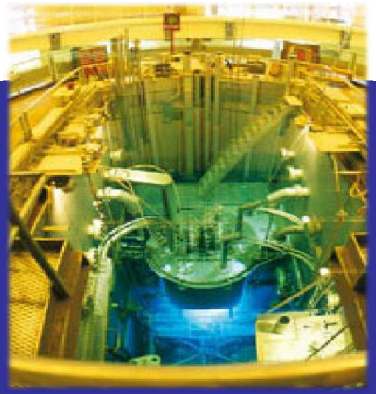
Overview of Physical Protection Systems

SAND2011-0971P



Michael Strosinski & Michelle Stevens
Sandia National Laboratories

23 February 2011

Sandia National Laboratories

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. SAND2009-2801P

National Nuclear Security Administration

Introduction

- **Nuclear Energy Corporation of South Africa (NECSA) introductions**
- **Sandia team**
  - Michelle Stevens
  - Michael Strosinski
- **SNL and NECSA cooperation to date**
  - Memorandum of understanding (MOU)
  - 2010 FIFA World Cup
  - Physical protection enhancements
- **Purpose of today's briefing**

Objectives

- **Provide answers to the following questions**
  - What is a physical protection system (PPS)?
  - What are the elements of a PPS?
  - What constitutes an effective PPS?
  - How can effective security be realized while minimizing cost and operational impacts?
  - How can Sandia help NECSA achieve a greater level of physical security for high-risk nuclear and radiologic materials?

What is a Physical Protection System?

- **A physical protection system is an integrated set of *personnel*, *equipment*, and *procedures* that prevent the completion of a malicious act**

- **What is a malicious act?**

  - **THEFT**: unauthorized removal of material

  - **SABOTAGE**: damage that leads to a release

  - Per International Atomic Energy Agency (IAEA), *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, a *malicious act* is the act or attempt to remove or sabotage nuclear materials

International Guidance on Level of Protection

- **INFCIRC/225/Revision 5**
  - Provides a set of recommendations on requirements for the physical protection of nuclear material (in use, in 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
  - Addresses the current threat environment and ensures conformance to the Convention on Physical Protection of Nuclear Material (CPPNM)

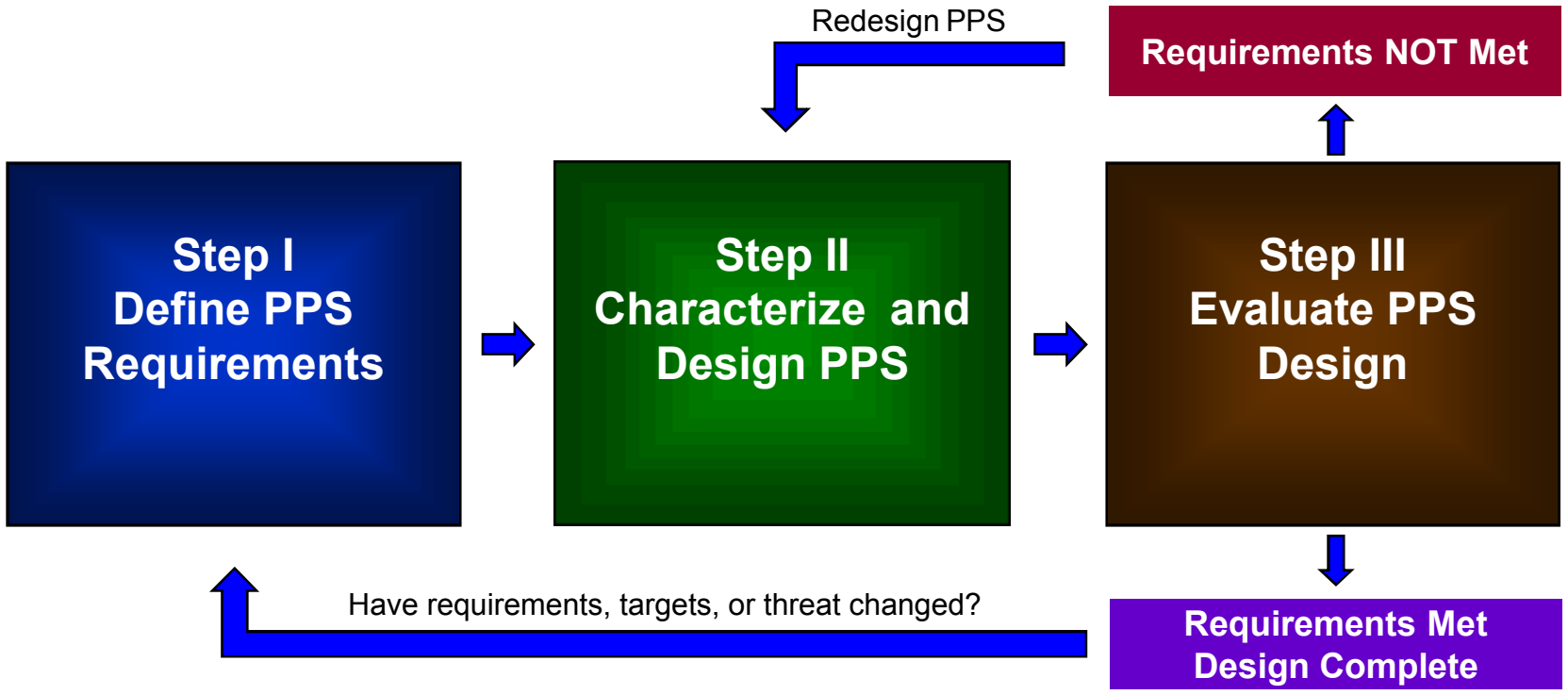
Physical Protection System Objectives*

- **Protect against unauthorized removal of nuclear material in use, in storage, and during transport based on the site's or State's defined threat**
- **Protect against sabotage of nuclear facilities and sabotage of nuclear material in use, in storage, and during transport**
- **Ensure the implementation of rapid and comprehensive measures by the State to locate and recover missing or stolen nuclear material**
- **Mitigate or minimize the radiological consequences of sabotage**

* IAEA document GC(45)/INF/14, September 2001

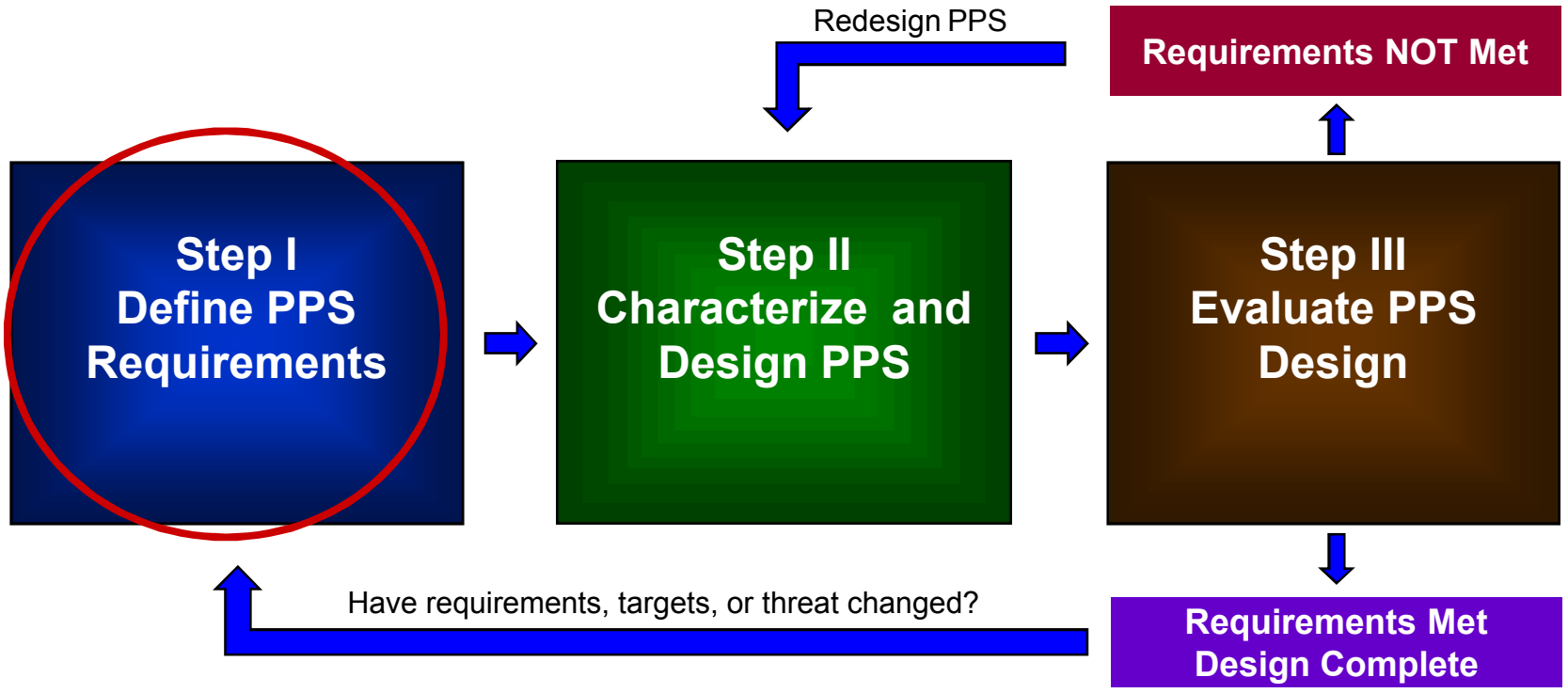
Systems Engineering Process for PPS Design

