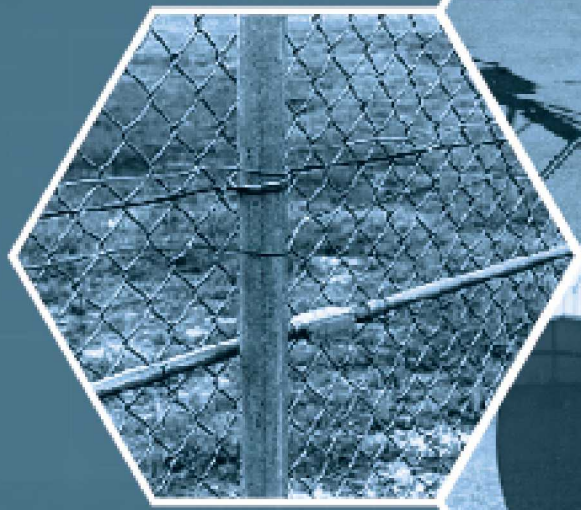
SAND2014-17195PE



# Foundations of Physical Protection Systems

Day 1

# WORKSHOP OVERVIEW

# Workshop Outline

- Workshop Overview and Introductions
- Background on Protection of Nuclear and Radioactive Material
- Overview of DEPO Process – Performance-based approach to physical security
- Various Exercises including Performance Testing of Passive Infrared Sensor
- Potential Tour

# Workshop Objectives

- After completing this workshop, you should be able to:
  - Explain the design and evaluation process outline (DEPO)
  - Understand the elements of a physical protection system
  - Develop an understanding of the fundamental principles of performance testing

# Introduction of Workshop Participants

- Please introduce yourself to the class
  - Name
  - Organization and job
  - Nuclear security / physical protection experience
  - What are your expectations for this course
  - What are your favorite activities outside of work

# Logistics

- Class schedule
  - Course material
  - Start and end time
  - Breaks, lunches
  - Presentations, subgroup exercises
- Cellphones and pagers
- Exits

# Day 1 Agenda

- Introduction to the International Nuclear Security Regime
- Overview of INFCIRC225/Rev.5
- Introduction to Nuclear Security & the Design Evaluation Process Outline (DEPO)
- PPS Requirements and Facility Characterization
- Security by Design

Module 1

# INTRODUCTION TO THE INTERNATIONAL NUCLEAR SECURITY REGIME

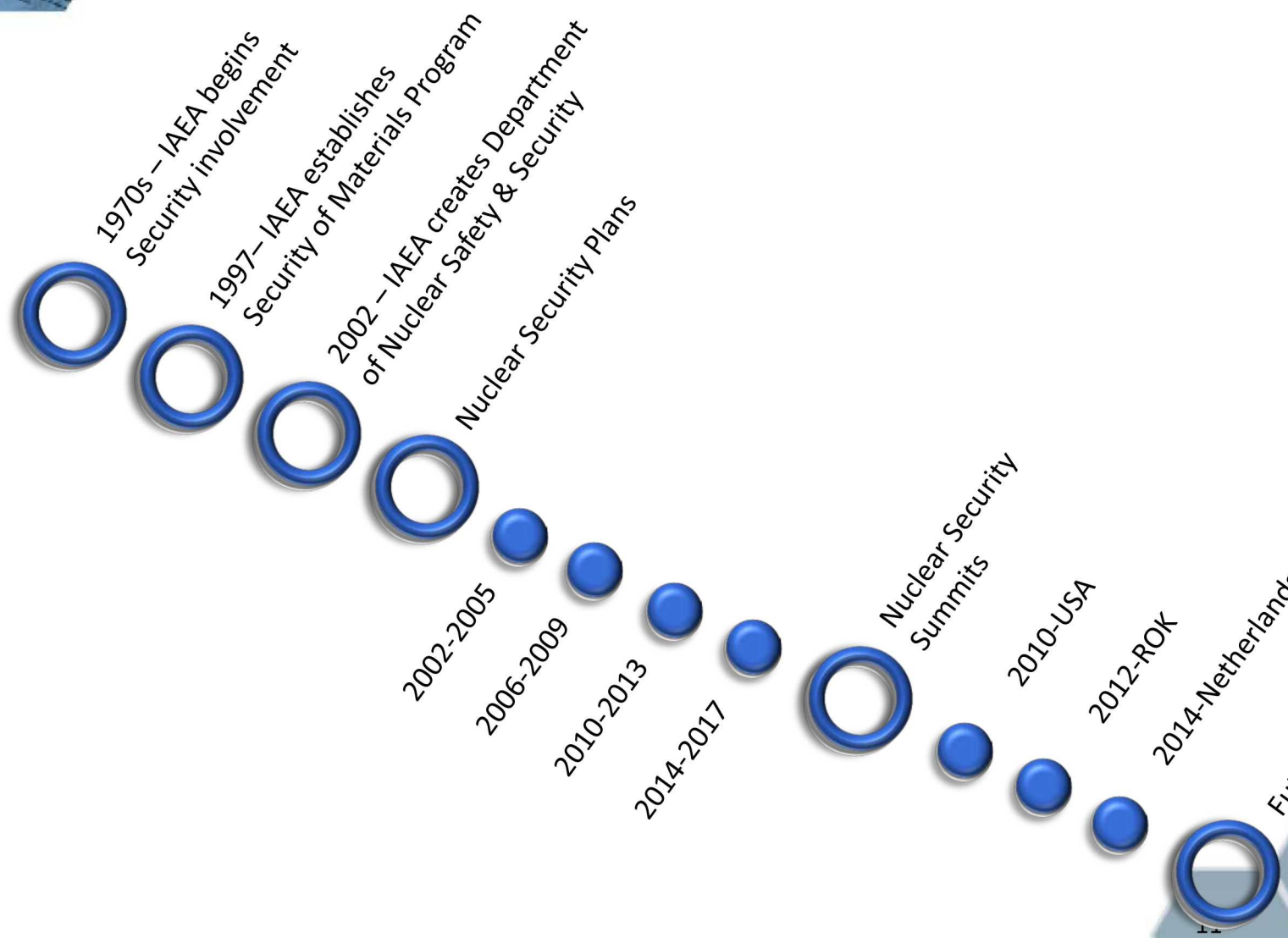
# Lecture Outline

1. Why is there an international nuclear security regime?
2. What is the international nuclear security regime?
3. How is the international nuclear security regime implemented?

# Importance of Nuclear Security

- Interview with IAEA Director for Nuclear Security
  - http://www.iaea.org/newscenter/multimedia/videos/nuclearsecurity/200112/mrabit//index.html

# International Security Regime Timeline



# Risk of Nuclear Material

"The risk that nuclear or other radioactive material could be used in criminal or intentional unauthorized acts remains a matter of concern internationally and continues to be regarded as a threat to international security"

– IAEA Nuclear Security Plan 2014-2017

# Non-Proliferation Goals by IAEA

- Contribute to global efforts to secure nuclear and other radiological material in use/storage/transport and
- Assist States in implementing full range of international legal instruments for nuclear security

# International Documents

| Fundamental Nuclear Security Documents | |
|---|---|
| Convention on the Physical Protection of Nuclear Material (CPPNM) | Only legally binding undertaking in the area of physical protection of nuclear material used for peaceful purposes |
| 2005 Amendment to the Convention on the Physical Protection of Nuclear Material | Extends above protection measures to nuclear facilities/materials in peaceful domestic use, storage, or transport; expands cooperation among States regarding locating/recovering/mitigating missing material |
| International Convention for the Suppression of Acts of Nuclear Terrorism | Seeks to criminalize unlawful/intentional possession or use of nuclear materials or nuclear facility sabotage |
| Security Council Resolutions 1373 (2001) and 1540 (2004) | 1373 – calls all States to become party to all international instruments for nuclear security<br>1540 - calls all States to become party to the CPPNM (and amendment) and IAEA Code of Conduct |
| Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities (INFCIRC/225/Rev.5) | Internationally accepted document for protection of nuclear material. This document utilizes a graded approach for against theft and sabotage of nuclear material. |

# State's Nuclear Security Regime

- Per INFCIRC/225/Rev/5: "The **overall objective** of a State's nuclear security regime is to protect persons, property, society, and the environment from *malicious acts* involving *nuclear material* and other radioactive material." – Section 2.1

***Cornerstone for physical protection***

# Nuclear Security Regime

- An effective nuclear security infrastructure requires a **multi-disciplinary** approach with :
  - Clearly defined legal and regulatory systems
  - Human resource development
  - Established procedures and functions
  - Technical support at regional/national/ facility levels

# Nuclear Security Summit Goals

| Nuclear Security Summits | |
|---|---|
| Washington, D.C., USA (2010) | 1. First international gathering focused on preventing nuclear terrorism<br>2. Brought security of special nuclear materials to global forefront<br>3. Reiterated need for increased international cooperation |
| Seoul, Republic of Korea (2012) | 1. Progress report on 2010 Summit<br>2. Included emphasis on integration of security and safety<br>3. Call for sustained, concrete efforts at global collaboration |
| The Hague, Netherlands (2014) | 1. Reducing the amount of dangerous nuclear material in the world<br>2. Improving the security of all nuclear material and radioactive sources<br>3. Improving international cooperation |

# Nuclear Security International Guidelines

- **Nuclear Security Fundamentals:** contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations.
- **Recommendations**: present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.
- **Implementing Guides:** provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation.
- **Technical Guidance:** publications comprise: **Reference Manuals**, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; **Training Guides**, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and **Service Guides**, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

# Summary: Nuclear Security Regime

- Nuclear and radioactive material pose a unique and significant threat
- The international security regime is a framework of international legal instruments implemented at a national and facility level
- Implement best practices in nuclear security at the international, State, facility, and individual level

Module 2

# OVERVIEW OF NUCLEAR SECURITY INFCIRC225/REV.5

# Lecture Outline

1. Describe the history of INFCIRC225/Rev.5
2. List the four objectives of INFCIRC225/Rev.5
3. Describe stakeholders responsibilities
4. Identify the elements of INFCIRC225/Rev.5

# History of INFCIRC/225

- INFCIRC/225 has been the de facto international standard for the physical protection of nuclear material for decades
- Originally prepared by a panel of experts convened by the IAEA Director General in 1972
- First published in the INFCIRC series in 1975
- Subsequently revised by member-state experts in
  - 1977 (Rev.1)
  - 1989 (Rev.2)
  - 1993 (Rev.3)
  - 1999 (Rev.4)
  - 2011(Rev.5)
- Revision 5 is also IAEA Nuclear Security Series No. 13

# History: List of NSS Documents

| NSS-# | Title | Type |
|---|---|---|
| No. 1 | Technical and functional specifications for border monitoring equipment | Reference Manual |
| No. 2 | Nuclear forensics support | Reference Manual |
| No. 3 | Monitoring for radioactive material in international mail transported by public postal operators | Reference Manual |
| No. 4 | Engineering safety aspects of the protection of nuclear power plants against sabotage | Technical Guide |
| No. 5 | Identification of radioactive sources and devices | Reference Manual |
| No. 6 | Combating illicit trafficking in nuclear and other radioactive material | Reference Manual |
| No. 7 | Nuclear security culture | Implementing Guide |
| No. 8 | Preventive and Protective Measures Against Insider Threats | Implementing Guide |
| No. 9 | Security in the transport of radioactive material | Implementing Guide |
| No. 10 | Development, use and maintenance of the design basis threat | Implementing Guide |
| No. 11 | Security of radioactive sources | Implementing Guide |
| No. 12 | Educational programme in nuclear security | Technical Guide |
| No. 13 | Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5) | Recommendation |
| No. 14 | Nuclear security recommendations on radioactive material and associated facilities | Recommendation |
| No. 15 | Nuclear security recommendations on nuclear and other radioactive material out of regulatory control | Recommendation |
| No. 16 | Identification of Vital Areas at Nuclear Facilities | Reference Manual |
| No. 17 | Computer security at nuclear facilities | Reference Manual |
| No. 18 | Nuclear security systems and measures for major public events | Implementing Guide |
| No. 19 | Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme | Implementing Guide |
| No. 20 | Objective and Essential Elements of a State's Nuclear Security Regime | Fundamentals |
| No. 21 | Nuclear security systems and measures for the detection of nuclear and other radioactive material out of regulatory control | Implementing Guide |

http://www-ns.iaea.org/security/nsspublications.asp?s=5&l=35

# History: Why Revision 5?

- The 9/11/2001 attack resulted in greater recognition of the risk nuclear terrorism
- The IAEA Board of Governors (BOG) and General Conference GC(45)/INF/14, 14 September, 2001
  - Published new Physical Protection Regime Objectives
  - Published the Fundamental Principles of Physical Protection

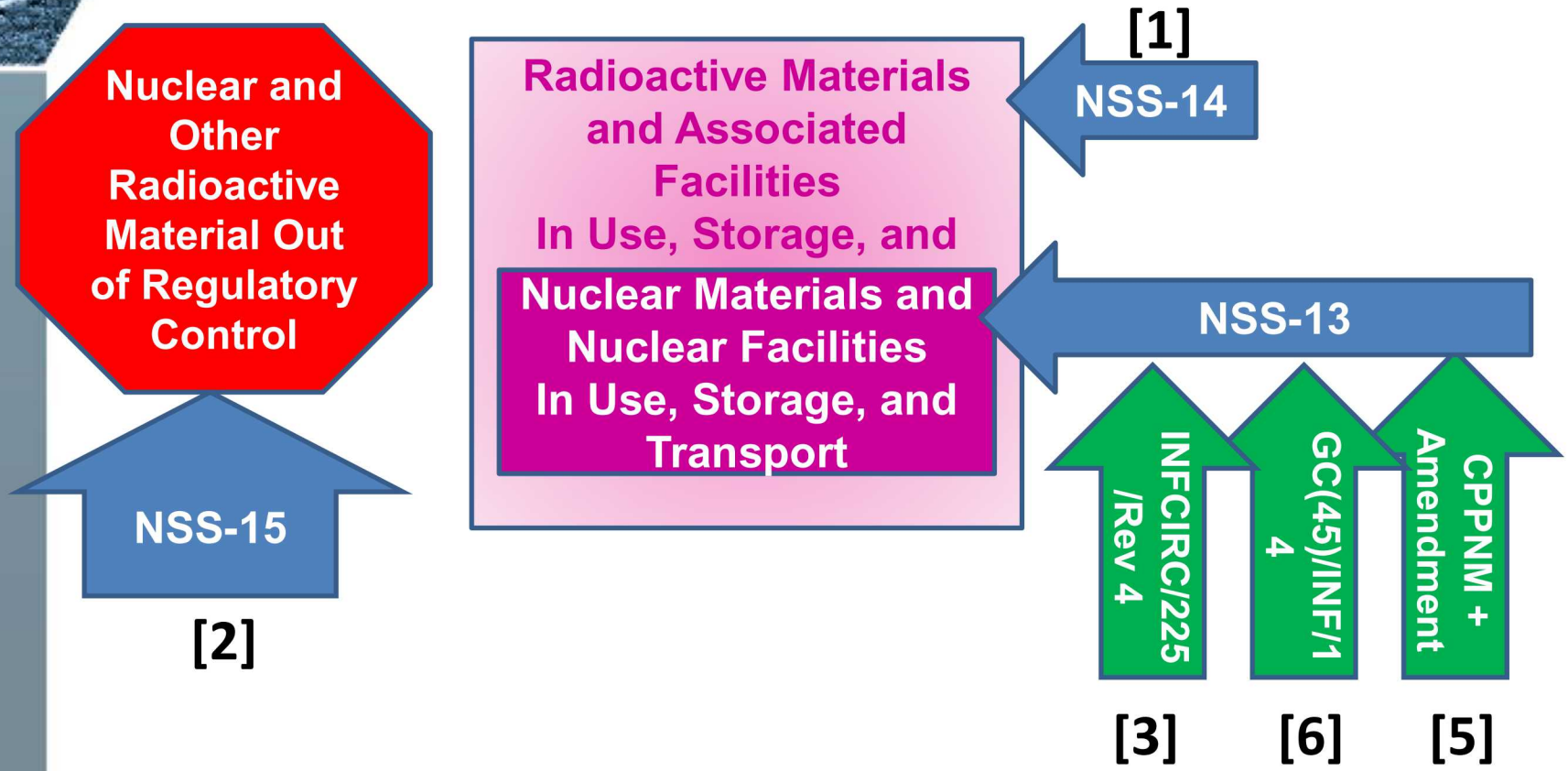
# History: Scope of INFCIRC/225/Revision 5

- Nuclear Material and Nuclear Facilities Used for Civil Purposes
- In Use and Storage/During Transport

# Four Objectives of State's Physical Protection Regime (2.1)

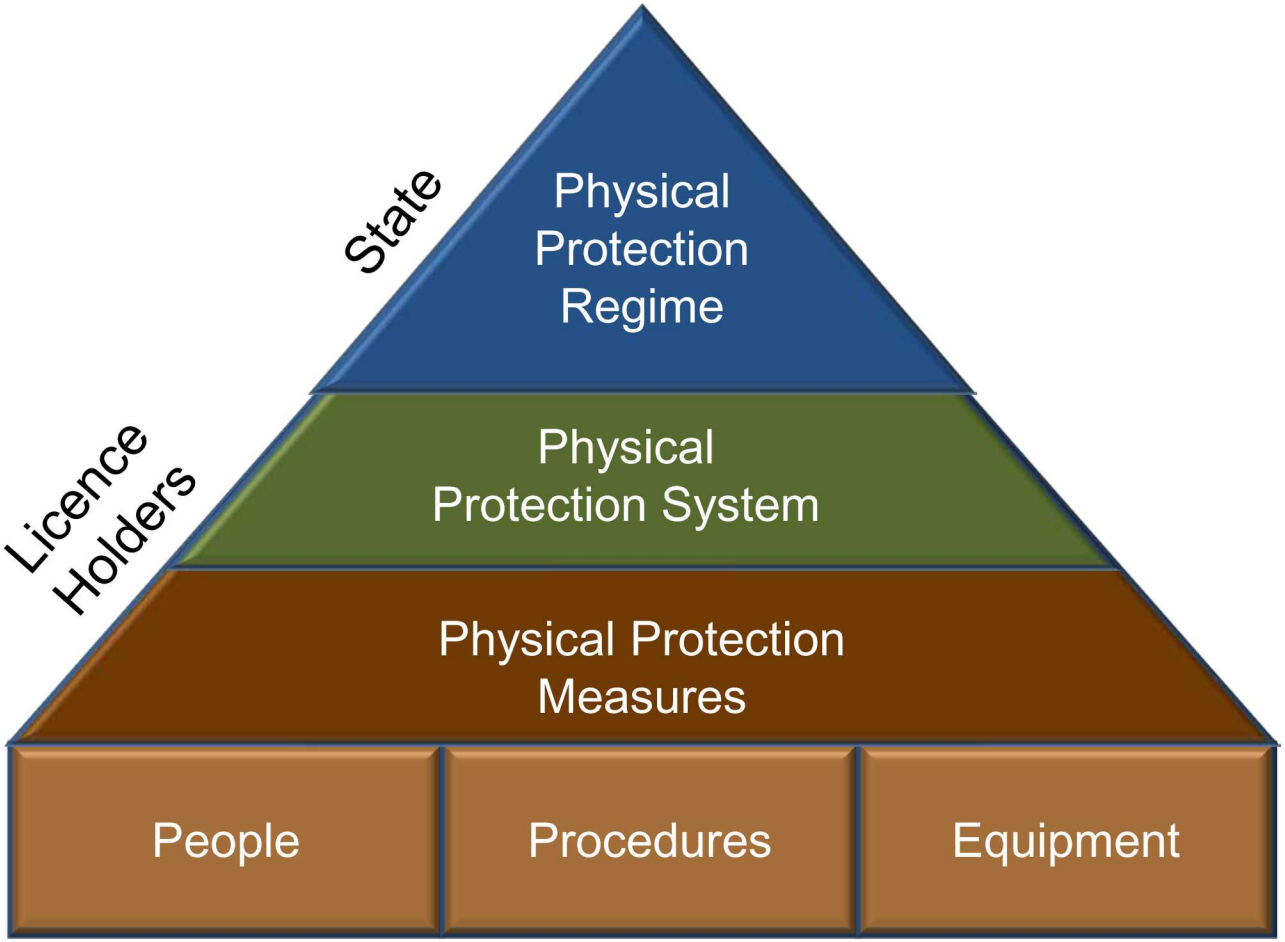
1. **To protect against unauthorized removal**: protecting against theft and other unlawful taking of nuclear material.
2. **To locate and recover missing nuclear material**: ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material.
3. **To protect against sabotage**: protecting nuclear material and nuclear facilities against sabotage.
4. **To mitigate or minimize effects of sabotage**: mitigating or minimizing the radiological consequences of sabotage.

# Four Objectives: Radioactive and Nuclear Security

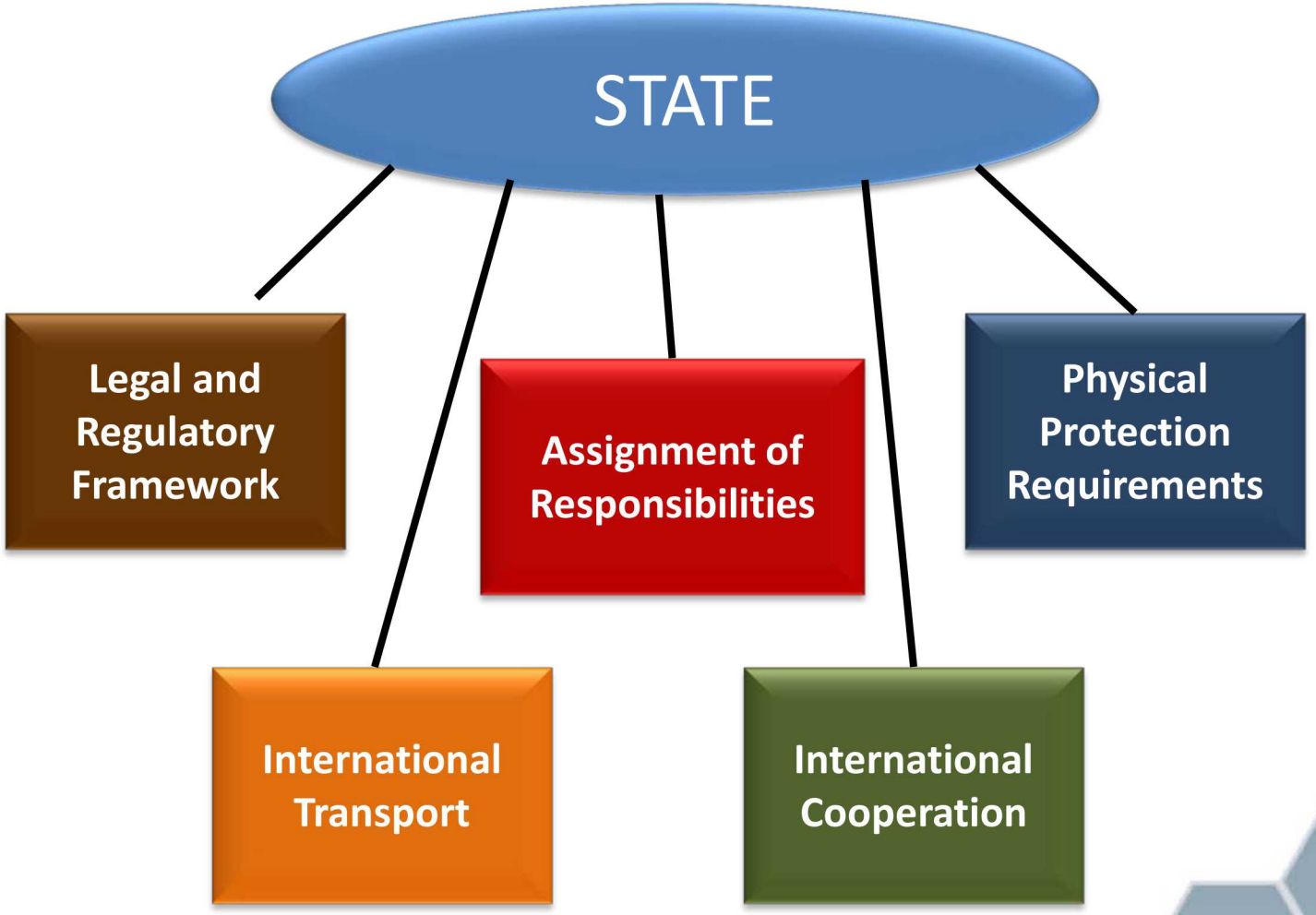



[4] International Legal Framework for Nuclear Security

# Stakeholder Responsibilities: Physical Protection



# Stakeholder Responsibilities: State



# Stakeholder Responsibilities: State

- Establishment, implementation, and maintenance of a physical protection regime
  - All nuclear material in use and storage
  - During transport
  - For all nuclear facilities
- Protection of nuclear material and nuclear facilities
  - Unauthorized removal
  - Sabotage

# Stakeholder Responsibilities: Competent Authority

- Designated by the State with clearly defined legal status and independent from
  - Applicants
  - Operators
  - Shippers
  - Carriers
- Provided adequate
  - Legal authority
  - Competence
  - Financial resources
  - Human resources

