Fundamentals of Physical Protection Systems and Site Assessment Workshop

SAND2006-4888P

Da Lat, Vietnam
August 22 – 23, 2006

Introduction

Sandia National Laboratories

National Nuclear Security Administration

VAEC

1.0 - The Protection of Nuclear Material/Facilities and Radioactive Materials: INFCIRC/225/Rev.4

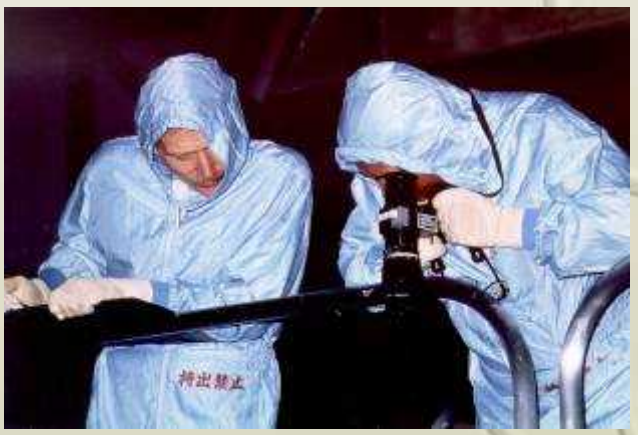
Sandia National Laboratories

NNSA
National Nuclear Security Administration

VAEC

IAEA Three Fold Mission

- Verify commitments to peaceful uses of nuclear material
- Provide *nuclear safety standards*
- Promote technology transfer



Safeguards and Physical Protection

State

- Regulates the control and accounting of nuclear material
- Regulates the physical protection of nuclear material

IAEA

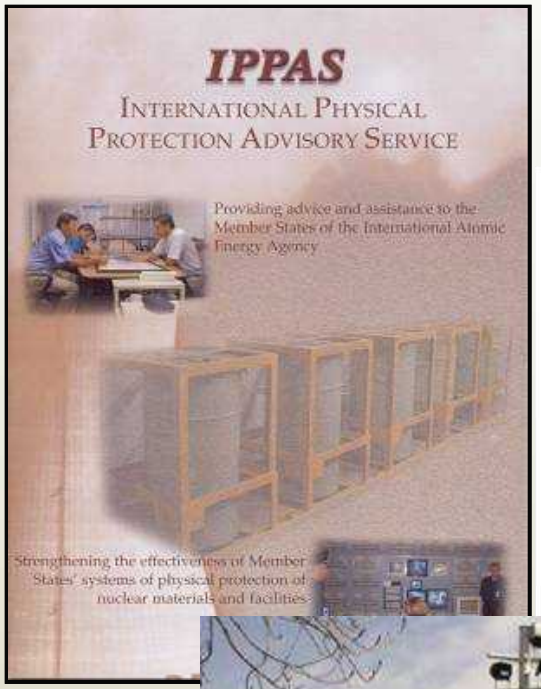
- Independently verifies material accounting data
- Promotes and assists in application of standards of physical protection

Nuclear Security Plan
Eight Major Areas

1) Protection of nuclear material
2) Protection of nuclear facilities
3) Security of radioactive materials
4) Illicit trafficking
5) Nuclear material accountancy
6) Emergency response
7) International legal instruments
8) Information coordination

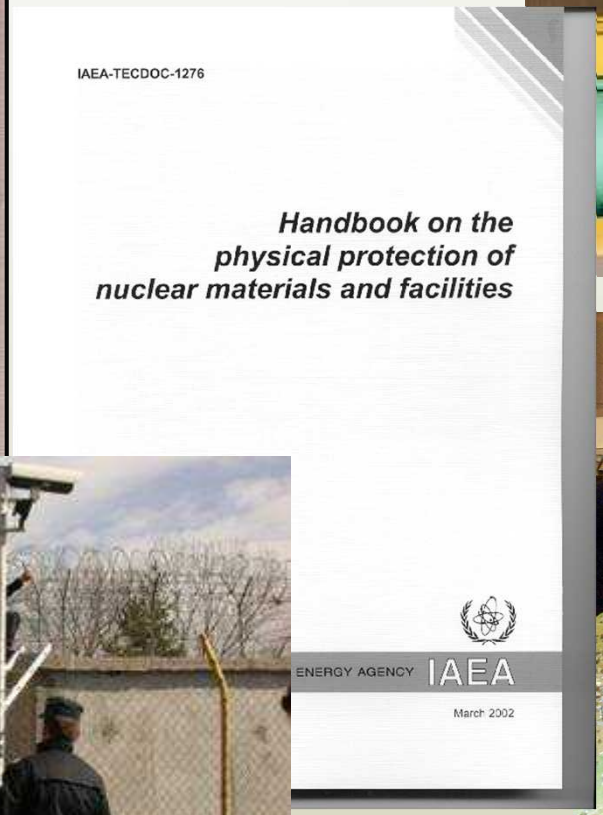
Physical Protection: Nuclear Material and Facilities