Design and evaluation process has three interdependent steps



Repeat process until requirements are met (an iterative process)

Systems Engineering Process for PPS Design



PPS Requirements

- **Three fundamental questions begin the process of defining requirements for a PPS**

1. What targets must be protected?
2. What threats must these targets be protected against?
3. What level of risk is acceptable?

1. What Targets Must Be Protected?

- **Theft targets**
  - Nuclear or radioactive materials
    - IAEA provides guidance on categorization of nuclear material and radioactive sources to determine the level of protection required

- **Sabotage targets**
  - Facilities housing nuclear or radioactive materials
  - Process or support equipment needed to prevent unacceptable radiological consequences

2. What Threats Must Be Protected Against?

- **The State/site defines the threat that the PPS is expected to withstand**
- **Threat must consider adversary**
  - Motivation
  - Intention
  - Capabilities
  - Size
- **Threat must consider both outsider and insider threats**
  - Outsider threat: protestors, terrorists, criminals
  - Insider threat: disgruntled employees, blackmailed employees
- **The defined threat defines the adversary attributes and characteristics that the PPS must be designed to defend against**
- **Threat is commonly referred to as the design basis threat (DBT)**

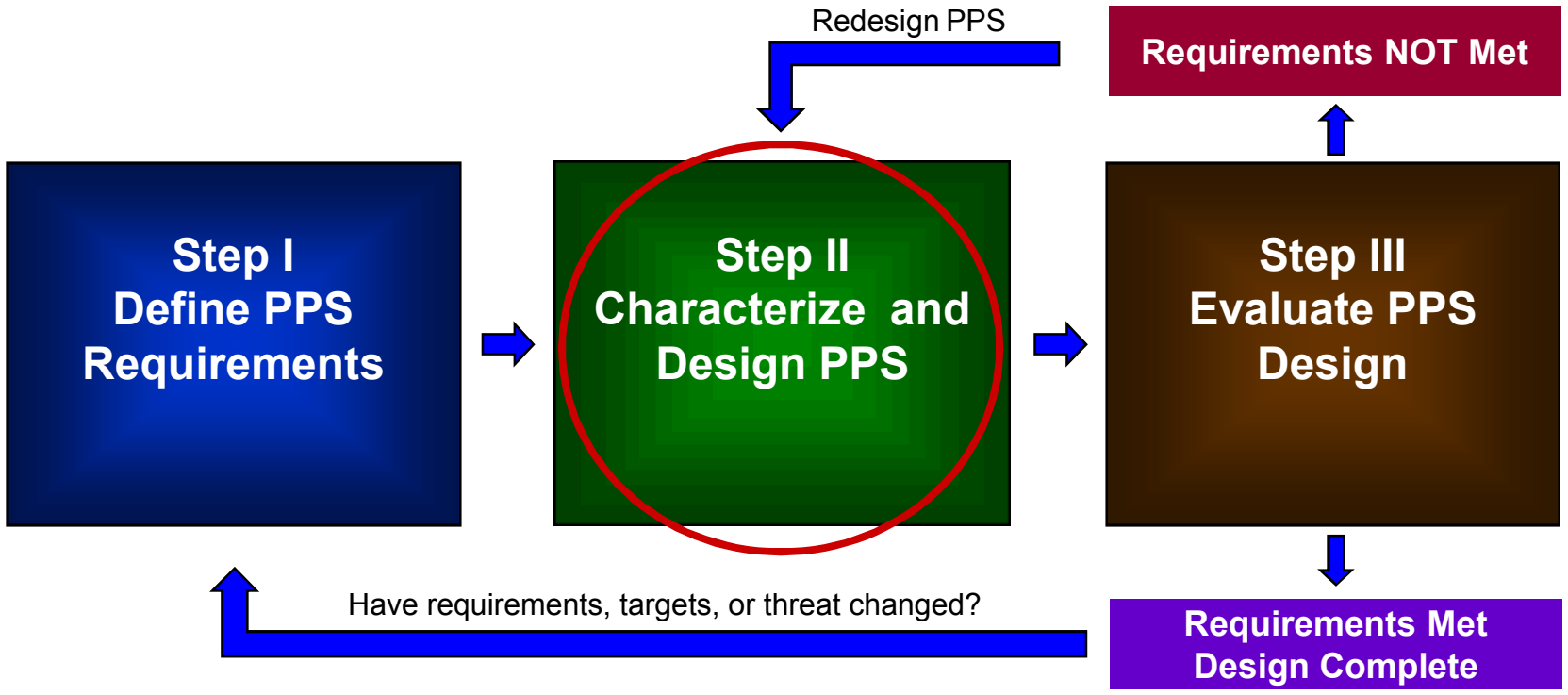
3. What Level of Risk is acceptable?

- **Level of security should reflect the potential consequences of malicious acts**
  - Higher potential consequences require higher levels of security (i.e., graded approach)
- **Effective security reduces the risk associated with the use of nuclear or other radioactive materials to an acceptable level**
- **Security implementation must strike a balance between risk, operational impact, and costs**

Potential 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, or blackmail
- Damage to reputation
- Legal liability