# Stakeholder Responsibilities: License Holder

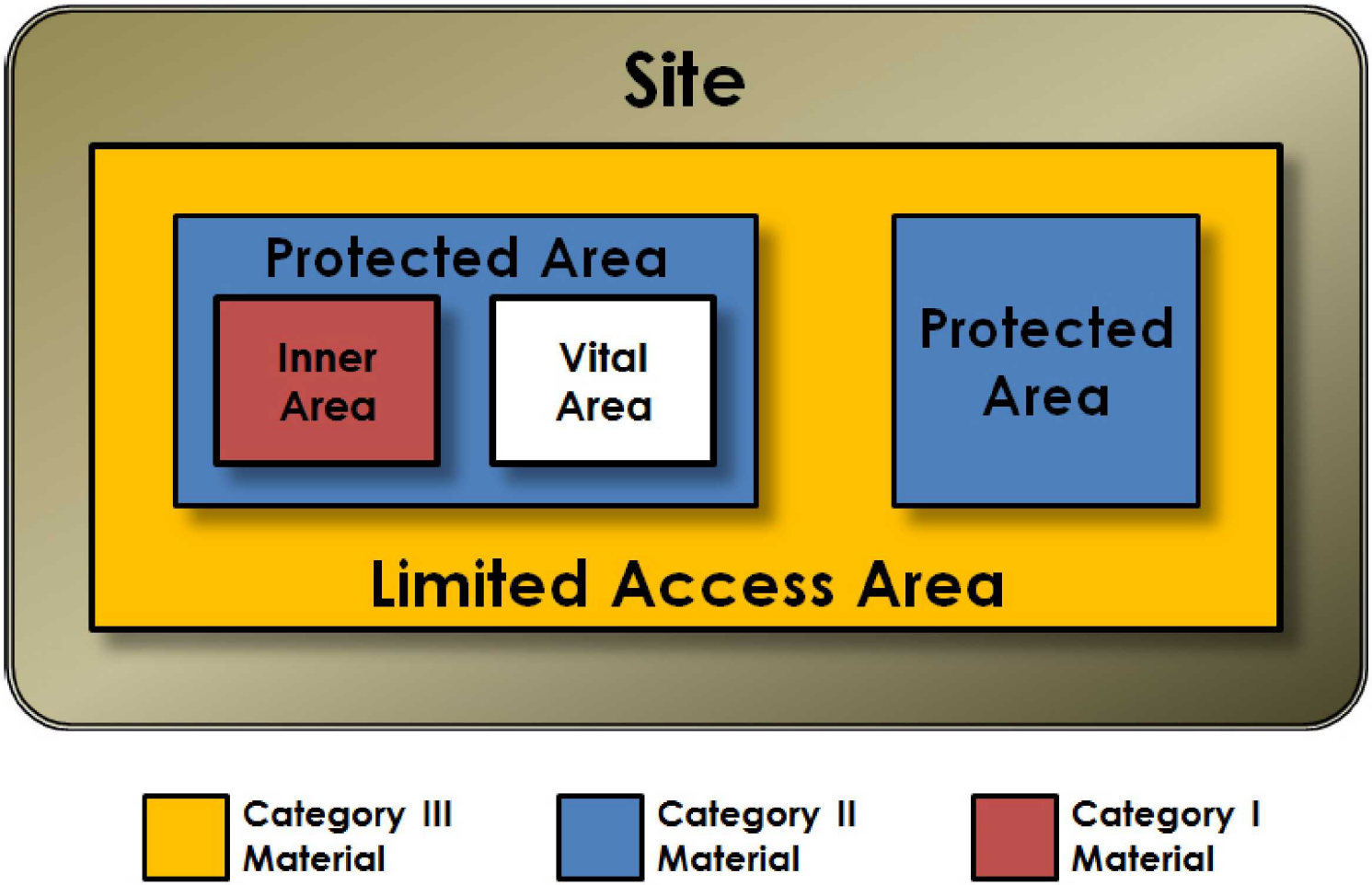
*Defined as operators or shipper/carriers*

- Compliance with regulations
- Cooperation & coordination with State entities having physical protection responsibilities
- Material accountancy and control
- Development of security plan and contingency plan
- Optimum site selection and design
- Development and implementation of means and procedures for evaluation and maintenance of the PPS
- Compensatory measures

# Elements of INFCIRC225/Rev.5 and the 12 Fundamental Principles of CPPNM

1. STATE RESPONSIBILITY (Fundamental Principle A)
2. INTERNATIONAL TRANSPORT (Fundamental Principle B)
3. ASSIGNMENT OF PHYSICAL PROTECTION RESPONSIBILITIES
4. LEGISLATIVE AND REGULATORY FRAMEWORK
   - Legislative and regulatory framework (Fundamental Principle C)
   - Competent authority (Fundamental Principle D)
   - Responsibilities of license holders (Fundamental Principle E)
5. INTERNATIONAL COOPERATION AND ASSISTANCE
6. IDENTIFICATION AND ASSESSMENT OF THREATS (Fundamental Principle G)
7. RISK-BASED PHYSICAL PROTECTION SYSTEM AND MEASURES
   - Risk management
   - Graded approach (Fundamental Principle H)
   - Defense in depth (Fundamental Principle I)
8. SUSTAINING THE PHYSICAL PROTECTION REGIME
   - Security Culture (Fundamental Principle F)
   - Quality Assurance (Fundamental Principle J)
   - Confidentiality (Fundamental Principle L)
   - Sustainability programme
9. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS (Fundamental Principle K: Contingency Plans)

# Elements: Graded Approach for Physical Protection

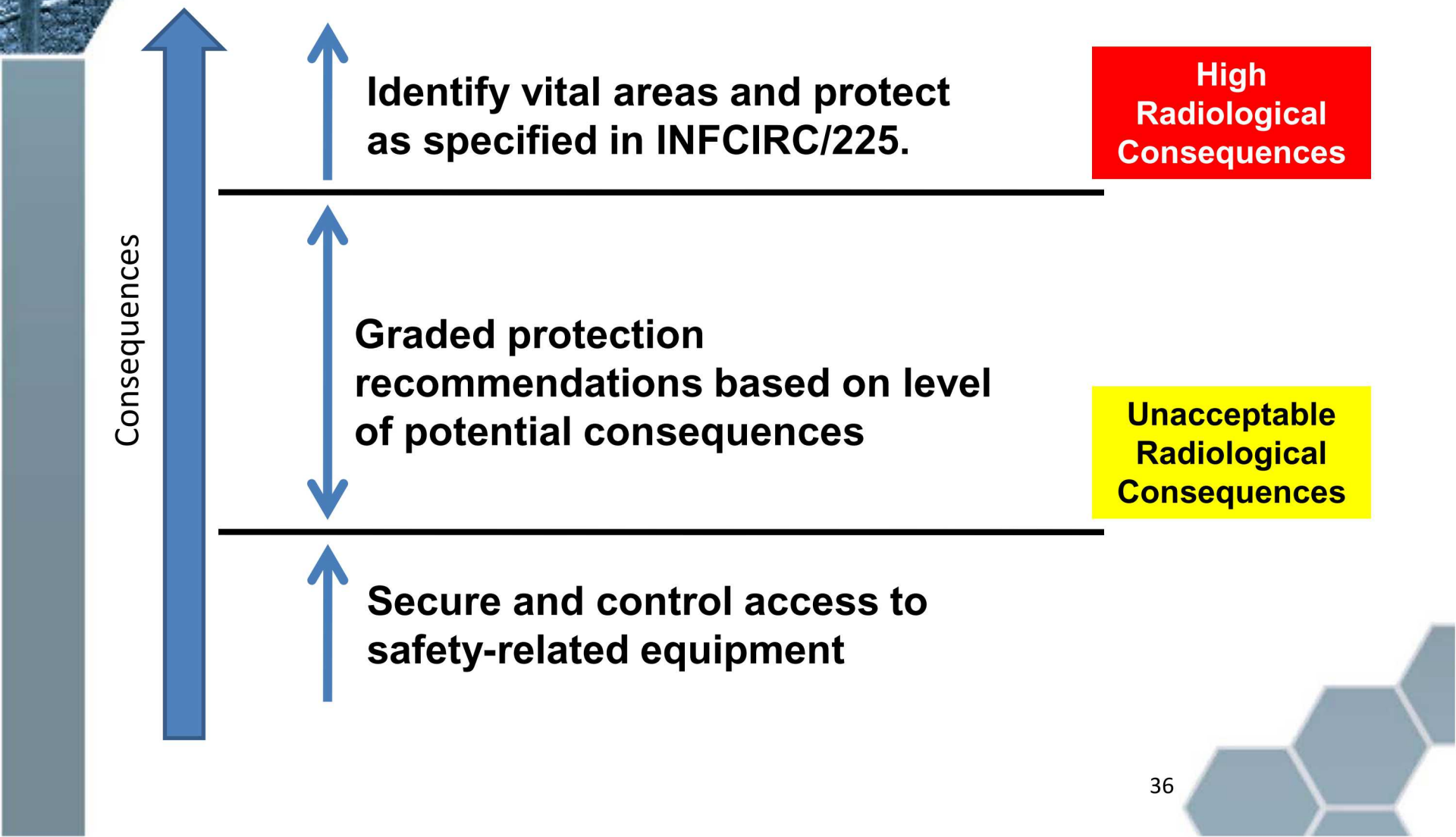


# Elements: Nuclear Material Categorization (IAEA Categorization)

| Material | Form | Category I | Category II | Category III[c] |
|---|---|---|---|---|
| 1. Plutonium | Unirradiated[b] | 2 kg 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]<br>- Uranium enriched to 20% $^{235}U$ or more | 5 kg or more | Less than 5 kg but more than 1 kg | 1 kg or less but more than 15 g |
| | - Uranium enriched to 10% $^{235}U$ but less than 20% $^{235}U$ | | 10 kg or more | Less than 10 kg but more than 1 kg |
| | - Uranium enriched above natural but less than 10% $^{235}U$ | | | 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 *transportation* taking all relevant factors into account.) | | | Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[d/e] | |

[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
[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 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 (100rad/hr) at one meter unshielded.

# Elements: Sabotage Consequences - URC and HRC



# Elements: Identification and Assessment of Threats

- Design Basis Threat (DBT) only required for
  - Category I material protection: 4.41
  - High radiological consequence facilities: 5.30
- Otherwise, the State should decide whether to use a threat assessment or design basis threat for other nuclear material and nuclear facilities
- The DBT is recommended for use as a common basis for design and implementation of PPS
- Threat considerations should include the
  - Insider threat, Cyber threats, Airborne threat, Stand-off attacks, Theft for off-site dispersal

# Elements: Recommendations for High Consequence Facilities (5.20-5.42)

- Extra emphasis on sabotage
- Includes but not limited to Nuclear Power Plants
- Requires protection measures for high consequence facilities analogous to those for Category I theft
- Discusses the protection of vital areas to prevent high radiological consequences
- Better integration with safety measures

# Elements: Recommendations for Measures to Mitigate or Minimize (5.44-5.58)

- New sets of recommendations for the State and operator
- Develop security contingency plans
  - Prevent further damage
  - Secure the facility
  - Protect emergency equipment and personnel
  - Response forces must be familiar with site, sabotage targets and knowledge of radiation protection
  - Contingency plan complements safety emergency plan by focusing on preventing further damage, securing the nuclear facility, and protecting emergency equipment and personnel

# Elements: Additional Considerations

- Risk management (3.41 - 3.42)
- Graded approach (3.43 - 3.44)
- Defence in depth (3.45 - 3.47)
- Nuclear Security Culture (3.48 – 3.51)
- Performance Testing (3.52 - 3.57)

# Elements: Greater Protection Against the Insider Threat

- NMACS systems integrated with physical protection systems to protect against insider threats
- Category I facilities
    - Inner area delay
    - Two-person rule
    - Vehicles, persons, and packages inspections inner areas
  - Category I and II facilities
    - Record of all persons with access to computer systems that control access to nuclear material
  - Category III facilities
    - Custody and shift inventory check for nuclear material handlers

# Elements: International Transport

- Continuous control of nuclear material while under jurisdiction of the State
- Custody transfer process
  - Fellow CPPNM party
  - Formal agreement for continued appropriate physical protection
  - Coordination and status communications
- Special provisions for Category I material
- New structure for Transport recommendations

# Elements: Contingency Plans Versus Emergency Plans

**Contingency Plan**

- Includes measures which focus on preventing further damage, on securing the nuclear facility, and on protecting emergency equipment and personnel

**Emergency Plan**

- Consists of measures to ensure mitigation or minimization of the radiological consequences as well as human errors, equipment failures and natural disasters

Contingency plans and emergency plans should be comprehensive and complementary.

# Summary: Nuclear Security INFCIRC225/Rev.5

- INFCIRC/225/Revision 5 was revised to address an increased threat environment and ensure its compatibility with and guidance for implementation of the Amended CPPNM
- Revision 5 contains many strengthened recommendations for the protection of nuclear material during use, storage and transport

Exercise

# INFCIRC225 EXERCISE

Module 3

# INTRODUCTION TO NUCLEAR SECURITY & THE DESIGN EVALUATION PROCESS OUTLINE (DEPO)

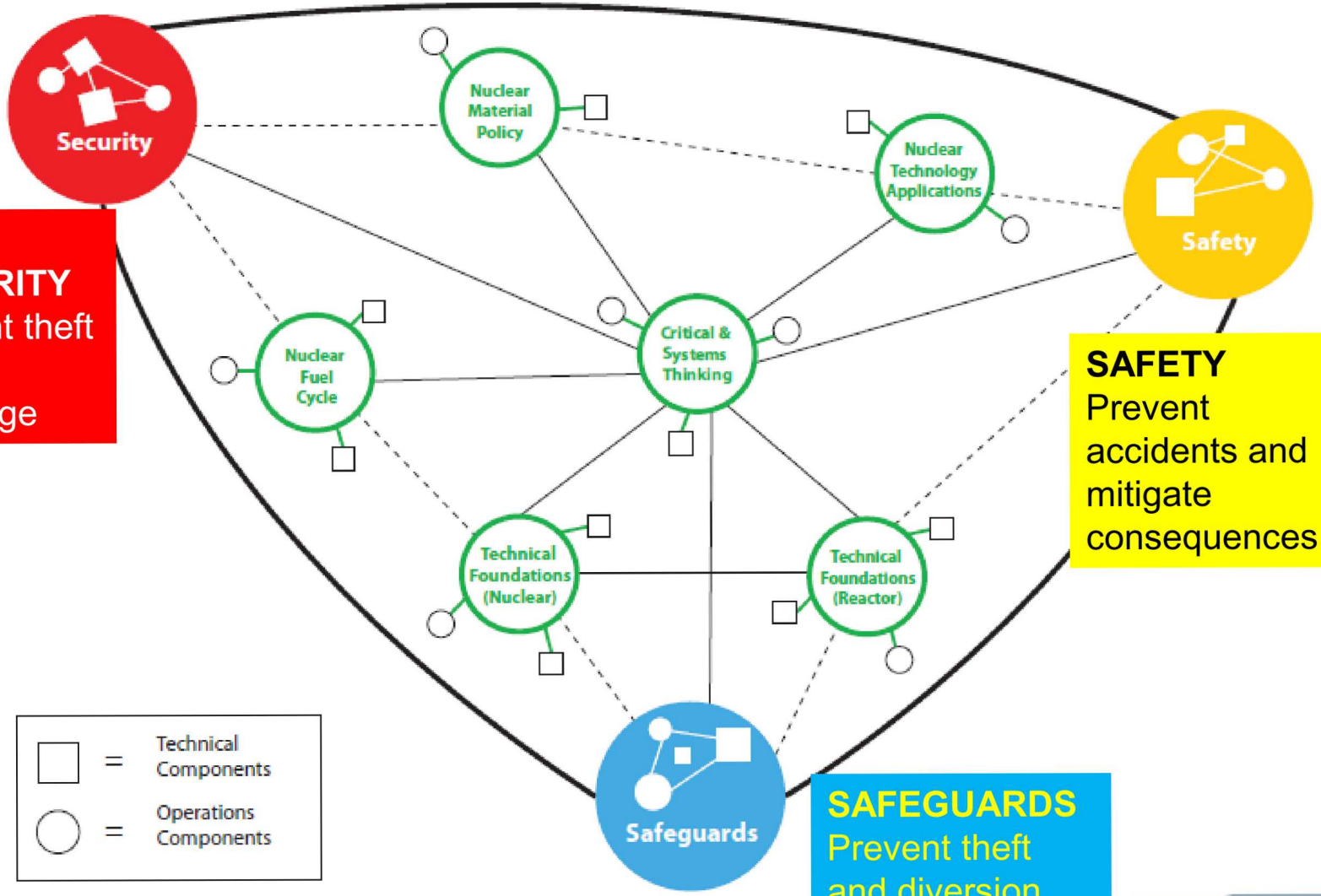
# Lecture Outline

1. Understand the need to identify how nuclear security may be part of an “Integrated 3S” mindset
2. List the objectives of a Physical Protection System (PPS)
3. Recognize different approaches for the design and evaluation of PPS
4. Identify the approach used globally endorsed by the IAEA to design and evaluate PPS
5. List the three basic steps in the Design and Evaluation Process Outline (DEPO)

# Integrated 3S Mindset

- Critical and systems approach
- Integration by design
- Complement processes in 3S approach
- Provide more efficient response to potential theft event
- Utilize safeguards measures for theft events
- Utilize safety measures for sabotage events
- Consider Insider and Cyber threats

# 3S Interrelationships: A Systems Approach




**SECURITY**
Prevent theft and sabotage

**SAFETY**
Prevent accidents and mitigate consequences

**SAFEGUARDS**
Prevent theft and diversion

# Objectives of a PPS

- Protect against unauthorized removal of nuclear materials during use, storage, and transport (theft)
- Protect against sabotage of nuclear facilities and sabotage of nuclear material during use, storage, and transport

***Note: In this course "sabotage" means radiological sabotage.***

# Approaches for the Design and Evaluation of PPS

- Expert
- Features
- Component Criteria
- System Performance

# Expert Approach

- Performs PPS design and evaluation activities relying on personal knowledge and experience
- Example:
  - Experts design and evaluate physical protection system based on prior personal experience

# Expert Approach

- Advantages:
  - Less time (for design/evaluation)
  - Lower cost
  - Can be insightful

- Disadvantages:
  - No metric
  - Subjective
  - Inconsistent (among experts)
  - Can have a limited focus

# Features Approach

- PPS design and evaluation based on specification and implementation of a required set of features
- Example:
  - Two intrusion sensors with video assessment
  - Security locks on gates, doors, and containers
  - Central Alarm Station
  - 24/7 response force

# Features Approach

- Advantages:
  - Clear requirements
  - Easy to regulate/inspect
  - Consistent among facilities


- Disadvantages:
  - No performance metric
  - May be inadequate
  - May be excessive
  - May provide false sense of security

# Component Criteria Approach

- Standards approach to PPS design and evaluation that uses performance criteria for some security features
- Example:
  - Perimeter security zone will detect intruder running (speed), crawling (speed), or jumping (height) with a 95% probability of detection and a 90% confidence level.

# Component Criteria Approach

- Advantages:
  - Clear requirements
  - Consistent among facilities
  - Performance metric for protection elements
- Disadvantages:
  - Requires testing
  - More difficult to inspect
  - No system performance metric

# PPS Design and Evaluation Approaches

| Approach | Requirement | Metric |
|---|---|---|
| Expert | Satisfy expert | Opinion |
| Features | Include required features | Presence of features |
| Component Criteria | Include required features that meet specific standard | Presence of feature a performance standa |
| System Performance | Prevent theft or sabotage of nuclear material | System Effectiveness |

INFCIRC/225/Rev. 5 - "The State should define requirements for the PPS"

# System Performance Approach

- A systems engineering approach to the design and evaluation of PPS based on specifying and achieving an overall system effectiveness against the Design Basis Threat (DBT) for theft and sabotage.
- Example:
  - PPS will prevent the adversary from success with a system effectiveness against theft or sabotage.

***Note: In this course "sabotage" means radiological sabotage.***

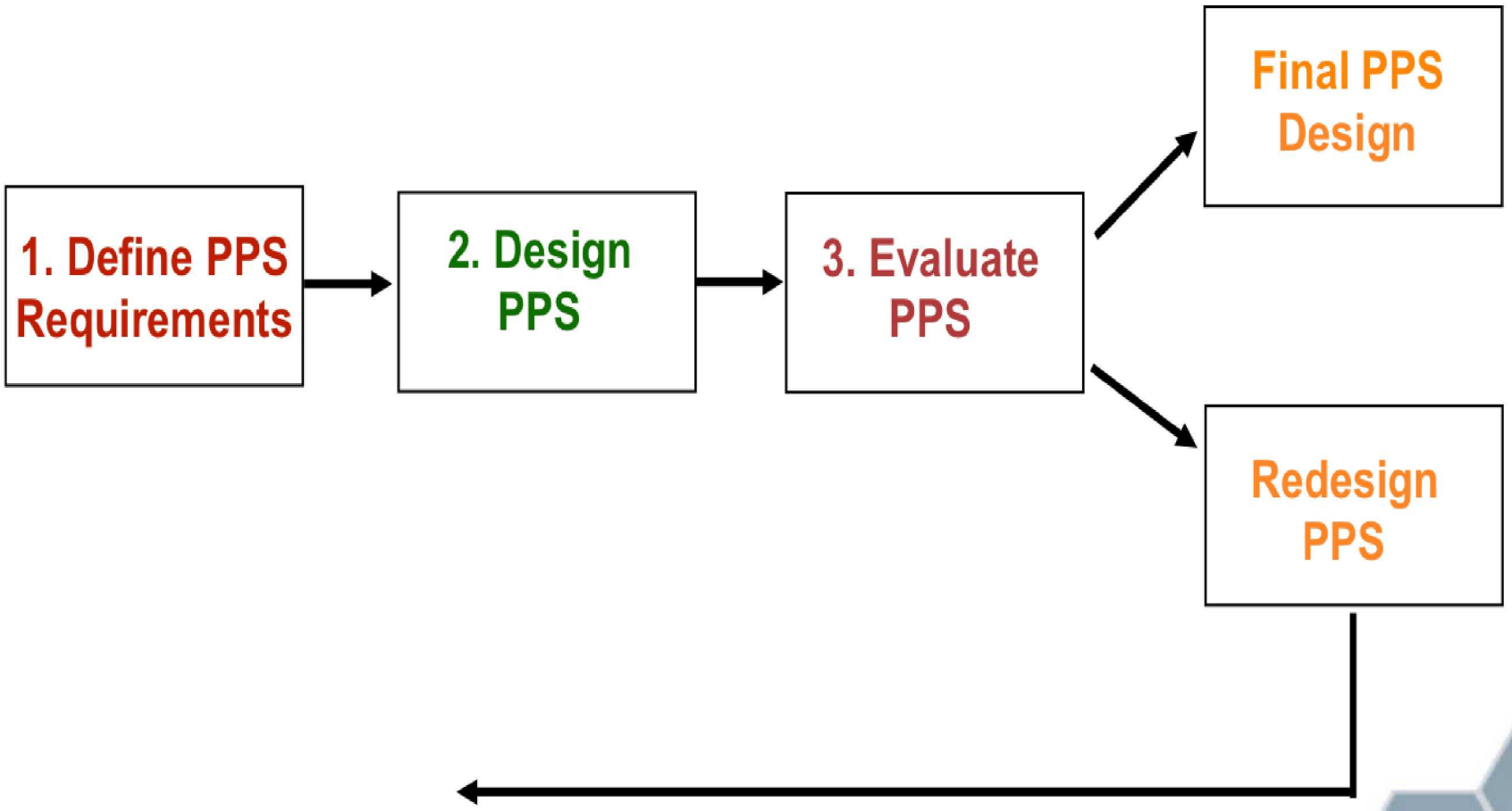
# System Performance Approach

- Advantages:
  - System performance metric
  - Better resource allocation
  - Increased confidence in PPS
- Disadvantages:
  - Requires more performance testing
  - More difficult regulation and inspection
  - Requires system effectiveness policy

# IAEA Endorsed Approach

- IAEA-endorsed (and globally accepted) performance based PPS effectiveness, design, and evaluation approach
- In practice, State systems of physical protection generally include a mixture of performance-based and prescriptive approaches

# Design and Evaluation Process Outline (DEPO)



# Summary: Nuclear Security & DEPO

- Understand that elements of nuclear security impacts and is impacted by nuclear safety and safeguards
- The objectives of a PPS are:
  - Protect against unauthorized removal of nuclear material (theft).
  - Protect against sabotage of nuclear facilities and material (sabotage).
- PPS design and evaluation approaches include expert, features, component criteria, and system performance
- Performance-based PPS effectiveness approach
- Three basic steps of DEPO are define PPS requirements, design PPS, and evaluate PPS

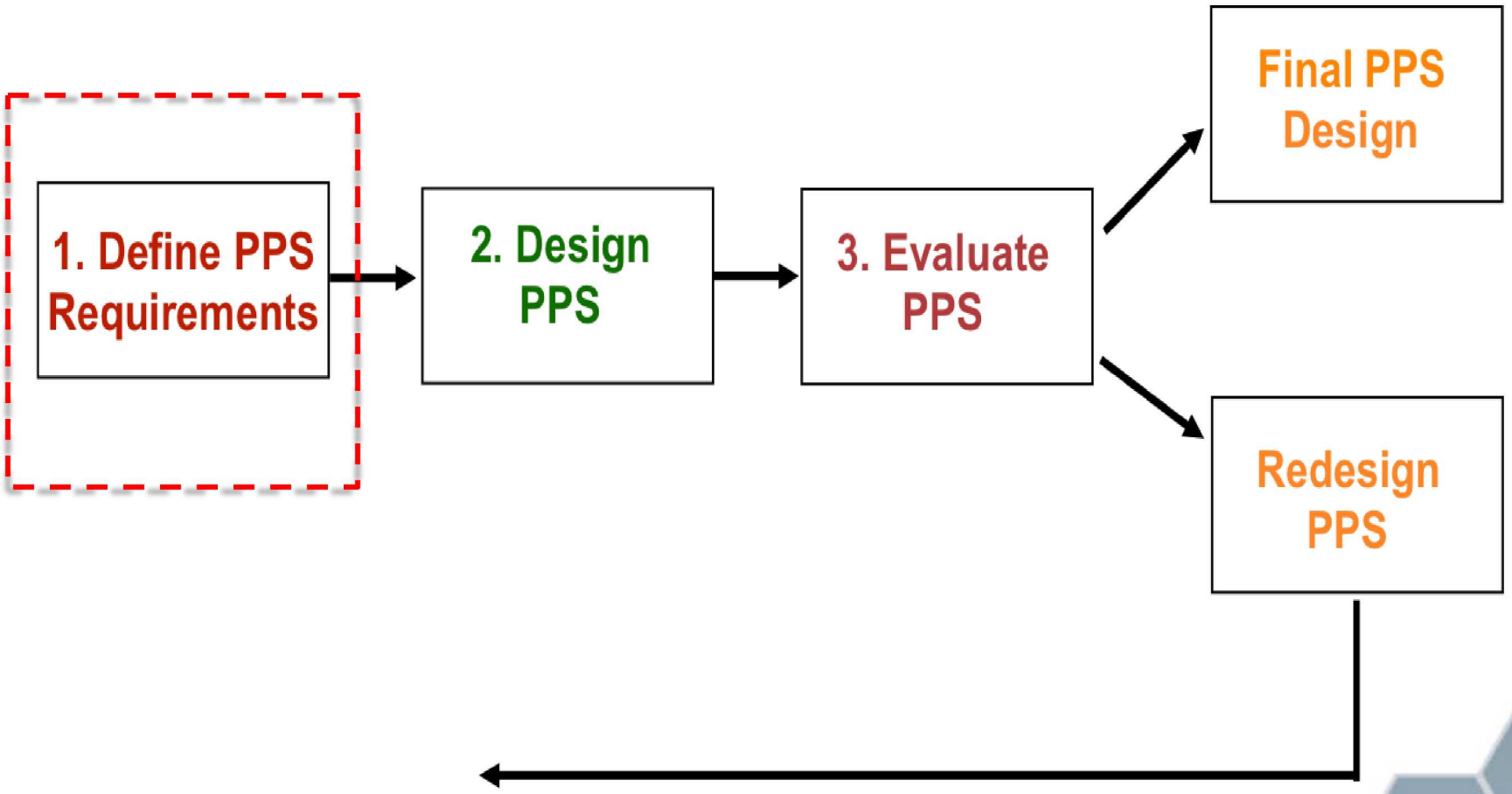
Module 4

# INTRODUCTION TO DEFINING PPS REQUIREMENTS & FACILITY CHARACTERIZATION

# Lecture Outline

1. Define the requirements of a PPS
2. Describe facility characterization
3. Discuss the type of data that is required to accurately apply Design and Evaluations Process Outline (DEPO) for a performance based approach