IPPAS



Fresh fuel upgrade

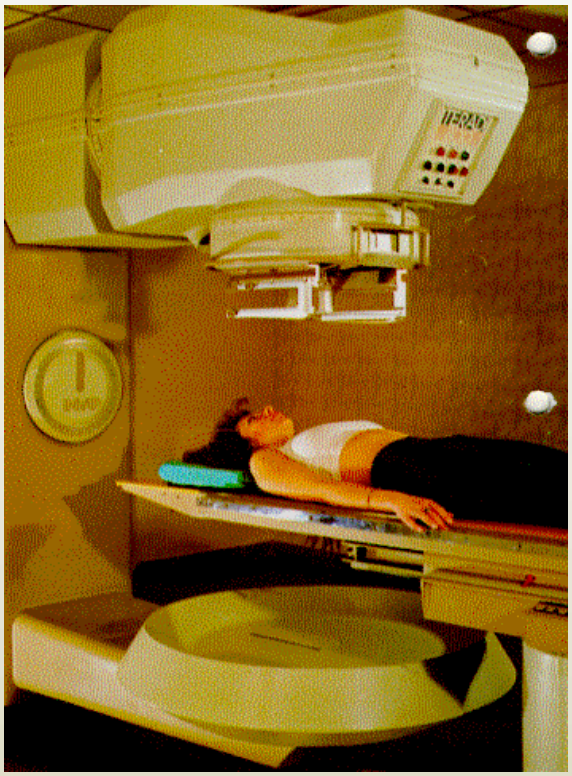
Handbook



China training course

Performance testing

Security of Radioactive Material



Radio-therapy source

Abandoned Radio-therapy source

Code of conduct

Industrial radiography source

Illicit Trafficking

Involving Nuclear and Other Radioactive Materials

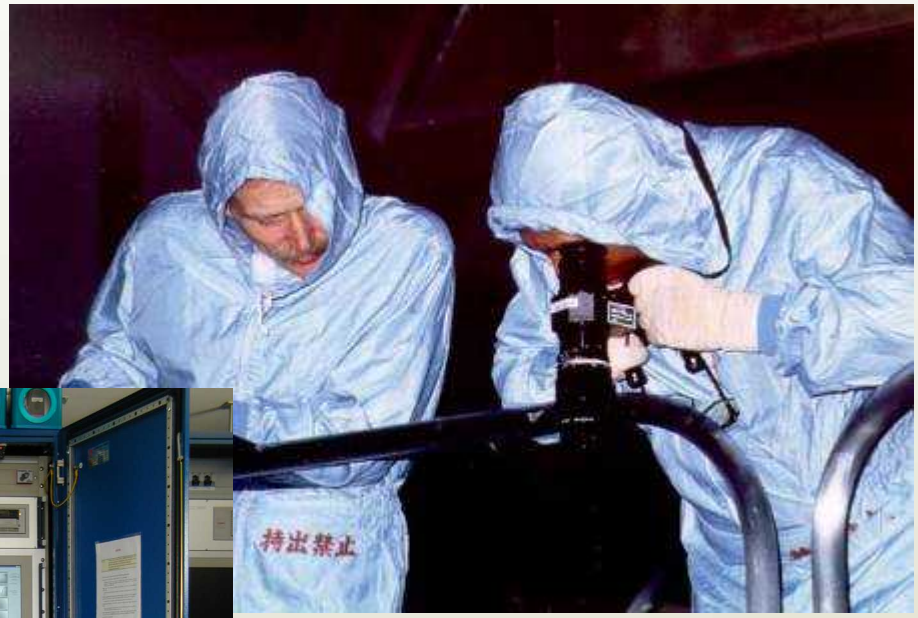
Guidance

Border monitoring

Vienna airport

Nuclear Material Accountancy and Control

Spent fuel measurements

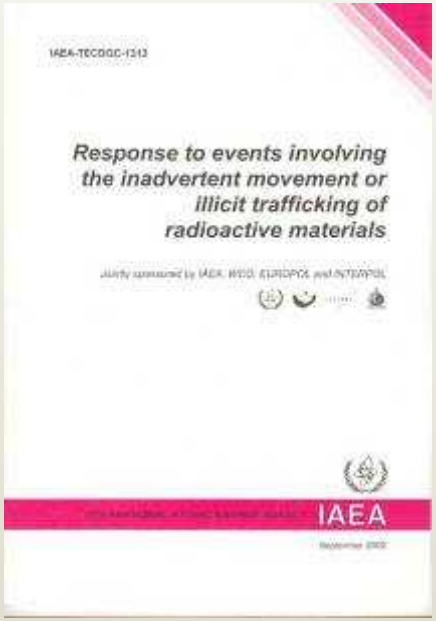


Non-destructive measurements

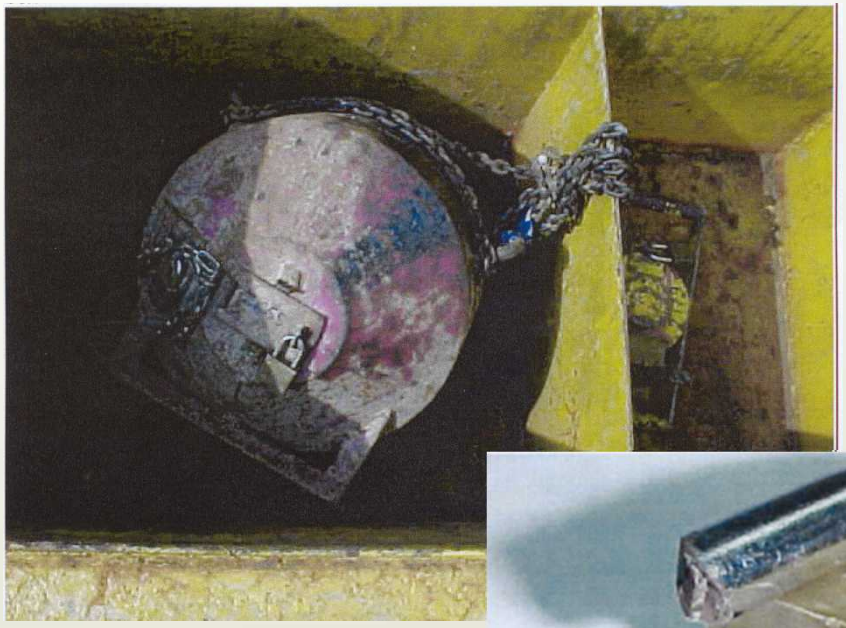
Video surveillance

Seals

Response to Malicious Acts



Guidance on response

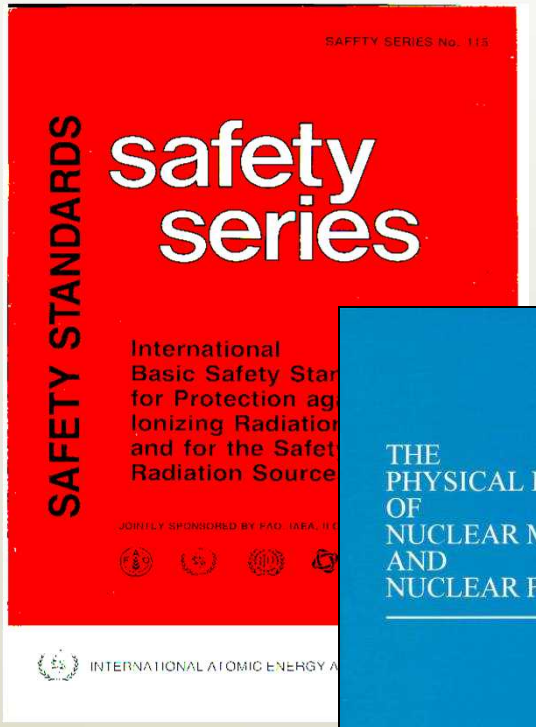


Industrial source

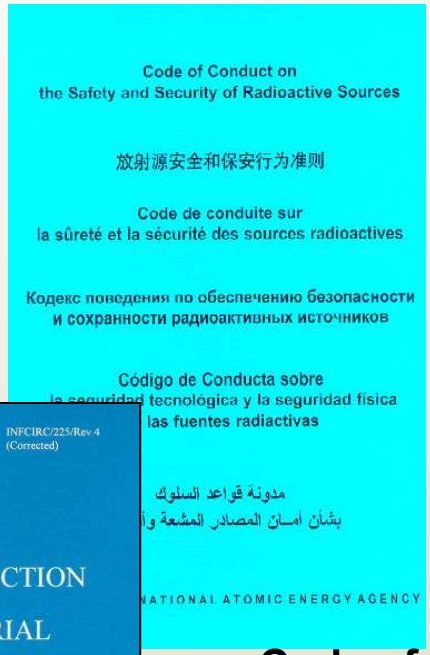
Lock from stolen source

International Agreements, Guidelines

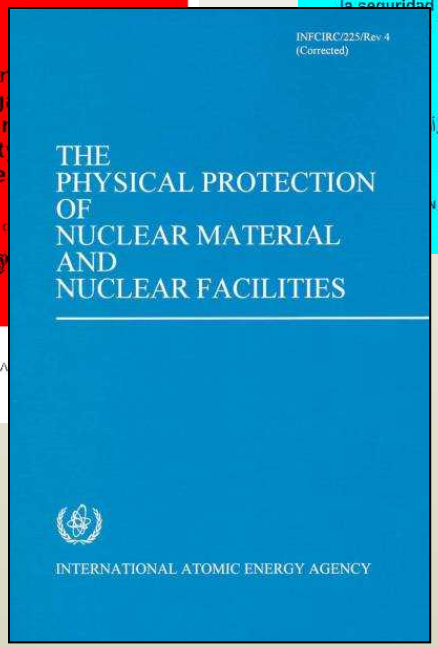
Adherence and Implementation



Basic Safety Series

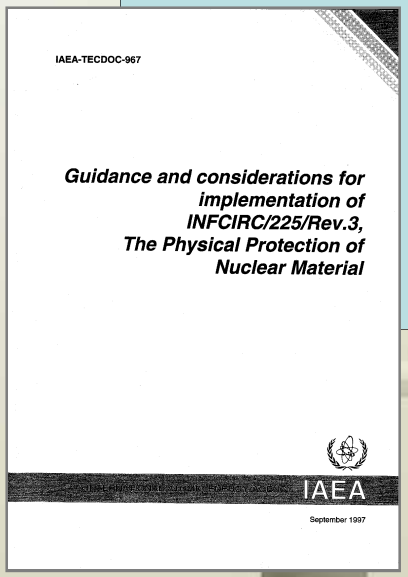


Code of Conduct



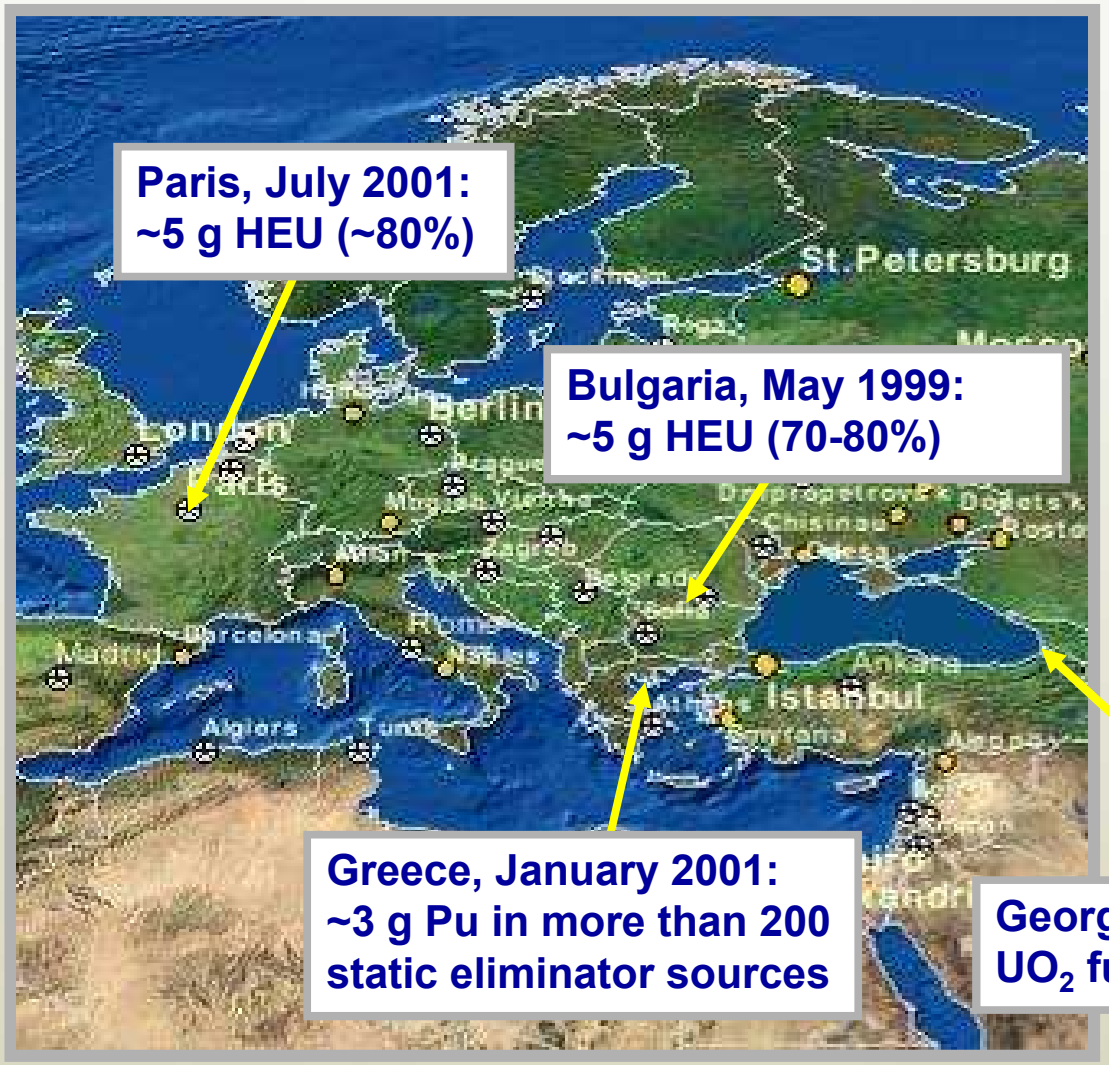
INFCIRC/225

Convention on the Physical Protection of Nuclear Material



INFCIRC/225 Guidance

Coordination, Information Management

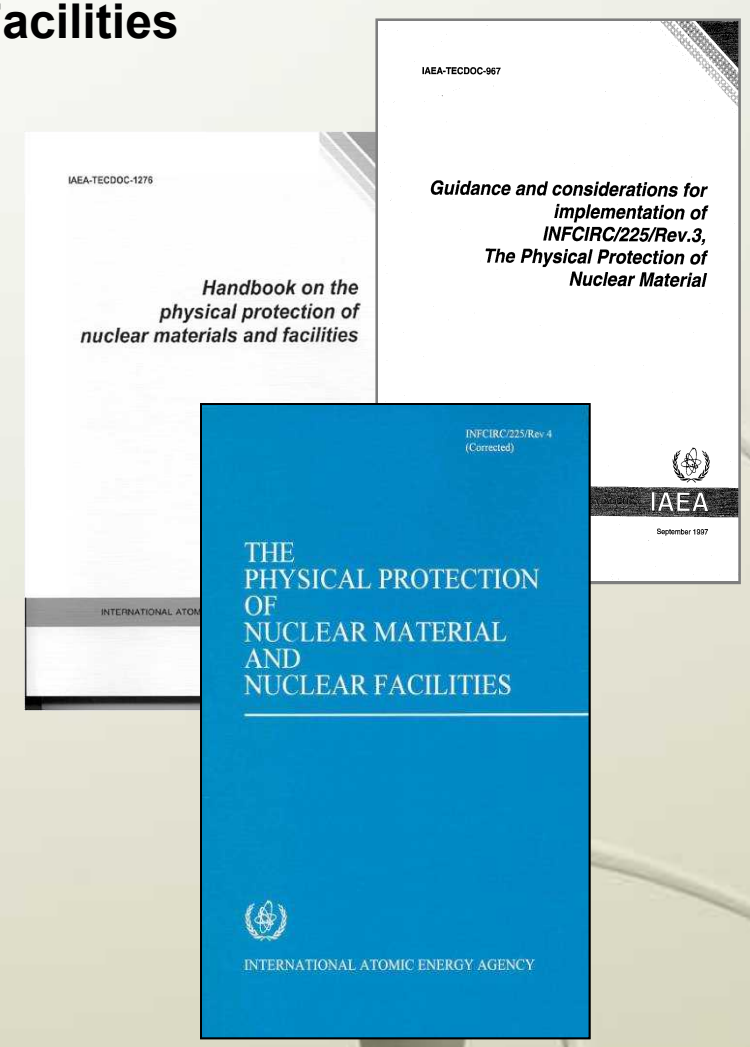


Recent illicit trafficking events

Seized HEU
Czech Republic

Physical Protection Regime:
Nuclear Material and Facilities

- Convention on the Physical Protection of Nuclear Material
- Security Fundamentals
- INFCIRC/225/Rev. 4
- TECDOC 967
- TECDOC 1276: Handbook



Physical Protection Objectives

- Protect against theft
- Protect against sabotage

Fundamental Principles

- A: State responsibility
- B: Responsibilities during transport
- C: Legislative / regulatory framework
- D: Competent authority
- E: Responsibility of license holder
- F: Security culture

Fundamental Principles

- G: Threat
- H: Graded approach
- I: Defense in depth
- J: Quality assurance
- K: Contingency plans
- L: Confidentiality

INFCIRC 225
Provides Recommendations

- Elements of States' system of physical protection
- Categorisation of nuclear material (I,II,III)
- Recommendations for physical protection
- International recognition, but no legal basis
- Legal and regulatory basis in many states

Material Categorization

Defines Level of Protection

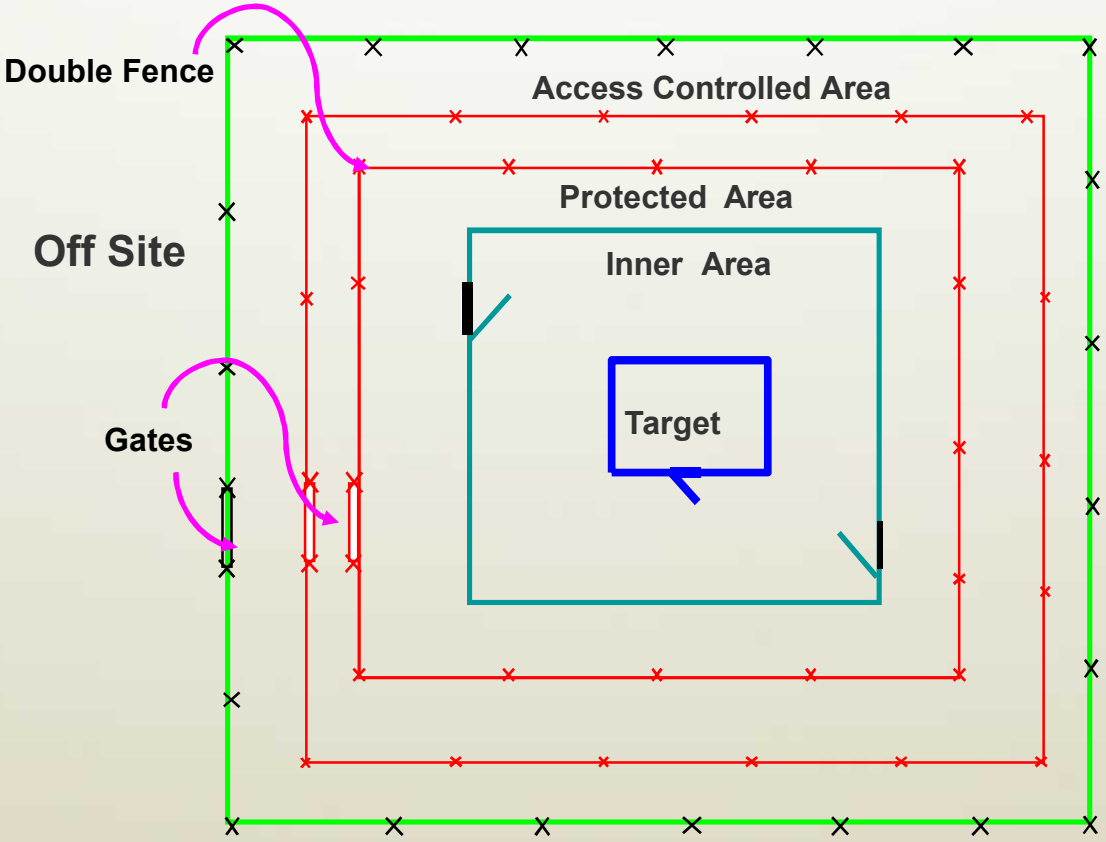
	1 SQ	Category		
		I	II	III
Pu, U^{233}	8 kg	≥2 kg	500 g- 2 kg	15-500 g
HEU ≥20%	25 kg	≥5 kg	1-5 kg	15 g-1 kg
LEU >10% <10%			≥ 10 kg	1-10 kg ≥10 kg
Irradiated fuel			DU, natural, thorium, LEU	

225 Recommendations
No Legal Obligations

- Theft: Material Attractiveness
  - Cat. 1: Use / storage in inner and protection areas
  - Cat. 2: Use / storage in protected area
  - Cat. 3: Use / storage in access controlled area
- Sabotage: Radiological Consequences
  - Primary concern for power reactors
  - Vital areas located within protected areas; determined in cooperation with safety specialists

Implementation Guidance

Contained in TECDOC and Handbook



Hierarchy

Legal Obligation

CPPNM
International transport
Criminal offenses

Security Fundamentals
Objectives, Principles

Recommendation INFCIRC/225

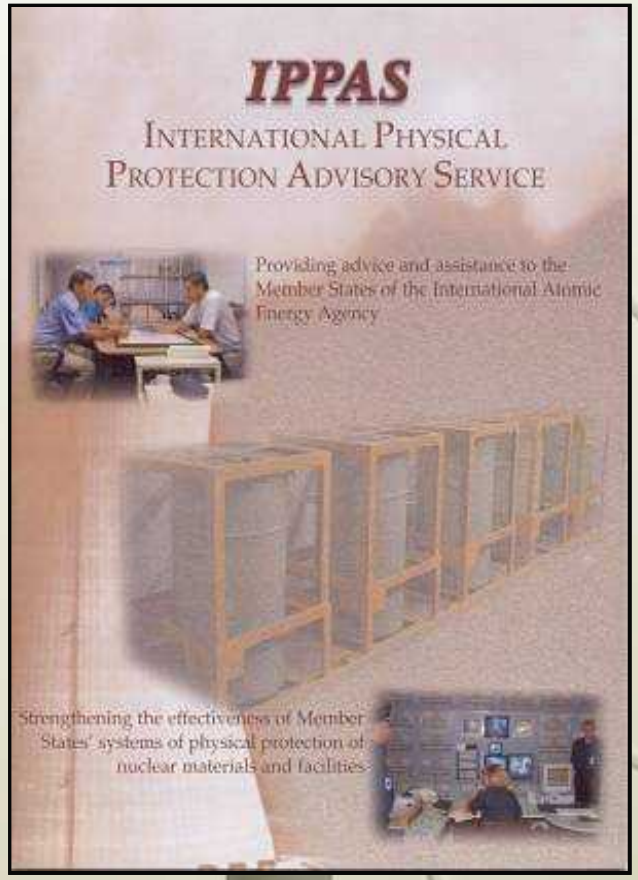
Guidance

TECDOC 967
TECDOC 1276

IPPAS

International Physical Protection Advisory Service

- Improving national programs
- Service organized in 1996
- Fundamental to IAEA program of improving physical protection
- Conducts reviews of national systems of physical protection



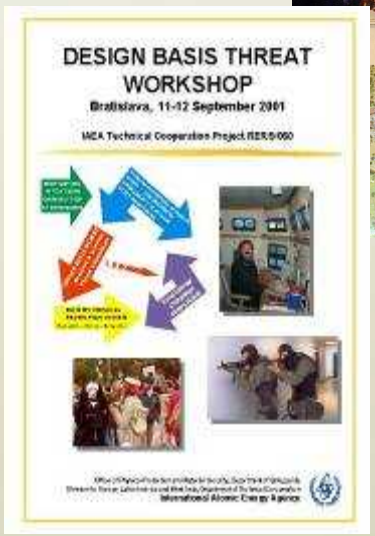
IPPAS Brochure

IPPAS Team Reviews

Physical protection training

Conveying a methodology and a Security Culture

- International courses
- Regional courses, different languages
- Regional events for exchange of information
- National Workshops
  - Design Basis Threat
  - System design
  - Vital area identification

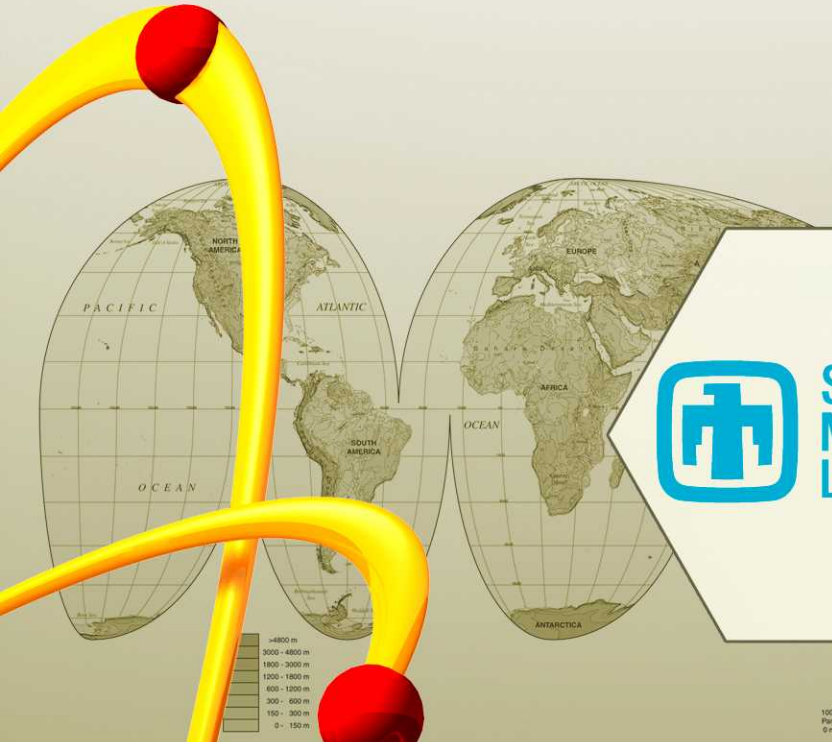


Strengthening Physical Protection

Universal application of effective physical protection

- Promoting and developing standards and recommendations
- Assisting in application of standards and recommendations

1.1 – General Understanding of Threat



Sandia National Laboratories

NNSA
National Nuclear Security Administration

VAEC

What Is a Design Basis Threat?

- **Attributes and characteristics of an Adversary who might attempt theft for malicious uses**

- **Statement in IAEA INFCIRC/225/Rev.4 on the safety and security of Special Nuclear Material (SNM)**
  - "A design basis threat developed from an evaluation by the State of the threat of unauthorized removal of nuclear material and of sabotage of nuclear material and nuclear facilities is an essential element of a State's system of physical protection. The State should continuously review the threat, and evaluate the implications of any changes in that threat for the levels and the methods of physical protection."

Threat Assessment

An analysis that documents the credible motivations, intentions, and capabilities of potential adversaries that could cause undesirable consequences by sabotaging a facility or stealing SNM.