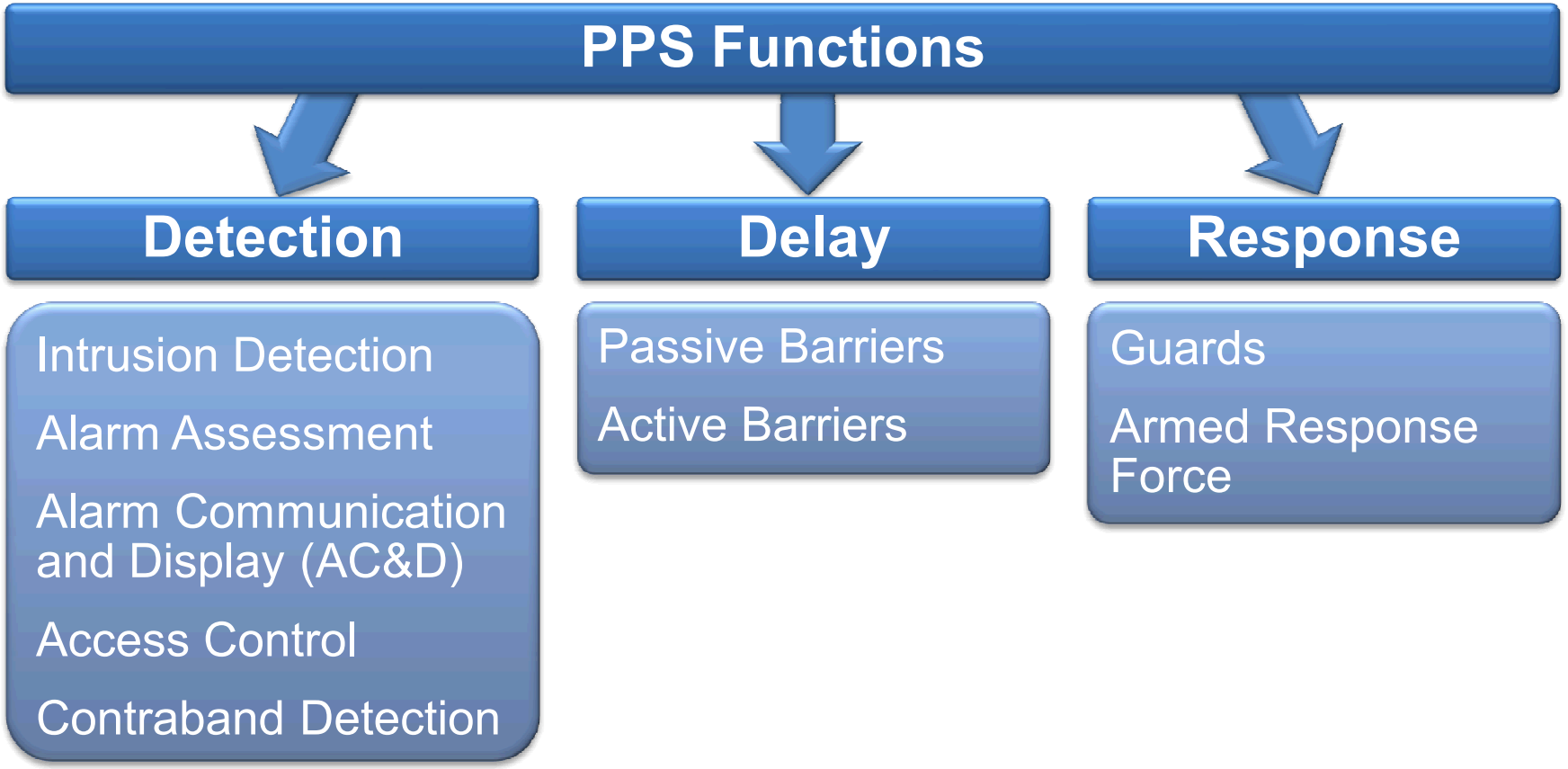
Systems Engineering Process for PPS Design



Balanced Physical Protection

- Effective security requires balance between detection, delay, and response
- With insufficient detection, the response force will be unaware that an attack is occurring
- With insufficient delay, the attack may be over before the response force can engage
- With insufficient response, the adversary will win the fight

Physical Protection System Functions



Develop System Design Options

Detection

- **Desired characteristics**
  - High probability of detection
  - Low nuisance alarm rate
  - 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

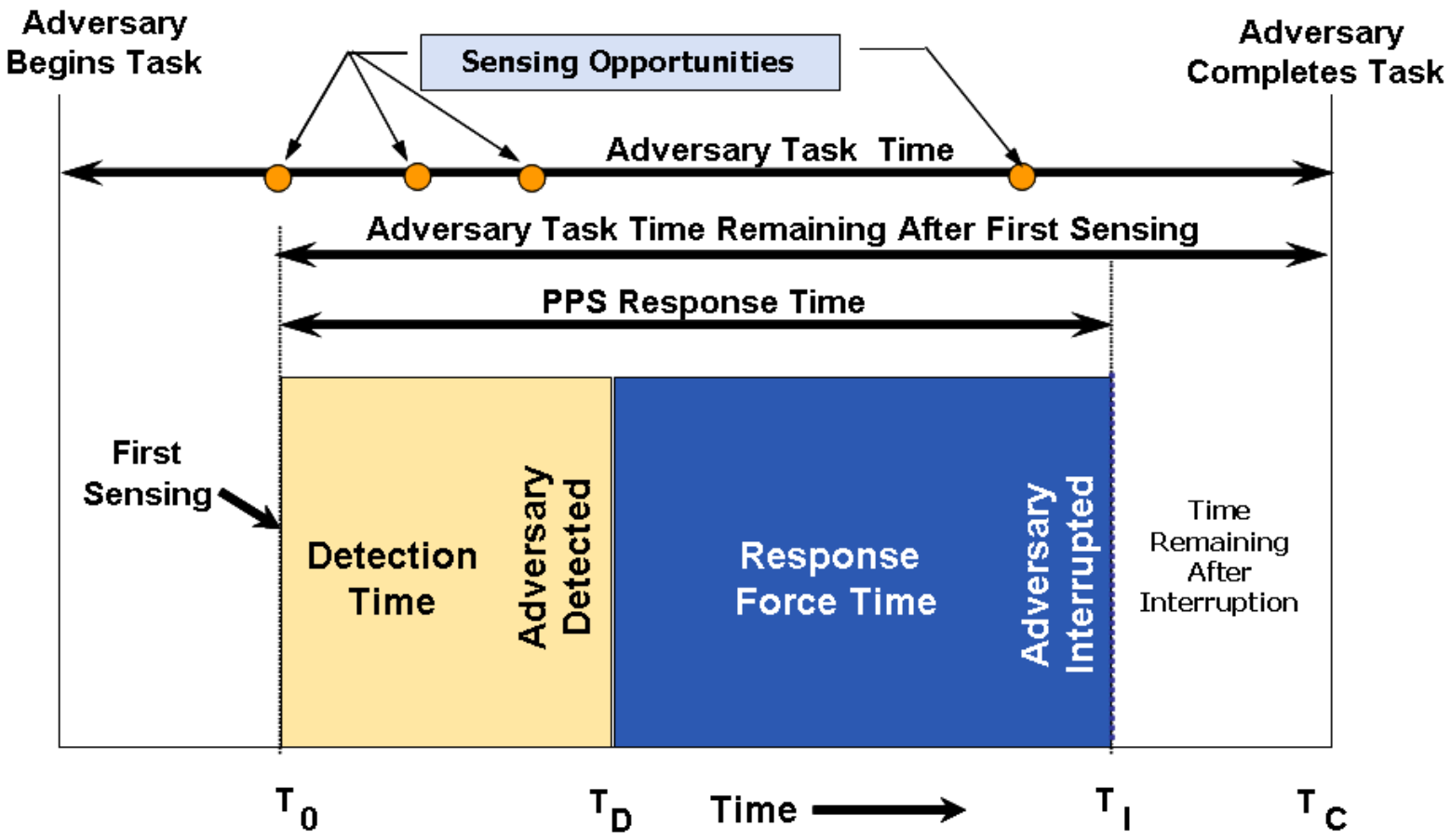
- **Desired characteristics**
  - Timely response
  - Effective in defeating DBT
  - Multiple, diverse communications
  - Proper equipment
  - Adequate training
- **Performance data**
- **Cost data**

Characteristics of an Effective PPS

- **Timely detection and rapid response**
- **System detection and response time must be less than adversary task completion time (timely detection)**
  - Detect intrusion earlier in protected areas
  - Reduce assessment time
  - Increase adversary task completion time (add delay)
  - Reduce response time
- **Balanced protection**
- **Protection in depth**
- **Minimum consequence of component failure**

"An alarm without assessment is not detection."