# Design and Evaluation Process Outline (DEPO)



# Define PPS Requirements

- Basic steps to define PPS requirements are to
  1. ***Characterize facility***
  2. Identify targets
  3. Define threat
  4. Define the risk

***Protect What?***
***From Whom?***
***How Well?***

# Facility Characterization

- Consider impact of facility characterization, on the DBT and the PPS
- Collect all relevant information from all available sources
  - Location (e.g., proximity to roads, major cities)
  - Environment (e.g., weather, terrain)
  - Infrastructure (e.g., construction, buildings, rooms)
  - Operations/Procedures (e.g., employees, work-day)
  - Safety
  - Other information

# Facility Characterization - Location

- Proximity to roads
- Major cities
- Neighbors (commercial, residential, others)
- Population density
- Borders of cities, states, countries
- Nearby hospitals and support
- Emergency response
- Evacuation routes

# Facility Characterization - Environment

- Siting criteria data
- Conditions that could effect security systems
- Natural habitat constraints (forests, animals, etc.)
- Varying weather patterns during year
  - rain, snow, wind, sandstorms, extreme heat
- Terrain for adversaries' advantage
- Release contamination patterns
- Water-based contamination

# Facility Characterization – Infrastructure

- Site boundaries, fencing, barriers
- Buildings (construction materials for walls, ceilings and floors), rooms, and access points
- Heating, ventilation, air conditioning, communication paths and types, power distribution system, environmentally controlled areas, and locations of hazardous materials.
- Consult drawings and then “Walk-Down” the facility

# Facility Characterization – Operations/Procedures

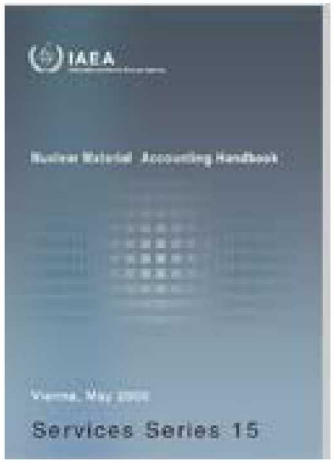
- Operational activities
  - Products and processes
  - Operational days, hours
  - Shift hours and shift changes
  - Number of employees
  - Visitors and vendors
  - Senior executive location


# Facility Characterization - Operations/Procedures

- Written policies and procedures
- Training policies and procedures
- Other written signs of corporate culture
- Unwritten policies and practices
- Management focus and values
- Safety and Security Culture
- Consider legal issues and constraints

# Facility Characterization - Operations/Procedures

– On-site location and specific movement of materials
  - Shipping and receiving process
  - Approvals and signatures
  - Tracking mechanisms
  - Material characteristics
  - Compensatory measures




# Other Information

- Political environment
- Surrounding community relations
- Facility and local law enforcement liaison
- Government priority and support
- Mutual aid agreements
- Local threat information


# Summary: PPS Requirements and Facility Characterization

- Characterize your facility using
  - Physical conditions
  - Facility operations
  - Policies and procedures
  - Regulatory requirements
  - Safety considerations
  - Legal issues
  - Corporate goals and objectives

Case Study

# PELINDABA VIDEO

Module 5

# SECURITY BY DESIGN

# Lecture Outline

1. Recognize that ALL the stakeholders must be identified and consulted to determine their roles, responsibilities, obligations and compliance
2. Recognize that good design integrates and coordinates security, safety and operations
3. Understand the use of safety and operational arrangements as security measures or in a security context
4. Understand Security Through Environmental Design (STED) concept

# Initial Stages

- Basic Questions for ALL stakeholders for an efficient and effective PPS –
  - What do we trying to achieve ?
  - Who are the stakeholders ?
  - What are their roles and responsibilities ?
  - What are the obligations and compliance ?
  - What needs to be acknowledged and done ?
  - How do we (or who) do it ?
- Good practice to revisit these question through the process to keep clear focus and reality check

# QUESTION :
# What are we trying to achieve with Security ?

- Securely (and safely) manage NM & facilities by policies, procedures and practices to ACCEPTABLE LEVELS *(Not What if)*
- Deter, delay, separate from or prevent unauthorized access or removal of NM
- Physical barriers to NM or facility
- Defense in Depth
- Balanced Measures
- STED

# What Needs to be Done

## Infrastructure Issues and Milestones

| Issues | Milestone 1 | Milestone 2 | Milestone 3 |
|---|---|---|---|
| National position | | | |
| Nuclear safety | | | |
| Management | | | |
| Funding and financing | | | |
| Legislative framework | | | |
| Safeguards | | | |
| Regulatory framework | | | |
| Radiation protection | | | |
| Electrical grid | | | |
| Human resources development | | | |
| Stakeholder involvement | | | |
| Site and supporting facilities | | | |
| Environmental protection | | | |
| Emergency planning | | | |
| Security and physical protection | | | |
| Nuclear fuel cycle | | | |
| Radioactive waste | | | |
| Industrial involvement | | | |
| Procurement | | | |

Conditions

Conditions

Conditions

# Security – Safety – Operations Interface

- Consult and meet safety and operations experts to provides coordinated, efficient and cost effective approach
- Use safety and operational (procedures and people) arrangements as security measures i.e. although they are actually safety and operations they can be used a in security context
- Provides integration and coordination
- Consider issues of access and egress as well as the hazards
- Security must be user friendly and practical to ensure an outcome of a good security culture

# Security Through Environmental Design (STED)

- Design process taking into account, addressing and utilizing surrounding environmental parameters when devising plans, programs, policies, buildings, or systems
- PPS design takes into account proposed, planned or existing
- Some examples –
  - Geography, location, topography, environment
  - Surrounds
  - Buildings, structures
  - Deterrence
  - Safety
  - Operations
  - Procedures and people

# Examples of STED (1)

- Interpreting significant structures for radiation protection as delay elements, e.g. thick walls, floors, ceilings, doors, etc. Buildings as vehicle crash protection.
- Buildings and facilities with clear lines for surveillance, detection and assessment (less security equipment)
- Deterrence – perceived as hard target
- Proposed safety and operational staff procedures
- Safety systems that reduce or mitigate unacceptable consequences
- Arranging access and egress points that also take into consideration or integrate safety

# Examples of STED (2)

- Segregation of areas and their relevant importance (vital area concept)
- Elimination of duplication of safety, operational and security measures on common element. Instead use a coordinated solution of the three different measures. Saves on unnecessary and costly conflicting overlaps of requirements i.e. integrated approach.
- Contingency, response plans and emergency services arrangements
- If considering an access point – what are the safety, security and operational needs in an integrated of coordinated approach?

# Operational Considerations

- Design must consider technology, system operator and stakeholders

**EACH ISSUE**

Reach rational agreement or compromise

- Needs for security
- Needs for safety
- Facilities operation
- Technology and performance
- Financial resources
- Human/staff resources

# Consultation

- Must engage ALL stakeholders (and provide fora) to ensure everyone is involved, “talking to each other” and “working together” -
  - Facility including -
    - Business and operations
    - Safety
    - Engineering
    - Security
  - Regulators
  - Contractors
  - Any other stakeholders

# Regulation

- Clear on compliance and regulators roles, responsibilities and jurisdiction -
  - National and international
  - Establish :
    - Licences
    - Compliance Table
    - Agreement approach (“In Principle” and “No Surprises”)
    - Acceptance Levels
    - Security linked to construction stage and regulatory stages of compliance
    - Site security arrangements and operations

# Compliance Table

- Good method to document what measures (in contexts) are actually being used to satisfy security PPS measure, element or licensing requirements
- Something that may appear to be unrelated as safety or operational measure actually has a strong security context to be part of the overall PPS
  - Legislation
  - Procedures
  - Personnel
  - Structures
  - Safety arrangements and response
  - More ?

# Security Planning and Evaluation

- Identify potential targets
- Threat Assessment and DBT by Competent Authority
- Consequence Analysis (CA) and Vulnerability Assessment (VA) by facility then reviewed by competent authority
- Security Risk Review (SRR) identifies relevant threats or events that could cause unacceptable consequences and their severity and treatments
- Construction Security Plan (CSP) and Site Security Plan (SSP) with supporting design and procedures by facility
- SSP and arrangements reviewed by competent authority and gives in principle agreement for license to construct with agreed stages or milestones

# Construction Security Plan (1)

Facility Operator prepares CSP for regulators

1. Objectives and policies
2. Roles and Responsibilities – Security Organizational Chart
3. Security Management
4. Site Security and Threat Assessment
5. Phases of construction
6. System of Physical Protection and Security
7. Access control and personnel security
8. IT and information security
9. Performance Assessment
10. Reporting
11. Review

# Construction Security Plan (2)

- CSP is part of overall Project's Construction Management Plan and overall organizational management
- Outlines responsibilities of -
- Regulator
- Contractor for construction site
- Facility management for –
  - Overall security
  - Monitoring day to day security
  - License and interacts with regulator
  - Regular meetings with contractor, facility management and regulator

# Construction Security Plan (3)

- Stages of Construction Examples

1. Bulk excavation
2. Preparation for, and pouring of, structural concrete
3. Installation of components
4. Cold Commissioning
5. Hot Commissioning

# Security Management and Security Culture

- Ensure the integration of people, procedures, operations and equipment for protection of facilities against theft, sabotage, or other malicious acts
- Take into consideration business and operations within risk management framework
  - Clear objectives, roles and responsibilities
  - Identification and acknowledgement of the threats
  - Good policies and procedures
  - User friendly systems, access and trustworthiness checks
  - Human performance, support and assistance to all levels of staff and performance monitoring

# Security Management “MENU” Approach

| | |
|---|---|
| **PHYSICAL** | Physical Barriers<br>Protected Areas<br>Secure areas and buildings<br>Security technology - access control, alarms, CCTV<br>Secure storage<br>Guarding |
| **PERSONNEL** | Photo Identification Badges<br>Pre-determined trustworthiness<br>Security Education and Awareness<br>Authorised access and limit to need<br>Visitor and contractor supervision and control |
| **ADMINISTRATIVE** | Authorisations and Delegations<br>Policies and Procedures<br>Confidentiality |
| **INFORMATION TECHNOLOGY** | Access Accounts<br>Passwords, screen savers<br>ITSA |

# Risk Management Approach

- Identifies relevant events that could cause unacceptable consequences and their severity
- RISK is measured in terms of likelihood and consequences
- Appropriate level of risk is assigned to each event based on the severity of the consequence and the likelihood of it occurring
- Outcome
- Risk Review identifies vulnerabilities and risks areas requiring treatment
- Keep risk within acceptable levels and decide what resources/ measures (“Menu”) to apply

# Security Scalability

- Include capabilities to increase PP elements with minimum effort
  - Changes in threats or threat environment
  - Transient change in threat level or type of threat
  - Upgrades to PP
- Identify what measures are scalable or unscaleable
  - Scalable measures
    - Eg. Additional guards, procedures, policies, restrict access, access control
    - Quickly put in place
  - Unscalable measures
    - Eg. Buildings, strong doors, walls - thickness & material, barriers, systems
    - Structural measures for high threat levels usually built during construction

# Summary

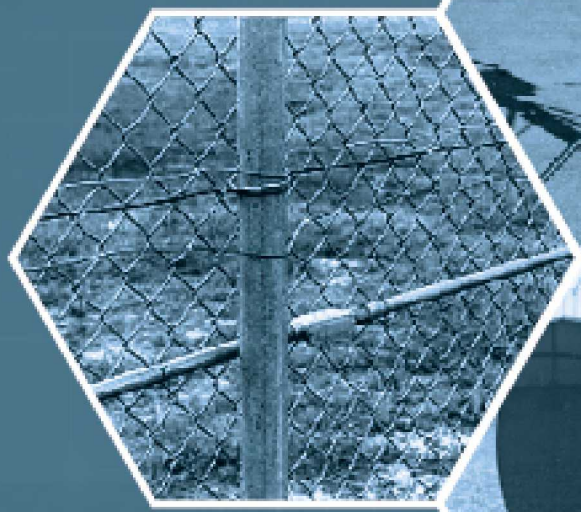
- ALL stakeholders must be identified and consulted to determine their roles, responsibilities, obligations and compliance
- Good design integrates and coordinates security, safety and operations
- Use safety and operational arrangements as security measures or in a security context
- Use Security Through Environmental Design (STED) concept

# Day 1 Summary

- Introduction to the International Nuclear Security Regime
- Overview of INFCIRC225/Rev.5
- Introduction to Nuclear Security & the Design Evaluation Process Outline (DEPO)
- PPS Requirements and Facility Characterization
- Security by Design

# Foundations of Physical Protection Systems

Day 2



# Day 2 Agenda

- Review of Day 1
- Target Identification
- Threat Definition
- Risk Management
- Introduction to PPS Design
- Intrusion Detection Systems
- Entry Control and Contraband

# DAY 1 REVIEW

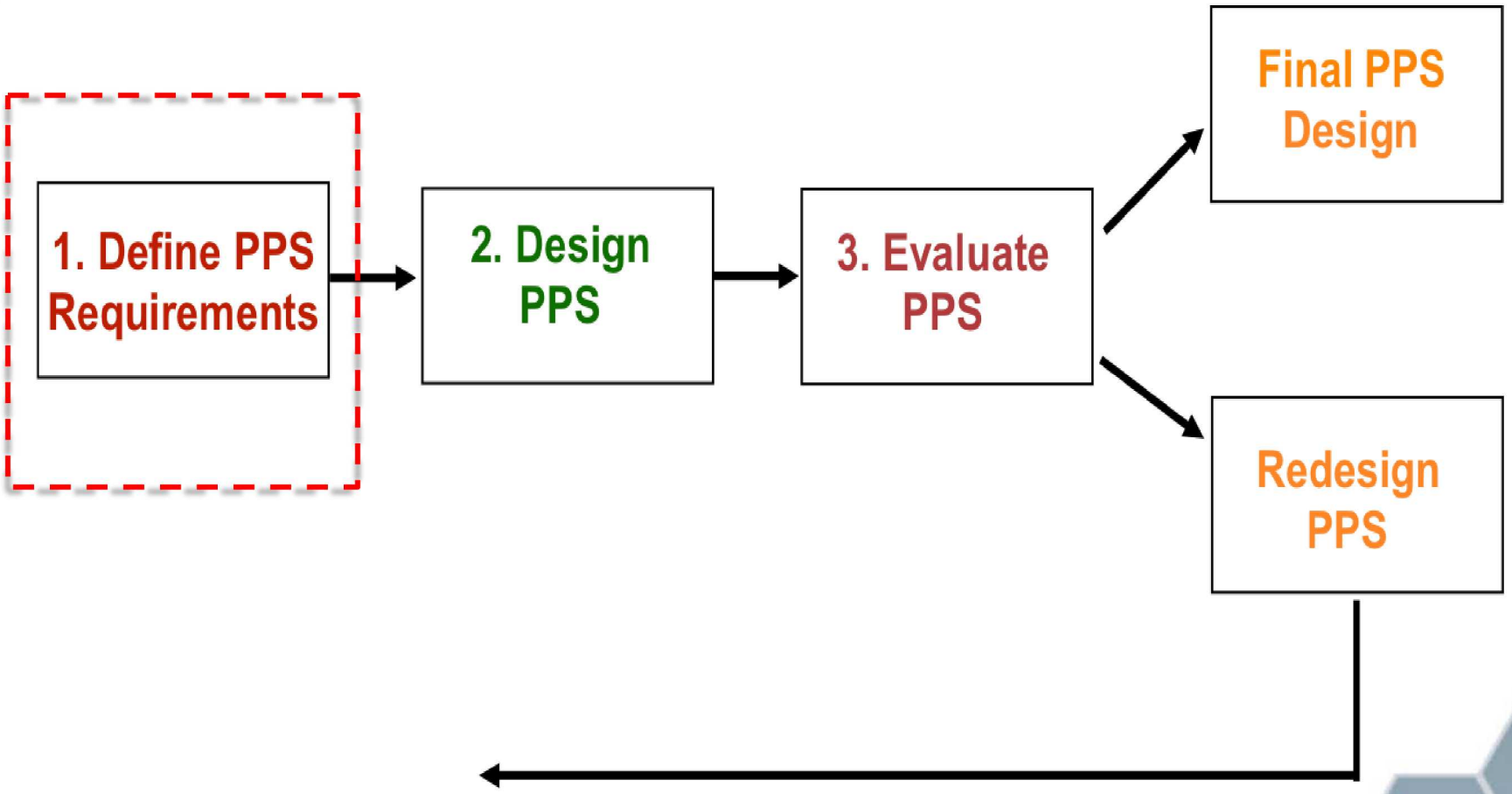
Module 6

# TARGET IDENTIFICATION

# Lecture Outline

1. Review types of nuclear security targets
2. Characterize different targets at facilities
3. Overview of Vital Area Identification
4. Describe Graded Approach for theft and sabotage
5. Understand how are targets are related to attack type

# Design and Evaluation Process Outline (DEPO)



# Define PPS Requirements

- Basic steps to define PPS requirements are to
  1. Characterize facility
  2. ***Identify targets***
  3. Define threat
  4. Define the risk

***Protect What?***
***From Whom?***
***How Well?***

# Types of Nuclear Security Targets

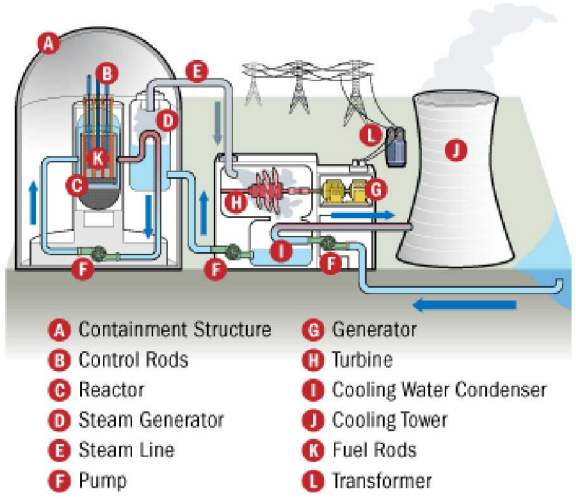
- Theft Targets
  - Nuclear or radioactive materials
- Sabotage Targets
  - Nuclear or radioactive materials
  - Process or support equipment needed to prevent unacceptable radiological consequences

# Types of Nuclear Security Targets

- Other potential targets
  - Facility may have other assets it chooses to protect
  - The design and evaluation process applies to any type of target
  - This workshop focuses on the prevention of theft or sabotage of nuclear or radioactive materials

# Characterize Different Targets at Facilities

- Determine regulatory or policy requirements
- Determine whether facility contains items that must be protected (potential targets)
- Categorize theft targets
- Identify vital areas (sabotage targets)
- Develop target location information



# Characterize Different Targets at Facilities

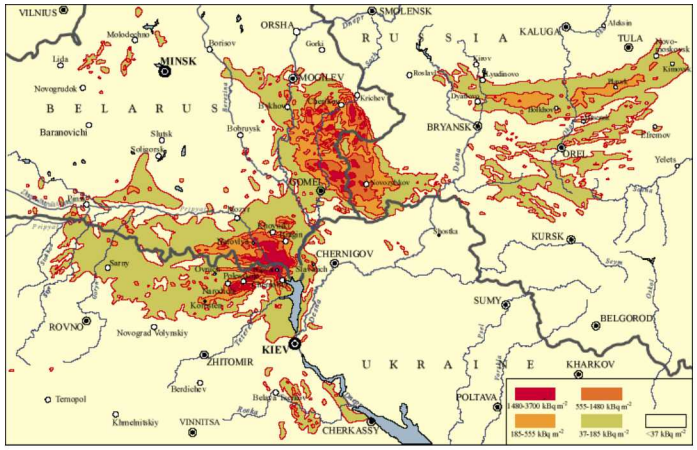
- Determine regulatory or policy requirements; for example:
  - Types of materials that must be protected
  - Radiation dose limits
  - High Radiological Consequence criteria

# Characterize Different Targets at Facilities

- Develop target location information
  - Physical areas in which theft or sabotage targets are located
  - Protect areas for theft or candidate vital areas for sabotage

# Characterize Different Targets at Facilities

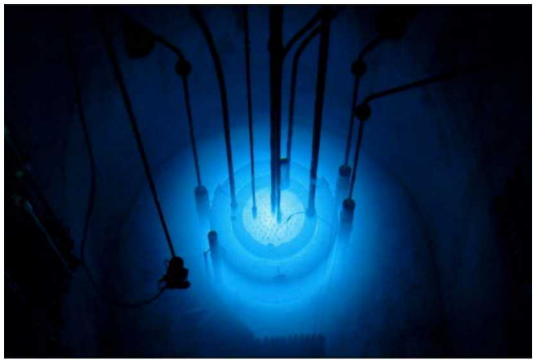
- Identify HRC criteria (sabotage targets)
  - State of facility
    - Core damage, etc.
  - Release or dose potential
  - Direct or indirect release
  - Hybrid criteria




Chernobyl accident provides illustration of potential sabotage consequences

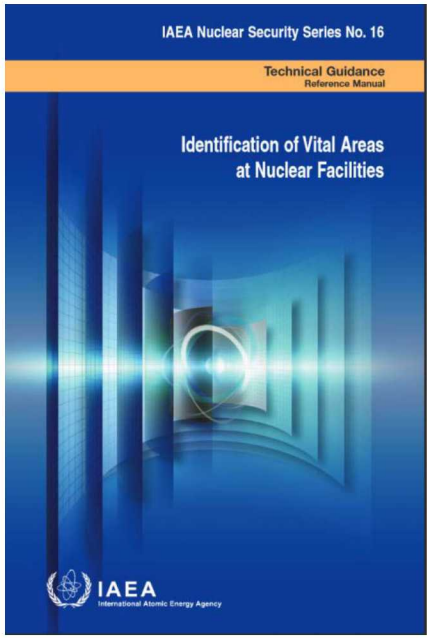
# Vital Area Identification

- Vital Area: An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences.



# Vital Area Identification

- Identify inventories capable of exceeding High Radiological Consequences (HRC) if released
- Utilizes extensive software for analysis
- Rely on various safety analysis documents for background information
- Analyze with Boolean algebra methods and process describe in NSS-16
- Protect locations of such inventories as vital areas



# Two Ways Sabotage May Lead to HRC

## Directly

- Adversary applies energy directly to the nuclear/radioactive material to cause dispersal
- Adversary must gain access to area in which material is located
  - Example: Explosive or incendiary device used to disperse the material

## Indirectly

- Adversary uses energy present in the material or process system to cause dispersal
- Requires initiating a process upset condition and disabling the systems designed to mitigate the upset
  - Example: Disable primary cooling system (initiating event), backup cooling capability (mitigating systems), and allow material to overheat
  - Adversary does not need to gain access to actual material

# Summary: Target Identification

- Target identification process steps
  - Determine regulatory requirements
  - Identify types and quantities of materials at facility
  - Identify theft target categories (INFCIRC/225)
  - Identify Sabotage targets
  - Define vital areas
  - Determine target locations
- Radiological sabotage is categorized according to HRC levels and its prevention relates to the protection of defined vital areas

Exercise

# TARGET IDENTIFICATION EXERCISE

Module 7

# THREAT DEFINITION

# Lecture Outline

1. Define the term “Design Basis Threat” (DBT)
2. Describe the need for DBT
3. Distinguish between a Threat Assessment and a DBT
4. Understand the organizations that may be involved in the DBT process
5. Discuss the types of adversary capabilities that should be addressed in the DBT development process
6. Explain the use of a DBT in the threat-based approach to physical protection

# Define PPS Requirements

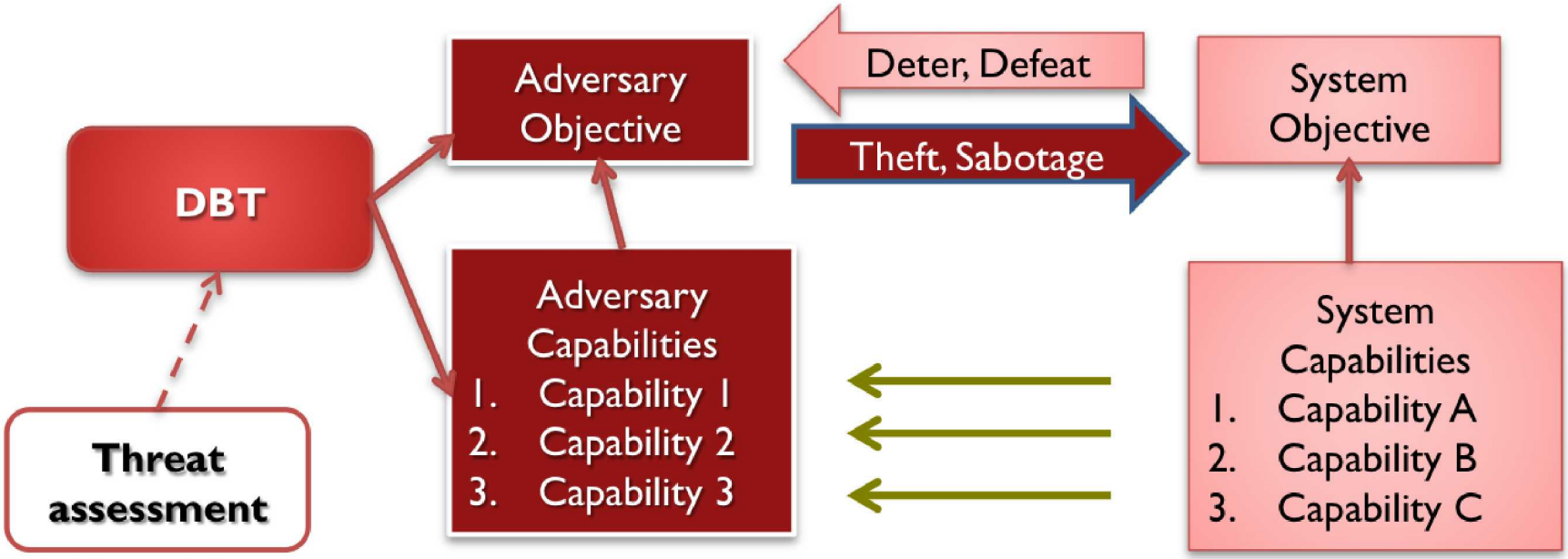
- Basic steps to define PPS requirements are to
  1. Characterize facility
  2. Identify targets
  3. ***Define threat***
  4. Define the risk