Design Basis Threat Definition

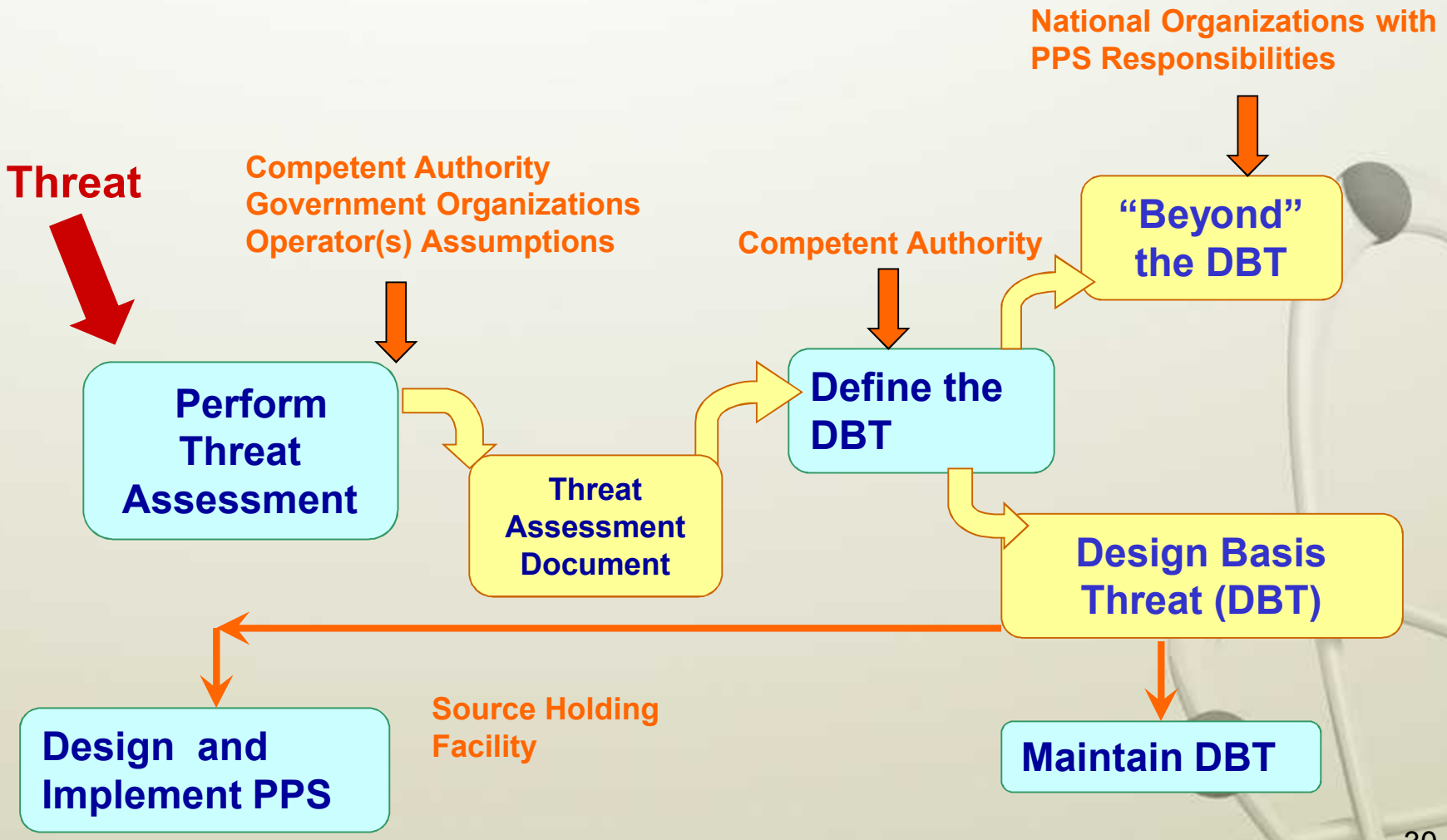
- A process that evaluates many factors from the Threat Assessment Document to develop a Design Basis Threat (DBT)

- Competent Authority is responsible for this process

The Value of a Design Basis Threat (DBT)

- The DBT provides a rational basis for:
  - Making and justifying decisions
    - By the operators
    - By the competent authority
  - The design of a physical protection system (PPS)
    - Ensuring sufficient countermeasures
    - Avoiding unnecessary countermeasures
  - Evaluating the adequacy of a physical protection system

Design Basis Threat (DBT) Life Cycle



Identify Categories of Threats

- External Threat
  - Protestors, Terrorists, Criminals
- Internal Threat
  - An Insider is anyone with authorized, unescorted access who could
    - 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 w/ Insider
  - Support Structure

Identify Sources of Threat-Related Information

- The competent authority needs input from many sources to describe the motivations, intentions, and capabilities of potential adversaries.
  - Reliable Sources, Not Just Hearsay
  - State Intelligence Services may be Best Source
- Other sources of information in threat
  - Ministries of Interior and Foreign Affairs
  - Department of Defense
  - Transportation and Aviation Ministries
  - Customs Agency and Coast Guard
  - State and Local Law Enforcement Agencies
  - Operators

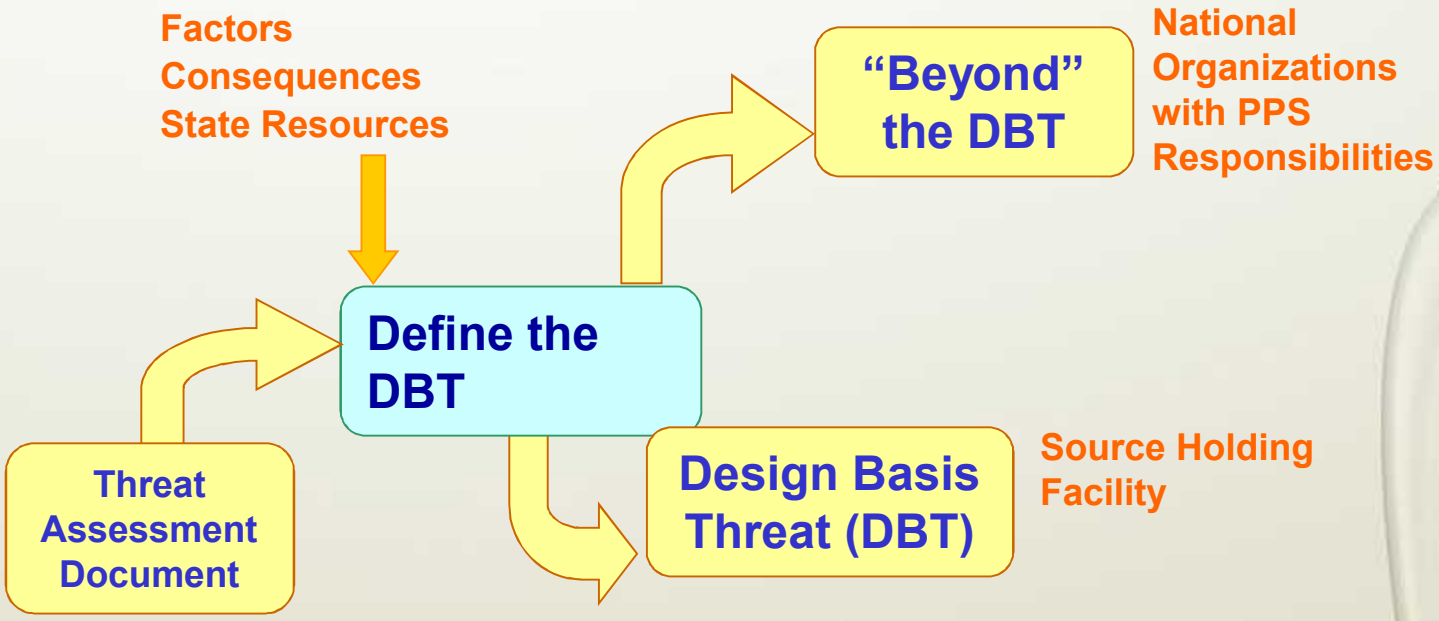
Formalize Threat Assessment Document and Gain Consensus

- Extract a description of motivations, intentions, and capabilities from the organized information
- Conduct a broad peer review
- Develop consensus (vitally important) among organizations

Threat Assessment Matrix

	EXTERNAL THREAT		
	Protestors	Terrorists	Criminals
MOTIVATION			
INTENTIONS Theft or Sabotage			
CAPABILITIES			
NUMBERS			
WEAPONS			
EXPLOSIVES Type & Amount			
TOOLS Power or Hand Tools			
TRANSPORTATION Ground, Air, Water			
TECHNICAL SKILLS			
FUNDING			
INSIDER COLLUSION			
SUPPORT STRUCTURE			
OTHER			

Creating the DBT



Competent authority uses the Threat Assessment as a basis for creating a Design Basis Threat (DBT)

Updating the Threat Assessment Document

- Producing the Threat Assessment Document (TAD) is not an isolated, one-time-only activity.
- The TAD must be maintained.
- Review and revision initiators
  - Period of time
  - Significant event
  - Significant change in domestic or international regulation, policy, or guidance relevant to the TAD

Session 1.1 – Workshop Exercise

	EXTERNAL THREAT		
	Protestors	Terrorists	Criminals
MOTIVATION			
INTENTIONS Theft or Sabotage			
CAPABILITIES			
NUMBERS			
WEAPONS			
EXPLOSIVES Type & Amount			
TOOLS Power or Hand Tools			
TRANSPORTATION Ground, Air, Water			
TECHNICAL SKILLS			
FUNDING			
INSIDER COLLUSION			
SUPPORT STRUCTURE			
OTHER			

Summary
Session 1.1 –Design Basis Threat

- A DBT definition is necessary for design and evaluation of a PPS at a nuclear material holding facility
- Many different agencies are necessary to create a Threat Assessment Document
- The competent authority decides the DBT level which is then sent to the facility
- The DBT must be updated and kept current
- There is value to using a standard format and process for the DBT definition

1.2 – General Understanding of Risk

Sandia National Laboratories

NNSA
National Nuclear Security Administration

VAEC

Risk Definition

- Risk is the likelihood of experiencing a defined set of consequences
- Involves both the likelihood of occurrence of an event and the magnitude of the consequences of the event:

$$R = P * C$$

- If the event of concern is a successful attack on a facility:

$$R = [P_A * P_{S\backslash A}] * C$$

  - P_A = Probability of Adversary Attack
  - $P_{S\backslash A}$ = Probability of adversary success, given the attack occurs
  - C = Consequences of a successful attack

PPS Risk Equation

- If an attack occurs, it either succeeds or fails

$$P_{S\backslash A} = 1 - P_E$$

  - P_E = Probability of effectiveness of the physical protection system

- PPS Risk Equation

$$R = [P_A * (1 - P_E)] * C$$

Conditional Risk

- PPS Risk Equation

$$R = [P_A * (1 - P_E)] * C$$

- Probability of attack is very difficult to estimate
- Usually consider the conditional risk (risk given that the attack occurs)
- Conditional risk equation

$$R_C = [1 - P_E] * C$$

Consequence Factor (C)

- Normalizes consequences of theft of various materials or sabotage
- Established by competent authority
- Range 0 (negligible) to 1.0 (very high)
- Theft Consequence Factors (examples)
  - Weapons (1.0)
  - Plutonium metal (0.8)
  - Low enriched uranium (0.1)
- Sabotage Consequence Factors
  - Based on exposure levels to general public

Probability of Effectiveness (P_E)

- Sometimes called "System Effectiveness"

  $P_E = P_I * P_N$

  - P_I = Probability of Interruption
  - P_N = Probability of Neutralization
- P_I is an estimate of the likelihood that the response force arrives before the adversary completes the attack
- P_N is an estimate of the likelihood that the response force will prevent the adversary from completing the attack once interrupted

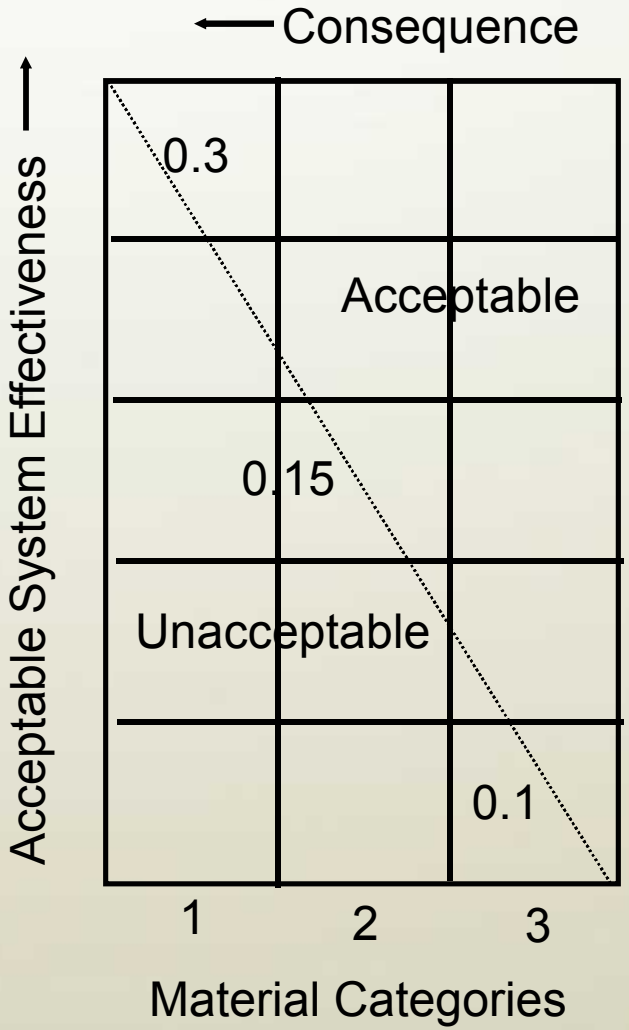
PPS Performance Requirements

$$R_C = [1 - P_E] * C$$

$$R_C = [1 - P_I * P_N] * C$$

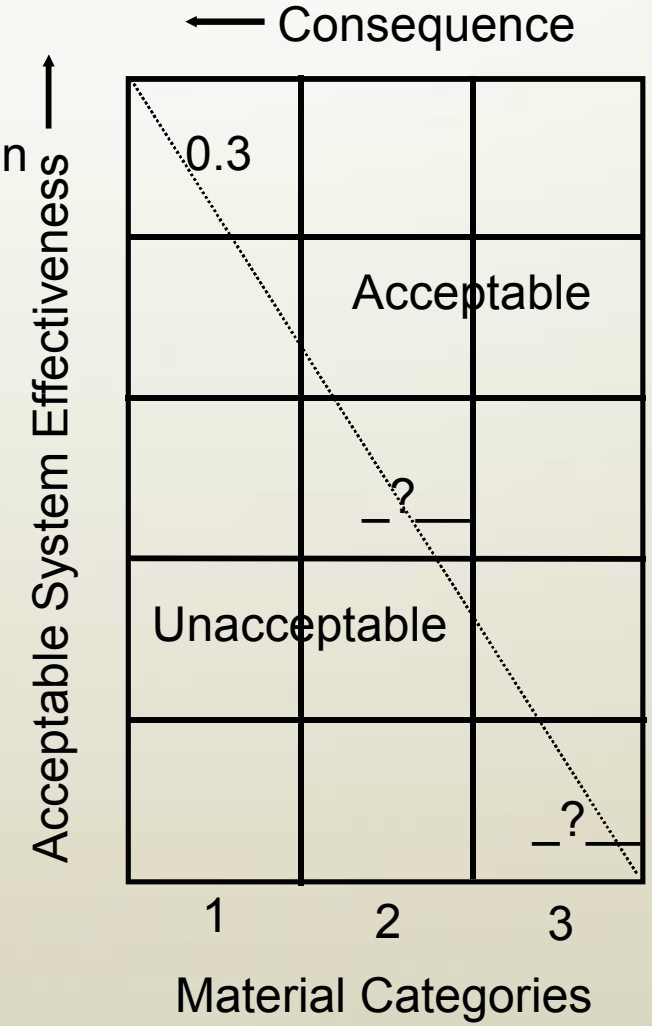
- There is some level of risk that competent authority will accept
- PPS performance requirement (PE) should be related to potential consequences of an attack to maintain risk at an acceptable level
- Competent authority may establish a minimum P_E for different source categories

System Effectiveness Specification (Just a Class Example)



Session 1.2 – Workshop Exercise

Remember:
$P_E = P_I * P_N$
P_N=Neutralization
P_I=Interruption



Session 1.2 – General Understanding of Risk Summary

- Classical Risk Equation is as follows;

$$R = P_A * [1 - (P_I * P_N)] * C$$

- Not knowing P_A leads us to use Conditional Risk

$$R_C = [1 - (P_I * P_N)] * C$$

- Keeping risk relatively constant, the competent authority can specify system effectiveness for each category of sources.