Adversary Time Line

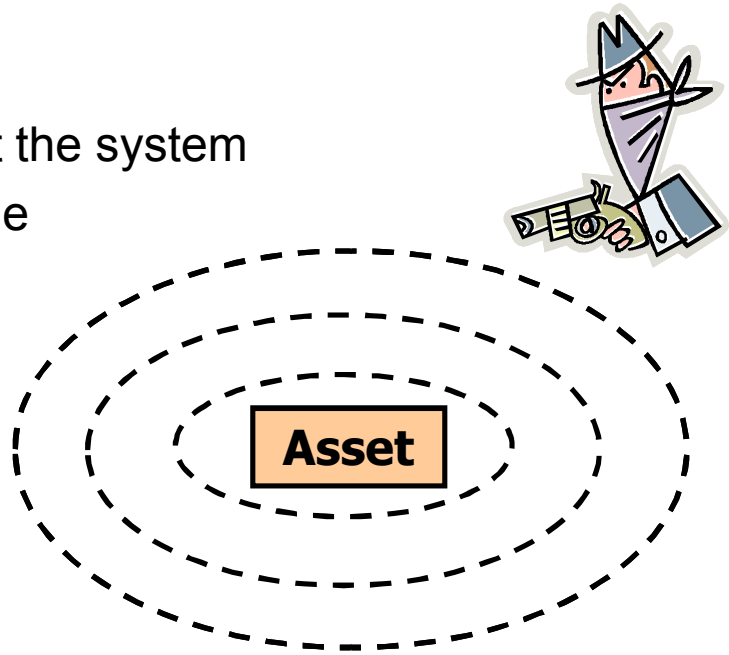


Balanced Protection

- **An adversary will likely chose the easiest path/method to achieve a goal**
- **Balanced protection is achieved when all plausible paths an adversary could take are equivalent in terms of time and difficulty to accomplish**
  - System does not have any weaknesses that an adversary could exploit
- **Example of lack of balance**
  - Upgrading steel doors to “vault doors” in a room with windows
  - Money spent on the vault doors is wasted if there is already an easier way into the room (through the windows)

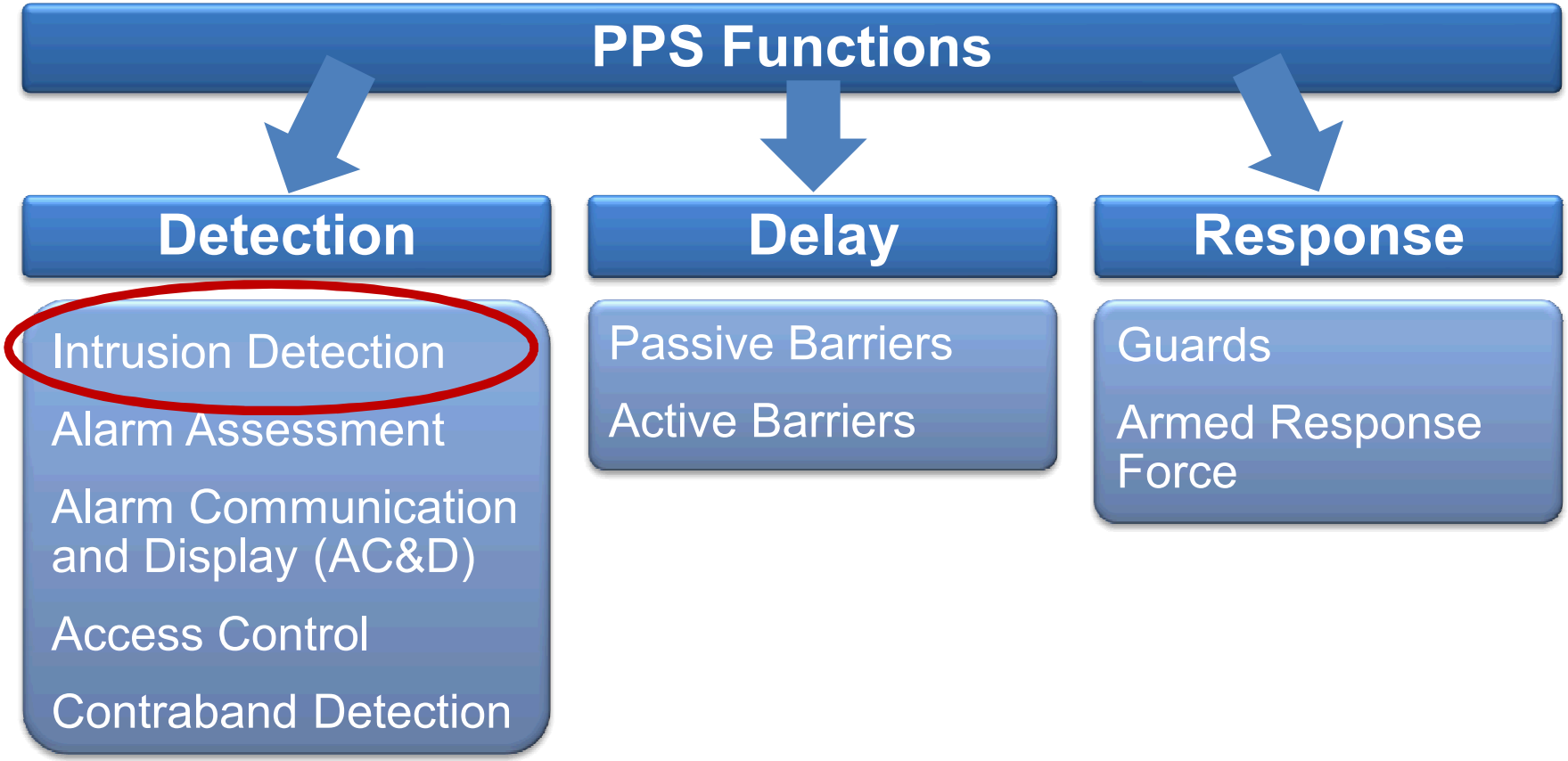
Protection in Depth

- **Adversary must defeat or avoid a number of protection features in sequence**
- **Protection in depth should**
  - Start at the target and work out
  - Increase the adversary's uncertainty about the system
  - Require more extensive preparations by the adversary prior to attacking the system
  - Create additional steps where the adversary may fail or abort their mission
  - Require more time for the adversary to access the target