***Protect What?***
***From Whom?***
***How Well?***

# Design Basis Threat (DBT) Definition

- "The attributes & characteristics of:
  - Potential insider &/or external adversaries who might attempt unauthorized removal or sabotage against which a PPS is designed & evaluated. (NSS-10, Sec 2, p.4)
  - Threats for which the State organizations & the operators have protection responsibilities & accountability. (NSS-10, Sec 6)

# DBT Structure and Purpose



# Need for DBT

- The Security Engineering Problem: High consequence, low probability event
  - How much security is enough? How do we know?
  - Intelligence estimates are incomplete & change faster than the engineering process can complete

# Need for DBT

- Security Engineering Need: stable, detailed, defensible, design criteria to support:
  - Efficient allocation of resources
  - More objective, less arbitrary design
  - A performance baseline for evaluation of proposed changes
  - Delegation of physical protection responsibilities
  - INFCIRC 225 recommends DBT for
    - Cat 1 material or HRC targets

# DBT Attributes

- Reasonable, based on:
  - Best available intelligence information
  - State-specific policy considerations
- Defendable:
  - Provides technical basis for defining performance requirements
- Cost-Effective:
  - Supports efficient & effective allocation of resources
- Confidence:
  - Helps provide assurance that level of protection is adequate

# Threat Assessment Definition

- "An evaluation of the threats – based on available intelligence, law enforcement, & open source information – that describes the motivations, intentions & capabilities of these threats." (INFCIRC/225)

# Threat Assessment and DBT

- A threat assessment is the preliminary stage for developing a DBT
- Threat assessment process has three parts:
  1. Input
  2. Analysis
  3. Output

# Threat Assessment Process

1. Input – A review of existing, actual threat data
2. Analysis – A determination of which threats may be considered applicable to nuclear facilities. Includes an assessment of postulated threat characteristics & capabilities
3. Output – A documented threat assessment listing postulated, credible threats to the State's nuclear facilities

# Organizations Involved in DBT Process

- State
- Competent authority
- Intelligence organizations
- License holders / Operators
- Other organizations


***Good communication & coordination is essential for the DBT***

# Organizations Involved in DBT Process

- State
  - Has overall responsibility for the development, implementation, and maintenance
  - Ensure legal framework, determination of unacceptable consequences, DBT development roles and responsibilities defined, effective coordination between DBT developers and DBT users

***Good communication & coordination is essential for the DBT***

# Organizations Involved in DBT Process

- Competent authority
  - Governmental organization designated by a State to carry out security functions (225/Rev 5)
  - Leads the DBT process; establishes regulatory framework; oversees implementation and maintenance of DBT (technical, economic and policy factors)

***Good communication & coordination is essential for the DBT***

# Organizations Involved in DBT Process

- Intelligence organizations
  - Coordinates among all State intelligence organizations (internal, international, civil, military)
  - Collects, analyzes and assesses data and information on potential threats to nuclear materials and facilities

***Good communication & coordination is essential for the DBT***

# Organizations Involved in DBT Process

- License holders / Operators
  - Any entity licensed or authorized to undertake the operation of a nuclear facility (225/Rev.5)
  - Implements effective protection measures in accordance with DBT responsibilities and consistent with CA regulatory guidance
  - Reports security incidents that may aid in understanding local threats (includes incidents from insiders)
  - Financial, operational, and safety impacts of preliminary DBT decisions

***Good communication & coordination is essential for the DBT***

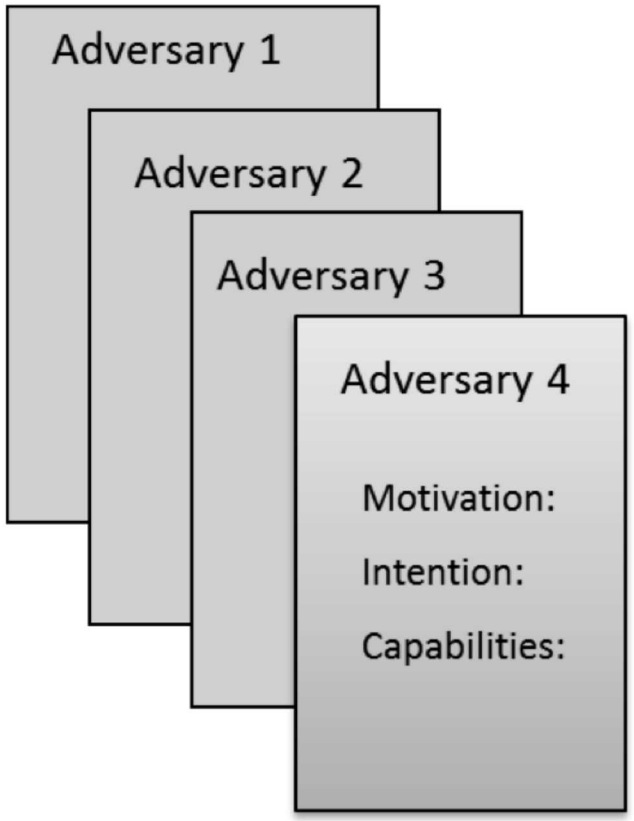
# Additional Organizations Involved in DBT Process

- Law enforcement
- Customs/border control
- Military
- National government teams
- Safety and Safeguards Experts

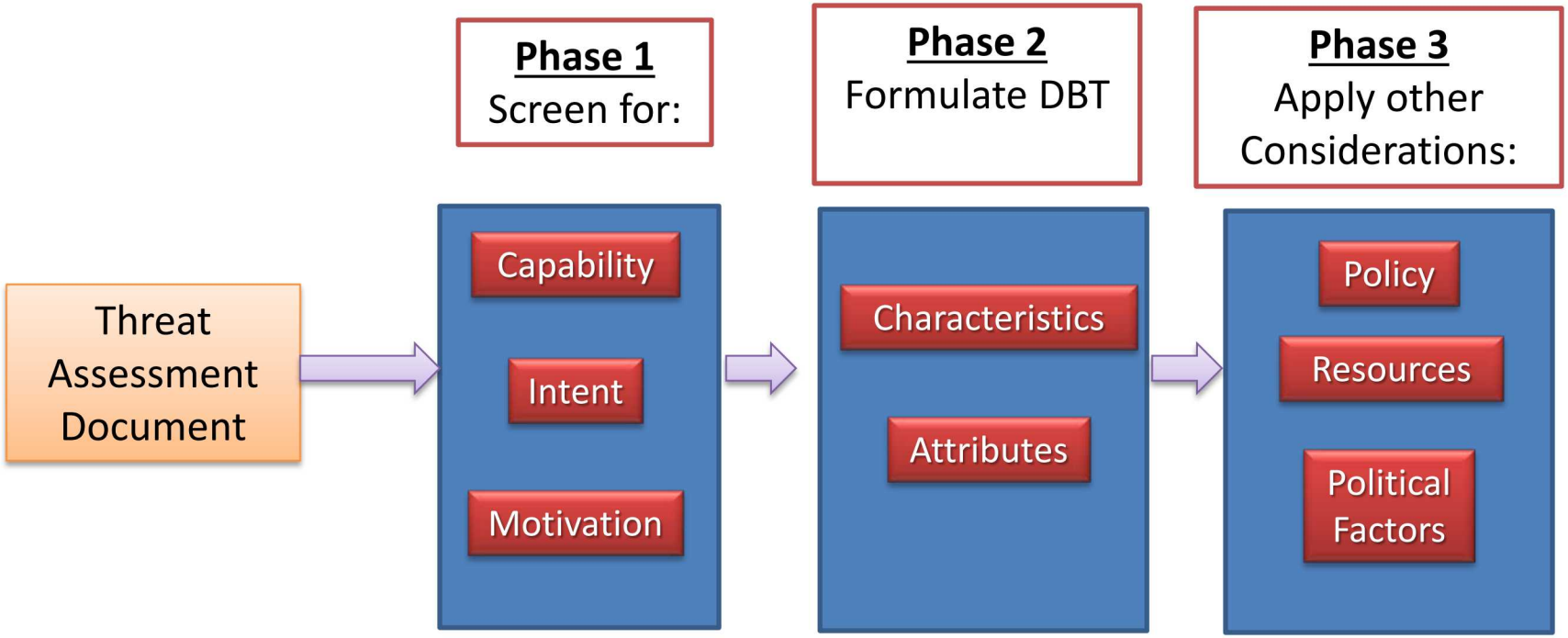
***Good communication & coordination is essential for the DBT***

# Adversary Capabilities to be Addressed

- Numbers
- Weapons and equipment
- Explosives
- Knowledge, skills, and training
- Tactics
- Transportation methods
- Insider assistance

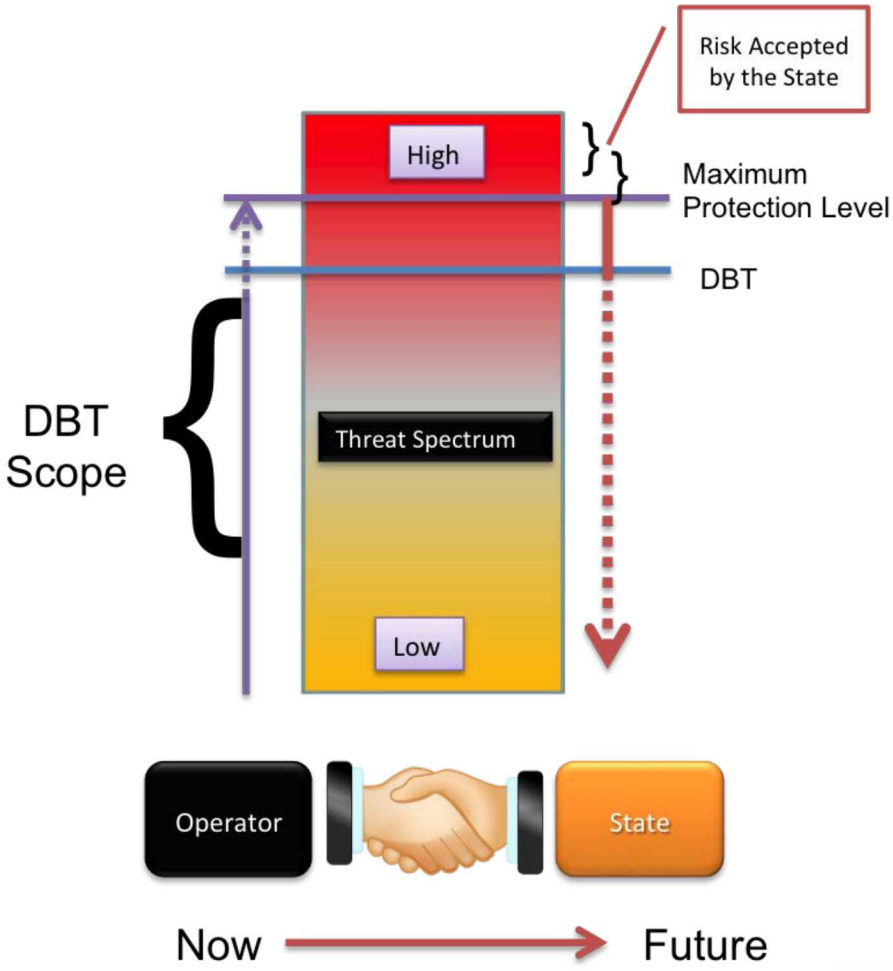


# DBT Development Process Overview



# DBT – The Output

- Two Outputs
  - The DBT (may be more than one)
  - Out-of-scope threats
- Primary responsibility:
  - DBT Threats - Operator
  - Maximum credible threats - State



# DBT Influence on PPS Design

- Threat scenarios form the basis for understanding the threat & evaluating security performance
- Threat scenarios based on the DBT
  - Adversary objectives & tactics
- Threat scenarios identify vulnerabilities for mitigation by the PPS

# DBT Maintenance

- Things change
  - The threat
  - Change in nuclear program
  - The political, legal, security, & resource environment
- Plan for change
  - Review cycles
  - Change criteria
  - Evaluation
- Same process used as for developing a DBT
- Review may change the DBT

# Summary: Threat Definition

- DBT supports security risk management as part of the regulatory framework
- Potential adversary motivation, intentions, & capabilities are the main drivers for a performance-based PPS
- Relevant adversary capabilities are formulated in a DBT
- Principal roles in DBT development include the State, Regulatory Authority, Intelligence Organizations, License Holders, & other organizations
- Competent Authority is responsible for developing, implementing & maintaining a DBT
- Licensees are responsible for implementing protection measures against the DBT

Module 8

# RISK MANAGEMENT AND REGULATORY REQUIREMENTS

# Lesson Outline

1. Define risk and risk management
2. Recognize the security risk equation
3. Describe three generic ways to reduce risk
4. Identify two approaches competent authorities can use to establish requirements for physical protection systems

# Define PPS Requirements

- Basic steps to define PPS requirements are to

1. Characterize facility
2. Identify targets
3. Define threat
4. ***Define the risk***

***Protect What?***
***From Whom?***
***How Well?***

# General Definition: Security Risk

- ***Risk***: Possibility of future harm or loss as the result of the occurrence of some undesired event
  - The likelihood that the undesired event occurs
  - The consequences of the occurrence of the undesired event
- ***Security Risk***: Possibility of future harm or loss due to malicious actions of persons or groups of persons
  - The likelihood that malicious acts are successfully carried out
  - The consequences – a measure of harm or loss – of those acts

# General Risk Equation

- Risk, **R**, can be described adequately using a product model:

**R = P * C**

*Where* **R** = Risk
**P** = Likelihood or probability of an event occurring
**C** = Consequences of the event

- **Safety Risk** is the product of the likelihood of an initiating (abnormal) event and the magnitude of consequences of the event
  - The event is random (due to equipment failure, natural disaster, or other random occurrence)
- **Security Risk** is the product of the likelihood of a successful adversary attack that causes an undesired event and the consequences of the event
  - Event is result of intentional malicious act by a person or persons
  - Event is not random

# Likelihood of Successful Attack

- The likelihood of a successful attack is dependent on two factors:
  - The likelihood or probability of a malicious attack by an adversary
  - The likelihood or probability that the malicious attack is successful, given that it is attempted
- Thus the probability of a successful attack can be written as:

$$P = P_A * P_S$$

*Where* $P_A$ = Probability of attack

$P_S$ = Probability that the attack is successful if it is attempted

# System Effectiveness

- A physical protection system is intended to reduce the adversary's probability of a successful attack:
  - Either the physical protection system is effective and the adversary is defeated or the physical protection system is defeated and the adversary is successful
  - Thus

$$P_E + P_S = 1$$

*Where* $P_E$ = Probability that physical protection system is effective in preventing the undesired event

$P_S$ = Probability that the attack is successful if it is attempted

# Security Risk Equation

- Based on these concepts the security risk equation becomes:

$$R = P * C$$
$$R = P_A * P_S * C$$
$$R = P_A * (1 - P_E) * C$$

- The three risk factors are interdependent
- The more effective the PPS, the lower the risk

# Security Risk Management

- **Risk management** : the process of identifying and applying measures that reduce or mitigate the risk of an undesired event

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

- According to the security risk equation, security risk management or risk reduction can be accomplished in three ways:
  1. Reduce the likelihood of an adversary attack, $P_A$
  2. Increase the effectiveness of the physical protection system, $P_E$
  3. Reduce the severity of the consequences, **C**, should an attack succeed

# Risk Reduction Strategies

- Risk reduction in a State's nuclear program becomes a problem in resource management:
  - Cost-effective physical protection systems
  - Consolidation to fewer locations
  - Conversion to less attractive materials
  - Final disposition of excess materials
  - Consistent coordination and joint exercises
  - Utilization of 3S integrated approach

# Regulatory Approaches

- The State's Competent Authority has two general approaches to establishing requirements for the Licensees and verifying their compliance:
  - Prescriptive approach
  - Performance approach
- In practice, many states use a combination of performance and prescriptive requirements

# Summary: Risk Management and Regulatory Requirements

- **Risk**: the possibility of harm or loss
- **Risk management**: the process of identifying and applying measures that reduce or mitigate risk
- Security risk equation: $\mathbf{R = P_A * (1 - P_E) * C}$
- Three ways to reduce risk:
  - Reduce the likelihood of an adversary attack, $P_A$
  - Increase the effectiveness of the physical protection system, $P_E$
  - Reduce the severity of the consequences, C, should an attack succeed
- Two approaches competent authorities can use to establish requirements for physical protection systems:
  - Prescriptive and Performance approach

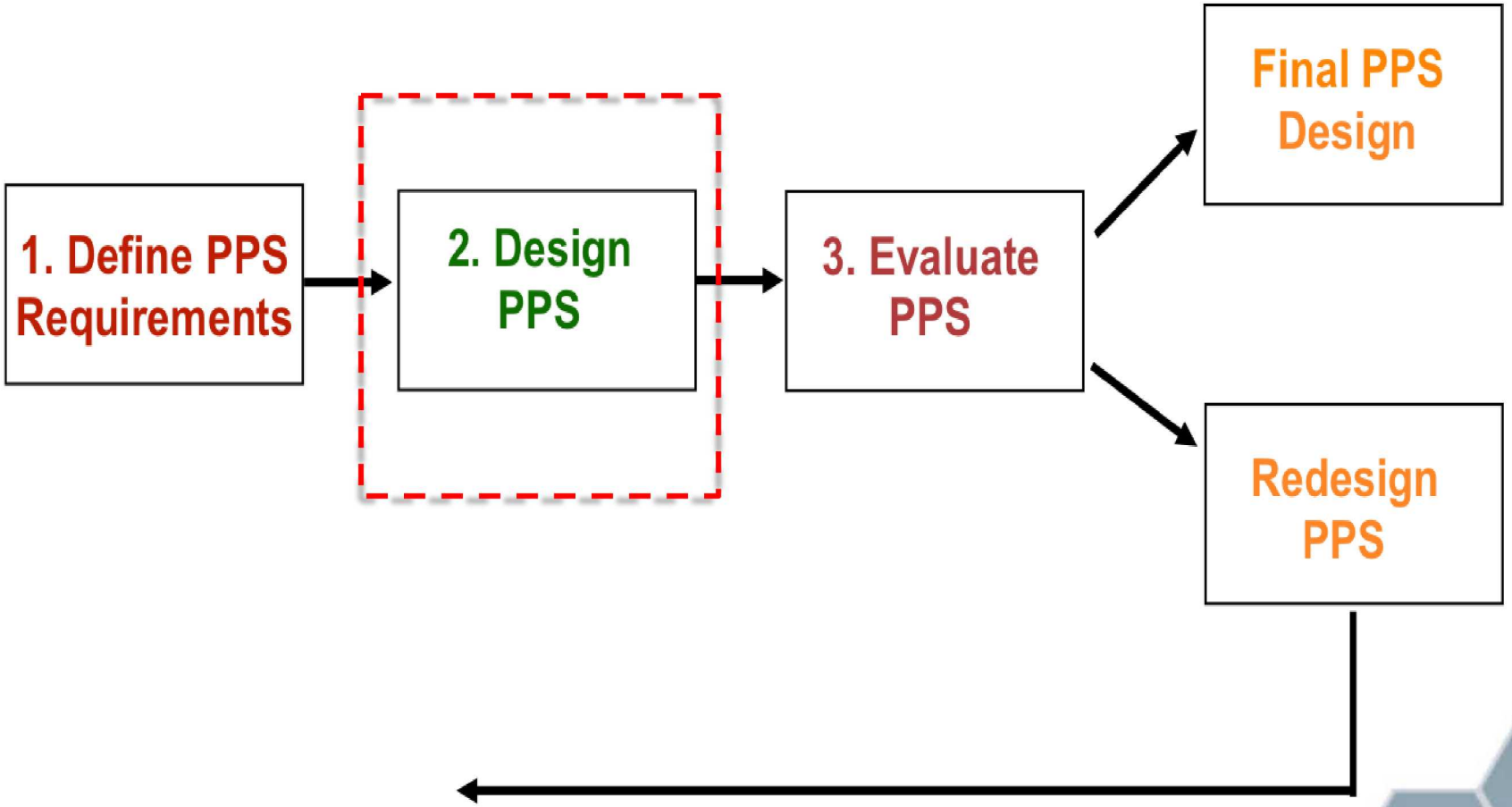
Module 9

# INTRODUCTION TO PPS DESIGN

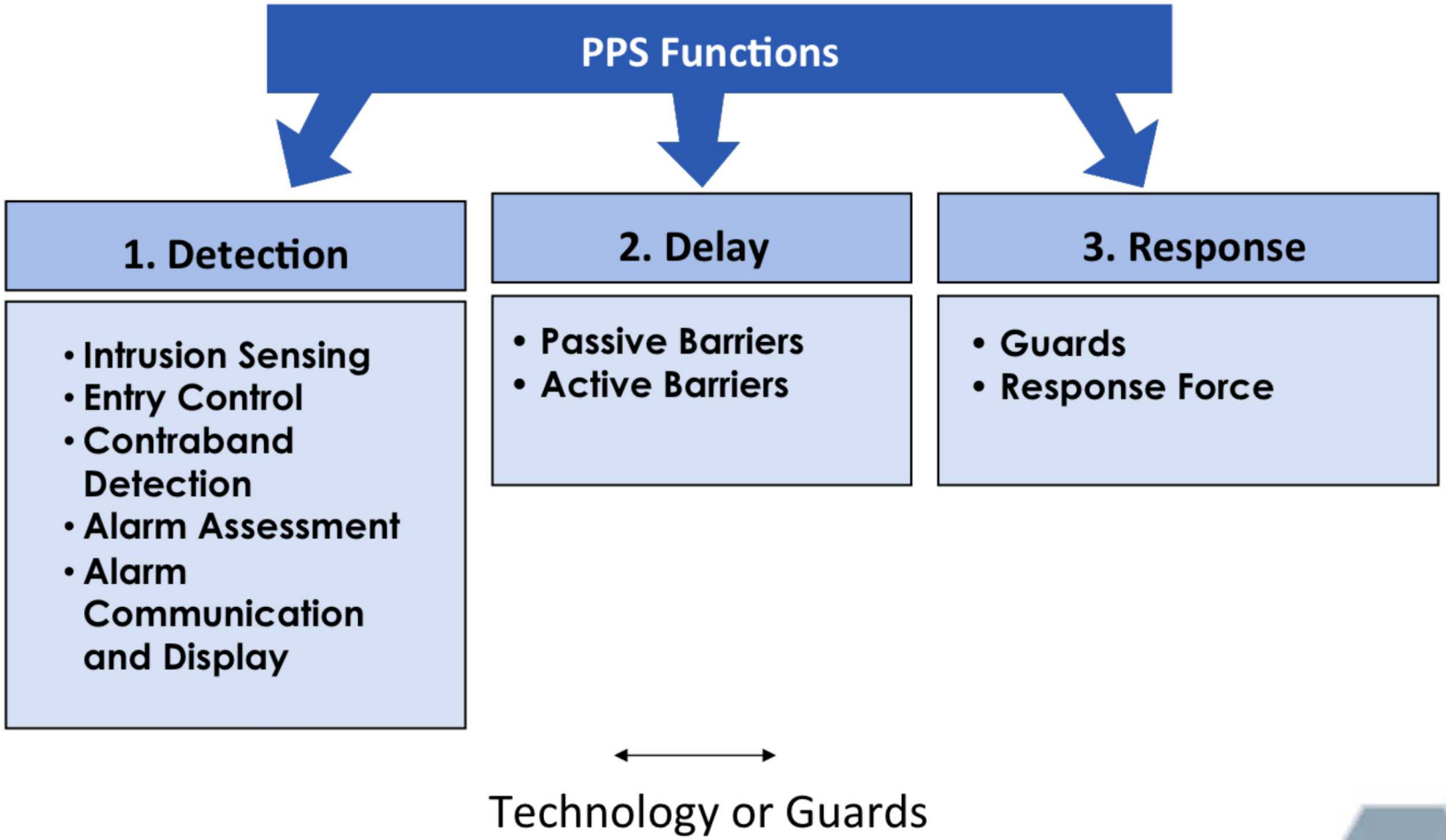
# Lecture Outline

1. Identify the three functions of a PPS
2. List the performance measures of a PPS
3. Describe the principle of timely detection
4. Discuss three system engineering design principles

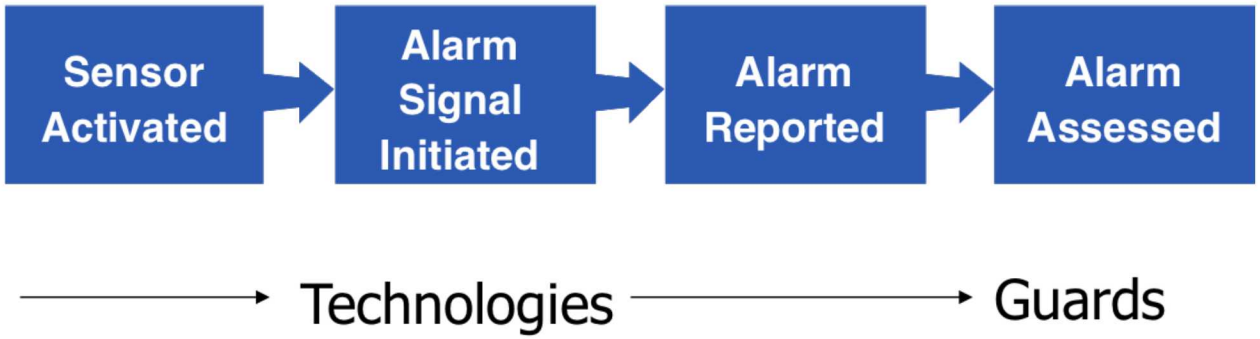
# Design and Evaluation Process Outline (DEPO)