$$P_E = (P_I * P_N)$$

- We then design and test to meet this acceptable level of system effectiveness

1.3 – Physical Protection Principles

Sandia National Laboratories

NNSA
National Nuclear Security Administration

VAEC

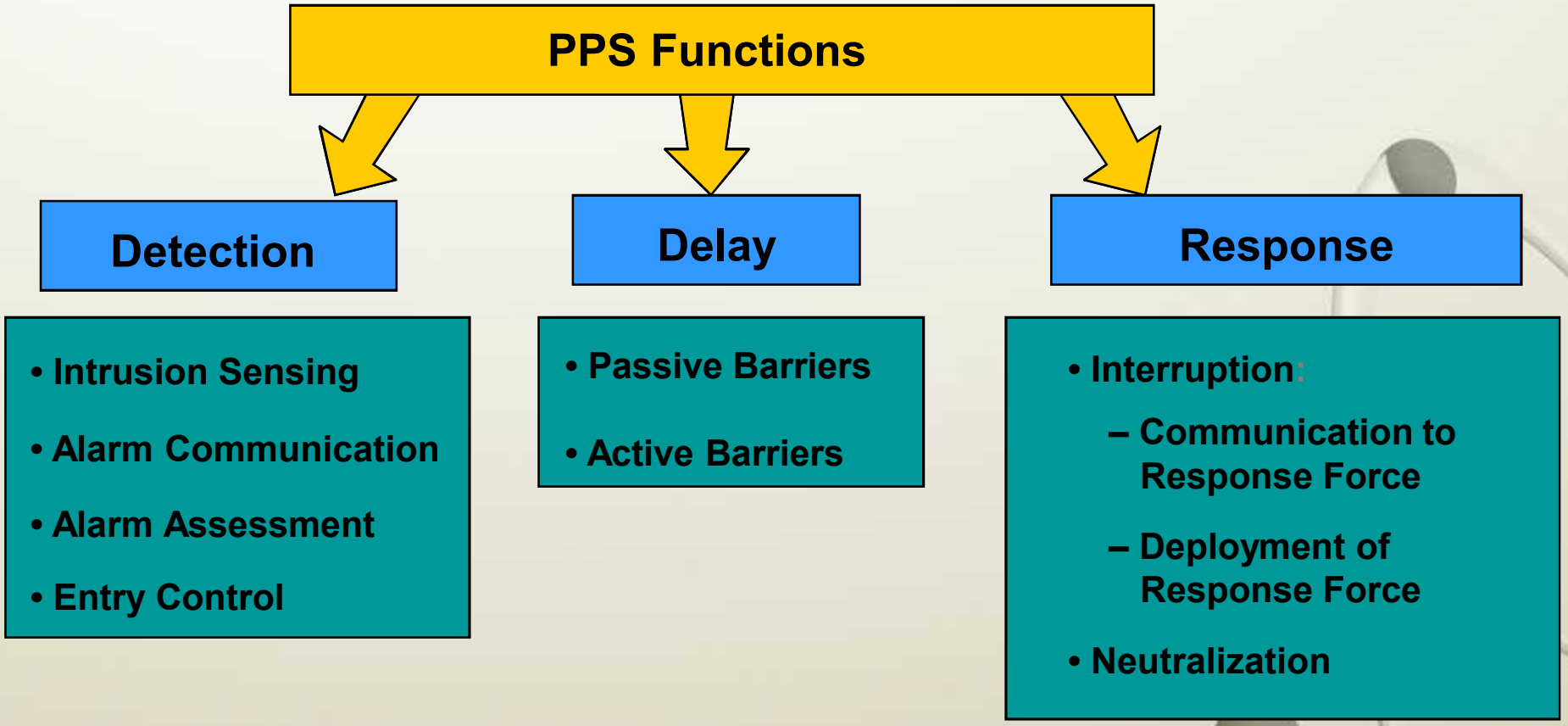
Physical Protection System

A physical protection system is the integration of people, procedures, and equipment for the protection of assets or facilities against theft or sabotage.

Objective: Prevent Theft and Sabotage

- Deter the Adversary
  - Implement a PPS which all adversaries perceive as too difficult to defeat
  - Problem: deterrence is impossible to measure
- Defeat the adversary with PPS
  - PPS functions required: detection, delay, response
  - Actions of response force prevent adversary from accomplishing his goal

PPS Functions

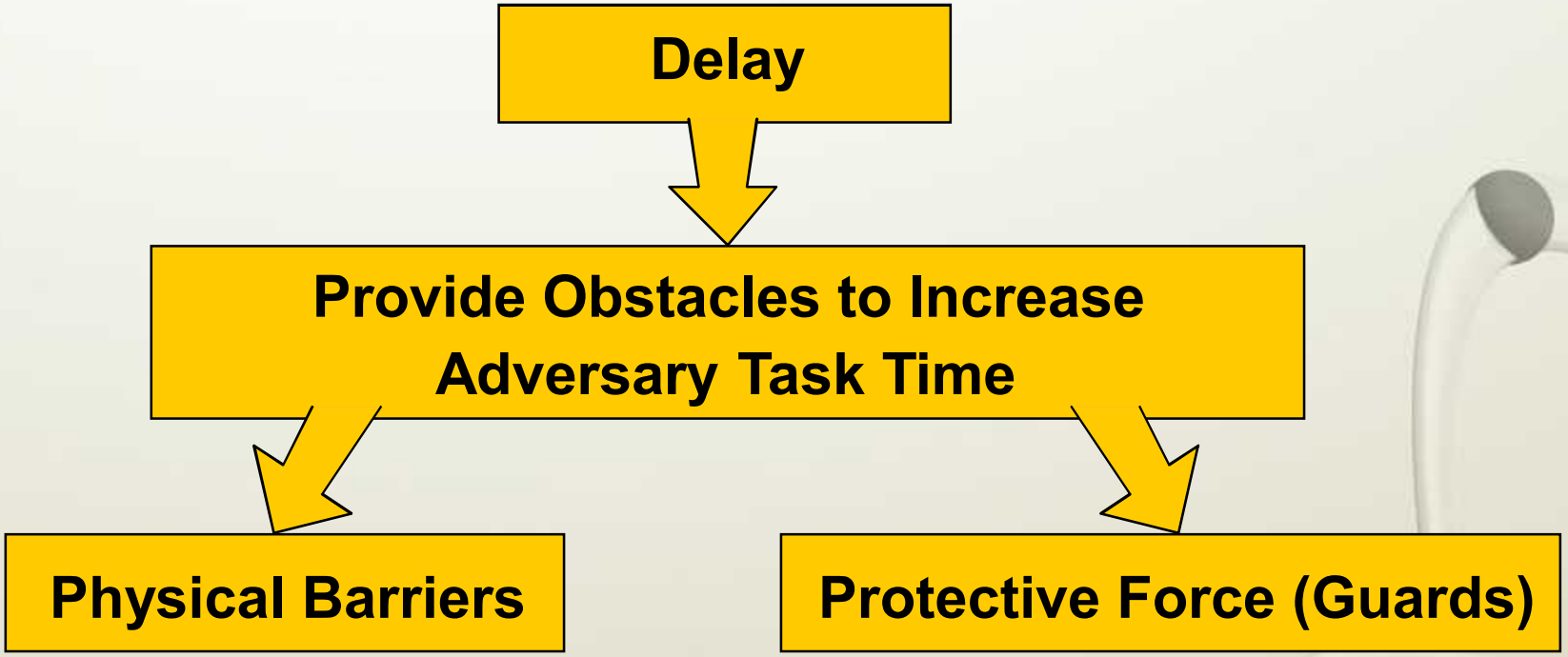


Detection

Performance Measures:

- Probability of Sensor Alarm (P_S)
- Time for Communication and Assessment (T_C)
- Frequency of Nuisance Alarms (NAR)
- Probability of Assessment (P_A)
- $P_D = F(P_S, T_C, NAR, P_A)$

Delay

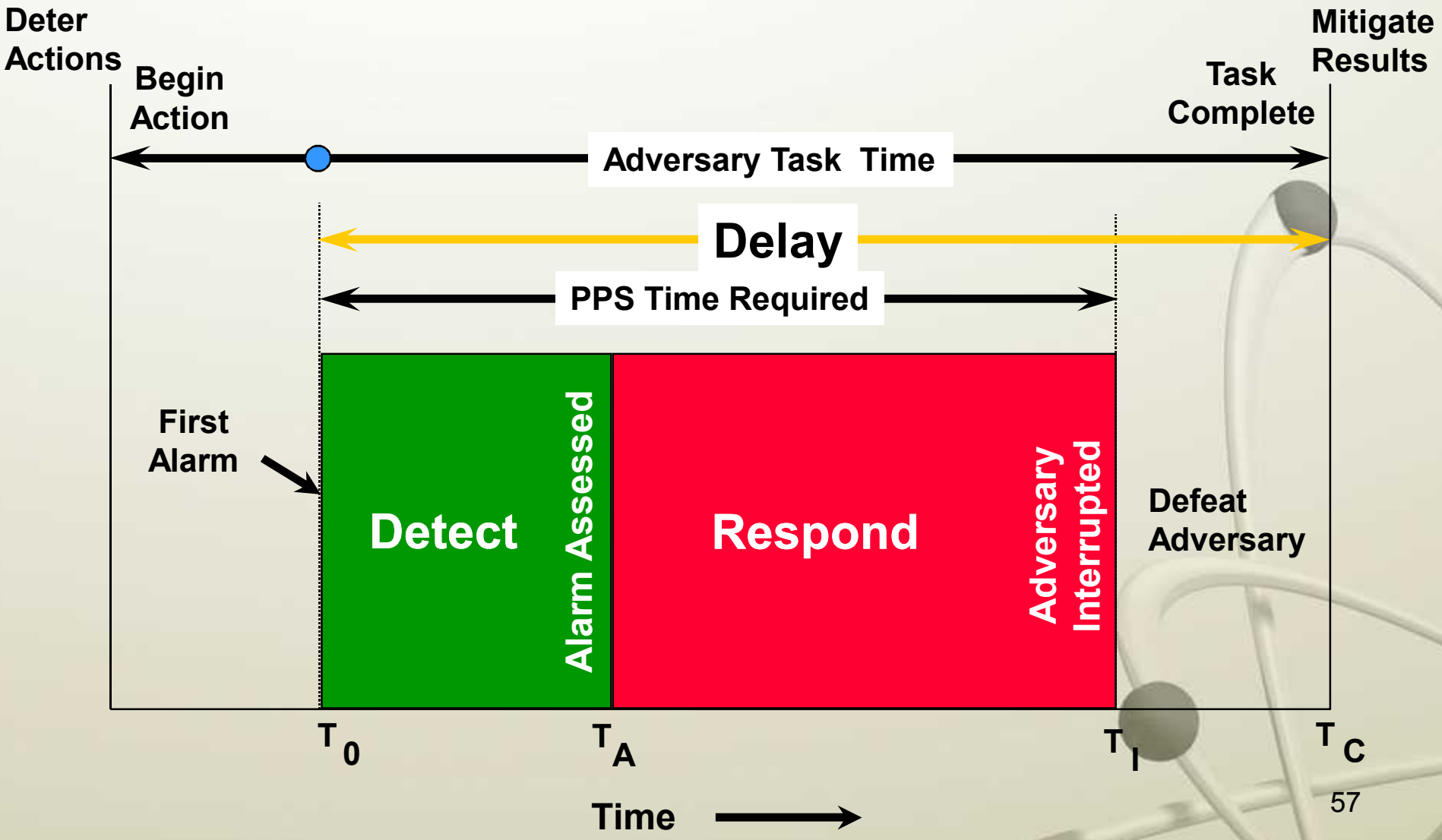


- Performance Measure: Time to Defeat Obstacles

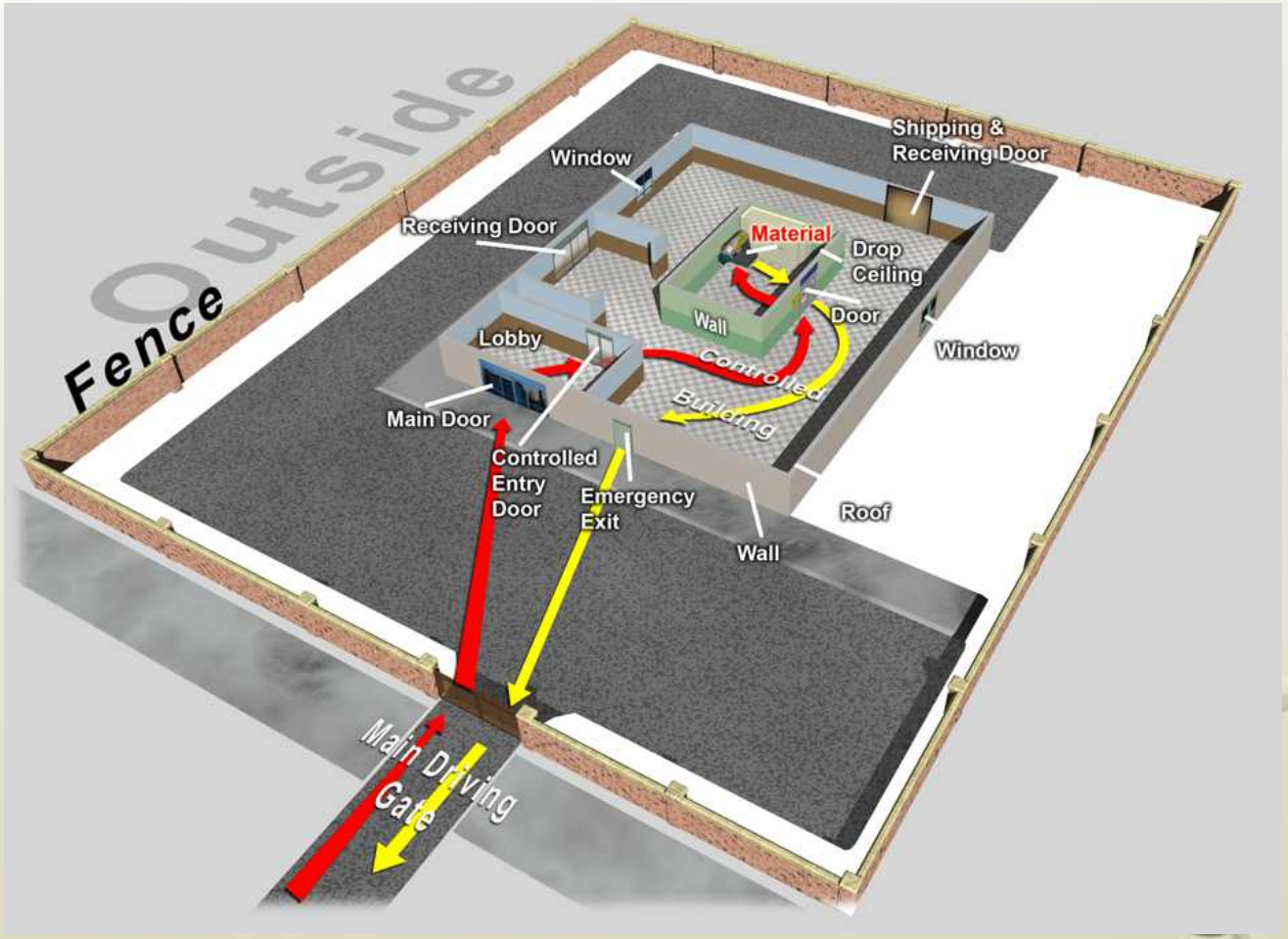
Response

- Performance measures
  - Probability of communication to response force
  - Time to communicate
  - Probability of deployment to adversary location
  - Time to deploy
  - Response force effectiveness

