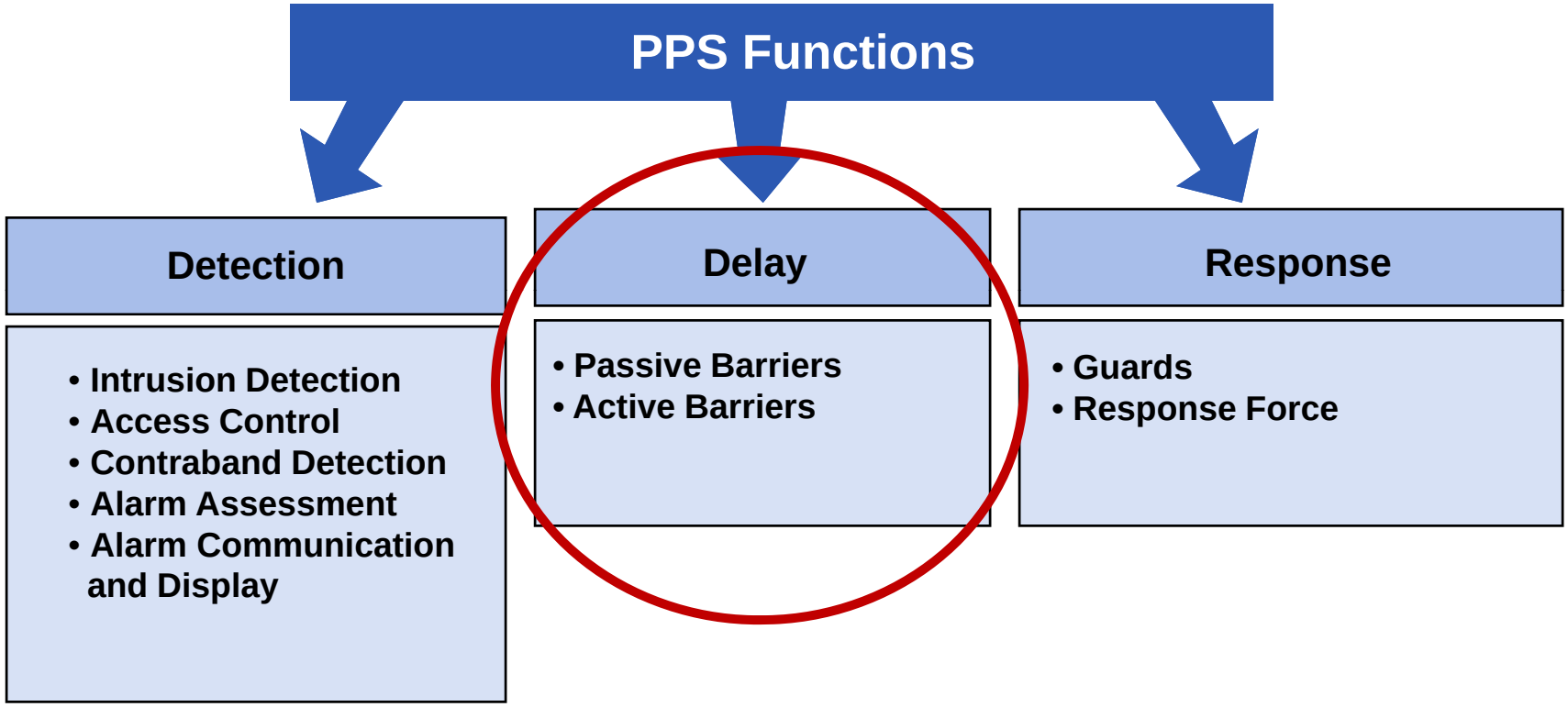
Vehicles

Portals or Stationary Inspection

Features of a Good Access Control/ Contraband Detection System

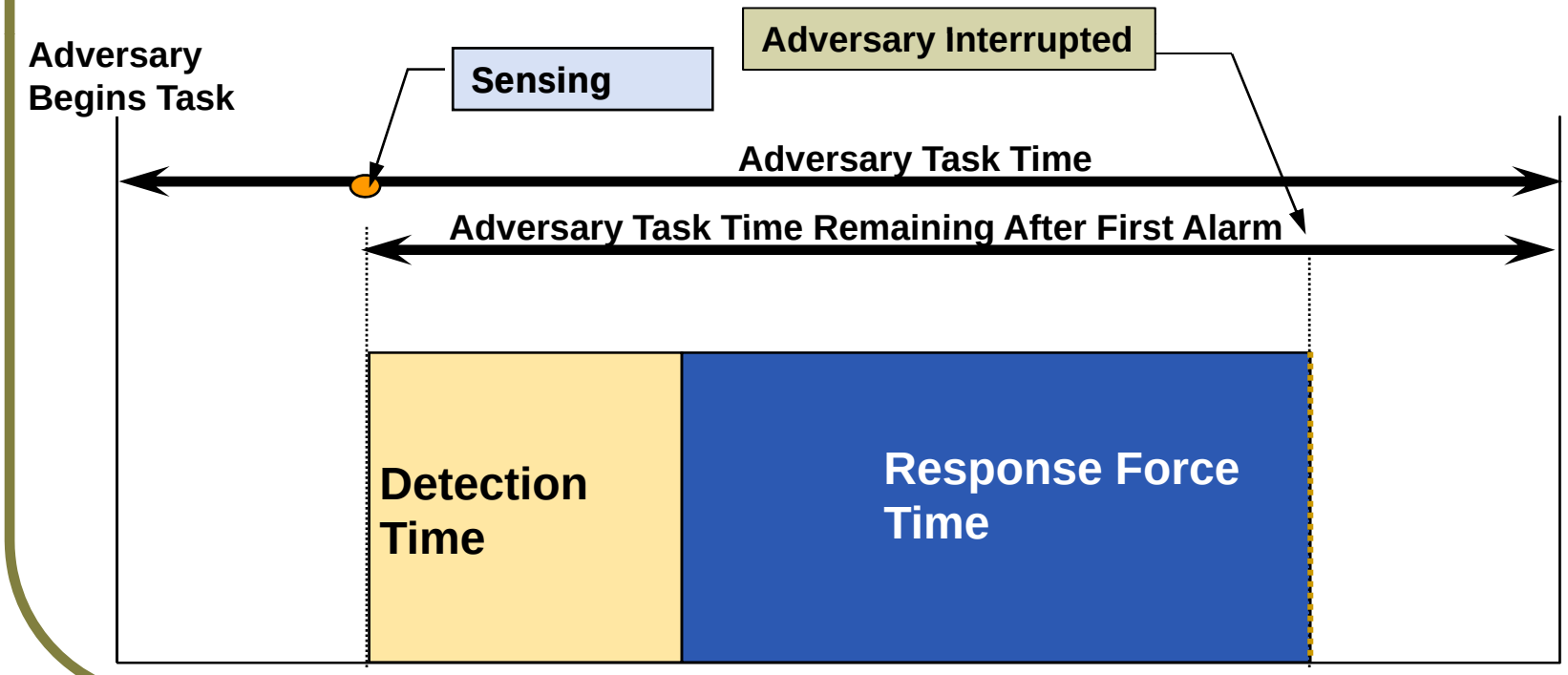
- Implements site requirements for limiting access to only those with access authorization
- Integrated with Physical Boundary
  - Personnel and Vehicle Entry
    - Blocks passage until access verification is complete
    - Provides secondary inspection and verification for specialty cases
    - Procedures for non-standard and emergency conditions
  - Interfaces with Intrusion Detection System
- Accommodates normal operating requirements
  - Peak throughput
  - Routine personnel, equipment, and material movement

Role of Delay



Purpose of Access Delay System

- After detection, delay elements prevent completion of a malevolent act by providing delay until response forces can arrive.



Characteristics of Good Access Delay

- Provides Delay after Detection
- Exhibits a balanced design
  - No weak links
  - Considers all adversary paths, tools, and skills
- Employs defense-in-depth by delay-in-depth
  - Different defeat tools and skills required
  - Multiple barriers
  - Different barriers
- Does not compromise safety

Types of Access Delay

- Passive Barriers include structural elements:
  - Doors, walls, floors, locks, vents, ducts, and fences
  - Always fail secure
  - Conventional construction
    - Provides minimal delay against formidable threat; e.g., explosives
    - Can detain an adversary at predictable locations
  - Upgraded construction
    - Adds some delay
    - Design should maintain balanced protection

Types of Access Delay

- Guards/Response Force
  - Flexible and continuous delay element
  - Provide minimal delay when adversaries use force except when in fixed and protected positions
  - Additional guards used in contingency plans