# Three Functions of a PPS



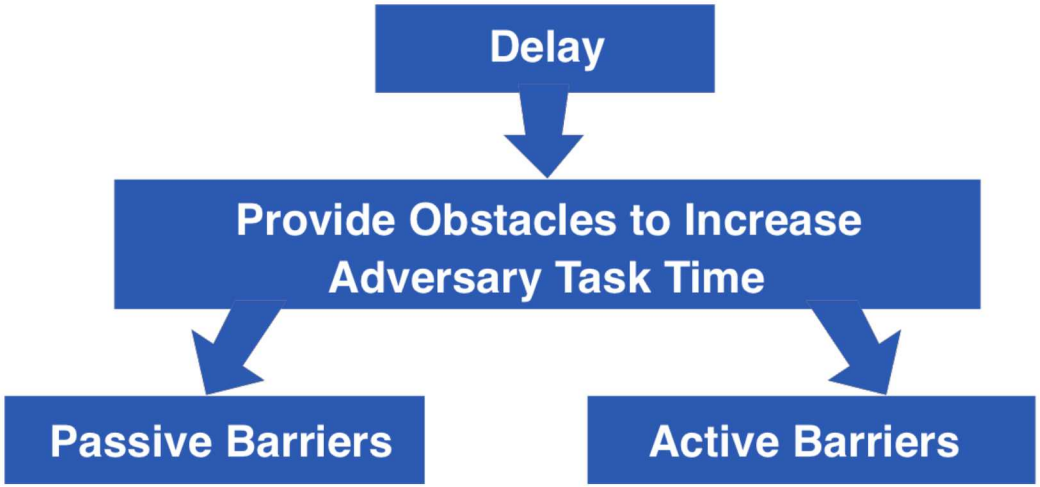
# Detection




Performance measures:

- Probability of sensor alarm ($P_S$)
- Communication and assessment time ($T_C$)
- Probability of correct assessment ($P_A$)
- Nuisance alarm rate (NAR)
- Probability of detection $P_D = F(P_S, T_C, P_A, NAR)$

# Delay




Performance measures

- Time to penetrate or bypass barriers
- Time to travel across areas

# Response


Performance measures

- Probability of communication to response force
- Communication time
- Probability of deployment to adversary location
- Deployment time
- Response force effectiveness (Probabilities of interruption ($P_I$) and neutralization ($P_N$))

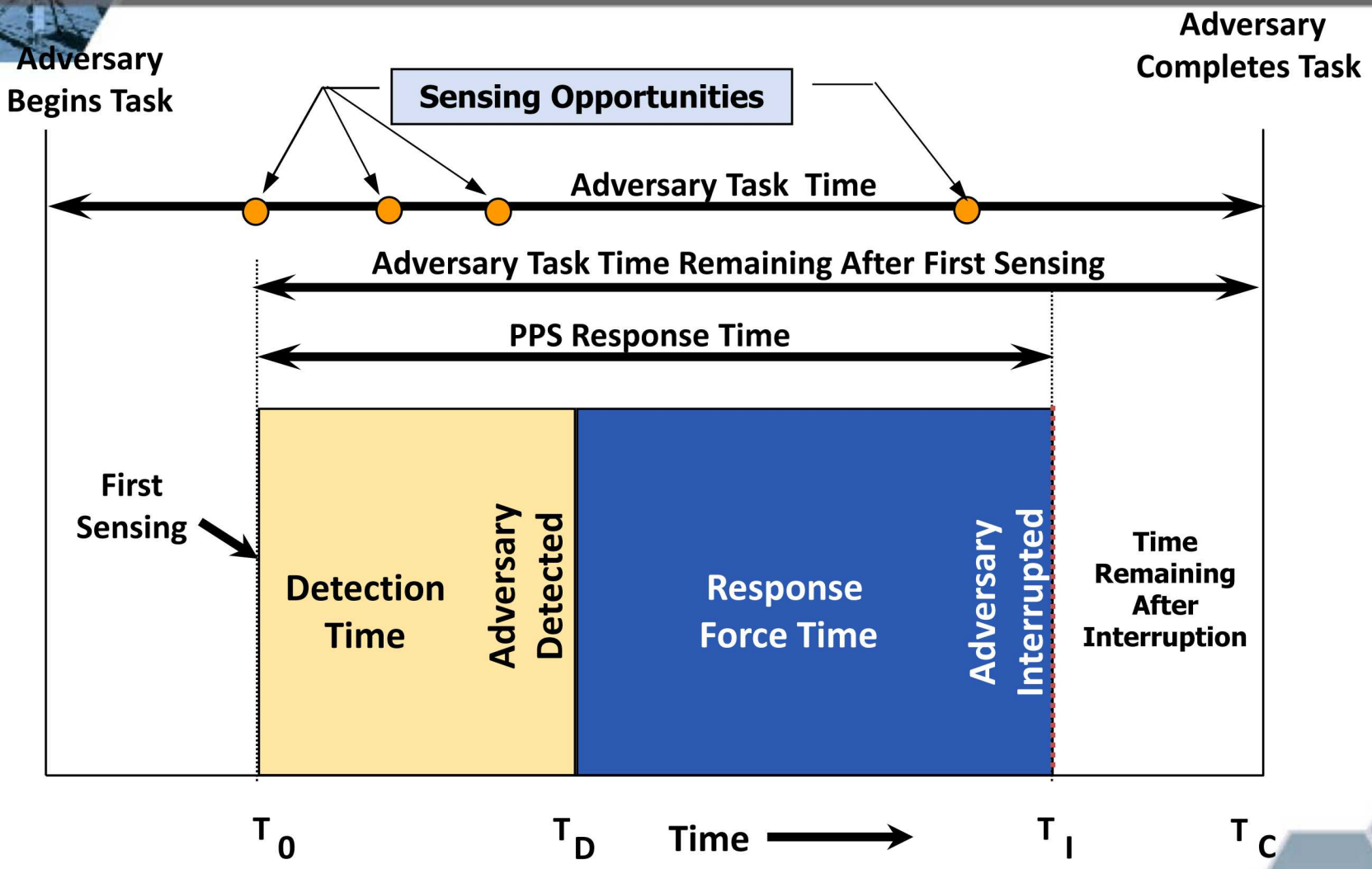
# Two Competing Timelines

- Adversary Timeline
  - Cross areas
  - Penetrate or bypass barriers
  - Remove or sabotage target
- PPS Timeline
  - Detection, Delay & Response process
- Overlay of two timelines illustrates requirement for PPS effectiveness

# Principle of Timely Detection

- To interrupt the adversary before the theft or sabotage task is completed, the PPS response time must be less than the adversary task time remaining after the first sensing.

# Adversary and PPS Timelines



# Principle of Timely Detection

- Critical Detection Point (CDP): The last sensing opportunity along an adversary path for which the PPS response time is less than the adversary task time remaining after the first sensing
- To be an effective PPS, timely detection must be achieved against the DBT along all adversary paths

# System Engineering Design Principles

- **Balance Protection**: provides adequate protection against all potential adversaries along all paths to the target
- **Defense in Depth**: uses multiple diverse protective measures along each potential adversary path
- **High Reliability**: implementing design features that reduce the likelihood of system failure

# Summary: PPS Design

- Three functions of a PPS
  - Detection, Delay and Response
- Competing Timelines
  - Adversary and PPS
- Timely Detection
  - To interrupt the adversary before the theft or sabotage task is completed, the PPS response time must be less than the adversary task time remaining after the first sensing.
- Design Principles
  - Balanced Protection
  - Defense in Depth
  - High Reliability

Module 10

# INTRUSION DETECTION SYSTEMS

# Lecture Outline

1. Identify the role of intrusion detection systems
2. Identify system classifications
3. Describe conditions that affect detection systems
4. Recognize the definition of “protection-in-depth”
5. Recognize system technologies
6. Recognize the characteristics of a good intrusion detection system design

# Role of Intrusion Detection Systems

- PPS functions
- Detection (Delay, Response)
  - Exterior intrusion detection
  - Interior intrusion detection
  - Assessment
  - Alarm communication and display
  - Entry control

# Role of Intrusion Detection Systems

- Probability of detection, $P_D = F(P_S, T_C, P_A, NAR)$
  - Probability of sensor alarm ($P_S$)
  - Communication and assessment time ($T_C$)
  - Probability of correct assessment ($P_A$)
  - Nuisance alarm rate (NAR)

Probability of Detection ($P_D$)

$P_D = P_S * P_A$

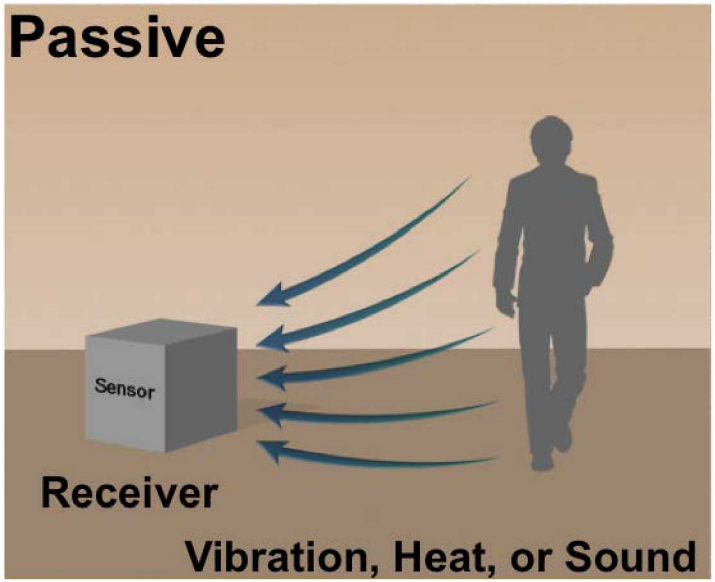
# System Classifications

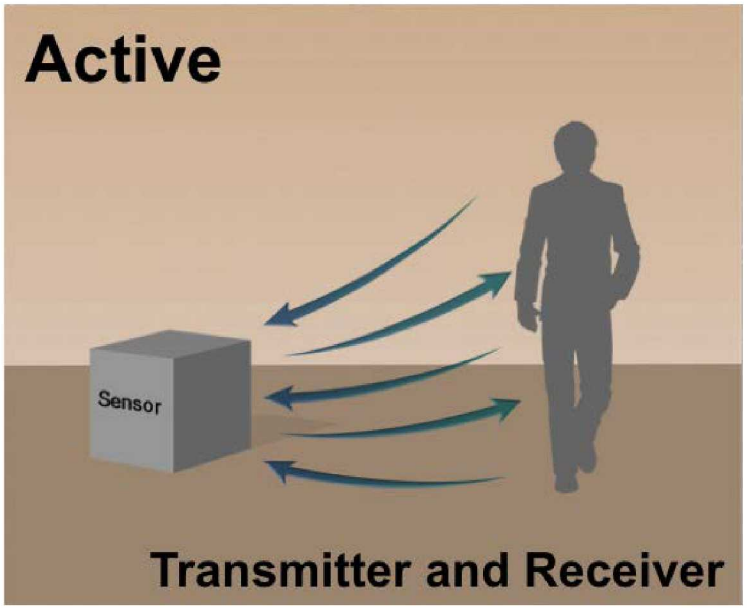
- Exterior and interior
  - Passive (P) or active (A)
  - Covert (C) or visible (V)
  - Volumetric (VOL) or line detection (L)
- Exterior only
  - Line of sight (LOS) or terrain following (TF)

# System Classifications: Exterior

| | Passive or Active | Covert or Visible | LOS or Terrain Following | Volumetric or Line Detection |
|---|---|---|---|---|
| **Buried Line** | | | | |
| Ported Coax | A | C | TF | VOL |
| Fiber Optic Cables | P | C | TF | L |
| **Fence Associated** | | | | |
| Fence Disturbance | P | V | TF | L |
| Sensor Fence | P | V | TF | L |
| Electric Field | A | V | TF | VOL |
| **Freestanding** | | | | |
| Active Infrared | A | V | LOS | L/VOL |
| Passive Infrared | P | V | LOS | VOL |
| Bistatic Microwave | A | V | LOS | VOL |
| Dual Technology | A | V | LOS | VOL |
| Video Motion | P | C | LOS | VOL |

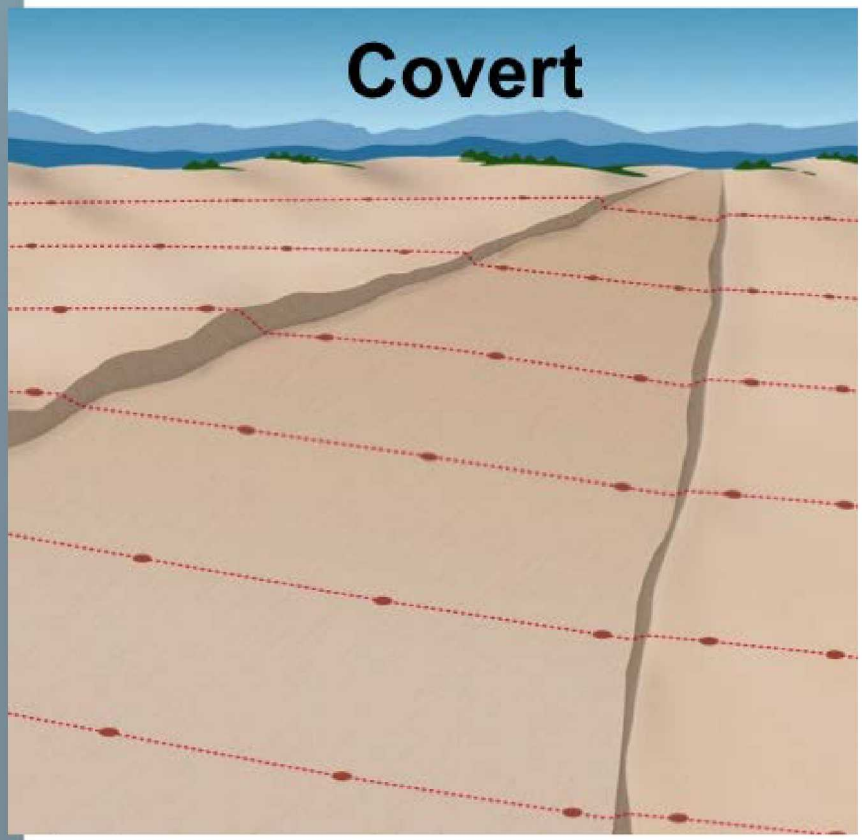
# Passive or Active



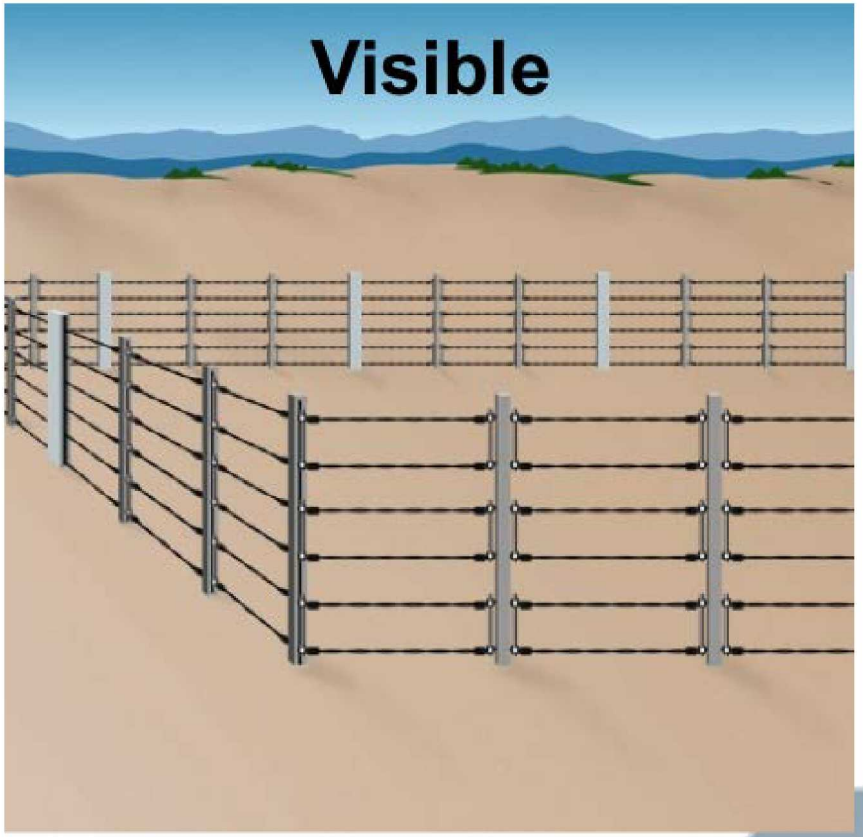



# Covert or Visible

- Sensors hidden from view
- More difficult for intruder to detect



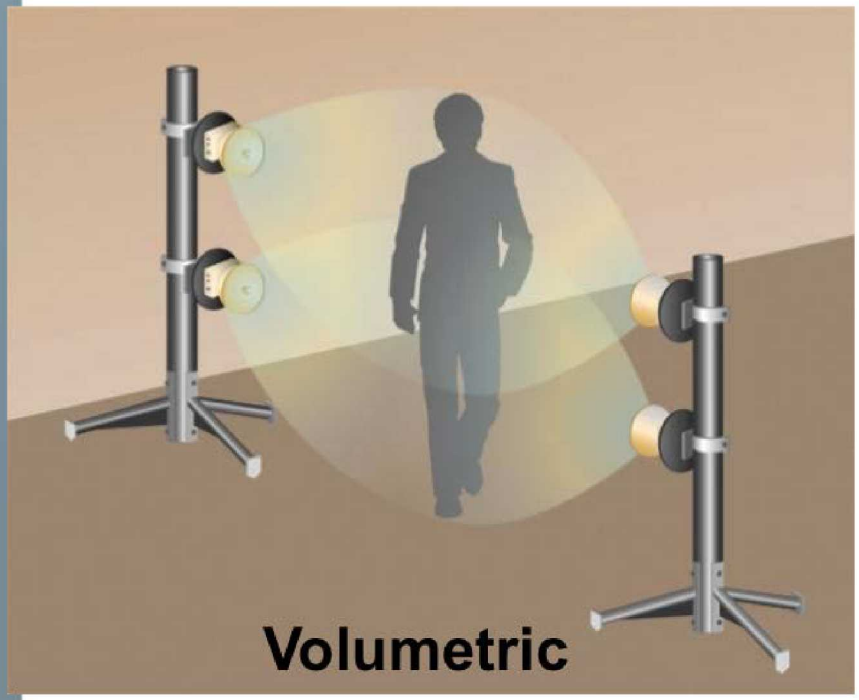

- Sensors in plain view
- Simpler to install and repair



# Volumetric or Line Detection

- Detection in a volume of space
- Detection volume is not visible

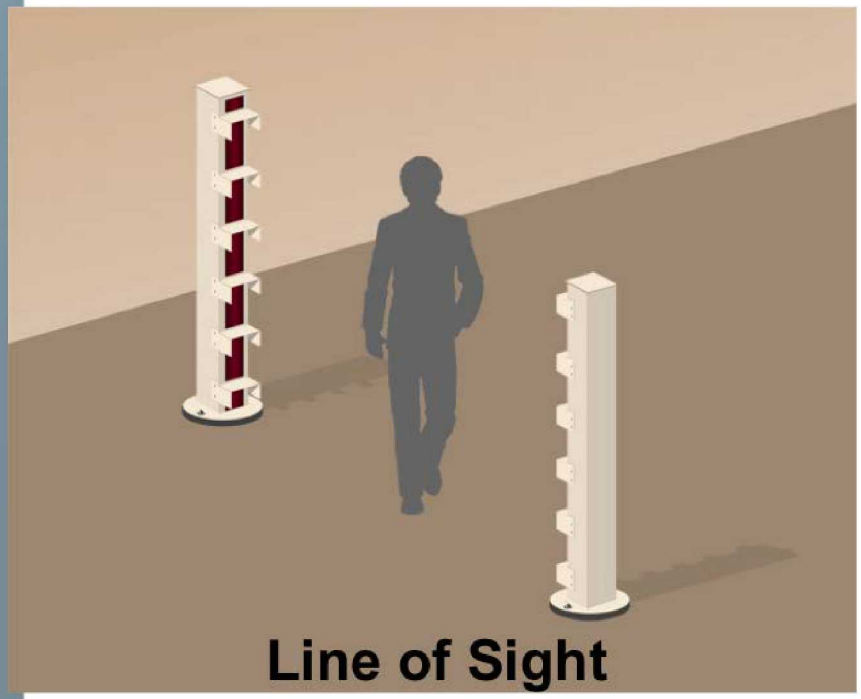
- Detection along a line or plane
- Detection zone easily identified

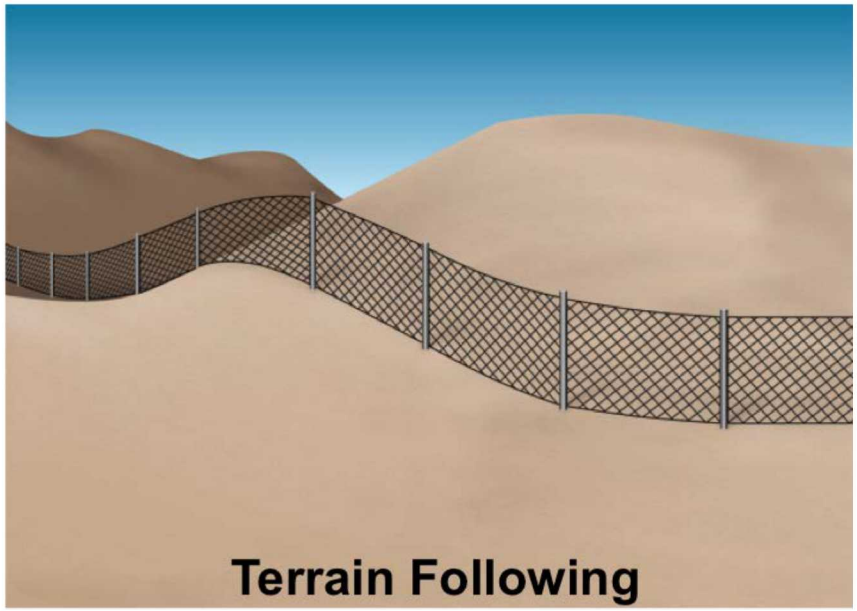



# Line of Sight or Terrain Following

- No obstacles in the detection space
- Requires flat ground surface

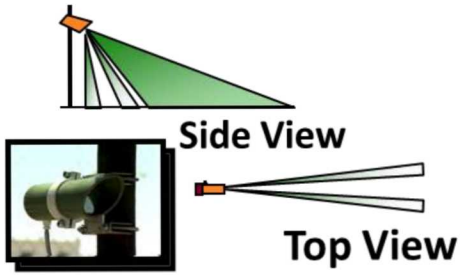
- Sensors detect over flat or irregular terrain



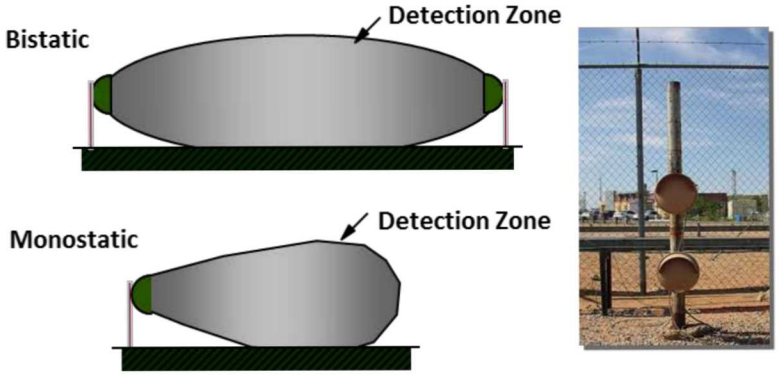
# Exterior Systems

Tautwire

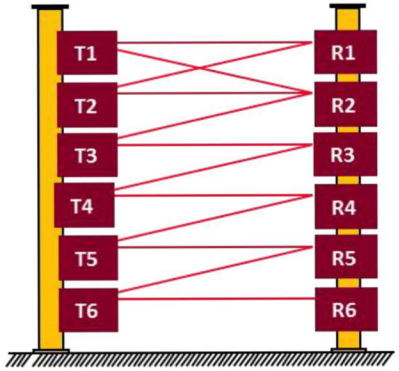



Passive Infrared

Fence Disturbance




Microwave



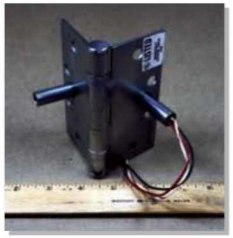

Active Infrared

# Complimentary Perimeter System

# System Classifications: Interior

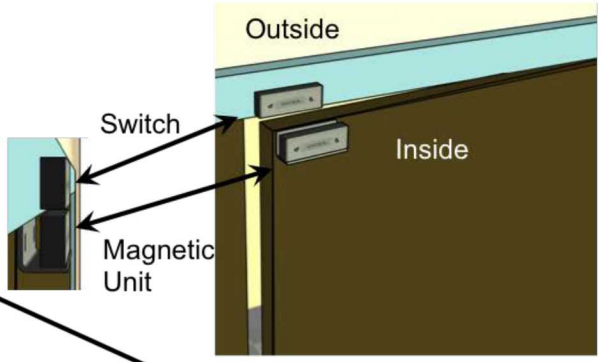
| | Passive or Active | Covert or Visible | Volumetric or Line Detection |
|---|---|---|---|
| **Proximity** | | | |
| Capacitance | P | V/C | VOL |
| **Interior Motion** | | | |
| Microwave | A | V | VOL |
| Passive Infrared | P | V | VOL |
| Dual Technology | A | V | VOL |
| **Boundary Penetration** | | | |
| Electromechanical (BMS) | P | V/C | L |
| Vibration | P | V/C | L |
| Glass Break | P | V/C | L |
| Active Infrared | A | V | L |
| Fiber Optic | P | C | L |