The Principle of Timely Detection



Example Nuclear Facility
SNM Storage Vault



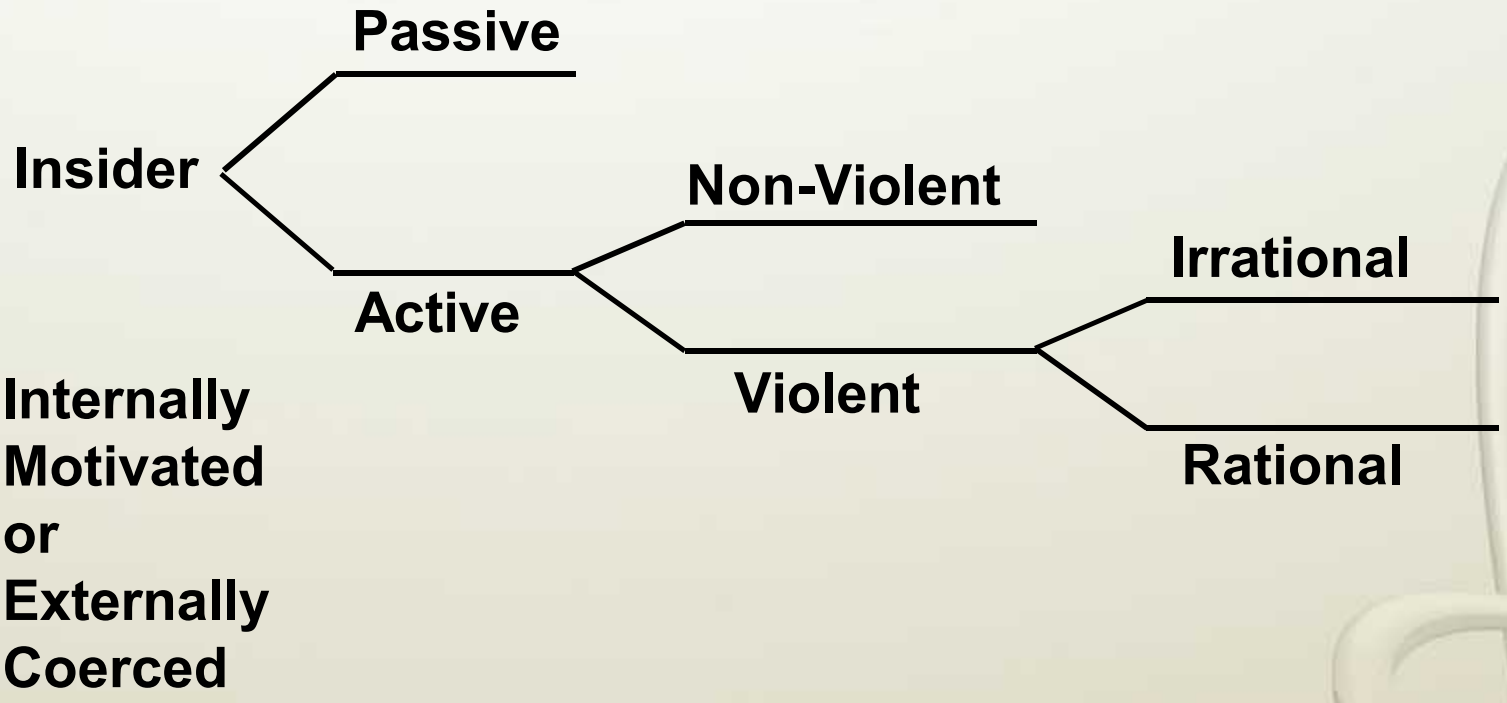
Neutralization

- Very difficult to measure
- Subject matter experts
- Force-on-force exercises
- Computer models
  - ITC model
  - JCATS
- Right people
- Right equipment

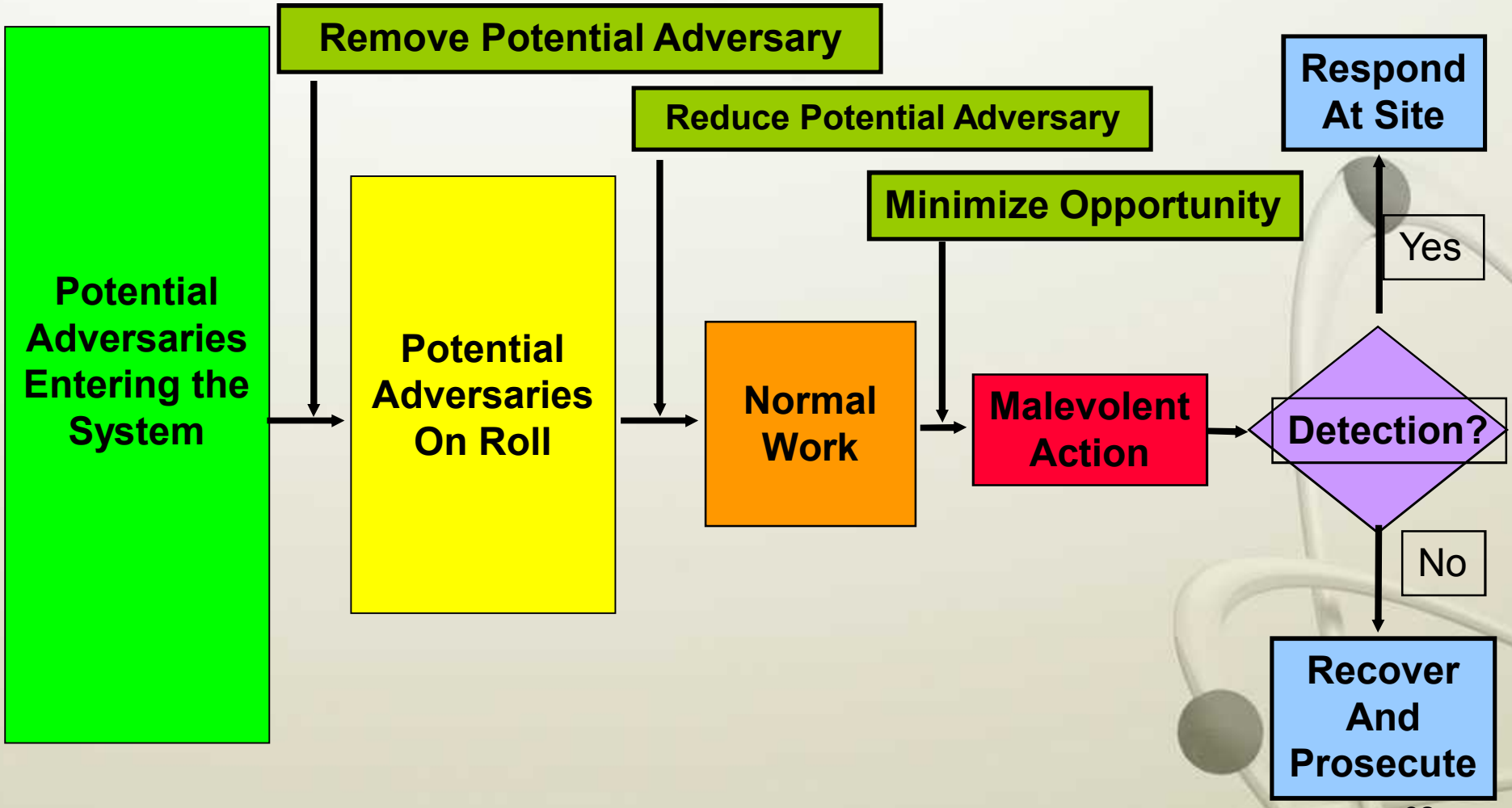
Interaction with Outside Agencies

- Written agreement or understanding
- Key issues for consideration
  - Role of support agencies
  - Communication with support agencies
  - Off-site operations
- Joint training exercises

Insider Characteristics



Insider Protection System Approach



Characteristics of an Effective Physical Protection System

- Protection-in-depth
  - Series of detectors better than a single one
  - Prefer to use complementary sensors that use different principles
- Balanced protection
  - Does not create an easy path for adversary
  - Applies to Detection as well as Delay
- Sufficient protection but not too much
  - Enough Detection, Delay, and Response
  - Meet the “System Effectiveness” criteria
- One feature can compensate for another's weakness

Graded Physical Protection Requirements

- The level of protection required for nuclear material should be commensurate with the attractiveness of the material.
- Graded concept of security measures based on risk.

Session 1.3 – Physical Protection Principles Summary

- While we would like to deter the adversary, we must be prepared to defeat him.
- We use Detection, Delay, and Response working together to interrupt the adversary.
- We use the response force to neutralize the adversary.
- Consider outsider and insider scenarios.
- The level of required protection should be commensurate with the potential consequence.

1.4 – Physical Protection Equipment

Key Physical Protection System Elements

- Access Control
- Contraband Detection
- Intrusion Detection
- Alarm Assessment

Basis of Personnel Entry Control

- Something you know
  - Personal Identification Number (PIN)
  - Password
- Something you have
  - Key
  - Card
- Something you are
  - Biometric Feature (i.e., Fingerprints)

Hand-geometry Biometrics

Combining these factors increase security.

Fingerprint Scanner

Entry and Exit
Access Control Readers

Magnetic swipe or Proximity

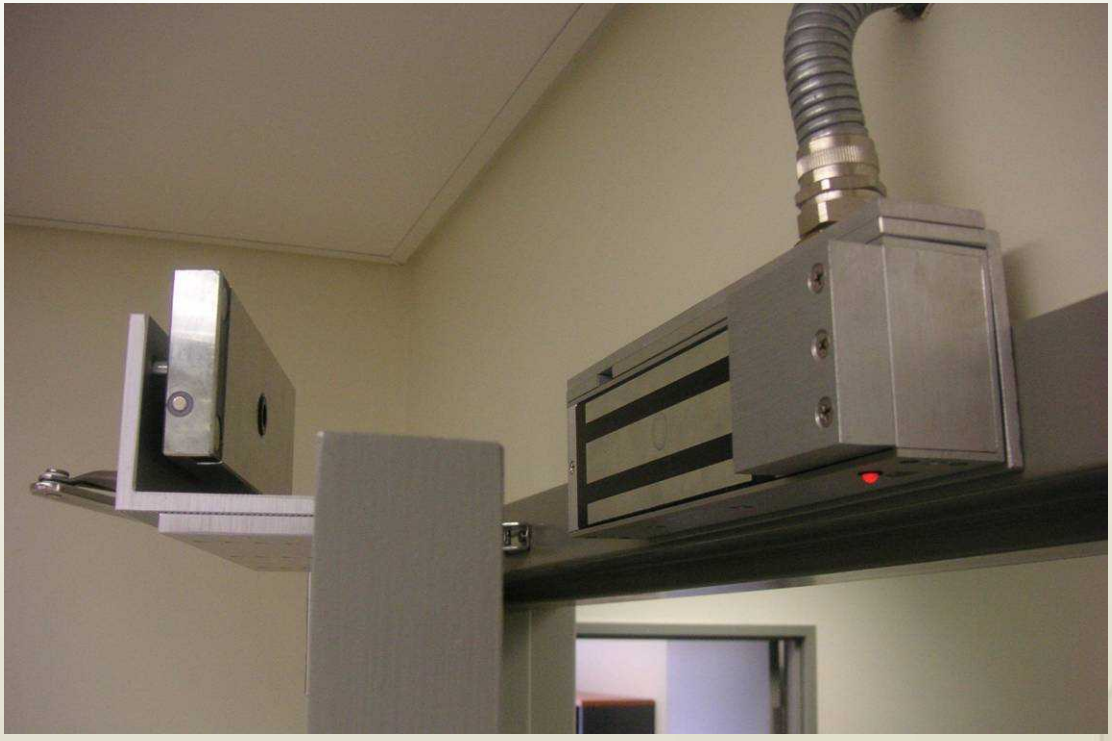
Access Control Entry

Video Intercom

External

Internal

Magnetic Door Lock



CCTV Cameras

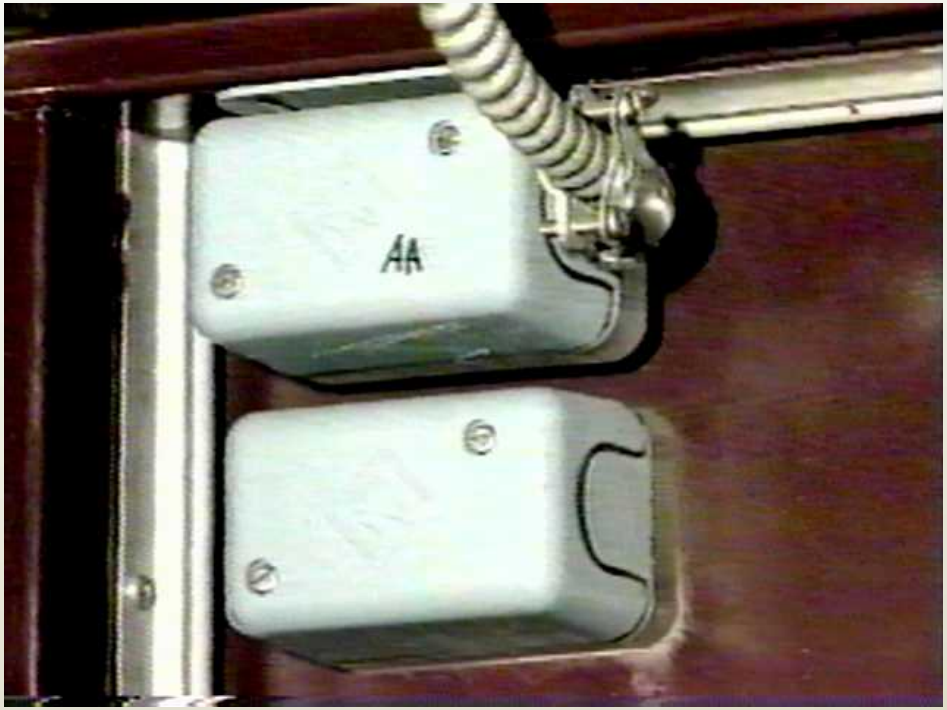
External
Fixed

Internal
Pan/Tilt/Zoom

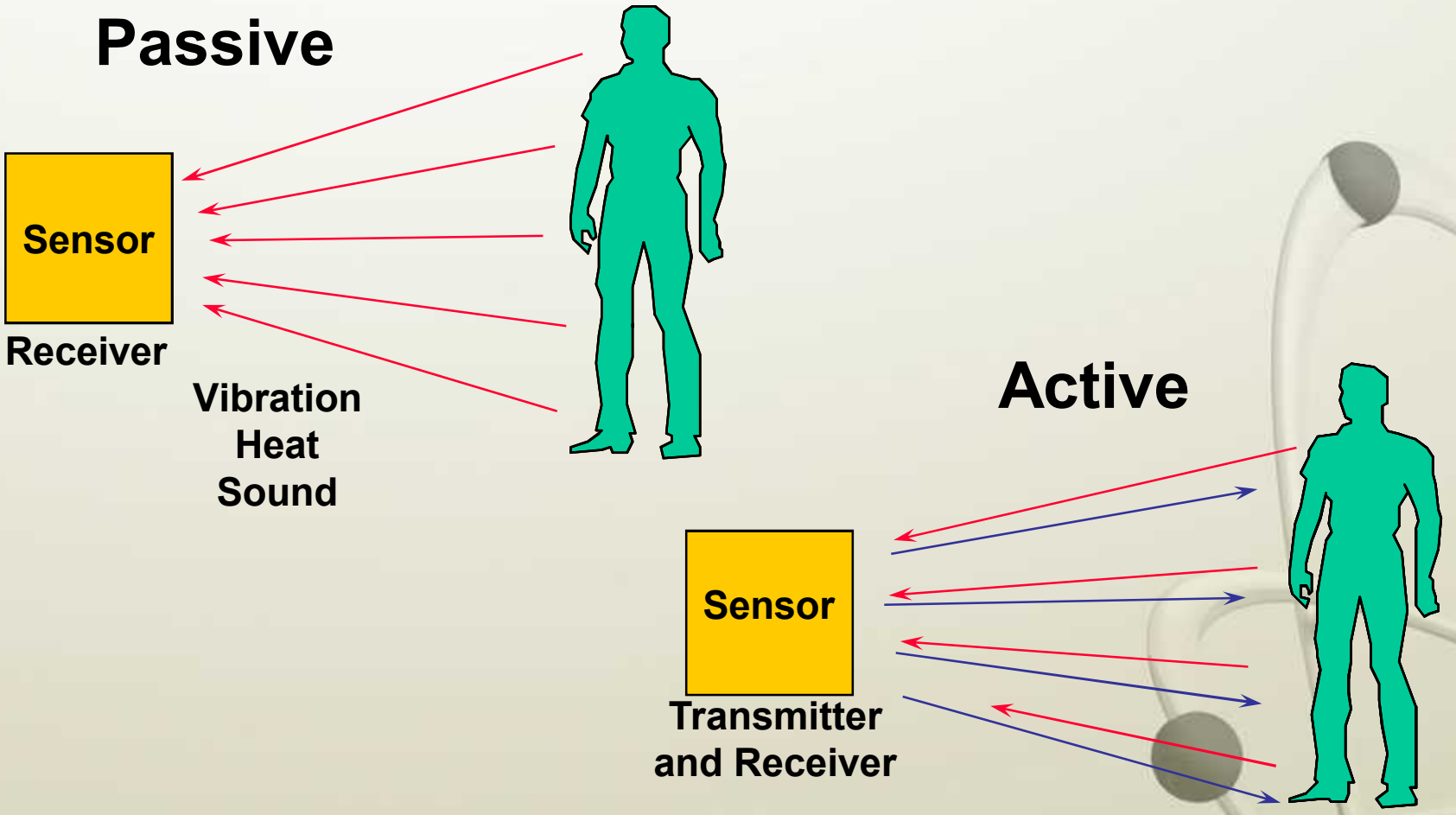
Metal Detection

- Types of detectors
  - Continuous wave
  - Pulsed field
  - Magnetometer
- Factors that affect sensitivity
  - Orientation
  - Ferromagnetic materials
  - Shape
  - Speed
  - Environment
  - Location in Field