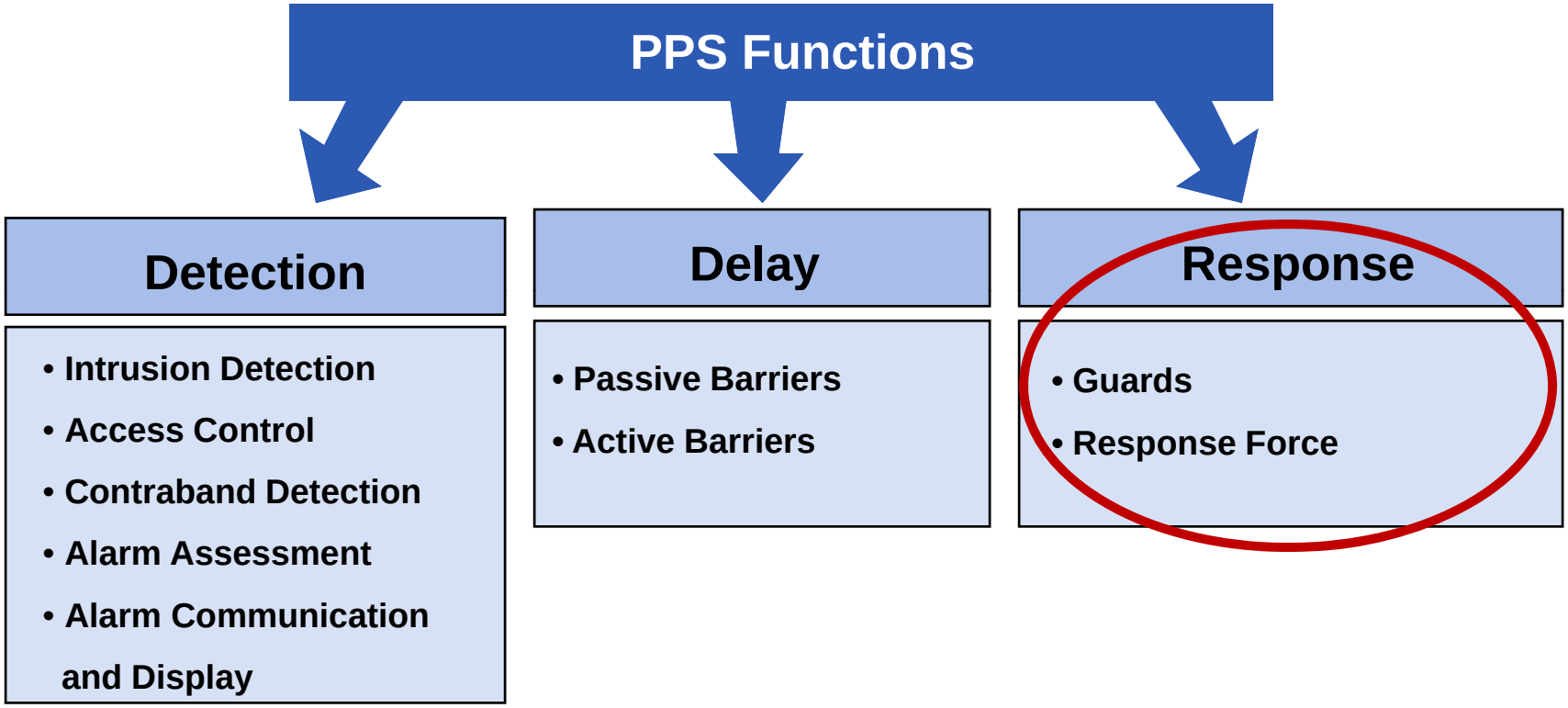
Types of Access Delay

- Activated Barriers
  - Are not in place until activated by
    - guard
    - intrusion detection
    - combination
  - Include chemical fogs and smokes, foams, and irritants
  - Good for most types of threats
  - Safety considerations for unintended activation

Compensatory Measures

- Barriers must be considered in relation to the adversary's objective as defined in the DBT.
- Barriers must be in place 100% of the time, or compensatory measures must be taken.
- Compensatory measures include the following:
  - Personnel entry points: doors or turnstiles
  - Vehicle entry control point: Sally Port configuration; i.e., two barriers in series
  - Vault door: provides added protection; must be guarded when open or accessed

Role of Response



- Response follows Detection and occurs in parallel with Delay.