No single-point failures

Role of Intrusion Detection



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

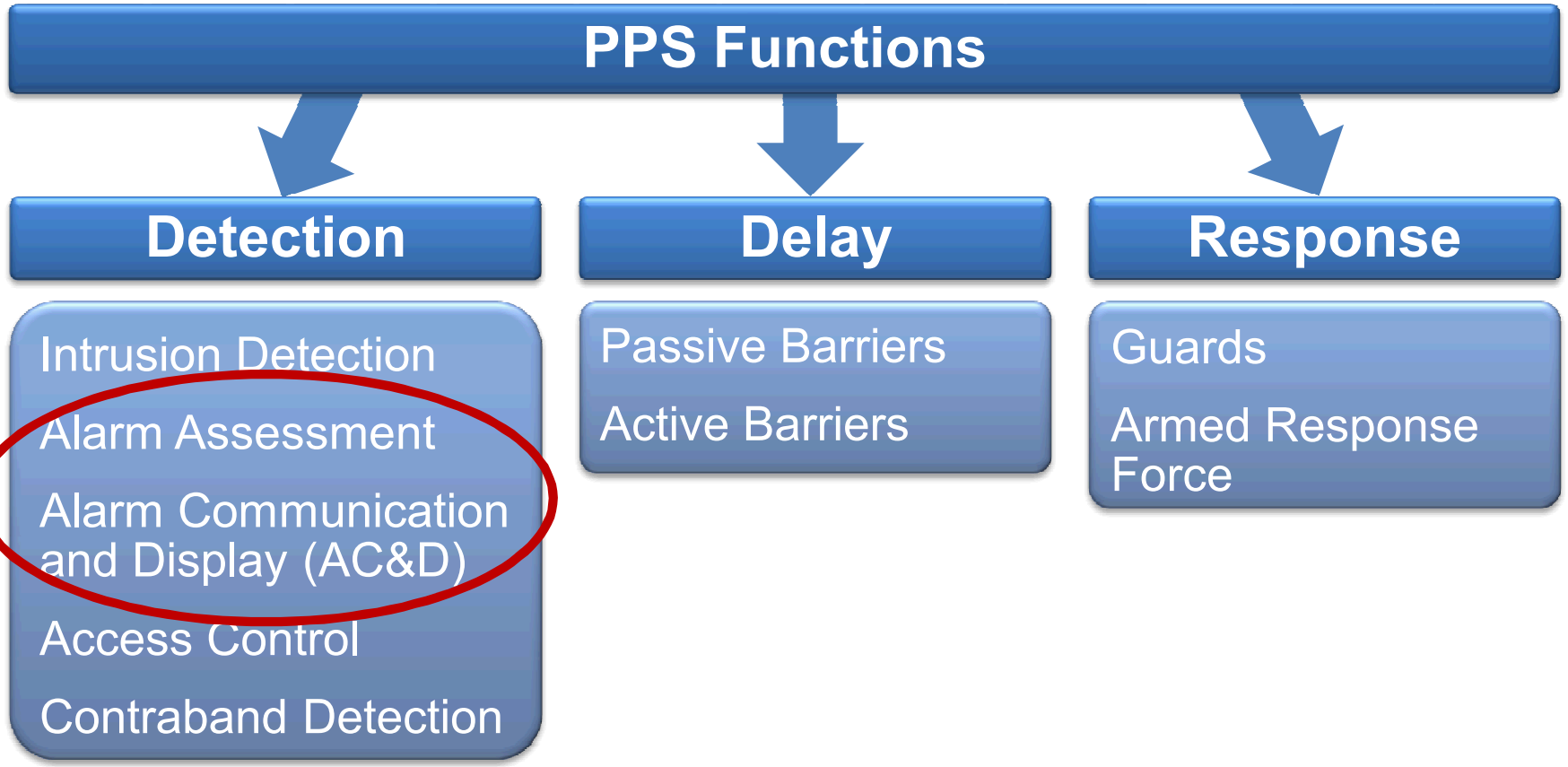
Vulnerability to Defeat

- **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**

Design Characteristics of a Good Intrusion Detection System

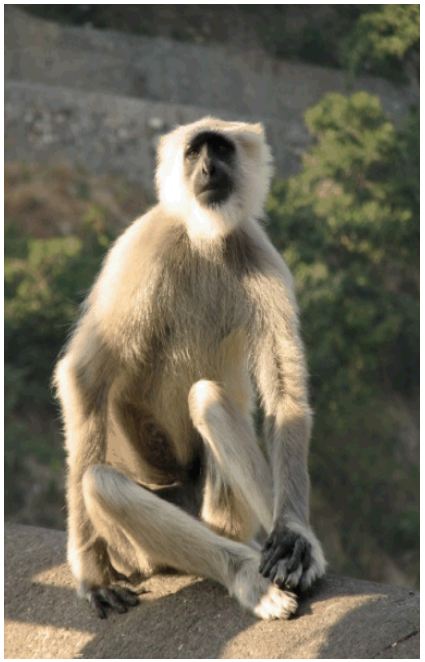
- **Design to highest probability of detection with a minimum of nuisance alarms**
- **Design to minimize vulnerability to defeat**
  - Integration with the barrier system
  - Continuous line of detection with overlapping detection zones
  - Protection of system and system components
  - Use of complementary and different types of sensors
  - Sensor selection for physical and industrial environment
- **Integrate with alarm assessment system that is staffed 24/7**

Alarm Assessment, Communication, and Display



Purpose of Alarm Assessment

- **Determine the cause of each sensor alarm**
  - Intrusion alarm (threat)
  - Nuisance alarm
  - False alarm
  - Maintenance or test
- **Provide details for response**
  - Who
  - What
  - Where
  - How many



Methods of Alarm Assessment

Guard/Response Force

Pros:
- Effective for small areas when combined with intrusion alarms
- Allows for immediate response

Cons:
- Requires extensive manpower to provide adequate coverage
- Human efficacy an issue when not combined with intrusion alarms

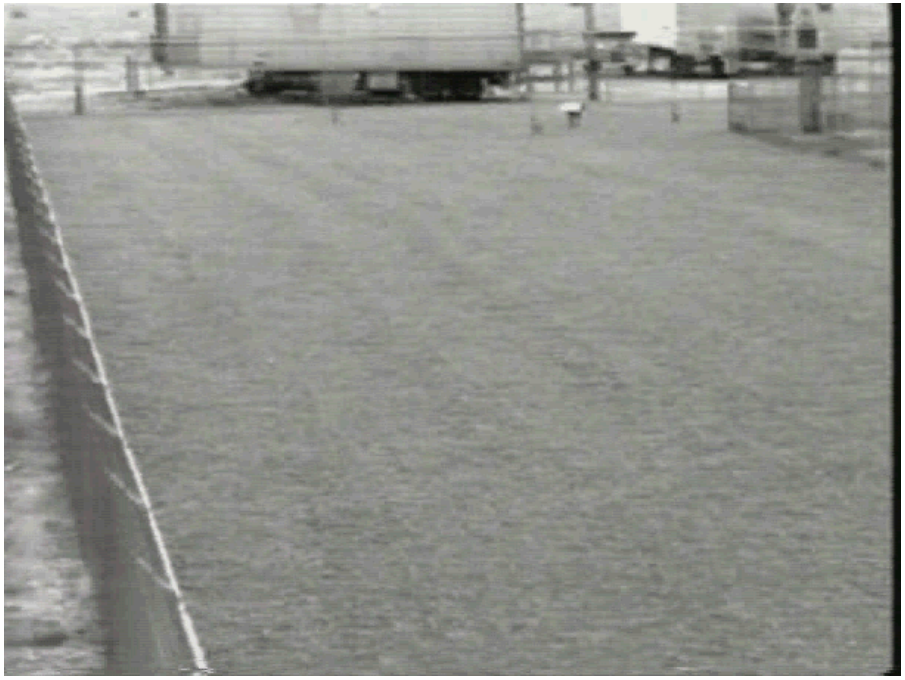
Assessment Cameras

Pros:
- Rapid assessment for large areas
- Reduces impact and cost of personnel

Cons:
- Cost of infrastructure
- Maintenance
- Response Force assessment may still be required

Video Assessment

- **Video assessment is alarm-initiated video of a sensor detection zone at the time of an intrusion alarm.**