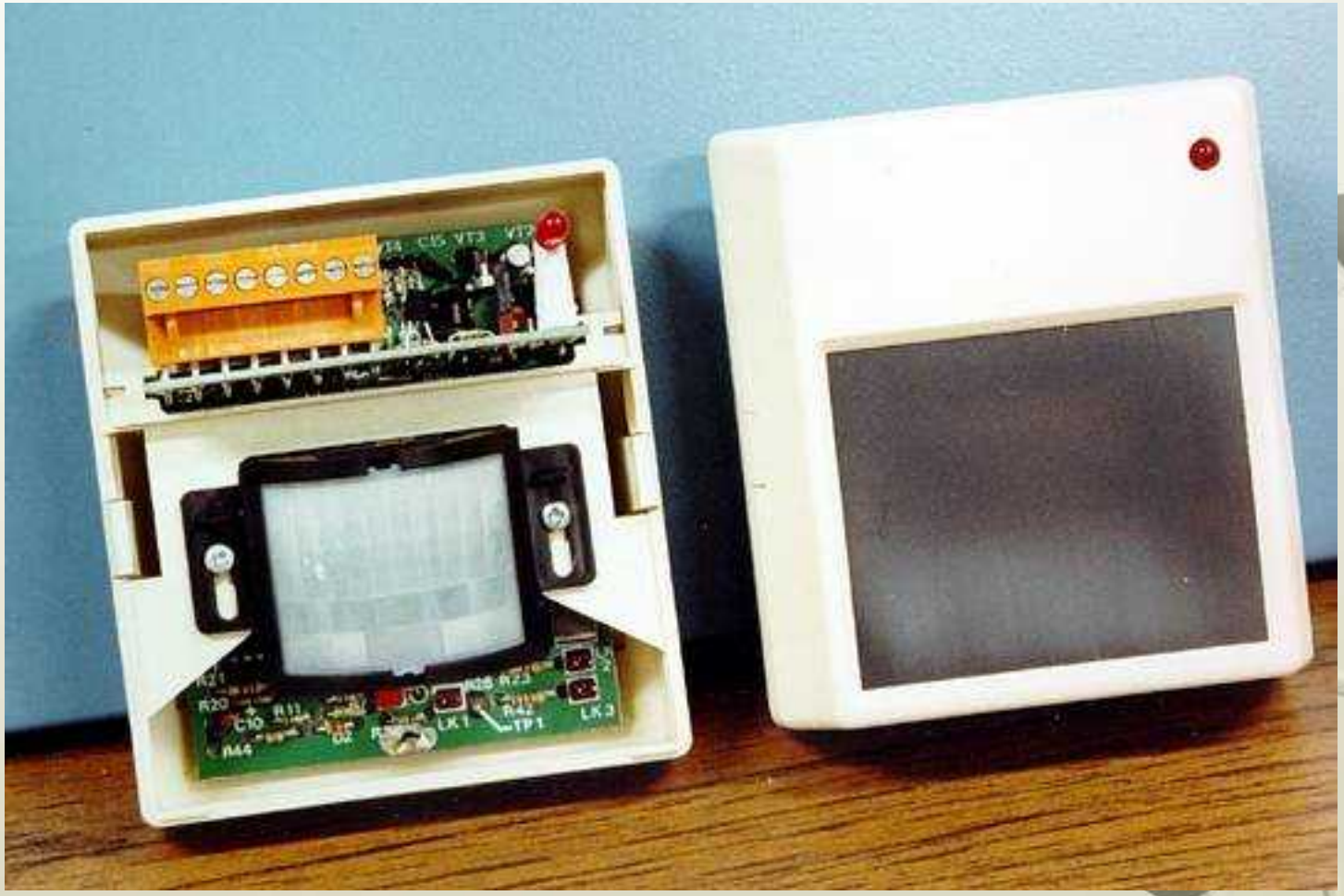
Balanced Magnetic Switch



Passive or Active



Passive Infrared Sensor



360° Dual Technology Detector

Interior Microwave Sensor

Alarm Assessment

- Assessment
  - Use of video to monitor a sensor-specific area when triggered by an alarm
  - Prevents responding to every nuisance alarm
  - Provides information and assessment to aid in the response
- Display of Alarm
  - Must be rapid, clear, and allow for some delay if the operator is not attentive
- Action Texts

Lighting System

- Function
  - Illuminate scene for nighttime operation
- Major types
  - Incandescent
  - Mercury Vapor
  - High Pressure Sodium
  - Low Pressure Sodium
  - Near Infrared

Characteristics of an Effective Physical Protection System

- Protection-in-depth
  - Series of detectors better than a single one
  - Prefer to use complementary sensors that use different principles
- Balanced protection
  - Does not create an easy path for adversary
  - Applies to Detection as well as Delay
- Sufficient protection but not too much
  - Enough Detection, Delay, and Response
  - Meet the “System Effectiveness” criteria
- One feature can compensate for another's weakness

1.5 – Design and Evaluation of Physical Protection: Performance Based Approach

Sandia National Laboratories

National Nuclear Security Administration

VAEC

Performance Method Overview

- Performance based method is used to assess how your Physical Protection System (PPS) performs against the Design Basis Threat Definition (DBT).
- An analysis using the principle of “Timely Detection” determines a numeric value for PPS effectiveness
  - $P_E = P_I * P_N$
  - P_E is the probability that a PPS will Detect and Defeat the DBT along the Worst Path and Worst Scenario (for you)
  - Every other possible path and scenario will produce a higher probability
- Competent authority must establish an acceptable risk for your specific material (or combination of materials)
- If a PPS upgrade is needed, choose the least expensive and least intrusive acceptable solution

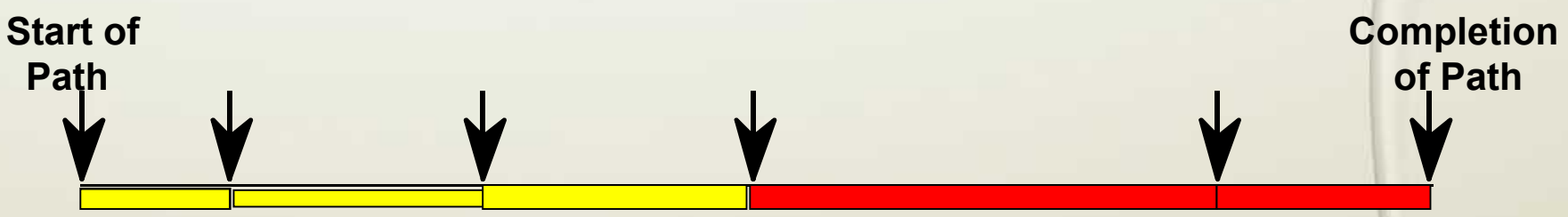
Performance Method Outline
(Common to Prescriptive Method as Well)

- **Understand your facility**
  - Physical conditions (maps, pictures, charts, walk-downs)
  - Facility operations (hours, employees, numbers)
  - Facility policies and procedures (PPS procedures)
  - Regulatory requirements (enforced conditions)
  - Safety considerations (requirements for safety)
- **Categorize your Special Nuclear Material**
  - Categorize material according to INFCIRC/225/Rev.4, Section 5.0
  - Determine Security Upgrade Requirements from INFCIRC/225/Rev.4, Section 6.0
- **Develop your Design Basis Threat (DBT) Definition**
  - Written description of the threat to your facility
  - Usually prepared by competent authority
  - Does not include some features of the Threat Assessment that are “Beyond the DBT”

Performance Method Outline
(Continued and Unique to Performance)

- An analysis using the principle of "Timely Detection" produces system effectiveness
  - Select the worst (for you) path and scenario
  - Draw a time line using fastest times for DBT to accomplish attack tasks
    - Ignore any detection-avoiding techniques
    - Use consistent units of seconds or minutes
  - Place detection points and the Probability of Detection (P_D) on the time line
    - Values for DBT using detection-avoiding techniques

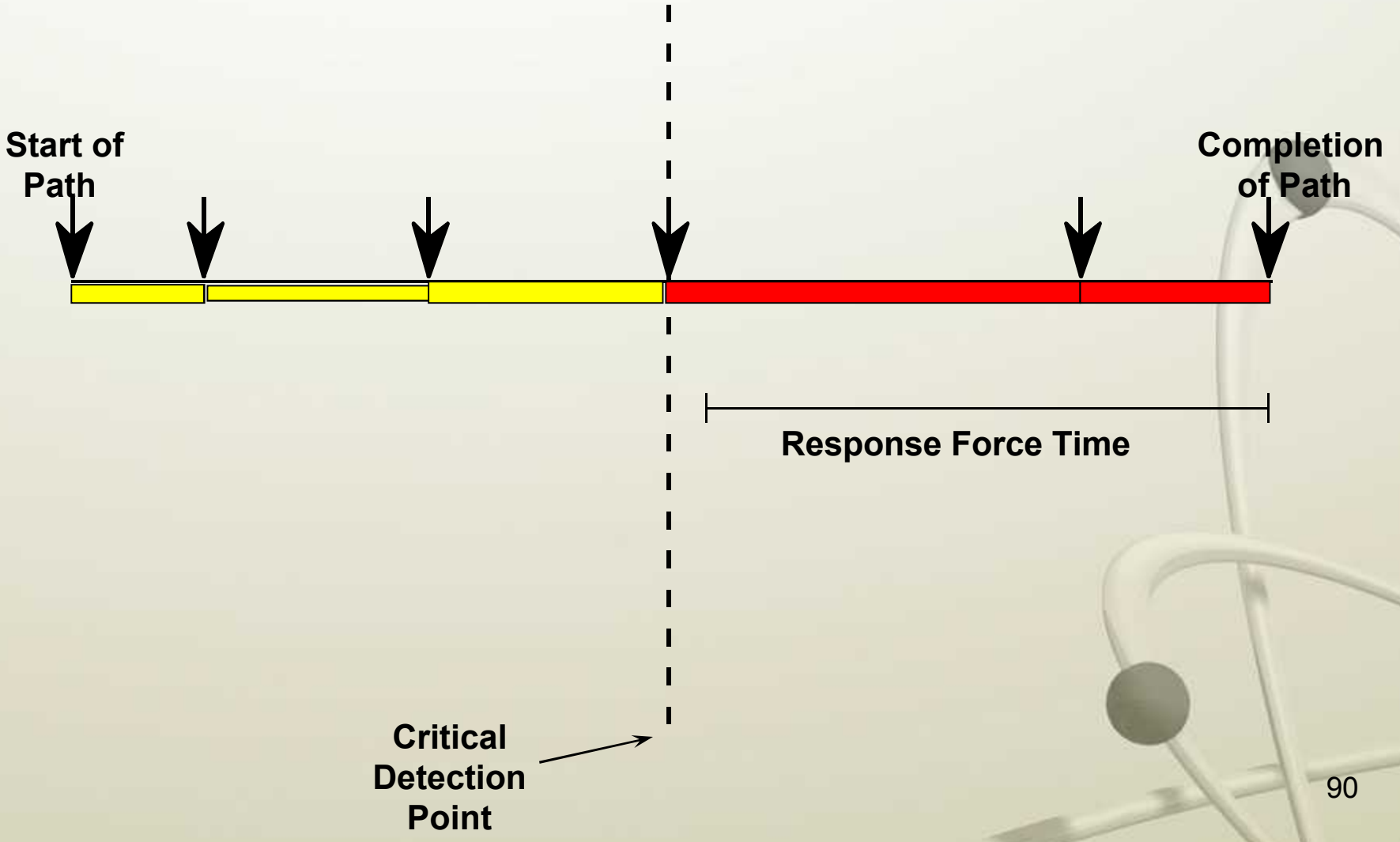
Attack Time Line



Performance Method Outline
(Continued)

- Determine response force time
  - Time from getting an alarm to having the response force in a position to interrupt adversary
  - Includes assessment, communication, travel, and muster times
  - Response force objective - interrupt adversary before he gets off site with SNM
  - Note this has nothing to do with defeating adversary
- Determine the Critical Detection Point (CDP) on the time line
  - Mark off the response force time from the end of the time line
  - CDP is the last detection point where detection can occur and the response force can arrive in time to interrupt the adversary

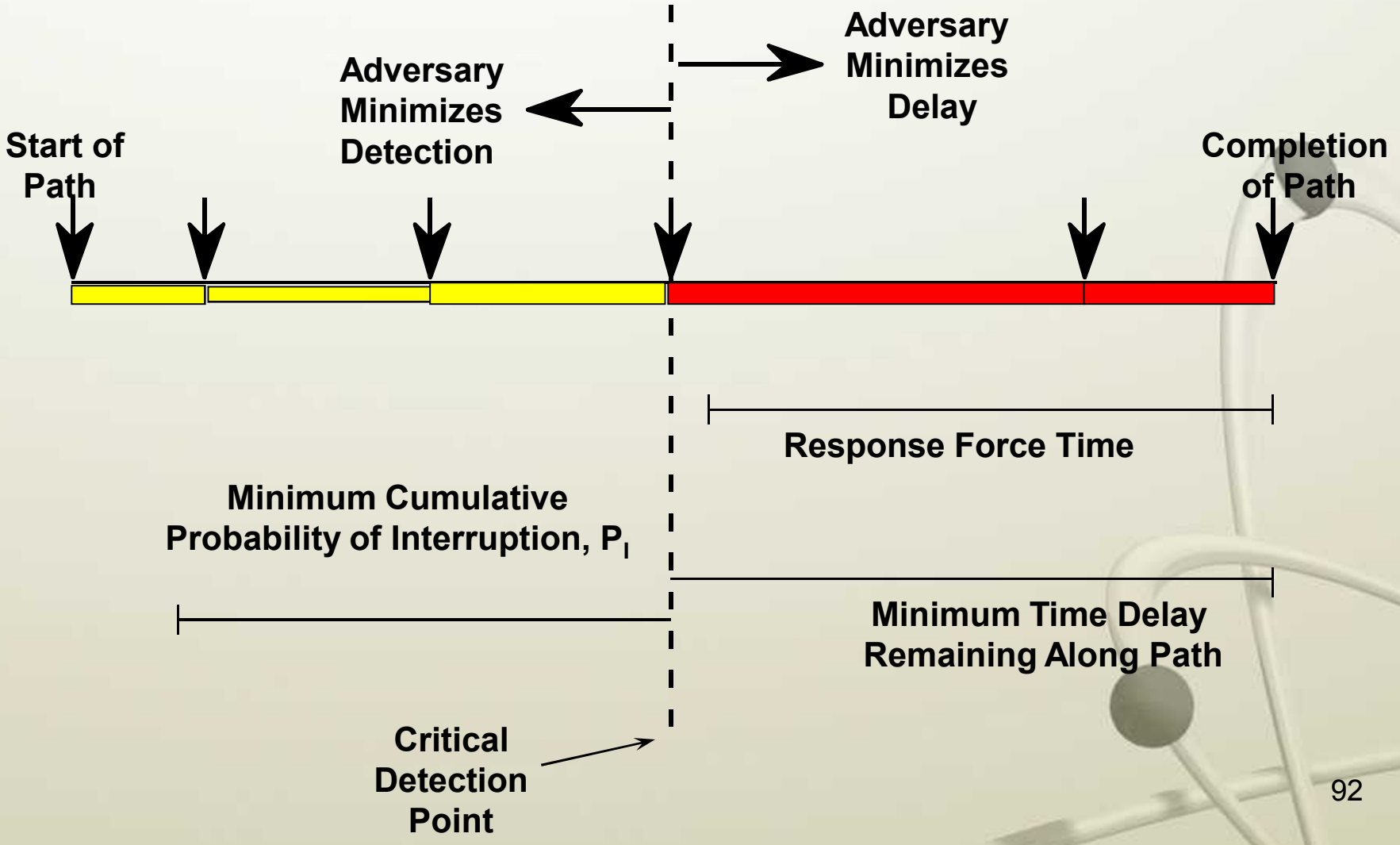
Graphical Representation of Principle of Timely Detection



Performance Method Outline
(Continued)

- Combine all probabilities of Detection P_D up to and including the CDP
  - Combine by multiplying probabilities of non-detection and then subtract the product from 1
  - $P_I=1-[(1-P_{D1})*(1-P_{D2})*\ldots(1-P_{Dcdp})]$
  - Resulting value of Probability of Interruption (P_I) is;
    - Probability that your system will detect and respond to the DBT along the worst path and worst scenario (for you)
    - Every other possible path and scenario will produce a higher P_I