Guards and Response Forces

Guard Forces:
People that perform routine, day-to-day duties

Response Forces:
Persons responsible for the delay, interruption, and/or neutralization of an adversary

- Considerations
  - Staffing the guard and response forces – direct or contract employees
  - Role of support agencies – written agreements
  - Legal Do's and Don'ts
  - Contingency planning
  - Staffing and attrition

Role for Response

- **Interruption** – Successful arrival of the Response Force at an appropriate location to capture or detain the adversary
  - Requires
    - Accurate communication to response force
    - Effective deployment of response force
- **Neutralization** – Successfully stops the adversary before the adversary's goal is accomplished
  - Response Force kills, captures, or causes the adversary to flee
  - Use-of-Force continuum

Role for Response

- Use-of-Force Continuum

Presence => verbal => use of hands => less lethal => deadly force

=> => => =>

Strategies

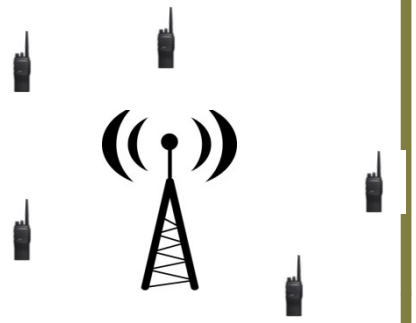
- Four strategies for interruption and neutralization
  - **Denial** – preventing adversaries from getting to an asset
  - **Containment** – preventing adversaries from leaving the site with an asset
  - **Recapture** – taking over by force a critical location on the site occupied by adversaries
  - **Pursuit and Recovery** (contingency) – attempting to recover an asset removed from the site by adversaries

Deployment of the Response Force

- Deployment is the action of initiating personnel response to confront the adversary and requires Planning, Training, and Practice
- Response Force Equipment
  - Weapons – non-lethal and lethal
  - Personnel survivability– body armor, gas masks, chemical/biological suits, armored vehicles, fighting positions
  - Miscellaneous – night vision , flashlights, hand cuffs, load-bearing vest
  - Communication Equipment

Communication with Response Personnel

- Vital to command and control
  - Situational awareness
  - Duress



- Multiple mechanisms for operations and contingency
  - Pagers
  - Phones – cell or land lines
  - Sirens and lights
  - Intercoms and public address systems
  - Computer terminals
  - Duress systems