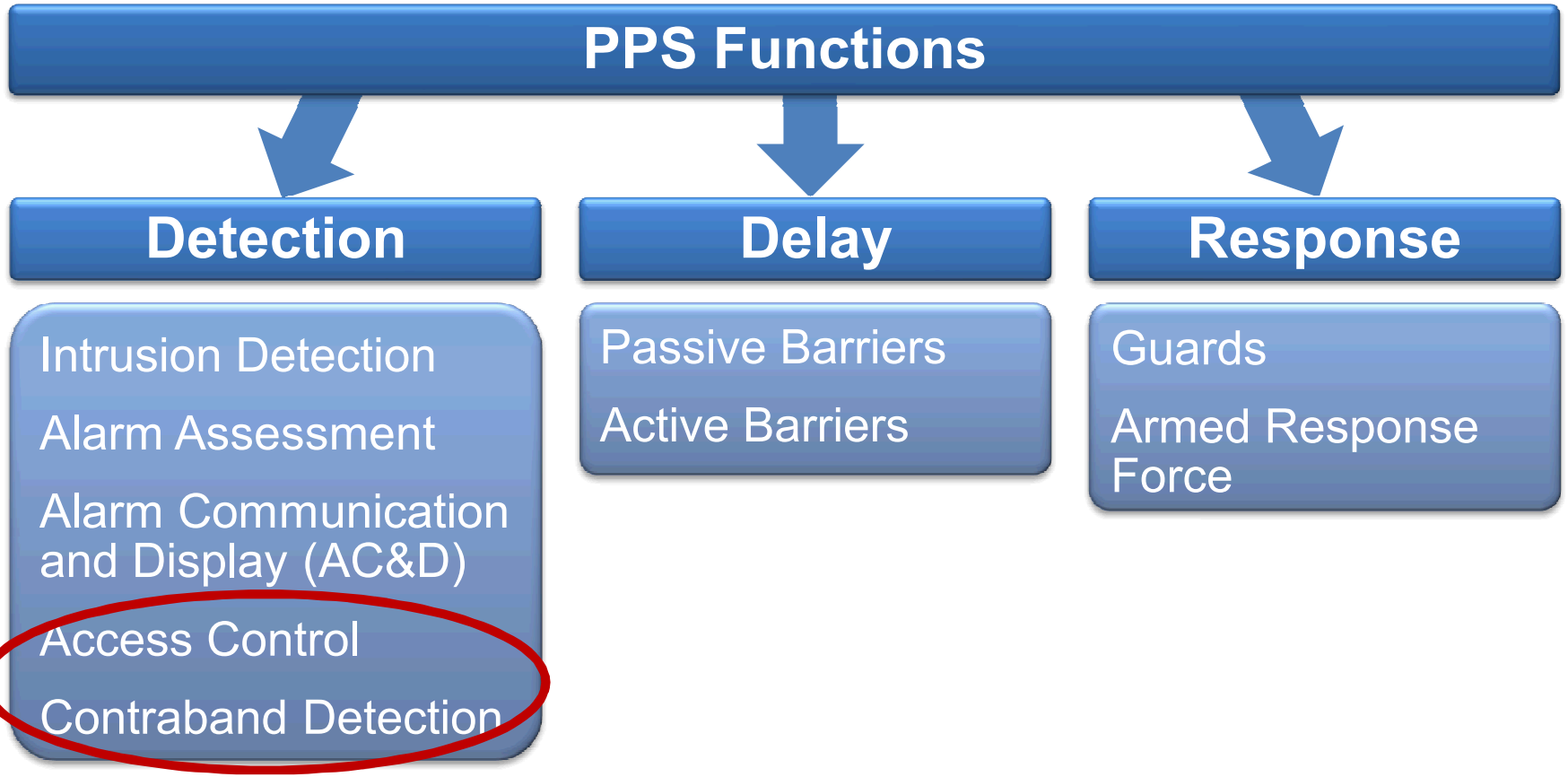
- **Video assessment is integral to the AC&D system.**

Operator Functions of AC&D System

Features of a Good Central Alarm Station

- **Staffed 24 hours a day, 7 days a week**
- **Provides overall status of site "security system"**
  - Alarm annunciation – audible, visual, location
  - Video displays are linked to alarm outputs
- **Provides effective communication between the central alarm station (CAS) and Response Forces**
- **Interfaces with access control**
- **Provides a robust and reliable system**
- **Has protection measures for system components and information**
- **Designed for ergonomics**
  - Number of CAS operators
  - Information management
    - Presents information quickly and effectively
    - Logs information