Graphical Representation of Principle of Timely Detection



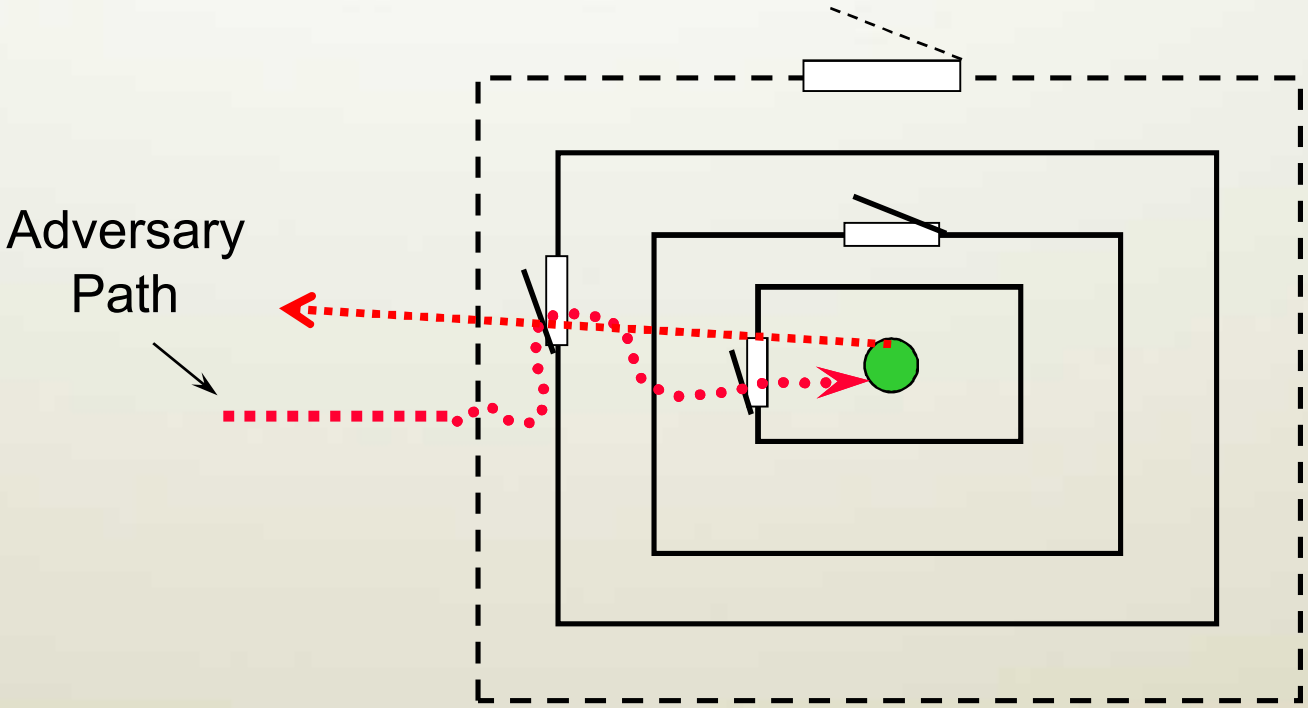
Performance Method Outline
(Continued)

- Determine your response force effectiveness
  - Compare the training, equipment, motivation of response force to the DBT
  - Compare the number of response personnel to the DBT number
  - Make a judgment on the Probability of Neutralization, P_N
- Compute system effectiveness by multiplying $P_I * P_N$
  - Resulting is a percentage probability of detecting and actually defeating the adversary (DBT)
  - Remember this is the worst case for You.

Performance Method Outline
(Continued)

- Determine the system effectiveness requirements
  - Provided by the competent authority
  - Based on risk to society of your particular material or combination of materials
- Determine if your computed system effectiveness meets the requirements
- If an upgrade is needed, choose the least expensive and least intrusive acceptable solution
  - Usually by placing delay upgrades near the material and detection further out from the material
  - Analytically test out a number of solutions

Session 1.5 - Workshop Exercise
Example Facility



Session 1.5 – Workshop Exercise
Timely Detection Example

Action	Minimum Time	Minimum Detection Probability	Maximum Non-detection Probability
Penetrate Fence	6 sec	0.1	0.9
Penetrate Outer Door	84 sec	0.6	0.4
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Acquire Material/Exit	90 sec	1.0	0.0

Response Force Time = 240 sec

What is P_I of this example? _____

If P_N is 0.5, what does that mean? _____

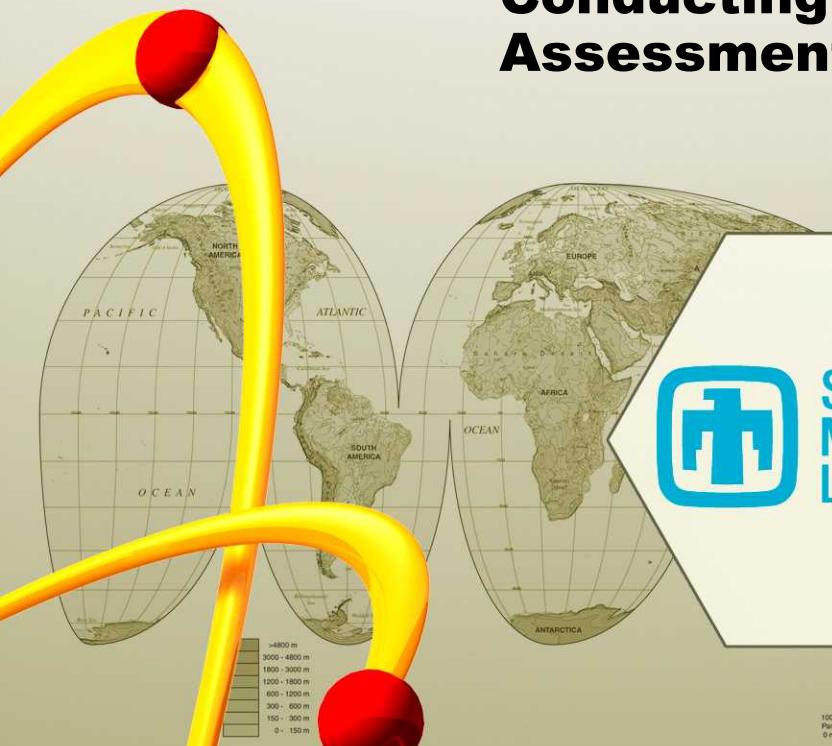
If the competent authority requires system effectiveness of 0.30, would you meet the criteria? _____

Session 1.5 – Performance Based Approach to Assessment and Upgrade Summary

- Performance based approach estimates how your PPS performs against the DBT
- Analysis uses the principle of “Timely Detection” to determine a numeric value for PPS effectiveness
- Competent authority must establish an acceptable PPS effectiveness for your specific material (or combination of materials-roll-up)
- If an upgrade is needed, choose the least expensive and least intrusive acceptable solution

1.6 - Application of INFCIRC/225/Rev.4: The PP of NM and Nuclear Facilities

Section: Conducting Security Assessments Overview



National Nuclear Security Administration

Sandia National Laboratories

VAEC

Security Assessments

- Guidance Document
  - IAEA-INFCIRC/225/Rev.4 *Physical Protection of Nuclear Material and Nuclear Facilities*
- Assessments are a methodology for identifying security risks and developing solutions
- Assessments can be by a regulatory body or self-assessment by facility personnel
- Assessments should be a continuous process
  - Site situations change
    - New missions
    - Changes in material inventories
    - Construction
    - New threats

Material Storage Security Assessments

- Radioactive waste storage facilities
- Research institutes where material is in use
- Security of Material
  - In Use
  - In Storage
  - In Transport

Understand Facility Mission and the Uses of Special Nuclear Material

- Review facility's activities and its effect on physical protection operations
- Ensures the integration of the physical protection program into facility operations
- Impact on facility missions and operations
- Highest level of risk reduction

Facility Activities can include:

- Access Control
- Production
- Maintenance
- Training Program
- Transportation
- Emergency Operations
  - Evacuations
- Compensatory Measures

Types of Special Nuclear Material

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	Unirradiated[b] -uranium enriched to 20% ^{235}U or more -uranium enriched to 10% ^{235}U but less than 20% ^{235}U - uranium enriched above natural, but less than 10% ^{235}U	5 kg or more	Less than 5 kg but more than 1 kg 10 kg or more	1 kg or less but more than 15 g Less than 10 kg but more than 1kg 10 kg or more
3. Uranium-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel (The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage, and transport taking all relevant factors into account.)			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[d/e]	

Types of Special Nuclear Material (Continued)

[a] All plutonium except that with isotopic concentration exceeding 80 % in plutonium-238.

[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr (100 rad/hr) at one meter unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[e] Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100 rad/hr) at one meter unshielded.

Elements of an Assessment

- Planning
  - Identification of material
  - Scope of assessment
  - Coordination with facilities
  - Evaluation criteria
- Conduct
  - Inbriefing
  - Assessment
  - Outbriefing
- Post Assessment Activities
  - Validation of findings
  - Corrective actions
  - Follow-up

INFCIRC/225/Rev.4

- Assign material to Categories based on material or national threats and vulnerability assessments

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15g
2. Uranium-235	Unirradiated[b] - uranium enriched to 20% ^{235}U or more - uranium enriched to 10% ^{235}U but less than 20% ^{235}U - uranium enriched above natural, but less than 10% ^{235}U	5 kg or more	Less than 5 kg but more than 1 kg 10 kg or more	1 kg or less but more than 15 g Less than 10 kg but more than 1kg 10 kg or more
3. Uranium-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15g
4. Irradiated Fuel (The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage, and transport taking all relevant factors into account.)			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[d/e]	

Specific Assessment Areas

- Material
- Security Group for Material
- Administrative Controls
- Inventories and Records
- Access Control Measures
- Technical Security Measures
- Response Capabilities
- Ideas for Improvement

Additional Areas for Consideration

- Management Organization
- Human Resource Analysis
- Training
- Configuration Management
- Performance Testing
- Budget Analyses
- Maintenance
- Plans and Procedures

Exercise Assessment Sheet

Exercise Assessment Sheet

Participant Name:

Facility Name:

Material Present:

Material in Use, Storage, or Transport:

Security Group for each Material:

Administrative Controls:

- Access Control Procedures
- Alarmed Access Points
- Key Control Procedures
- Records
- Inventories
- Regulations and Guidance
- Personnel Reliability
- Information Security

1

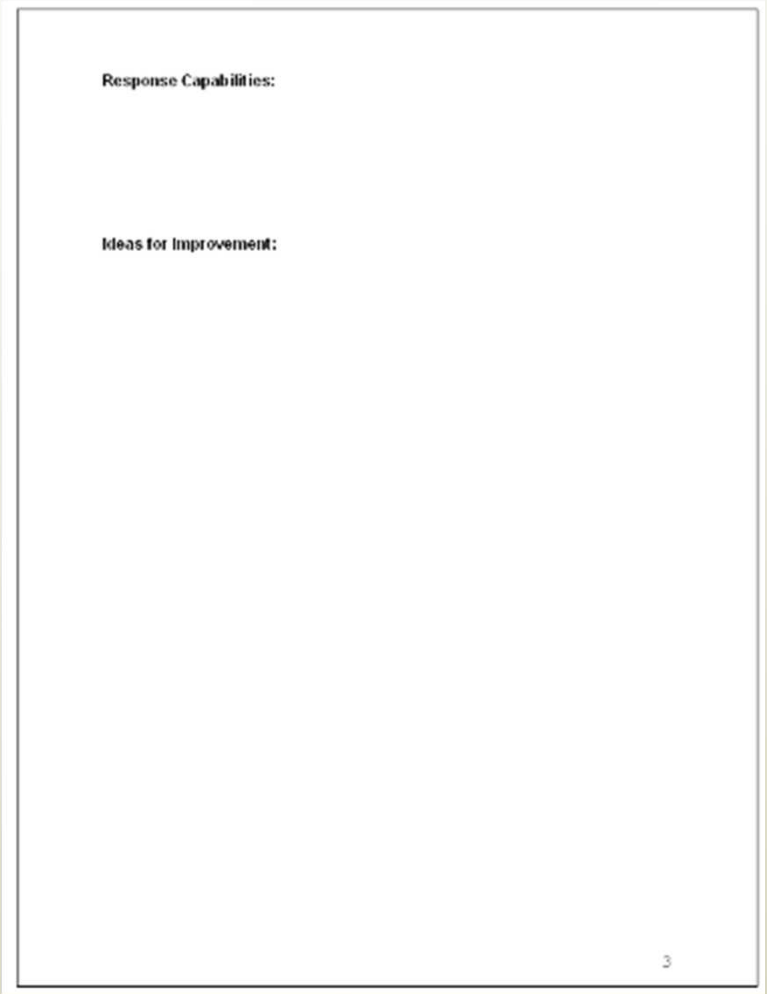
- Quality Assurance
- Safety and Security Culture
- Security Plans
- Emergency Response Plans
- Responses to Increased Threats

Technical Security Measures:

- Fences
- Walls
- Cages
- Transport Packaging
- Locks
- Containers
- Intrusion resistant source holding devices
- Intrusion Detection Systems
- CCTV
- Communications

2

Exercise Assessment Sheet



Response Capabilities:

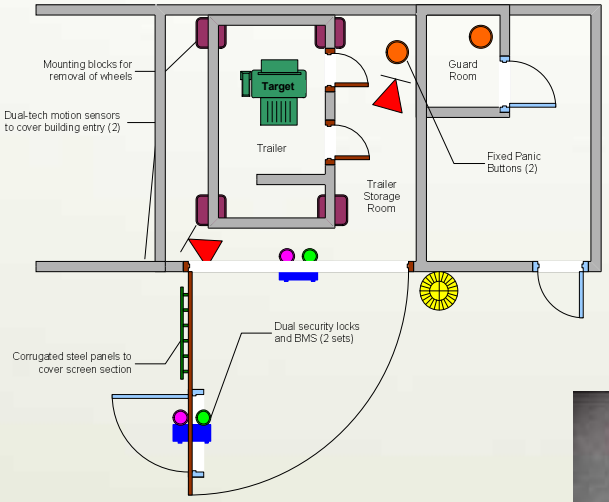
Ideas for Improvement:

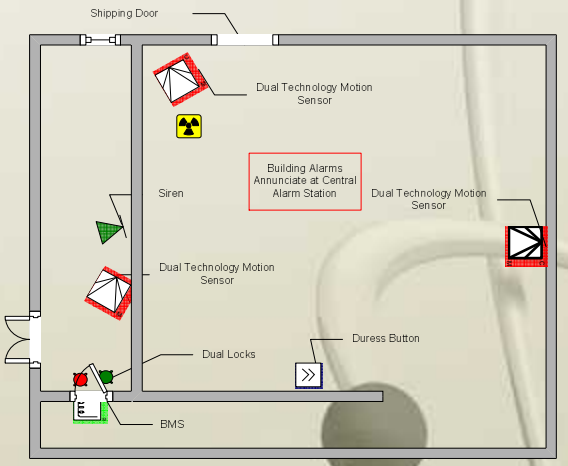
3

Post Assessment Activities

- Validation of Findings
- Corrective Actions
- Follow-up Actions

Physical Protection Upgrades Examples

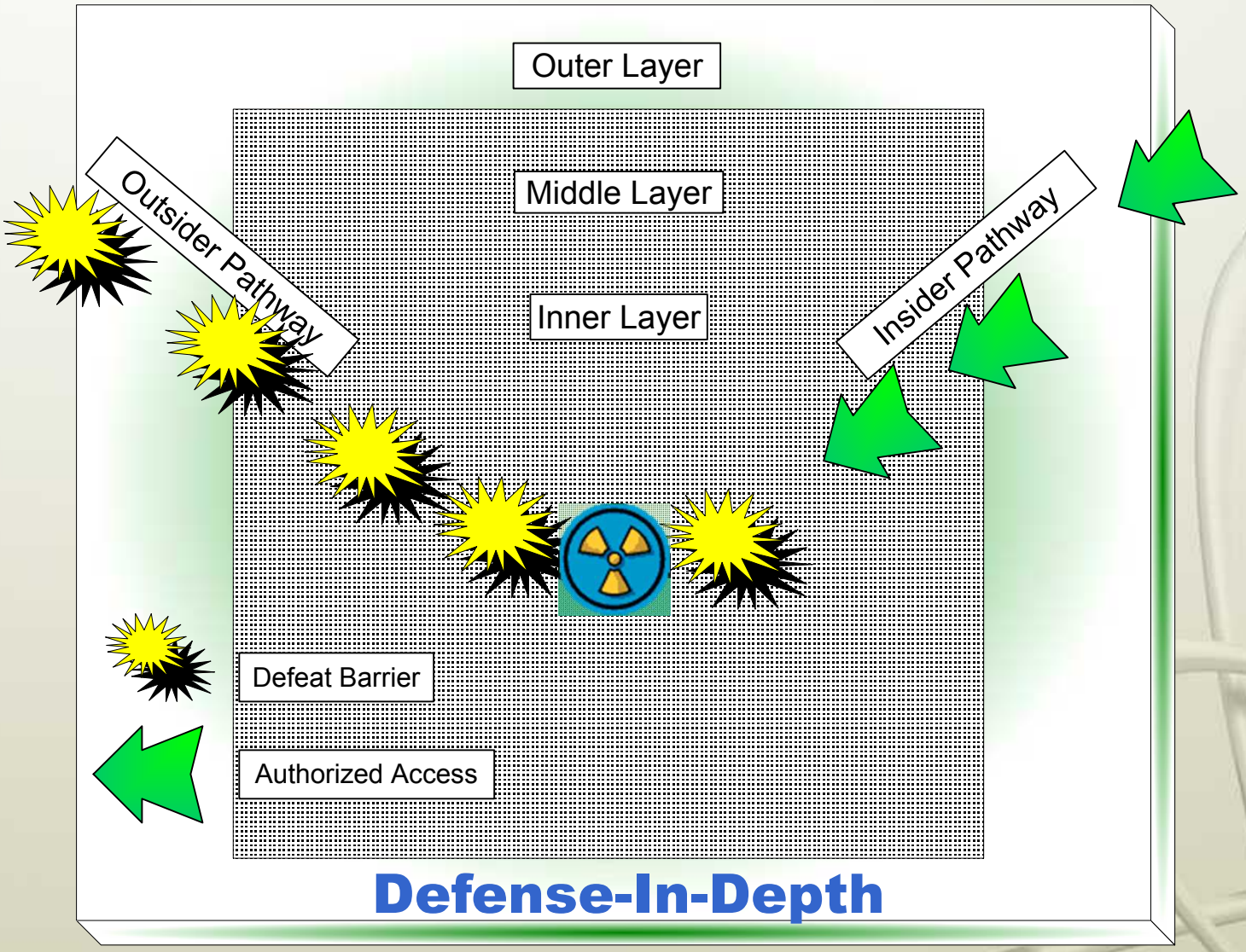




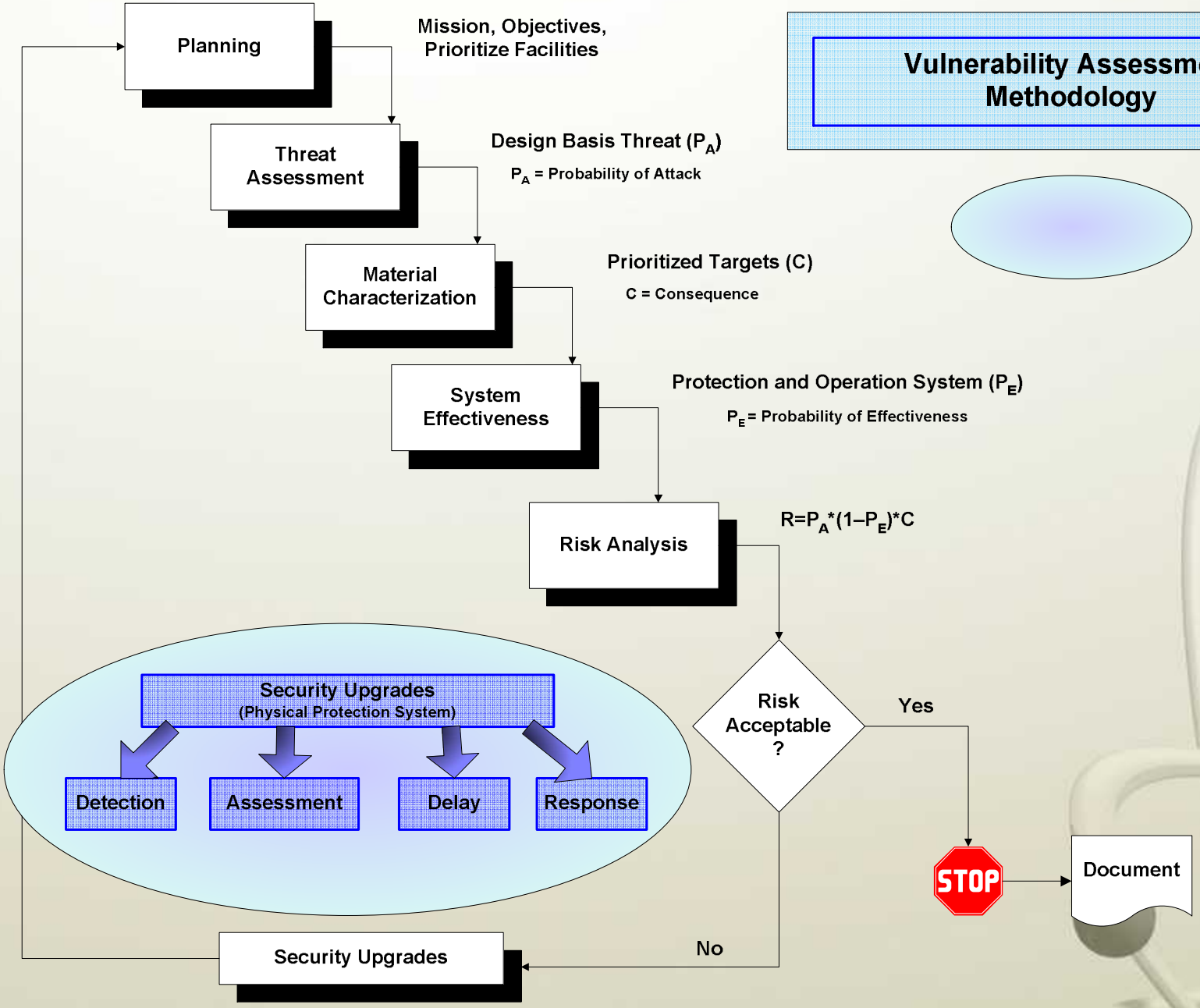
Types of Facilities

- Radioactive waste storage facilities
- Research institutes where material is in use

Facility Security Layers



Vulnerability Assessment Methodology



Principles of Physical Protection

- Security measures should prevent acquisition of material by those with malevolent intent by:
  - **Deterring** unauthorized access to material or material location
  - **Detecting** intrusion (i.e. motion sensors)
  - **Assessing** intrusion (i.e., cameras)
  - **Delaying** perpetrators (i.e. cages, tie-downs) until appropriate forces can respond
  - **Providing response** capabilities





Detection - Intrusion Detection Systems

- Exterior Motion Sensors
- Common Interior Motion Sensors
  - Microwave
  - Infrared
  - Ultrasonic
  - Dual Technology
- Balanced Magnetic Switches
- Duress/Panic Buttons









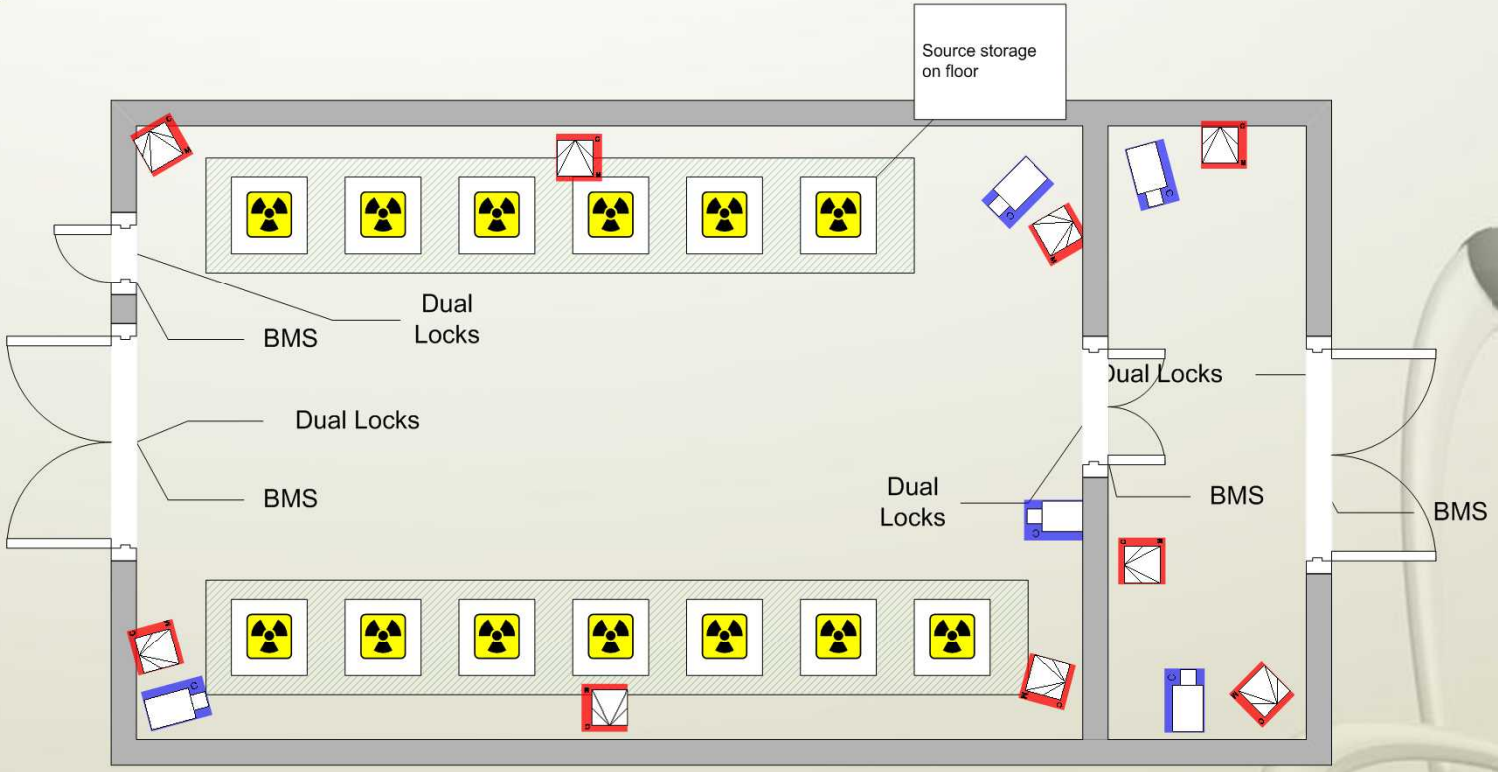

Assessment

- CCTV
  - Camera and Lens
  - Lighting
  - Video Recording
- Guards
- Staff

Delay - Barriers

- Fences
- Gates
- Vehicle Barriers
- Walls
- Doors
- Locks
- Containers

Example Material Storage Facility



Intrusion Detection System (IDS)
Dual Locking Systems
Duress Buttons
Facility Lighting
CCTV
Sources stored in cages
Onsite IDS and CCTV Monitoring
Offsite IDS Monitoring

1.7 Discussion and Review

2.1 Practical Exercise for Physical Protection of SNM

Sandia National Laboratories

NNSA
National Nuclear Security Administration

VAEC

Exercise Objective

- Understand background information for site visit
- Tour site
  - Observe what we have learned about basic security
  - Identify system strengths and deficiencies
- Take notes, drawings, ask questions

Background Information

- Mission(s), operations
- Layouts or schematics
- Critical processes and assets, locations
- Access points, entry control
- Existing security features
  - Detection, delay, and response
- Numbers of personnel
  - Operational and non-operational hours

Logistics

- Two groups of about 7
  - The site will provide operational personnel to act as tour guides
- Physical security overview
  - Boundary
  - Building and inside areas
  - Detection and assessment
  - Alarm reporting
  - Delay features
  - Security force
    - On-site / Off-site

Group Discussion

- General observations
  - Site / facility
  - Threats, targets
  - Existing PPS
    - Detection, delay, response
  - Potential vulnerabilities
  - System effectiveness
  - Recommendations

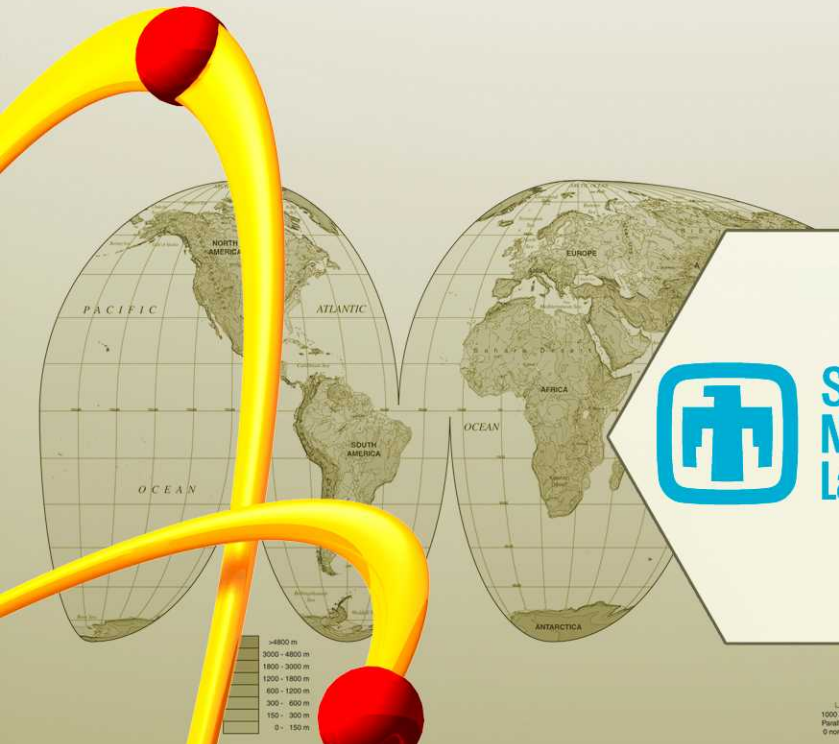
2.2 Practical Exercise Site Visit

Sandia National Laboratories

National Nuclear Security Administration

VAEC

2.3 Practical Exercise – Group Discussions



Sandia National Laboratories

National Nuclear Security Administration

VAEC

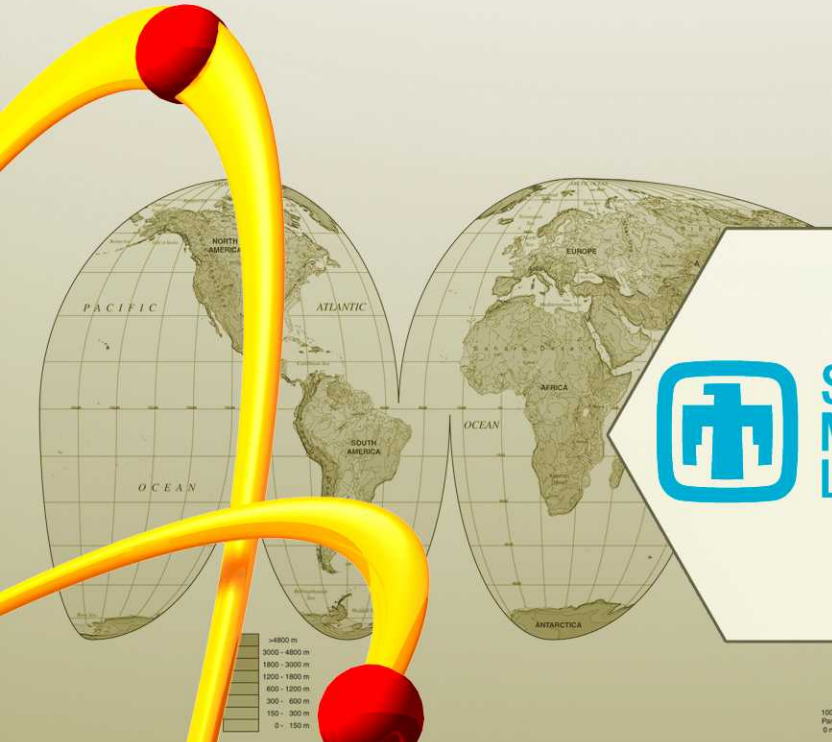
2.4 Practical Exercise – Group Reports

Sandia National Laboratories

National Nuclear Security Administration

VAEC

2.5 Review of Exercise Findings



Sandia National Laboratories

NNSA
National Nuclear Security Administration

VAEC