# Interior Systems



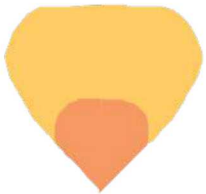
Covert BMS

Overt BMS

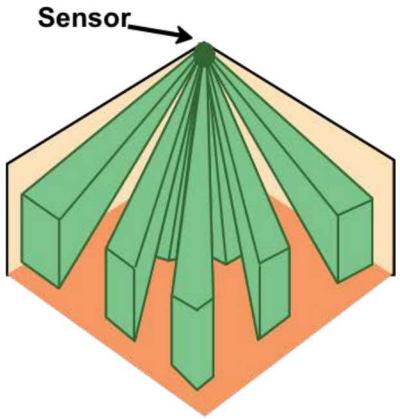


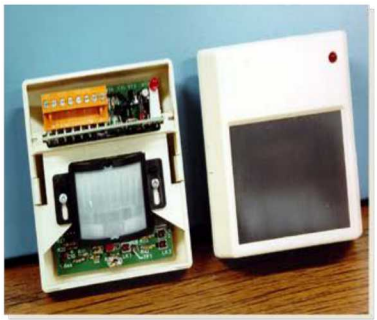

Balance Magnetic Switch


Vibration




Microwave

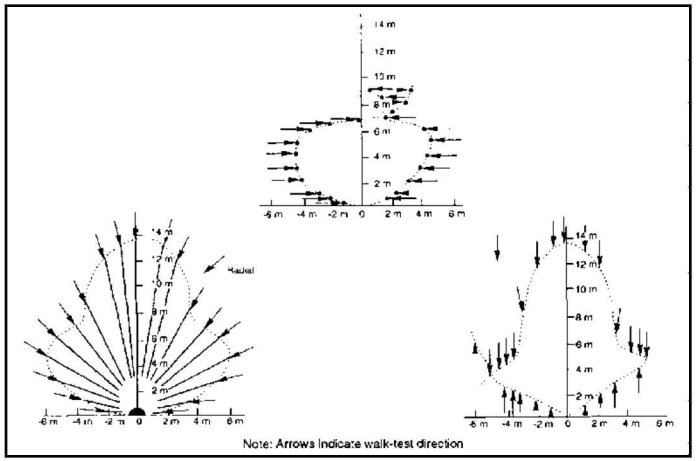


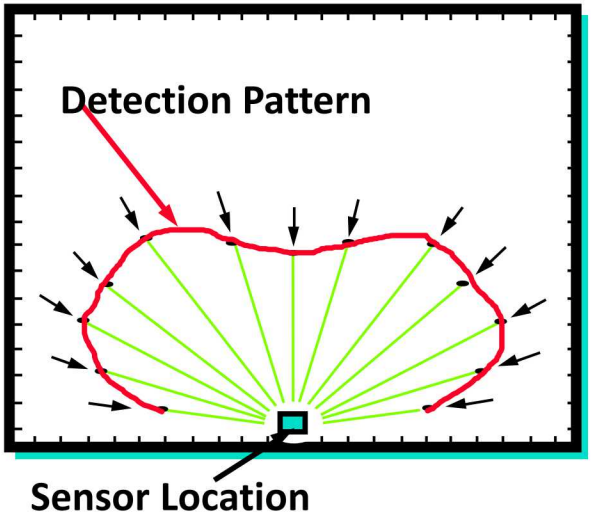
Passive Infrared

# Interior System Detection Zones

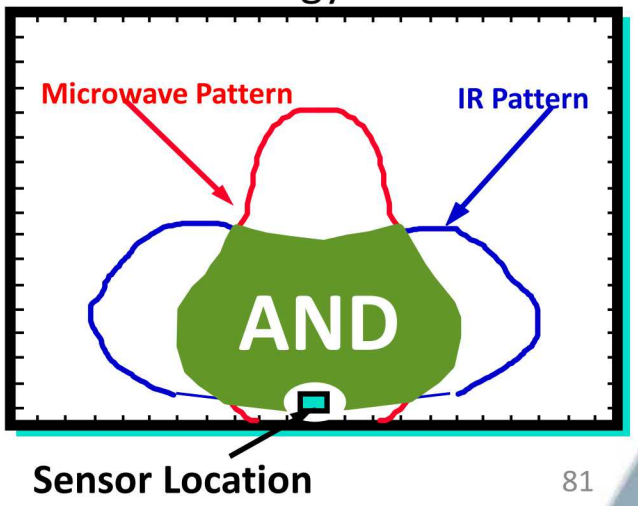
Interior Microwave




Passive Infrared



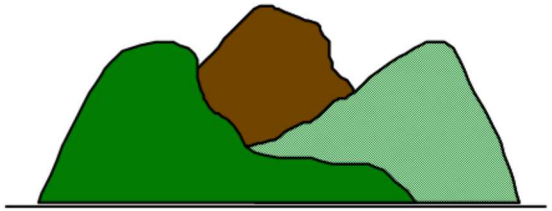

Dual Technology



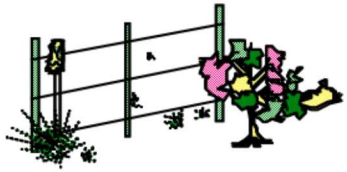

- Recorded Detection Zones Through Performance Testing
- Test various patterns and defeat strategies
- Consider various factors influence effectiveness

# Conditions that Affect Exterior Systems

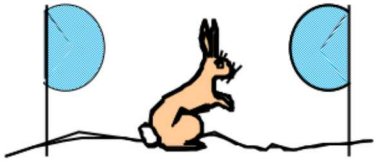
**Topography**



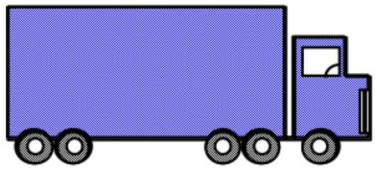
**Vegetation**

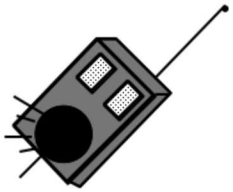


**Wildlife**

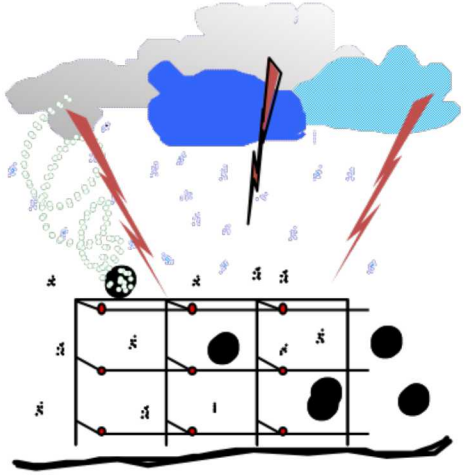


**Background Noise**

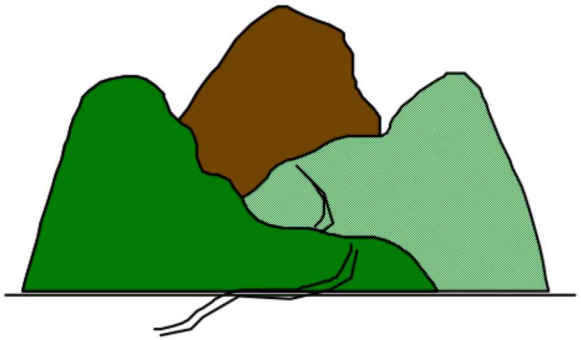




**Climate and Weather**



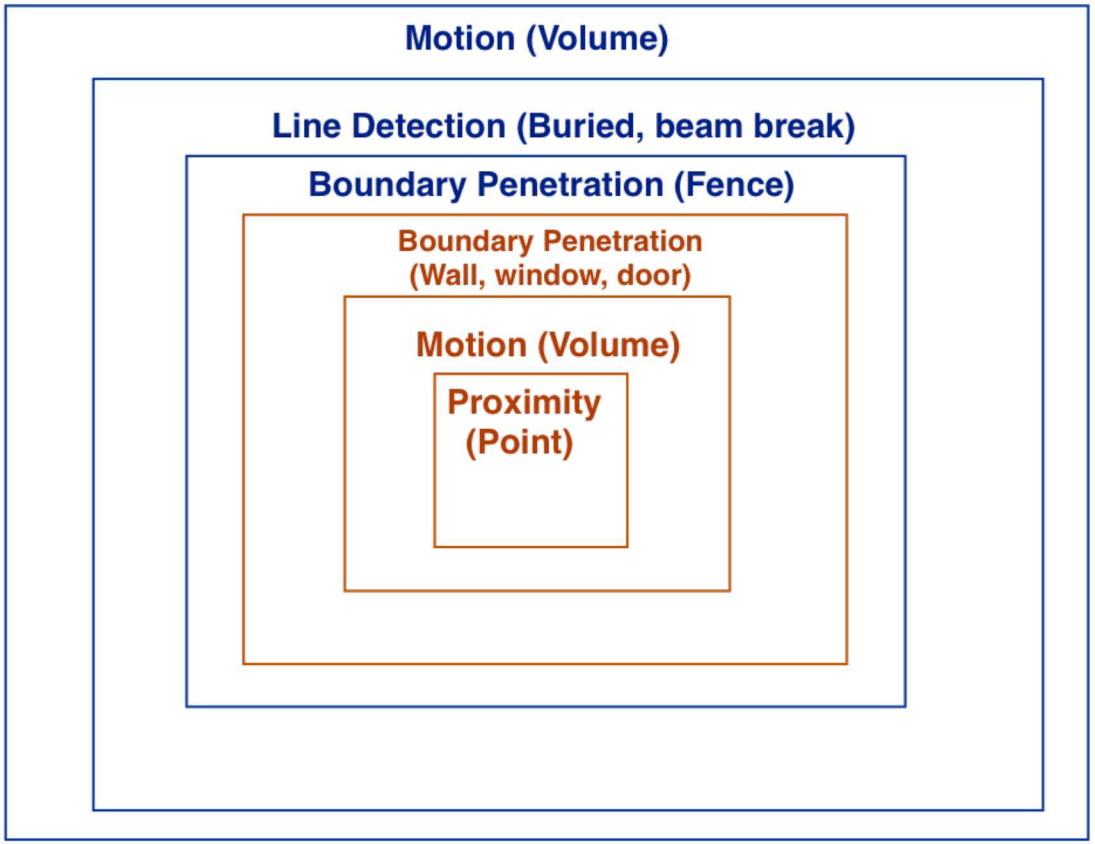
**Soil and Pavement**



# Conditions that Affect Interior Systems

- Electromagnetic radiation
- Nuclear radiation
- Acoustic energy
- Thermal radiation
- Optical effects
- Seismic phenomena
- Meteorological conditions

# Protection in Depth Definition




**Exterior Sensor Applications** **Interior Sensor Applications**

# Good Intrusion Detection System Design

- Continuous line of detection
- Protection in depth
- Complementary sensors
- Alarm combination and priority schemes
- Clear zone
- Sensor configuration
- Site-specific system
- Tamper indication
- High $P_D$

# Good Intrusion Detection System Design

- Suitable for physical and environmental conditions
- Low NAR and FAR
- Is properly installed: no loose mountings, wiring in conduit, proper location for sensors
- Self test capability
- Integration with barrier delay
- Integration with assessment system

# Summary: Intrusion Detection Systems

- Identify the role of intrusion detection systems
- Identify system classifications
- Describe conditions that affect detection systems
- Recognize the definition of “protection-in-depth”
- Recognize system technologies
- Recognize the characteristics of a good intrusion detection system design

Exercise

# SENSOR EXERCISE #1

Module 11

# ENTRY CONTROL & CONTRABAND DETECTION

# Lecture Outline

1. Recognize the purposes of entry control
2. Identify the fundamental criteria of entry control
3. Discuss different examples of entry control elements and technologies
4. Recognize the features of a good entry control system
5. Define contraband
6. Describe different types of detection

# Purposes of Entry Control

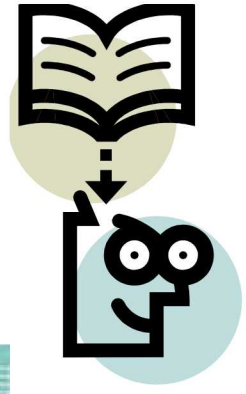
- The purpose of a perimeter security system is to provide a boundary around an area to prevent or detect unauthorized penetrations.
- The purpose of entry control is to complete that boundary in a way that securely allows authorized persons and materials to move in and out through that boundary.

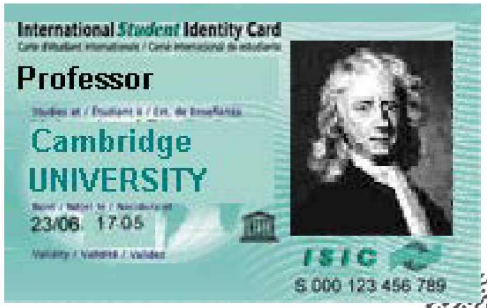
# Purposes of Entry Control

- The System must:
  - Allow entry of **authorized** persons
  - Prevent entry of **unauthorized** persons
  - Allow exit of **authorized** persons

# Fundamental Criteria of Entry Control

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





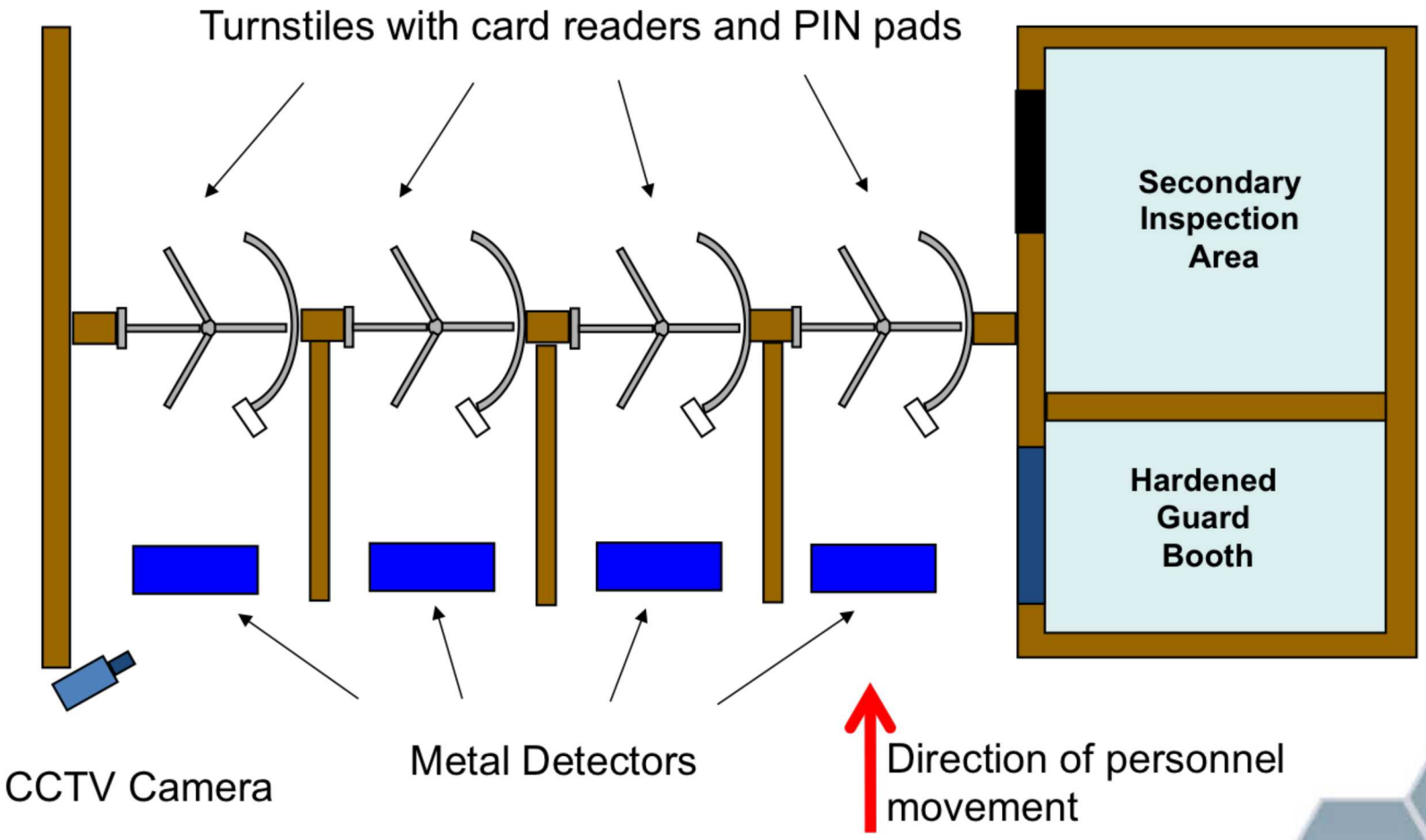

# Examples of Entry Control Elements and Technologies

***Combining two or all three criterion greatly increases security***

Badge swipe and PIN

Hand-geometry Biometrics

# Examples of Entry Control Elements and Technologies




***Application of Design Criteria***

# Features of a Good Entry Control System

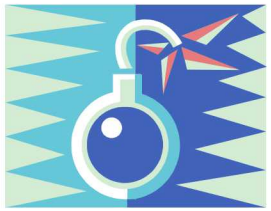
- Integration with the boundary
  - Cannot be bypassed
  - Block individuals until access authorization verified
  - Interfaces with alarm system
- Integration with the guards/response force
  - Protects guards
  - Area is under surveillance
  - Adequate training and procedures in place

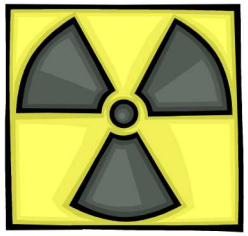
# Features of a Good Entry Control System

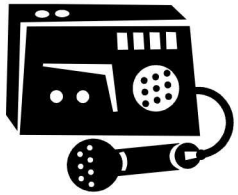
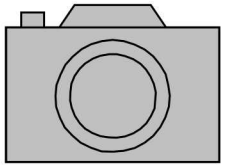
- Personnel integrate with system
  - Easy to use for entry and exit
  - Accommodates peak throughput (loads)
  - Accommodates special cases
  - Consider compensatory measures
  - Utilize Graded approach
  - Consistent performance testing program

# Contraband Defined

- Any object or material that is prohibited in a security area; also any device or material that can be used by an adversary to gain an advantage in an attempt to commit an act detrimental to a facility.




# Metal Detection

- Types of detectors
  - Continuous wave
  - Pulsed field
  - Magnetometer
- Factors that affect sensitivity
  - Orientation
  - Ferromagnetic materials
  - Shape
- Installation and use
- Weapons, shielding, and bomb detection

# Factors that Affect Operation of Metal Detectors

- Environment
  - Metal doors
  - Metal cabinets
  - Equipment operating nearby (example: fork lifts)
  - Electromagnetic sources (examples: radio transmitters, fluorescent lights)
- Type of metal
- Size and shape of object
- Orientation of metal object
- Location of metal object
- Speed

# Explosive Detection: Bulk vs. Trace

- Bulk
  - Detect a macroscopic amount of explosive directly
    - Guards, X-rays, personal search

- Trace
  - Detect minute amounts of residual explosive material in the form of vapor or particles
  - The vapor pressure of an explosive affects detectability
    - Ex: Nitroglycerin vs. trinitrotoluene (TNT) [340 vs. 8 parts per billion]

Personnel Portal


Bench top for swipe applications


Hand-held

# Trace Detection: Canine

- Method of choice for search applications – high mobility and ability to follow scent to its source
- Very fast and sensitive under optimal conditions; can detect any explosive
- Problematic for
  - Long-term, repetitive applications (dogs become tired)
  - Screening people (fear of dogs)
- Low purchase cost (~$10,000), but substantial upkeep costs (intensive training)
- Dogs available from a variety of sources

# Effective Contraband Detection

- A good system integrates complementary techniques
  - e.g. metal detection (for shielding) + radiation detection
- Consider the DBT for the types and amounts of weapons, tools, explosives
- Multiple methods and utilizing a graded approach
- Compensatory measures in event of failure
- Balance between guard force and technology
- Consider local rules, regulations and customs

# Summary: Entry Control

- The purpose of entry control is to allow authorized persons to move in and out through a protected area boundary
- Fundamental criteria:
  - Something you know
  - Something you have
  - Something you are
- Entry control elements include PINs, credential (bar code, magnetic strip, proximity, RFID, etc.) and biometric (fingerprint, hand geometry, facial recognition, iris scan, etc.) technologies
- A good entry control system addresses the interface with the protected area boundary, with the guard force and with personnel

# Summary: Contraband Detection

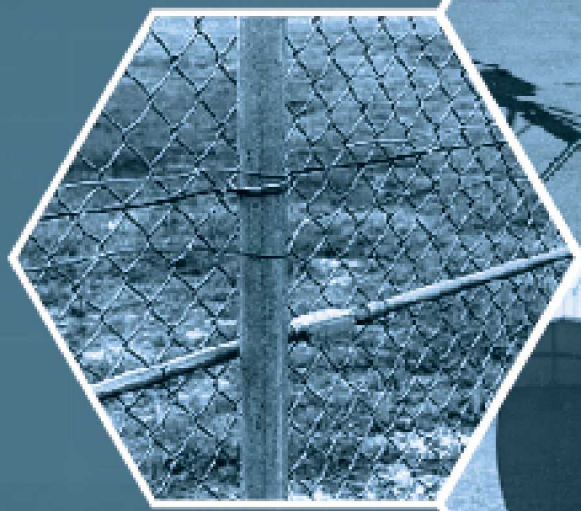
- Contraband is an item you prohibit in an area
  - weapons, tools, explosives, controlled material (NM)
- Techniques covered included:
  - Manual search (everything)
  - Metal detection (weapons, tools)
  - Package x-ray inspection (weapons, tools, explosives)
  - Explosives detection
  - Radiation detection (NM)
- A good system integrates complementary techniques
  - e.g. metal detection (for shielding) + radiation detection
- The DBT lists the types and amounts of weapons, tools, explosives you need to consider for contraband detection

Exercise

# SENSOR EXERCISE #2

# Day 2 Summary

- Target Identification
- Threat Definition
- Risk Management
- Introduction to PPS Design
- Intrusion Detection Systems
- Entry Control and Contraband



# Foundations of Physical Protection Systems

Day 3

# Day 3 Agenda

- Review of Day 2
- Alarm Assessment, Communication & Display
- Access Delay
- Response
- Performance Testing Measures

# DAY 2 REVIEW

Module 12

# ALARM ASSESSMENT, COMMUNICATION & DISPLAY

# Lecture Outline

1. Identify the purpose and methods of alarm assessment for a physical protection system
2. Recognize key differences between assessment and surveillance
3. Discuss the different levels of assessment resolution
4. Explain the role of alarm communications and display (AC&D) in the security system

# Purpose and Methods of Alarm Assessment

- Alarm assessment
  - Security operator determines the cause of an alarm
  - Completes the detection function
- Provides information if alarm is real or Nuisance/False alarm
- Provide information for response force action:
  - How many intruders
  - What equipment are intruders bringing in


**Detection is not complete without Assessment**

# Purpose and Methods of Alarm Assessment: Personnel Methods

**Advantages**

- Can provide detection capabilities
- Flexible deployment
- If intrusion, can provide immediate delay/response

**Disadvantages**

- Time between alarm and assessment reduces probability of correct assessment
- Can only tolerate a very limited number of nuisance alarms
- Manpower costs - expensive

# Purpose and Methods of Alarm Assessment: Technology Methods

## Advantages

- Minimal time between alarm and assessment
- Pre-alarm and post-alarm recording possible
- Efficient use of people
  - One person assess multiple areas
  - Operator alerted to alarm
  - Nuisance alarms quickly assessed
  - Electronics perform fairly consistently

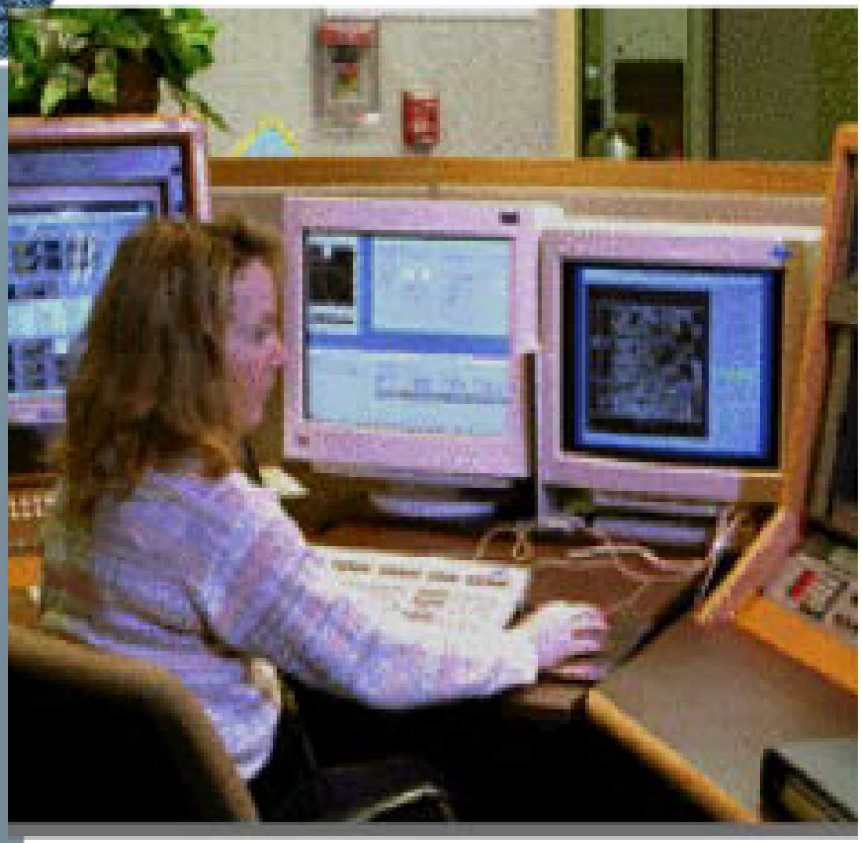
## Disadvantages

- Initial expense for infrastructure may be high
- Ongoing maintenance and testing
- Response force dispatch may be necessary for some events

# Key Differences Between Assessment and Surveillance

- **Assessment**: video display triggered by sensor alarm to determine if an intruder has penetrated a censored area

# Key Differences Between Assessment and Surveillance



- **Surveillance**: Continuous video monitoring of an area that does NOT have sensors

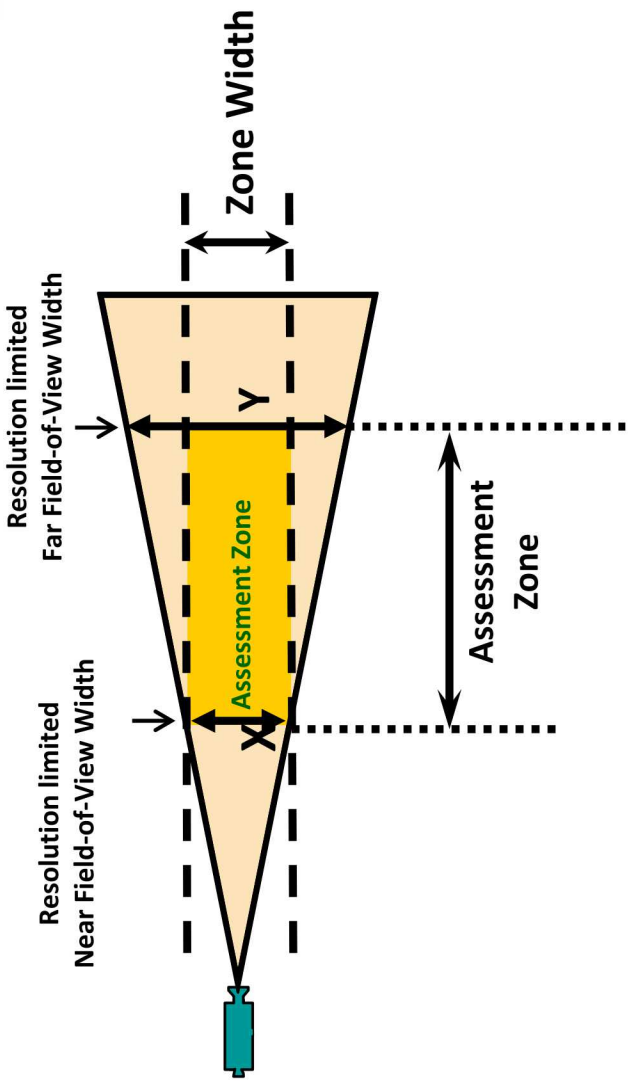
# Major Alarm Assessment Components

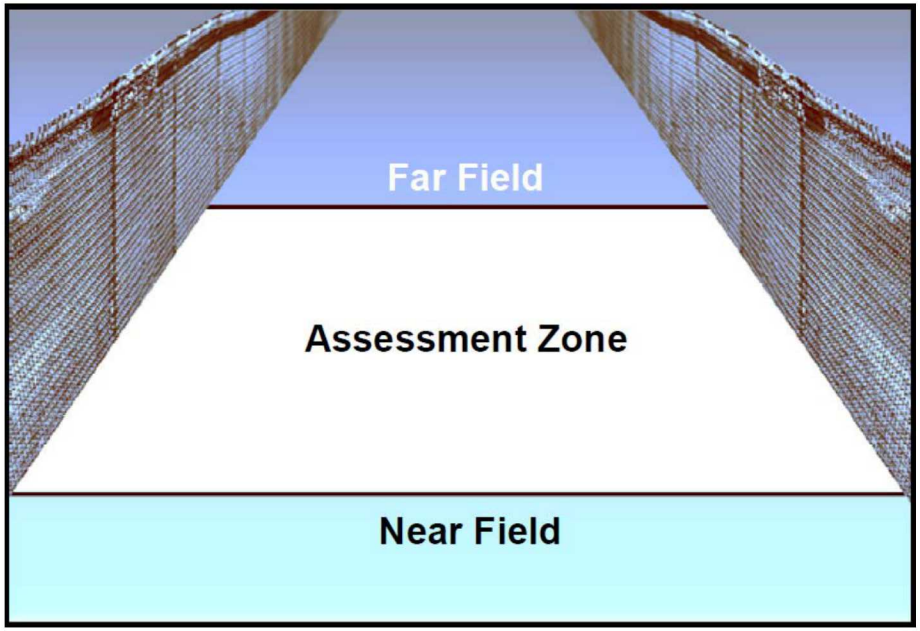
| Cameras | Lenses | Lighting |
|---|---|---|
| Color vs. B/W | Determines size of scene image captured | Illuminates scene for night assessment |
| Day/Night | Format | Allows camera to produce usable video |
| Infrared-enhanced | Focal length | Provide lighting for response personnel |
| Camera/Thermal Imager | Field of view | |
| | Aperture | |
| | Resolution | |

# Video Surveillance Application

- Low probability of detection
  - Used when time is not critical to an event
- Technology usually visible to public and used as a deterrent
- Loss of video leaves a single point failure in both the assessment and detection of the intrusion
- Can be useful for specific situations, such as extra coverage during deliveries or construction work
- Is usually only effective for short periods and for one person covering a single area

# Assessment Area: Monitor View



# Assessment Resolution

**Detection**: determine the presence of object

**Classification**: determine nuisance or real alarms

**Identification**: determine the identity of object

# Role of Alarm Communications and Display (AC&D)

- An alarm communication and display (AC&D) system transmits alarms signals from electronic devices and systems to a monitoring station and displays the information to an operator for action.