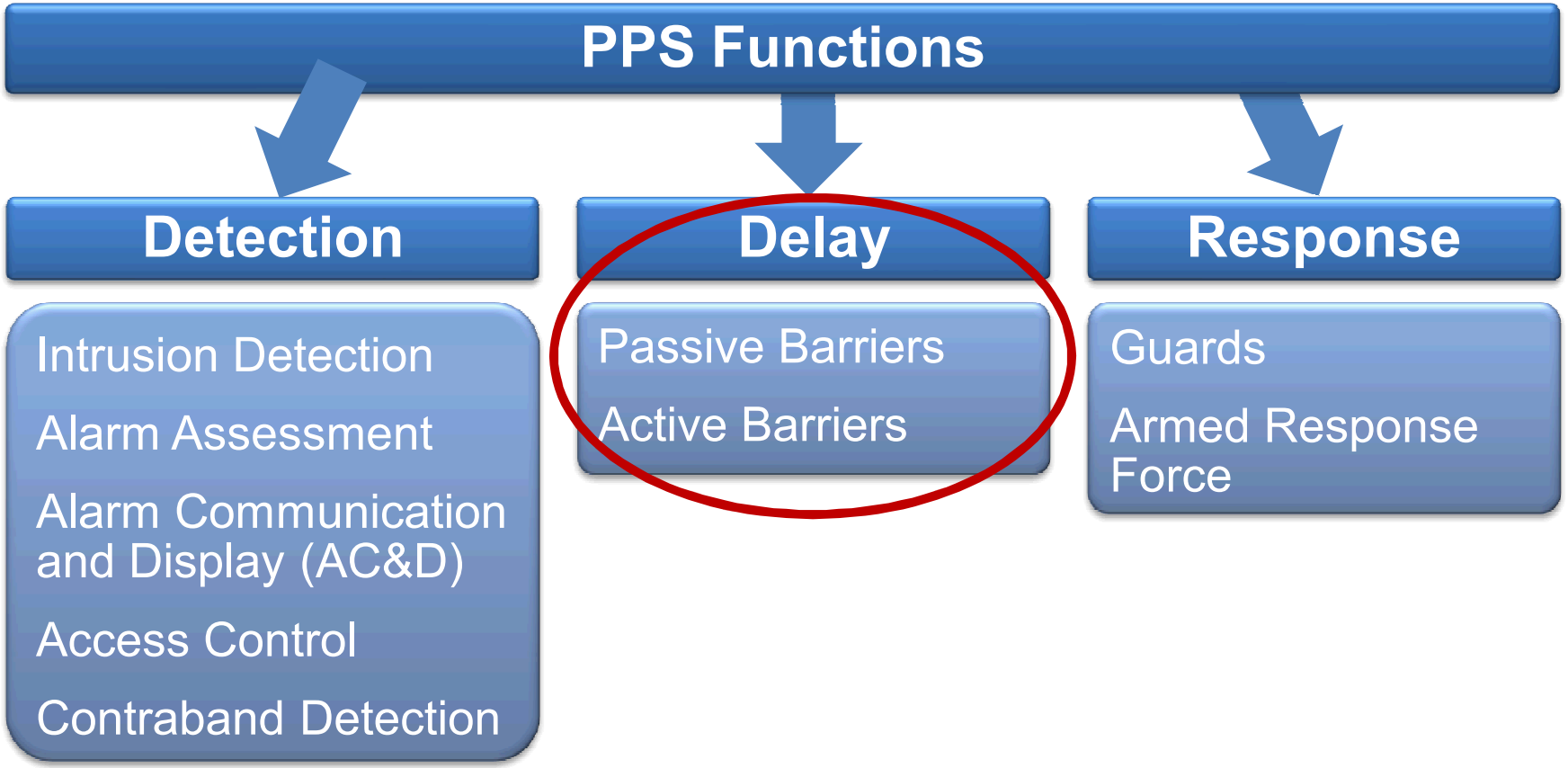
Access Control and Contraband Detection



Design Features for Contraband Detection

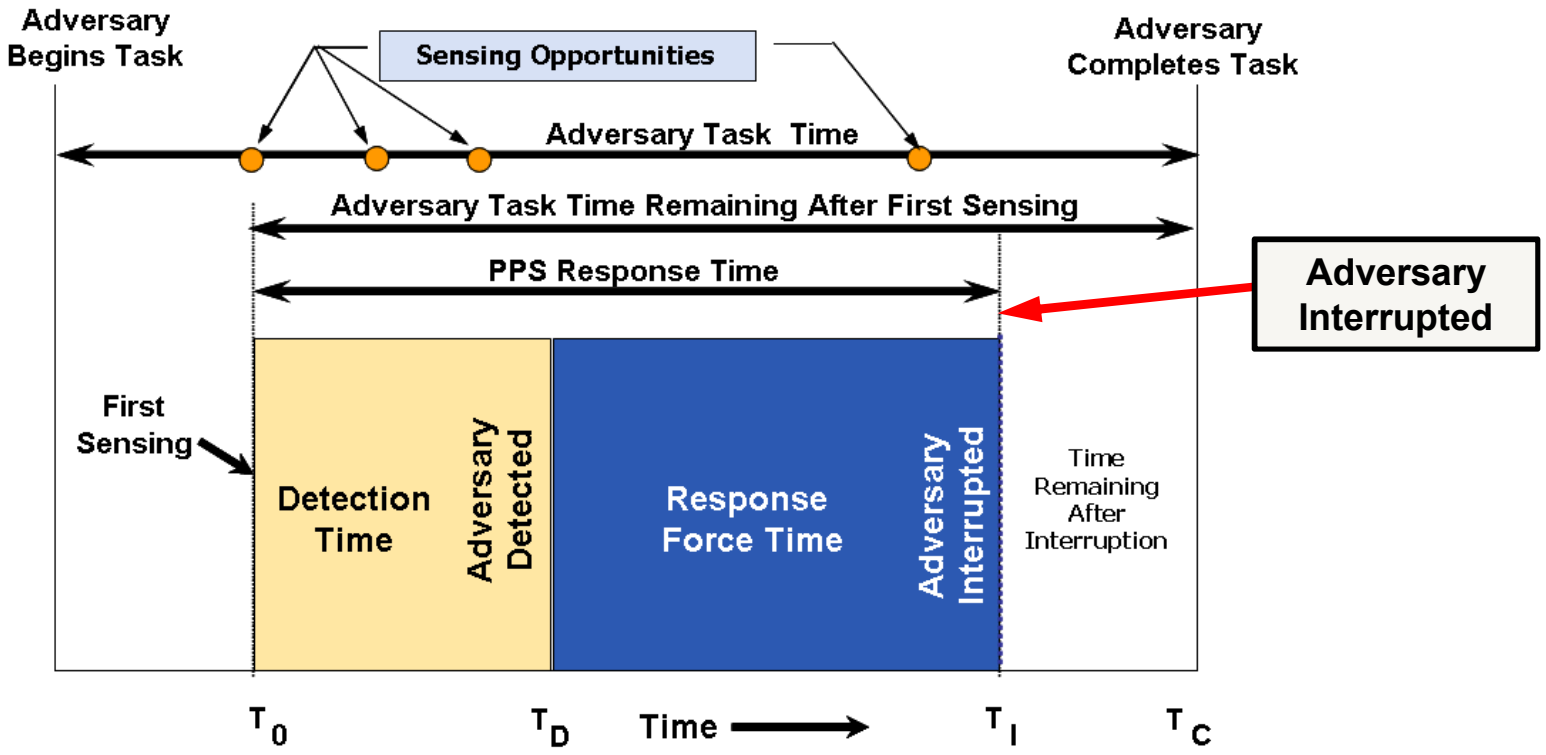
- **Limits access into the restricted area to only those personnel with proper authorization**
- **Personnel, vehicle, and package entry**
  - Blocks passage until access verification is complete
  - Provides secondary inspection and verification
  - Has procedures for non-standard, emergency, and special cases
- **Interfaces with intrusion detection system**
- **Accommodates normal operations**
  - 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**
  - Multiple barriers
  - Different defeat tools and skills required
  - Different barriers
- **Does not compromise safety**
- **Compensatory measures must be used when barriers are not in place**

Access Delay: Passive Barriers

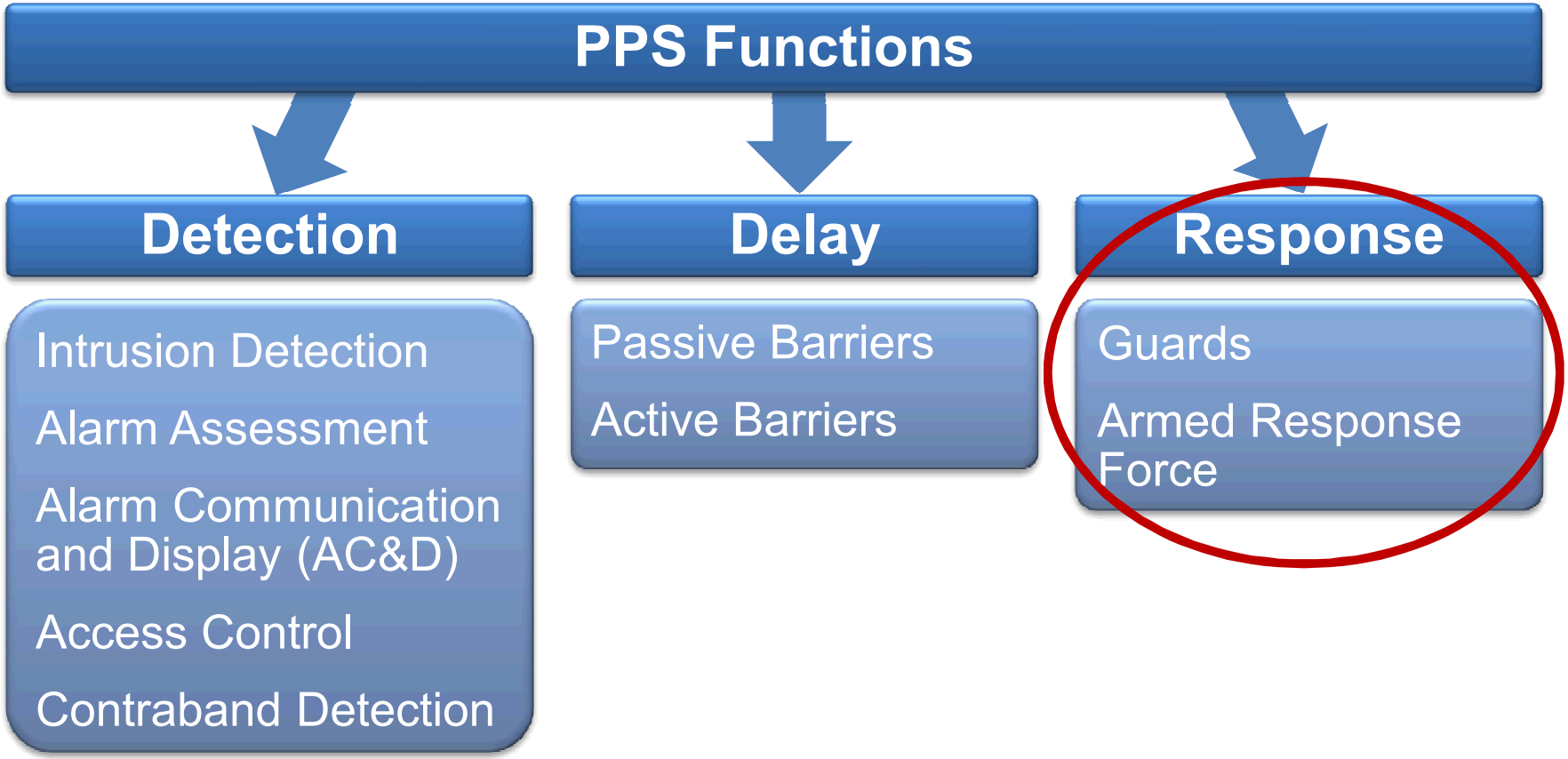
- **Structural elements**
- **Doors, walls, floors, locks, vents, ducts, and fences**
- **Vaults**
- **Conventional construction**
  - Provides minimal delay against formidable threat (e.g., explosives)
  - Can detain an adversary at predictable locations
- **Upgraded construction**
  - Adds some delay
  - Design should maintain balanced protection

Delay features must fail secure

Access Delay: Active Barriers

- **Barriers must normally be in secure position**
- **Active barriers may be controlled by security personnel**
- **Active barriers must be tailored to specific threats and scenarios**
- **Safety is a significant consideration**
  - Unintended activation

Role of Response



- **Response follows detection and occurs in parallel with delay.**

Response Strategies

- **Denial**
  - Preventing adversaries from getting to an asset
- **Containment**
  - Preventing adversaries from leaving the site with an asset
- **Recapture**
  - Use of force to secure a location occupied by adversaries
- **Pursuit and recovery (contingency)**
  - Recovery of an asset taken by adversaries