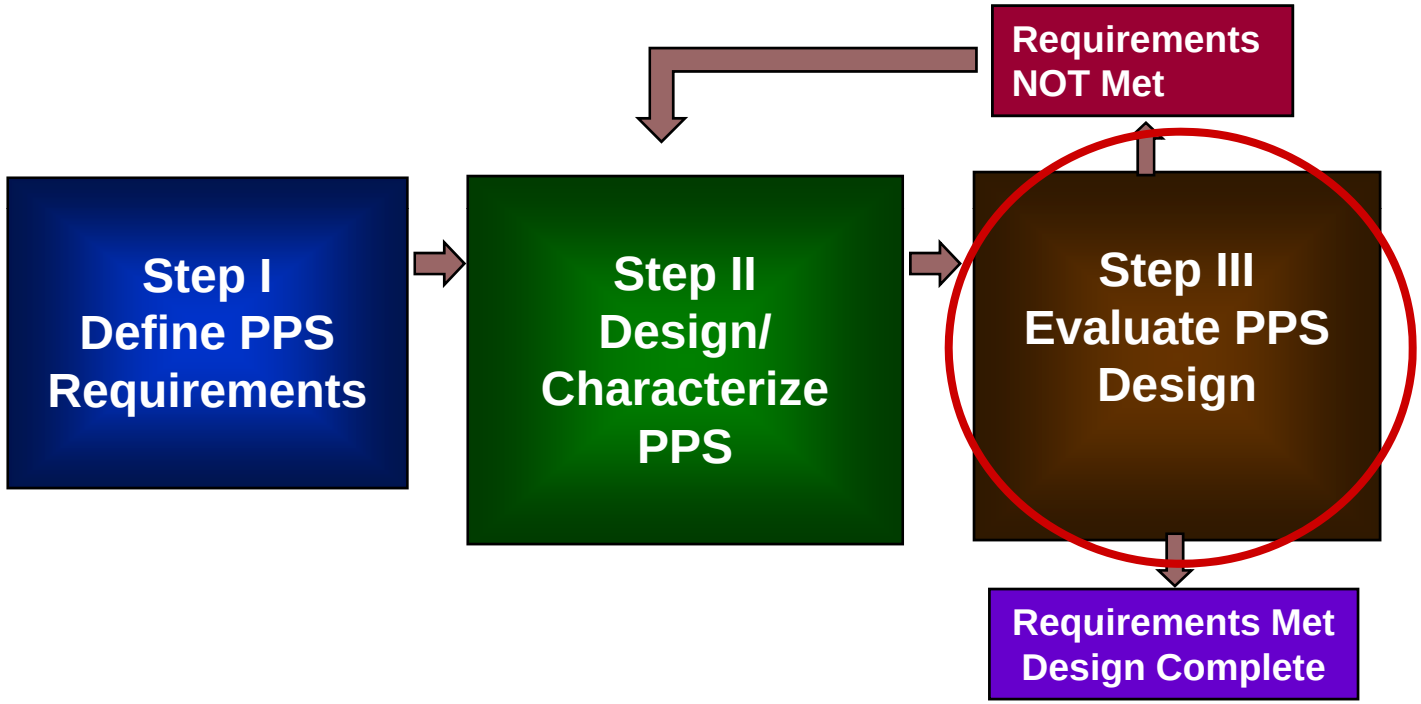
Response Force Training

- Training –
  - General use of equipment – weapons, gear, communication systems and AC&D system
  - Scenario-based – Guards and Response Forces for normal operations and contingency missions, understand tactics
  - Sustained and dynamic – maintains awareness of conditions and changes and proficiency
  - Performance based testing

    force-on-force exercises

Systems Engineering Process for PPS Design

Three interdependent steps required:



Repeat process until requirements are met (iterative process)

Relationship to INCIRC/225/Rev 5

- *4.4.2.4. To ensure that physical protection measures are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection, the State's competent authority should ensure that evaluations based on performance testing are conducted by operators at nuclear facilities and by shippers or carriers for transport. Evaluations should be reviewed by the State's competent authority, and should include administrative and technical measures, such as testing of detection, assessment and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the competent authority should ensure that corrective action is taken by the operator and by the shipper or carrier.*

Evaluation Objectives

The Competent Authority and Licensees have complementary objectives for the evaluation of PPS:

- Meet regulatory and licensee requirements
  - Self-assessment by licensee
  - Inspection by competent authority
  - Periodic re-validation
- Verify and/or improve PPS performance
  - Verify PPS satisfies requirements
  - Identify system deficiencies
  - Analyze system upgrades
  - Compare cost versus performance
  - Select/implement overall best option

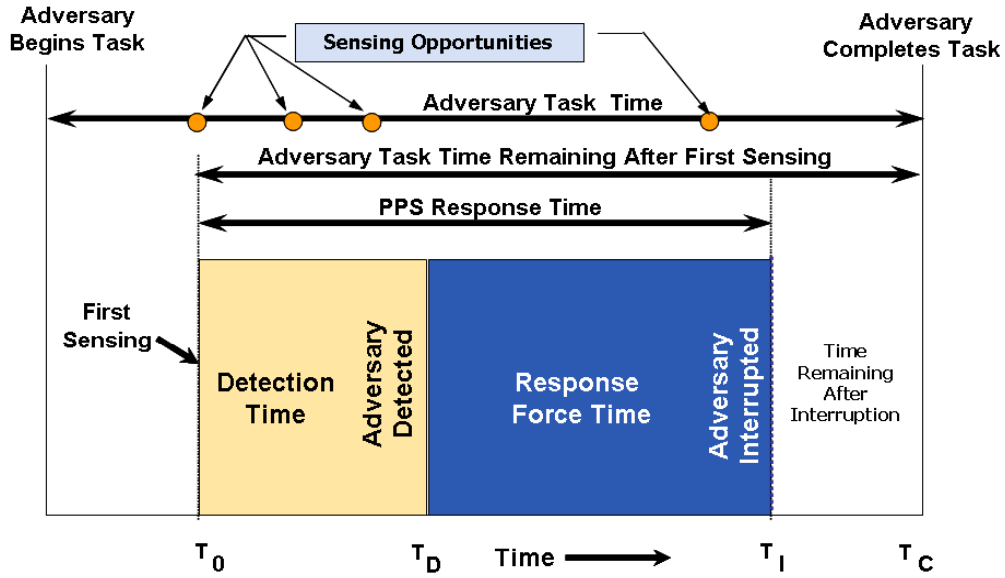
67

Evaluation Tools

- Path Analysis
  - Adversary Sequence Diagrams
  - Single/multipath software
- Neutralization Analysis
  - Modeling/Simulation
  - Table Top
  - Force-on-Force
- Scenario-based Analysis