# Communication & Display

- Alarm display is best understood by the following questions:
  - What information should be presented to the operator?
    - Zone status (secure, access, alarm)
    - Geographical locations
    - Procedural instructions
    - System status
    - Alarm history

# Communication & Display, cont'd.

- When should this information be presented (always, upon alarm, when requested)?
- How should the information be presented?
- How does the operator communicate with the system?
- How should the equipment be arranged at the operator's workstation?

# Summary: Assessment and AC&D

- Detection is not complete without Assessment
- The Key aspects and functions of the AC&D systems are:
  - Alarm Communication – how does information get from field to alarm station?
  - Alarm Display – what information should the operator see? How? When?
  - Operator – how does information undergo assessment?

# Summary: Assessment and AC&D, cont'd.

- AC&D Systems allow for alarm assessment
  - Completes the detection process by determining the cause of a sensor alarm through either technology or personnel
  - Assessment = video triggered by a sensor vs. surveillance = continuous video
- Assessment resolution has three levels:
  - Detection (lowest resolution)
  - Classification (middle resolution)
  - Identification (highest resolution)

Video

# DETECTION PERFORMANCE TESTING VIDEOS

Exercise

# SENSOR EXERCISE #3

Module 13

# ACCESS DELAY

# Lecture Outline

1. Identify the purpose of delay systems
2. Discuss three characteristics of a good barrier system design
3. Recognize the definition of penetration
4. Explain why detection must occur before delay

# Purpose of Delay Systems

- Access Delay: The element of a physical protection system designed to slow an adversary by use of physical barriers, activated delays, or responders after they have been detected.

# Penetration: Definition

- Penetration: When a person can pass through, over, under, or around the barrier
  - Penetration delay times depend on the type of attack, location of the attack, and the tools used
  - Multiple different barriers can extend penetration times

# Types and Characteristics of a Good Barrier System Design

## Response Force Guards

- Flexible
- Continuous operational cost
- Sensitive to numbers
- Subject to compromise

## Fixed or Structural Barriers

- In place; fail secure
- Commercially available
- Various vehicle barriers
- Weak against explosives
- Operational; aesthetic limits

## Dispensable Barriers

- Compact; rapidly deployed
- Maximize delay at target
- “Somewhat” threat independent
- Spurious activation; safety concerns

# Detection before Delay

- Delay should:
  - Follow detection
  - Be maximized at the target for cost effectiveness
  - Utilize balanced protection at layers
  - Be in depth with multiple barrier layers requiring the adversary to use different skills, better planning, and a variety of tools to defeat

# Possible Tools of an Adversary

# Structural Barriers

- Include walls, doors, windows, utility ports, roofs, and floors
- Conventional construction provides minimal delay against formidable threat
- Delay time depends on tools and type of attack
- Barriers can detain an adversary at predictable locations
- Multiple and different barriers are effective
- Barriers close to assets are usually the most cost effective

# Structural Barriers

- Access delay features should be present 100% of the time, or take compensatory measures
- Example—This massive door only provides delay <u>when closed and locked</u>
- Balance delay for all attack paths
- Integrate detection and response measures

# Attributes of Dispensable Barriers

- Exert minimum impact on operations
- Afford volume protection
- Provide adequate safety to personnel
- Operate independently of other barriers
- Offer multiple activation options
- Have long storage life
- Provide maximum delay at target
- Can be cost effective

# Dispensable Materials

Cold Smoke
Chemical Obscurant

Rigid Polyurethane Foam

Sticky Thermoplastic Foam

Aqueous Foam

Pyrotechnic Obscurant (Smoke)

# Summary: Delay

- Access Delay: The element of a physical protection system designed to slow an adversary by use of physical barriers, activated delays, or responders after they have been detected.
- Three characteristics of a good barrier system are:
  - Provides delay after detection
  - Exhibits balanced design; no weak links
  - Uses delay-in-depth

# Summary: Delay, cont'd.

- Penetration: when a person can pass through, over, under, or around the barrier
- Delay ONLY occurs after detection, assessment, and notification of the response force occurs, otherwise the delay does not factor into the PPS Timeline.

Video

# ACCESS DELAY PERFORMANCE TESTING VIDEOS

Module 14

# RESPONSE

# Lecture Outline

1. Distinguish between response force and guard functions
2. Discuss the two response force measures of performance
3. Discuss four major response strategies (methods of evaluating)
4. Identify the importance of adequate equipment and training

# Difference Between Response Force and Guard Force Duties

**Guard Forces**

- A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals during transport, controlling access and/or provide initial response

**Response Forces**

- Persons, on or off-site, who are armed and appropriately equipped and trained to counter an attempted unauthorized removal of nuclear material or an act of sabotage

# Legal Basis for Guards and Response Force

- Arrest authority and use of force by guards and response force officers typically has a basis in law.
- Some countries such as the United States allow the use of deadly force (neutralization) by non-police or military response forces.
  - Use of force does not always imply deadly force
  - Section 161k of the Atomic Energy Act of 1954 authorizes DOE and its contractors to use appropriate force to protect its facilities
  - US state laws govern the use of weapons by guards at NRC-licensed facilities

# Legal Basis for Guards and Response Force

- Use of force does not always imply deadly force
  - Force Continuum: A method established to direct response forces to use the minimum amount or force necessary to: control the situation, make an arrest, or perform other actions to stop the action of adversaries and prevent a malevolent act
  - Rules of Engagement: Define when a response force can use weapons against an adversary

# Force Continuum

**Presence ⇉ verbal ⇉ use of hands ⇉ less lethal ⇉ deadly force**

| Force Continuum | | | | | |
|---|---|---|---|---|---|
| Level of Force | | Method of Force | | Level of Resistance | Threat |
| VI | Deadly | Any force readily capable of causing death or serious physical injury | | Lethal | RESISTIVE |
| V | Serious Physical Control | Neck Restraint<br>Impact Weapon<br>Focused Blows<br>Mace (CN/CS) | OC RESTRAINTS | Omnious | |
| IV | Physical Control | Hair Takedown<br>Joint Takedown<br>Digital Control<br>Joint Come-along<br>Pressure Points<br>Electronic Stun Device<br>Temp. Restraints | | Active<br>Static | |
| III | Physical Contact | Escort Position<br>Directional Contact | | Verbal | Undecided |
| II | Verbal Communication | Direct Order<br>Questioning<br>Persuasion | | | |
| I | Presence | Display of Force Option<br>Body Language/Demeanor<br>Identification of Authority | | None | Complying |

***OC*** **oleoresin capsicum (Pepper Spray)**

***CN*** **chloracetophenone (Tear Gas)**

***CS*** **Ortho-chlorobenzalmalononitrile (Double Action Chemical Irritant)**

# Response Force Measures of Performance Overview

- Performance Measures
  - Interruption – The successful arrival of the response force at an appropriate location to stop the adversary.
  - Neutralization – When the response force kills, captures, or causes the adversary to flee before the adversary is able to complete their task.
- Methods of Evaluating
  - Limited Scope Performance Tests
  - Full Scale Performance Tests (Force on Force)
  - Computer Models
  - Expert Judgment

# Interruption

- Communication
  - Probability of communication to response force
- Deployment of the response force
  - To correct location
  - In time to stop the adversary

**Right time**

**Right place**

- Tactical requirements / training
  - Individual and team movement skills
  - Adequate use of cover and/or concealment
  - Actions on contact
    - Chance contact
    - Ambush response
  - Proper use of weapons
    - Understanding of limitations

# Neutralization

- Difficult to measure – methods include:
  - Limited Scope Performance Tests (LSPT)
  - Force-on-Force exercises
  - Subject matter experts
  - Computer models
    - Commercial
    - Proprietary

**Right plans, people, equipment, and training**

# Types of Response Force Strategies

- **Containment** : Preventing adversaries from leaving the site with an asset.
- **Denial**: Preventing adversaries from getting to 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.

# Defense in Depth

- Provides integrated, in-depth protection of site security assets.
- System should be organized in depth and contain mutually supporting elements coordinated to prevent gaps in responsibilities and performance.
- Protective force is dynamic link between each of the elements and ensures integration.
- Develop response plans to ensure potential weaknesses in physical security system are covered by protective force personnel.

# Equipment

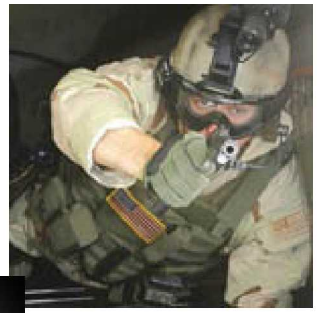
- Wide variety of types and models of equipment
  - Weapons (various types)
  - Protective gear (body armor and helmet, gas masks, chemical/biological suits)
  - Breaching equipment
  - Miscellaneous (flashlights, vest, night vision, handcuffs)
- Response equipment
  - Consider response equipment as a system, not as individual pieces of gear
- Consider DBT when determining what equipment is necessary

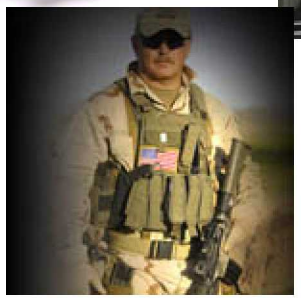
# Equipment

**Weapons**

**Protective Gear**


**Breaching Equipment**





**Miscellaneous**

# Response Force Survivability

- Response force survivability considerations
  - Based on DBT capability
  - Site-specific requirements
  - Target locations
  - Capabilities
  - Armored vehicles
  - Hardened posts
  - Fighting positions
  - Tactics
  - Training

# Response Force Survivability



**Armored Vehicles**

**Hardened Fighting Posts**

**Portable Fighting Positions**

# Training

- Critical part of the response force program
- Complex, dynamic response requirements require sustained, dynamic training
- Training should
  - include all contingency missions
  - be scenario-based and in a realistic environment
- Training schedule should be designed based on training needs analysis

# Interaction with Outside Agencies

- If the facility is utilizing outside or off-site agencies, protection requirements need to be carefully documented and rehearsed.
  - Written agreements or understandings
  - Key issues for consideration:
    - Role of support agencies
    - Agreements should be specific (number of responders, response time, locations of road blocks, etc.)
    - Integrated communications with support agencies
    - Off-site operations
  - Joint training exercises and validations

# Command, Control, and Communications (C3) Overview

- **Command**:  Exercise of authority (Decision making)  by response force leaders
- **Control**: Direction by response force leaders over assigned personnel to accomplish the mission
- **Communications**: Allow real time communication between the central alarm station, tactical leaders and response force in the field and allows tactical leaders to direct the actions of the response based on adversary actions.

# Summary: Response

- Guards and response forces have different response functions and authority, which should be based on a legal framework
- Response force measures of performance:
  - Interruption: successful arrival of response force to an adversary location
  - Neutralization: when response force kills, captures, or causes adversary to flee
- Response Strategies are based on the target (theft or sabotage) and include containment, denial, recapture, and pursuit/recovery
- Adequate equipment, training, and a robust command, control and communication system are essential for response effectiveness.

Discussion

# RESPONSE DISCUSSION

Module 15

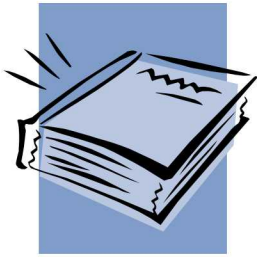
# PERFORMANCE TESTING MEASURES

# Lecture Outline

1. Identify what is performance testing.
2. Recognize performance testing recommendations from INFCIRC/225/Revision 5
3. Identify the purposes and importance of a guard/response testing program
4. Provide an overview of what a guard/response performance testing program must accomplish
5. Recognize the performance measures for a guard/response force
6. Recognize the three levels and associated tests of guard/response performance testing

# What is Performance Testing?

- Performance Testing is a means to realistically performance test the effectiveness of response force programs



- Testing the performance of
  - People (response force, guards, emergency services)
  - Equipment (weapons, vehicles, body armor)
  - Procedures (response, entry control, CAS)
- Performance Testing considers the following areas:
  - Planning (chain of command; area knowledge)
  - Tactics (cover and concealment; weapons limitations)
  - Training(protected targets; adversary scenarios)
  - Practice (maintain skills; contingency plans)

# Performance Testing Recommendations from INFCIRC/225/Revision 5

- Evaluations include exercises to test integrated system, including training and readiness of guards and response forces
- Operator should develop and implement means and procedures for evaluations, including performance testing and maintenance of the PPS
- Performance testing a PPS should include exercises to evaluate guards and response force effectiveness and timely response
- Performance testing of a PPS should be conducted annually

# Performance Tests

- *Performance test:* A test to evaluate the ability of an operating system element or total system to meet an established requirement
- Performance tests are methodical means to:
  - Establish or confirm a performance level of a PPS element
  - Provide comprehensive assurance of performance on a required basis
  - Determine element's baseline performance for system design
  - Test PPS elements over their planned range of operation
- Performance testing results
  - Identify if element(s) tested performed adequately
  - If not, identifies the weakness or substandard perform

# Purpose and Objectives

- Purpose of performance testing is to evaluate the performance of
  - People,
  - Procedures, and/or
  - Equipment, technology, hardware
- Objectives of performance testing:
  - Validate vulnerability analysis input data, assumptions, activities, results, and conclusions
  - Demonstrate protection capabilities
  - Ensure that the performance of protection elements provide adequate protection and acceptable risk





# Performance Testing Program

- A testing program is needed to ensure elements implemented comply with requirements
  - All elements of the PPS function at the appropriate level of performance and work together as an effective system
- Performance Testing Program must be developed to:
  - Validate system performance
  - Evaluate operational continuity of all protection system components
  - Test protection elements whose failure would reduce $P_E$ to an unacceptable level
- Testing program must be documented
  - Integral part of the overall physical protection program
- Requires performance test activities and results be documented

# Types of Testing

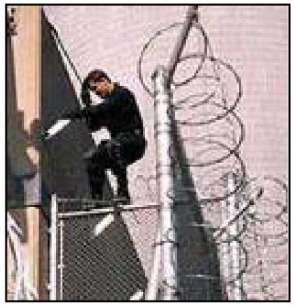
- Example types of tests that can measure effectiveness
  - Operability and functional tests
  - Sub-system performance test
  - Whole system performance tests

# Operability and Functional Tests

- Simple measure of operability – is it working?
- Simple measure of functionality – does it function as intended?
  - Performed on a frequent basis
  - Looks for significant malfunctions or outages
  - If the test fails, call maintenance and possibly take compensatory measures
- Examples (each shift):
  - Metal detectors
  - X-ray machines
  - Walk test a certain number of perimeter sectors to verify alarms are generated

# Sub-system Performance Testing

- Sub-system Performance Testing focuses on the performance and effectiveness of either individual components or parts of the overall PPS
- Conducted to
  - Evaluate the skills, capability, or knowledge of personnel
  - Test operations, procedures, or policy requirements
- Sub-system tests should be conducted realistically—they may be either scheduled or unannounced
  - Example: protective force response to an alarm



# Whole System Performance Tests

- Whole System Performance Tests are conducted to evaluate the overall effectiveness of all elements of an entire system

  - Or large portions of an entire system
    - Example: Force-on-force security exercise tests the overall effectiveness of all elements involved in a response to a site-specific threat and adversary capabilities

- Second example:

- Used to determine how effectively individual elements perform together to form an entire system

# When to Conduct Performance Tests

- On new and proposed PPS equipment to determine effectiveness and limitations
- On PPS equipment after initial installation and after maintenance to verify component performance
- On new and existing security procedures – determine whether
  - Personnel understand and follow the procedures
  - Personnel and equipment interact effectively
- Ensure that protection elements are performing as designed and provide the required protection level

# Performance Testing Process

- Plan the performance test
- Define test purpose, objectives, and standards
- Create a test plan
- Identify protection elements to be tested
  - Identify test locations
- Identify threats (capabilities) and develop scenarios
- Define testing methodology and evaluation criteria
- Define test controls
- Identify resource requirements
- Coordinate the tests and obtain approvals
- Identify compensatory measures
- Collect data; analyze, document, and critique test






# Planning a Performance Test

- Before performance testing is conducted it must be planned to ensure that the testing
  - Will be effective
  - Will provide valid VA data
  - Will provide valid PPS performance data

- Requires developing a written test plan
  - Contains specific and detailed information necessary for efficient and effective testing
- Time and effort in testing can be significant
  - Want to ensure that a proper test is conducted safely with minimal impact on operations and secu

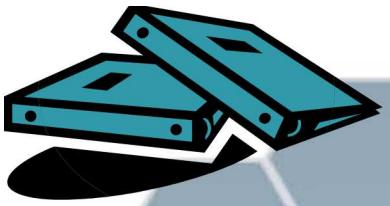
# Purpose, Objectives, and Standards

- For a performance test to be clearly understood, state the purpose, objectives, and performance standards
- *Purpose:* General statement of the overall desired outcome of the performance test (describes the expected result)
- *Objectives:* Elaboration of the purpose that describes the specific test objectives to be achieved
  - Test goals
  - Tasks to be tested
  - Conditions for the test

- *Performance standards*: Describes the level of performance that is expected
  - Ensure that the protection element tested performs as required
  - Maintain high $P_E$ and low risk

# Key Elements of Written Test Plans

1. Test purpose and objectives
2. Performance measures / standards
3. Test location
4. Element to be tested
5. Scenario description
6. Test methodology and evaluation criteria
7. Test controls
8. Resource requirements
9. Test coordination
10. Compensatory measures
11. Approval of performance test plans

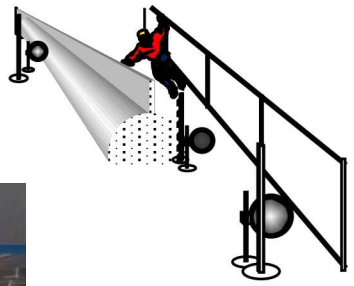


# Security Elements to be Tested and Test Location

- Identify / describe the specific security element(s)
- May need to performance test many security elements over the full spectrum of the protection system
  - Personnel, procedures, equipment / technology / hardware
- The test location should be consistent with
  - Security element(s) to be tested
  - Adversary threat (capabilities) and scenarios
- The test location should be realistic and incorporate
  - The appropriate time, lighting conditions, weather
  - Facility, terrain

# Adversary Threats, Capabilities, and Scenarios

- The PPS protection elements need to protect against the defined threat and capabilities
  - Based on the Design Basis Threat (DBT), what defeat methods may be applied to the element to be tested?
- Identify modes of attack (adversary capabilities) and develop scenarios
  - Run, walk, crawl, jump, tunnel, bridge
  - Use vehicle (air, land, water)
  - Cut, penetrate (hand / power tools)
  - Explosively penetrate
  - Deceive (falsify credential)



- Conservative approach for developing scenarios assumes skillful and cautious adversary

# Test Methodology and Evaluation Criteria

- Test methodology describes how the test will be conducted
  - List steps for planning and execution of test
  - Describe statistical models or mathematical formulas
  - No. of tests to be performed for each scenario
  - Pass / fail criteria
  - Methods for data analysis
  - Record calibration settings and equipment configurations

- Test evaluation criteria describe how the test will be assessed or scored
  - Criteria checklist for each objective listed
  - Criteria should be rated as pass or fail

# Performance Test Controls

- Performance test controls are put in place to limit the test activity
- Test controls are imposed to:
  - Maintain test integrity and validity
  - Ensure that the correct data is collected
  - Minimize risk of injury or impact on security
- Performance test controls are required to mitigate testing artificialities and environmental concerns
  - Some actions must be simulated by using a stimulus equivalent to the actual adversary action
  - Certain environmental conditions may be expected to degrade performance and should be tested
    - Day / night, weather, birds / animals

# Resource Requirements

- Resources includes anything it takes to conduct the performance test
- Some examples of resources are
  - Personnel
  - Time for the test
  - Equipment
  - Facility
  - Location
  - Funding
  - Adversaries
    - Weapons and equipment / tools
  - Logistical support
  - Safety requirements

# Test Coordination and Approval Process

- Identify and brief everyone involved in the test
  - Or make them aware that a test will be conducted
- Various stakeholders need to be coordinated:
  - Safety and Security
  - Facility operations, Management
  - Quality assurance, Human factors
  - Others
- Safety is very important - always an element of risk in performance testing
  - Conduct realistic testing without undue safety hazards
- The approval process describes:
  - How the test plan is approved
  - Who has to approve the test


# Compensatory Measures

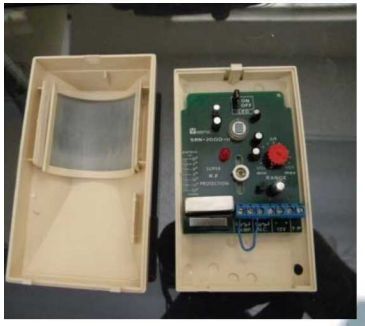
- Determine necessary compensation for any degradation of readiness experienced while conducting the test
- For example:
  - Are more post and patrols needed to ensure adequate protection during the performance test?
  - Does the test area need to be shut down or segregated to ensure the test is conducted safely and securely?
- Describe what will need to be implemented in the event of a test failure
  - If a security element fails during testing, what has to be done to compensate for the failure in the event that risk increases?