Guards, Response, and External Forces

- **Guards provide physical security functions (e.g., access control)**
- **Response Forces interrupt and neutralize adversaries**
- **External forces (e.g., South African Police) provide additional support**
- **Considerations**
  - Number of guards versus response forces
  - Direct or contract employees
  - Training
  - Role of external agencies – written agreements
  - Legal do's and don'ts
  - Contingency planning
  - Staffing and attrition

Process for Response

- **Interruption – successful arrival of the Response Force *in sufficient numbers* to begin to neutralize the adversary requires**
  - Identification and assessment of adversary actions
  - Accurate communication to the Response Force
  - Organization and equipping of the Response Force
  - Effective and rapid deployment of the Response Force to the appropriate area
- **Neutralization – successfully stopping the adversary *before the adversary's goal is accomplished* requires**
  - Effective command and communication
  - Sufficient force to neutralize the adversary (kill, capture, or cause the adversary to flee)
  - Compliance with applicable use-of-force laws

Response must "get to the fight in time" and "win the fight"

Use of Force Continuum

Presence → Verbal → Use of Hands → Less Lethal → Deadly Force

Response Force Communication

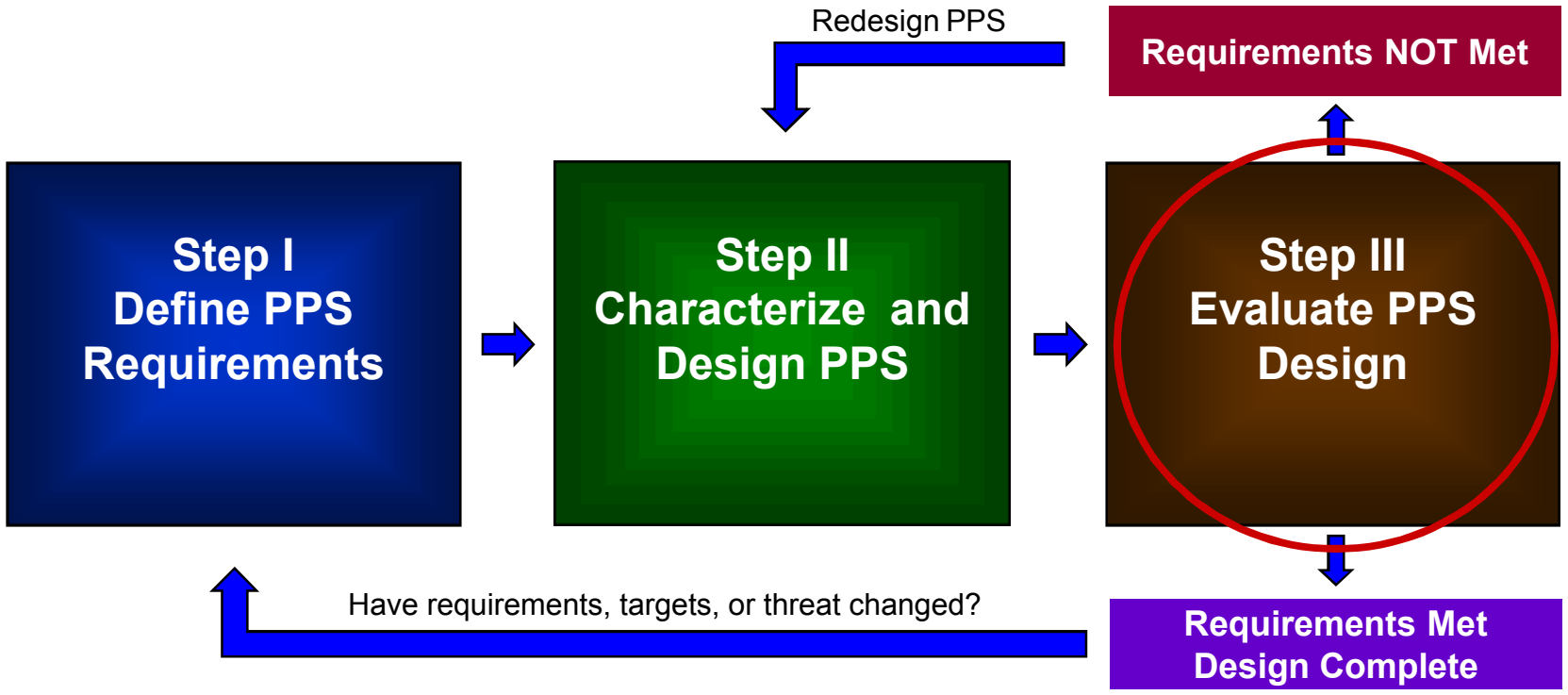
- **Vital to command and control**
  - Situational awareness
  - Duress both for facilities and alarm station personnel as well as for Response Force officers

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

Response Force Training

- **Effective response requires planning, training, and practice**
- **Scenario-based training**
  - Tabletop exercises
    - Command and control level
    - Operational level
- **Performance-based training evaluations**
  - Training based on National Key Point legislation
  - Force-on-force (FoF) exercises
  - Limited-scope performance tests (LSPT)
  - No-notice exercises
  - Response Force timing drills
  - Tactical exercises

Systems Engineering Process for PPS Design



Site Evaluation of a PPS

- **Evaluate the PPS to**
  - Ensure that all requirements are met
  - Ensure the PPS is effective (and to improve effectiveness)
  - Assess impacts on operations
  - Evaluate costs and performance
- **Evaluate PPS alternatives to determine the ideal system, considering**
  - PPS effectiveness
  - Operational impact
  - Development, operational, and sustainment costs
- **Numerous tools/techniques are available for evaluation**
- **Revise design to optimize effectiveness/cost/operational impacts**

State Evaluation of a PPS

- **The competent authority and licensees have complementary objectives for the evaluation of a PPS**
  - Meet regulatory and licensee requirements
  - Verify PPS satisfies requirements set by the State and competent authority
  - Inspection by competent authority
  - Periodic re-validation

47

Recurring Evaluation of a PPS

- **A PPS system must be regularly evaluated to ensure that**
  - System components (hardware) are functioning properly
  - Personnel and processes are effective
  - Changes in facilities or operations are addressed
  - Changes in targets or threats are addressed
  - Deficiencies and vulnerabilities are identified and corrected
  - Areas of improvement are identified
  - Ineffective actions are identified and eliminated
  - New system improvements are evaluated

INFCIRC/225/Revision 5, 3.21

…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.

Summary

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

BACKUP SLIDES

Fundamental Principles of INFCIRC/225/Revision 5

- **Fundamental Principle A: The responsibility for the establishment, implementation, and maintenance of the physical protection regime within a State rests entirely with the State.**
- **Fundamental Principle B: The State has responsibilities during international transport for nuclear materials.**
- **Fundamental Principle C: The State has a responsibility for establishing and maintaining a legislative and regulatory framework to govern physical protection.**
- **Fundamental Principle D: The State should establish or designate a competent authority.**

Fundamental Principles of INFCIRC/225/Revision 5

- **Fundamental Principle E: It is the responsibility of the license holders for implementing the various elements of physical protection of nuclear material and nuclear facilities.**
- **Fundamental Principle F: Organizations are responsible for instituting a security culture.**
- **Fundamental Principle G: Physical protection should be based on the State's current evaluation of threat.**
- **Fundamental Principle H: Physical protection requirements should be based on a graded approach.**

Fundamental Principles of INFCIRC/225/Revision 5

- **Fundamental Principle I: The State's requirements for physical protection should reflect a concept of defense in depth.**
- **Fundamental Principle J: Quality assurance policies and programs should be established for physical security activities.**
- **Fundamental Principle K: Contingency plans should be prepared and adequately exercised.**
- **Fundamental Principle L: Confidentiality of information that could compromise the physical protection system should be protected.**

Other Requirements

- **State/regulator requirements**
- **Operational requirements**
  - Access requirements
  - Peak throughput at access control points
  - Material movement requirements