Path Analysis Compares Two Timelines

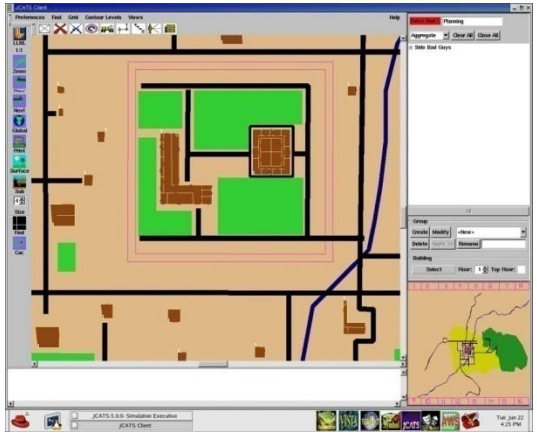
- Adversary and PPS Timelines are used to calculate probability of interruption:

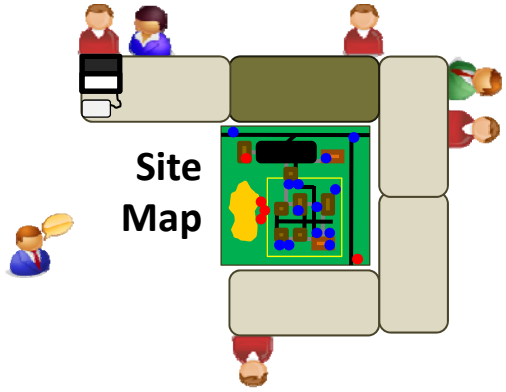


Metric: Probability of Interruption

Neutralization Analysis

- Neutralization models are used to estimate probability of neutralization
  - Computer Combat Simulation Methodology
  - Force-on-Force (FoF) Exercise Methodology (good at replicating individual behaviors)
  - Tabletop Exercise Methodology (good at replicating decision-making)





Metric: Probability of Neutralization

Minimizing cost and operational impacts of a PPS

- Define requirements
- Develop system design options
- Evaluate performance of system options
- Perform effectiveness/operational impact/cost comparison
- Select best system option

Define Requirements

- Operational requirements
  - Access requirements
  - Peak throughput at access control points
  - Material movement requirements
- PPS requirements
  - Targets that require protection
  - Design basis threat
  - Required Protection Level
- Characteristics of a good PPS system
  - Timely detection
  - Balanced protection
  - Protection-in-depth
  - Minimum consequence of component failure

Develop System Design Options

Detection

- **Desired characteristics**
  - High PD
  - Low NAR
  - Low vulnerability to defeat
  - Complementary sensors
  - Integrate with Alarm Assessment System
- **Performance data**
- **Cost data**

Delay

- **Desired characteristics**
  - Provides delay after detection
  - Exhibits balanced design (no weak links)
  - Different defeat tools and skills required
  - Considers all adversary paths, tools, and skills
- **Performance data**
- **Cost data**

Response

- **Desired characteristics**
  - Timely response
  - Effective in defeating DBT
  - Multiple, diverse communications
  - Proper equipment
  - Adequate training
- **Performance data**
- **Cost data**

Evaluate Performance of System Options

- Effectiveness Evaluation
  - Path Analysis
  - Neutralization analysis
  - Expert judgment
- Assessment of impacts on operation
- Cost Evaluation

Perform System Option Comparisons

- Effectiveness/Operational Impact/Cost Comparison
- Revise design to optimize effectiveness/ cost/operational impacts
- Select best option for implementation

Summary

- A physical protection system is an integrated set of personnel, procedures, and equipment intended to prevent the completion of a malicious act.
- An effective physical protection system provides:
  - Timely detection
  - Balanced protection
  - Protection-in-depth
  - Minimum consequence of component failure
- Cost and operational impacts of physical protection systems are minimized by using a systems engineering approach and performance evaluation models to develop cost-effective designs.