# Analyze, Document, and Critique

- Analyze the performance testing data to determine if the performance level is achieved
  - And if deficiencies exist
- Document the performance test results and mitigation measures if required
  - Test Report = test plan + data collected + analyses + results + conclusions
- Provide critique after the performance tests
  - Critical self-analysis, even after success, is essential to improvement
  - Critiques are an effective way is to draw out lessons learned
  - Should involve all test participants

# May Need to use Preliminary Tests

- Use preliminary tests to practice on unknown elemen
  - Allow for exploratory testing
- Tests will help refine the actual testing through initial data collection
  - Characterization of element
  - Interaction with environment
- Determine proper installation and configuration
  - Determine settings to minimize high NAR
- Determine areas of concern or uncertainty
  - Fully characterize the performance



# Performance Metrics for Detection Elements

Probability of Detection ($P_D$ )

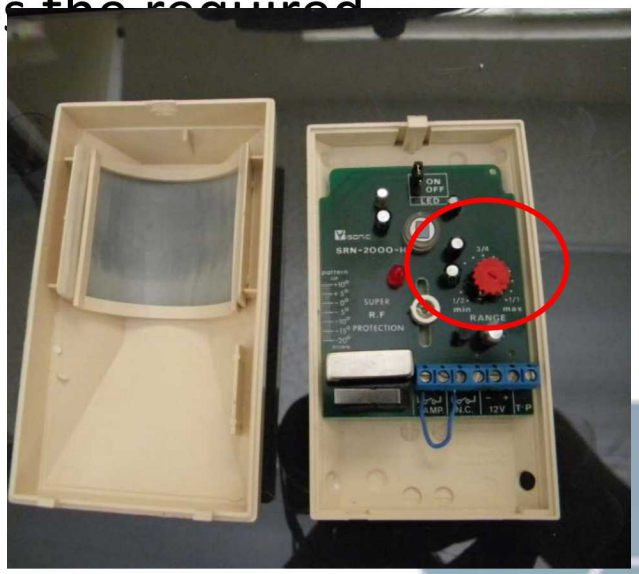
and Confidence Levels

# Testing Strategy

- Set an acceptable performance metric / standard
- Set an acceptable confidence level
- Conduct a reasonable number of tests
  - Importance of system element
  - Amount of time and resources available
  - Cost
- Plan for one or more stopping points in the testing when reasonable performance metric cannot be achieved

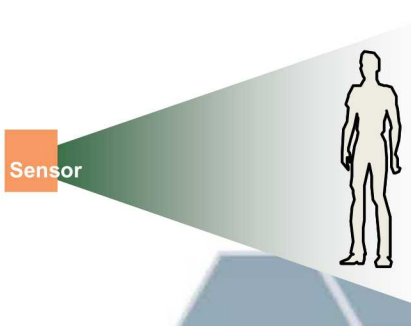
# For Detection Sensors - What Settings to Use

- Device calibration is a compromise between the following:
  - Probability of Detection, $P_D$
  - Nuisance Alarm Rate, NAR
- The sensor or detector should be set at the lowest sensitivity setting that provides the required performance
  - ↑ $P_D$ and ↓ Nuisance Alarm Rate



# Probability of Detection ($P_D$)

- $P_D$ - the likelihood that an intruder will be detected under a well defined set of conditions
  - $P_D = P_{Sensing} * P_{Assessment}$
- Conditions that influence $P_D$ value:
  - Intruder size and posture
  - Attack mode
    - Running, jumping, crawling, walking, etc.
  - Direction of attack
    - Parallel or tangential to the detection volume
  - Speed of intruder
    - Fast, slow
  - Sensitivity adjustment
  - Weather and environmental conditions
  - Condition of equipment



# Confidence Level

- Confidence is a statistical term – it's the confidence the analyst has in an estimated probability
  - Statistical confidence is a function of the number of trials performed
    - It's the likelihood that $P_D$ is at least the defined number
- More testing provides a higher confidence in the accuracy of the results of the test
  - If we perform no trials then we have no confidence that a performance level can be met
  - 100% confidence requires an infinite number of trials
- Usually expressed as a percentage

# Probability and Confidence Calculations for Binomial Data

$$CL = 1 - \sum_{k=0}^{m} \left( \frac{n!}{k!(n-k)!} \right) P_D^{(n-k)} \left(1 - P_D\right)^k$$

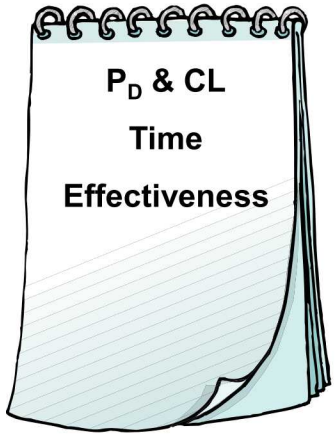
- *Where:*
  - *CL* is the confidence level
  - $P_D$ is the required probability of success (in this case detection)
  - *n* is the number of trials in a test
  - *m* is the number of allowed misses
- Typically computers are used numerically to create tables
  - http://www.elsevierdirect.com/companion.jsp?ISBN=9780750683524

# Single Sampling Plans

| Single Sampling Plan, No Failures Allowed | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $P_D$ | .85 | .90 | .95 | .85 | .90 | .95 | .85 | .90 | .95 |
| Confidence Level | .85 | .85 | .85 | .90 | .90 | .90 | .95 | .95 | .95 |
| Sample Size | 12 | 18 | 37 | 14 | 22 | 45 | 19 | 29 | 59 |
| **Single Sampling Plan, One Failure Allowed** | | | | | | | | | |
| $P_D$ | .85 | .90 | .95 | .85 | .90 | .95 | .85 | .90 | .95 |
| Confidence Level | .85 | .85 | .85 | .90 | .90 | .90 | .95 | .95 | .95 |
| Sample Size | 21 | 32 | 66 | 24 | 37 | 76 | 30 | 45 | 93 |


87

# Analyzing Test Results




- Statistical analysis
  - Probabilities and confidence levels
  - Delay times
  - Response times
  - Response effectiveness
- Limited testing often does not lend itself to statistical conclusions with high confidence
  - Subject matter expert judgment
- Lessons learned
  - Recommendations for future testing

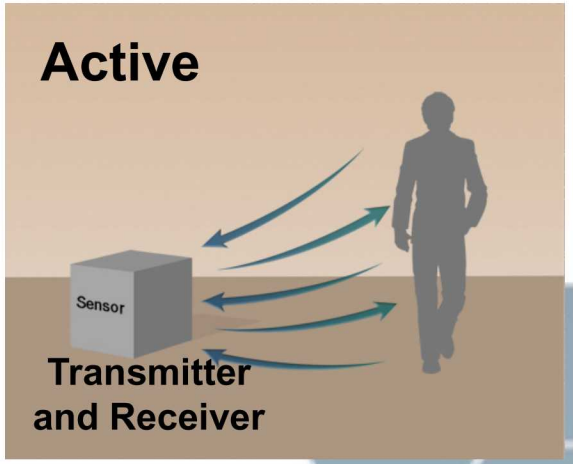
# Subgroup Exercises

- Performance Testing:
  - (3) Exterior sensors
    - Select acceptable Confidence Level (CL)
    - Data collected: $P_D$
  - Interior sensor
    - Select acceptable CL
    - Data collected: $P_D$
  - Delay
    - Data collected: Delay Times
  - Response
    - Data collected: Response Force Times

$$P_{Detection} = P_{Sensing} \times P_{Assessment}$$


# Detection Equipment Performance Test

- Sensor components are tested by a series of trials
- Each trial is an event where a device is provided with an input (stimulus) and the output (response) of the device is measured and recorded
- Data collected for this testing is $P_D$
  - Confidence level is selected prior to testing



# Delay Component Performance Testing

- Delay components are tested by
  - Installing the component in a realistic setting,
  - Attacking the component, and
  - Determining the time required to defeat the component
- The time required to defeat the component using a specific tool set is the delay time
- The data collected in this testing is delay time

# Purposes and Importance of a Guard/Response Testing Program

- Part of an overall performance testing program
- Must be developed to:
  - Validate the performance of response protection elements
  - Ensure that response protection elements are performing as designed
  - Test response elements whose failure would reduce protection to unacceptable level
  - Conduct at a frequency to achieve high level of confidence in the reliability of the element
  - Establish a documented performance testing process

# 3 Levels and Associated Tests of Guard/Response Performance Testing

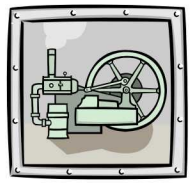
- Performance Testing Methodology
  - A combination of performance testing is used to evaluate the performance of the guard and response force
  - Divided into two categories
    - Sub-System Performance Testing
    - Whole System Performance Testing

# 3 Levels and Associated Tests of Guard/Response Performance Testing

- Sub-System Performance Testing
  - Level I
    - Time Motion Studies
    - Limited Scope Performance Test
  - Level II
    - Mission Drills (To demonstrate sustainability)
    - Alarm Response Assessments Performance Test
  - Level III
    - Response Function Performance Test
- Each level becomes more complex to conduct
- Each level consists of specialized controller/evaluator training

# Sub-System Performance Testing

- Sub-System Performance Testing narrowly focuses on the performance and effectiveness of either part of a whole system or an individual component for the guard and response force function
- Used to determine:
  - whether guard and response procedures are effective
  - whether personnel understand and follow the procedures
  - whether personnel and equipment interact effectively
- Testing individual components of the whole system



# Controller/Evaluator Roles

- Controllers:  People responsible for enforcing rules of engagement, safety rules, and other control measures
- Evaluators:  People responsible for observing and documenting exercise activities and conditions
- Controllers and evaluators should be specifically trained for each type of test
- Ensure that all safety and security requirements are met
- Maintain an environment free of the hazards associated with each test and method

# Level I: Time Motion Studies

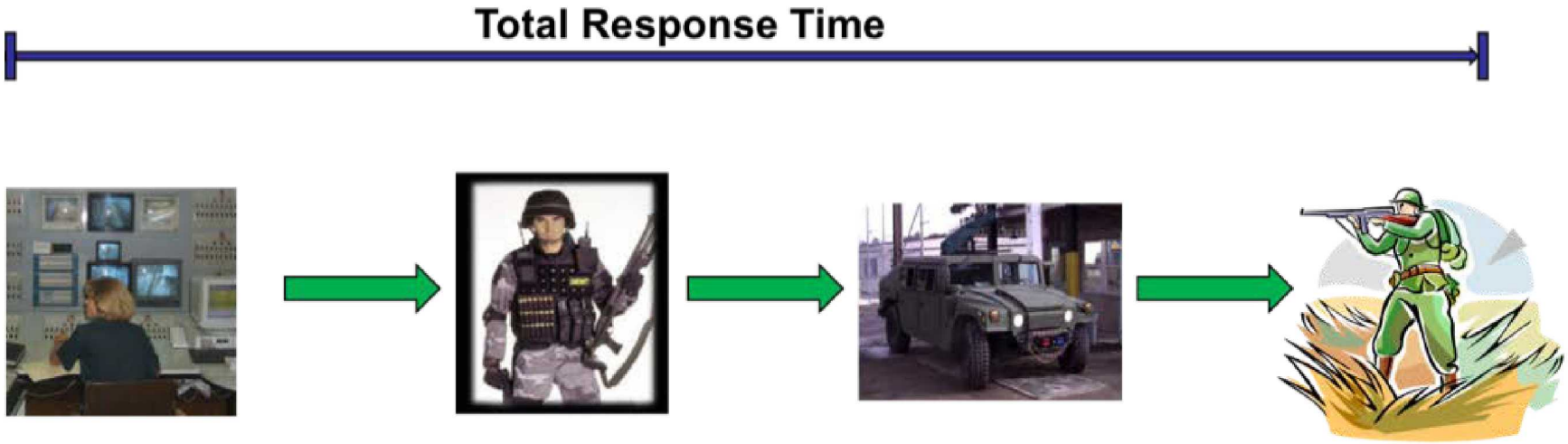
- Are considered the foundation for the response element
- Tests responders arriving to a designated response point during a required time
- Determines and validates required response times to arrive at various response locations derived from a response plan
- Conduct a large number of studies for each tactical position to quantitatively justify the average response time for each position

# Level I: Time Motion Studies

"How It Works"

- Time begins at the responder's origination point and is measured to the dedicated response point
- Included in the overall response time:
  - Don all required equipment and firearms
  - Travel or traverse time
  - Enter through entry gates, doors, or other type of barriers

# Level I: Time Motion Studies, cont'd.



# Level I: Limited Scope Performance Tests

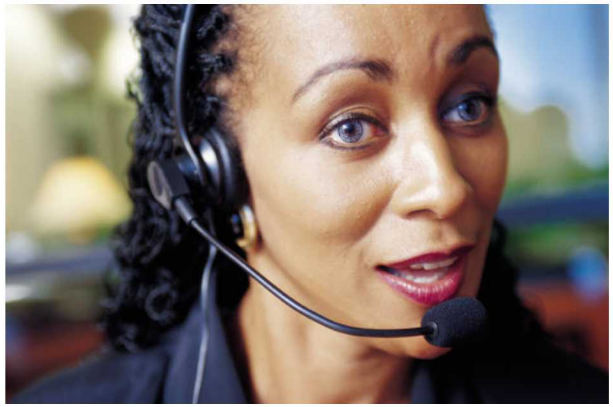
- Narrowly focus on the performance and effectiveness of a sub-set of response elements
- Used as a validation tool
- Used to determine or verify that the tested response elements work together
- Determine the level of a security force's skill or capability
- Validates possession of a requisite knowledge or skill to perform a specific task
- Validates the individual human element of the PPS
- Is a continuous process to validate probabilities documented within the vulnerability analysis

# Level II: Mission Drills

- Considered rehearsals for Limited Scope Performance Tests
- Maintain sustainability
- Training for Limited Scope Performance Tests
- Train the Trainer (Supervisors)
- Determine the level of a security force's skill or capability
- Reinforces the level of a security force's skill or capability
- Practice before you Play!

# Level II: Alarm Response and Assessment Performance Tests

- Performance test  response force readiness and response to an alarm at a specific location
- Measures specific performance actions :
  - Communications
  - Personnel protective measures
  - Equipment availability and serviceability
  - Coordination activities
  - Tactical Movement
- Tests are “no notice” performance tests
- Must be coordinated with facility representatives
  - Safety requirements are met
  - Security is not compromised
  - Limit disruption to operations

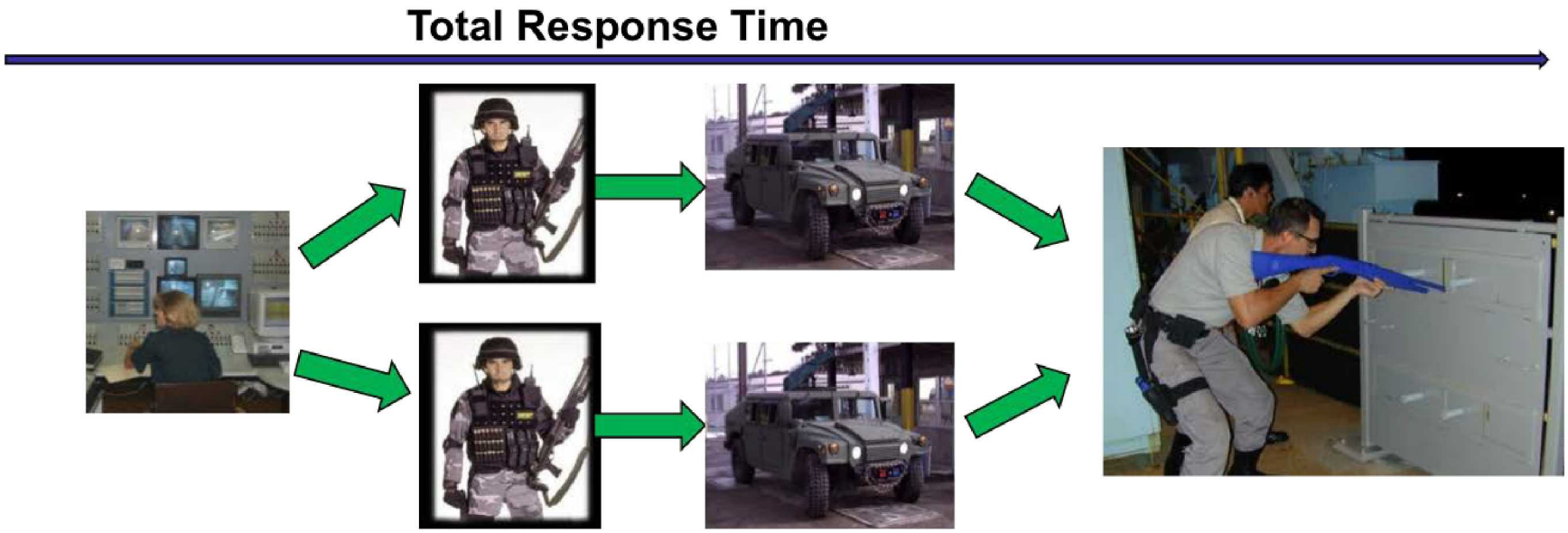


# Level III: Alarm Response and Assessment Performance Tests

"How It Works"

- Picture in Time: A representation of response force patrol locations at a specific time.
- Create a Picture In Time
- Position controllers with selected security force according to the Picture In Time
- A controller will intentionally simulate a breach at a designated alarm point to stimulate the security force response
- Each controller evaluates the response and documents results

# Level III: Alarm Response and Assessment Performance Tests, cont'd.



# Level III: Response Function Performance Test

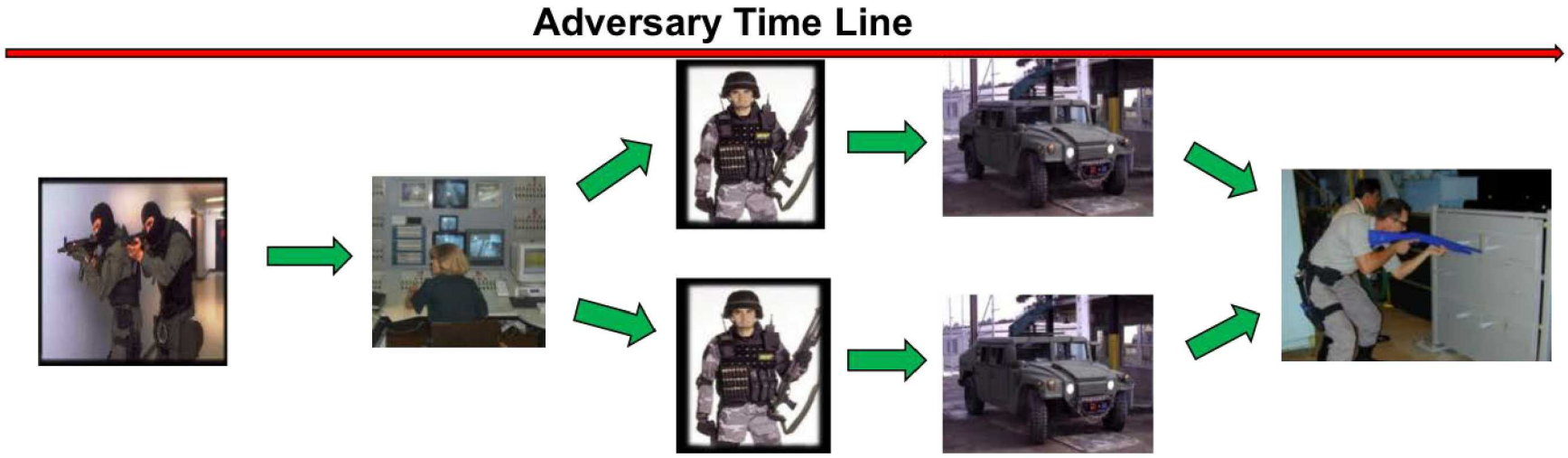
- Modified Force on Force exercise minimizing  resources
- Multiple Integrated Laser Engagement System or inert weapon systems is required
- Ensures security personnel know how to respond accordingly to their contingency plans
- Parts of detection, delay, and response functions are tested against fictitious yet credible adversary attack
- Ensures personnel are trained in command and control; communications; tactics; equipment; and weapons
- Uses adversary scenarios from DBT with reduced adversaries

# Level III: Response Function Performance Test

"How It Works"

- Create a Picture in Time
- Position controllers with selected guard, response force and adversary role player(s)
- Minimum of one adversary will intentionally trip a sensor simulate a breach at a designated alarm point to initiate the security force response
- Each controller evaluates the response and documents results

# Level III: Response Function Performance Test, cont'd.

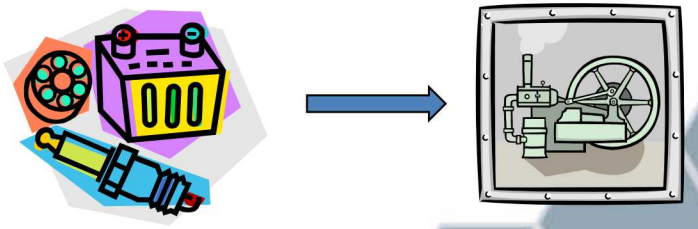


# Whole System Performance Testing

- Testing the sections of the whole system
  - Ensure individual components work together
  - Evaluate the overall performance of the PPS
- Two performance measure criteria are evaluated:
  - Interruption – The successful arrival of the response force at an appropriate location to stop the adversary.
  - Neutralization – When the response force kills, captures, or causes the adversary to flee before the adversary is able to complete their task.

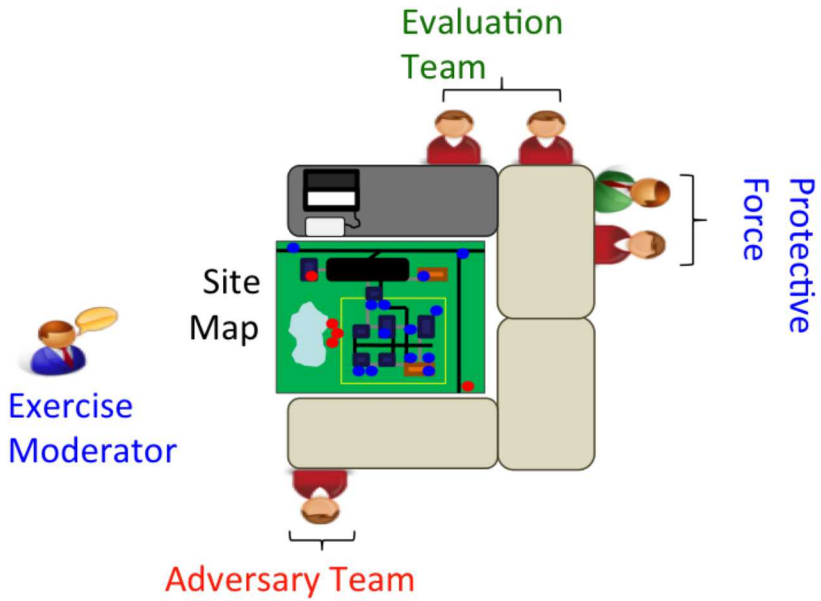
# Whole System Performance Testing, cont'd.

- Types of simulation methods to evaluate the overall performance of the PPS.
  - Table-Tops
  - Computer Simulations
  - Force-on-Force



# Table-Top Exercise

- A method of simulating an adversary attack on a site's existing or proposed PPS.
- Analyzes PPS Functions (Detection, Delay, Response)
- Provides insight into a PPS that can stand alone or be used in other analysis tools.



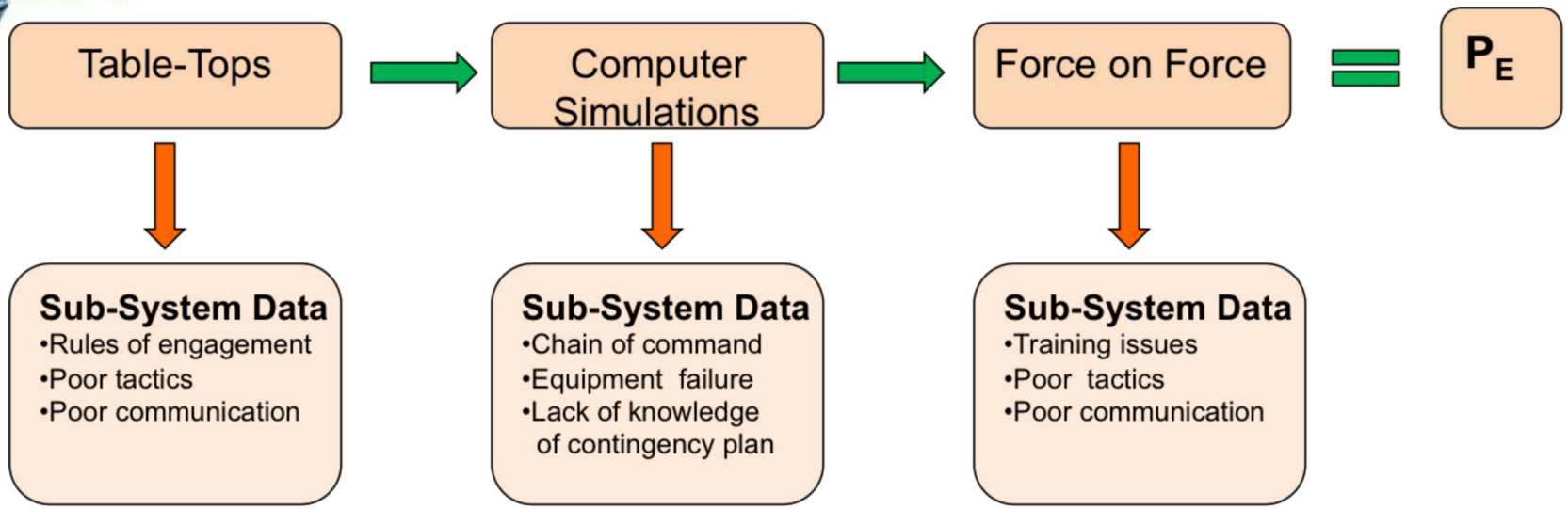
# Computer Simulations


- Computer simulation of small force engagement
- Determine effectiveness for tactical movement, weapon and explosive calculations, etc.
- Provide real-time results of engagements between the response force and an adversary
- Used to determine probabilistic PH/PK calculations

# Force-on-Force Exercise (IAEA INFCIRC/225/Revision 5)

- Force-on-Force Exercise: A performance test of the physical protection system that uses designated personnel in the role of an adversary force to simulate an attack consistent with the threat or the design basis”
- A full scale field simulation of an attack on a site involving all onsite guards and response forces

# Whole System Data Points




- Methods concurrently determine two types of data
  - PE for a PPS
  - Collects guard and response force sub-system performance testing data

# Summary

- Performance Testing is a means to realistically test the effectiveness of response force programs
- Ensures that response protection elements are performing as designed and provide the required protection level
- Sub-system and whole system performances testing are used to evaluate the performance of the guard and response force functions
- Three levels of response performance testing
  - Level I; Time Motion Studies and Limited Scope Performance Tests
  - Level II; Mission Drills and Alarm Response Assessment Performance Tests
  - Level III; Small-scale Force on Force Exercise

Exercise

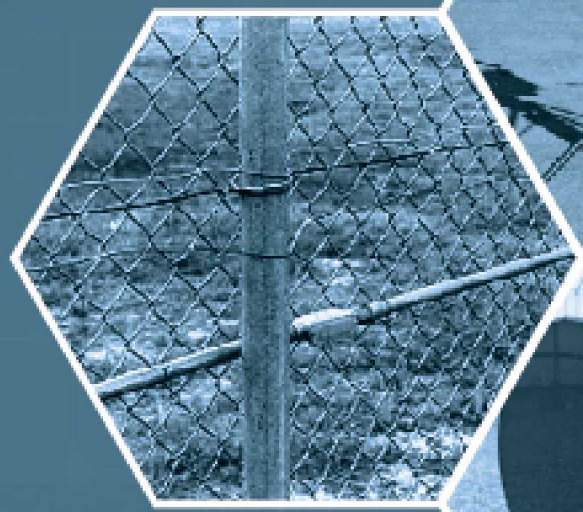
# SENSOR EXERCISE #4

# Day 3 Summary

- Alarm Assessment, Communication & Display
- Access Delay
- Response
- Performance Testing Measures

# Foundations of Physical Protection Systems

Day 4



# Day 4 Agenda

- Review of Day 3
- PPS Evaluation Overview
- Contingency Plan Overview
- Transportation Security
- Insider Analysis
- Nuclear Security Physical Protection Summary

# DAY 3 REVIEW

Group Presentations

# SENSOR EXERCISE #5

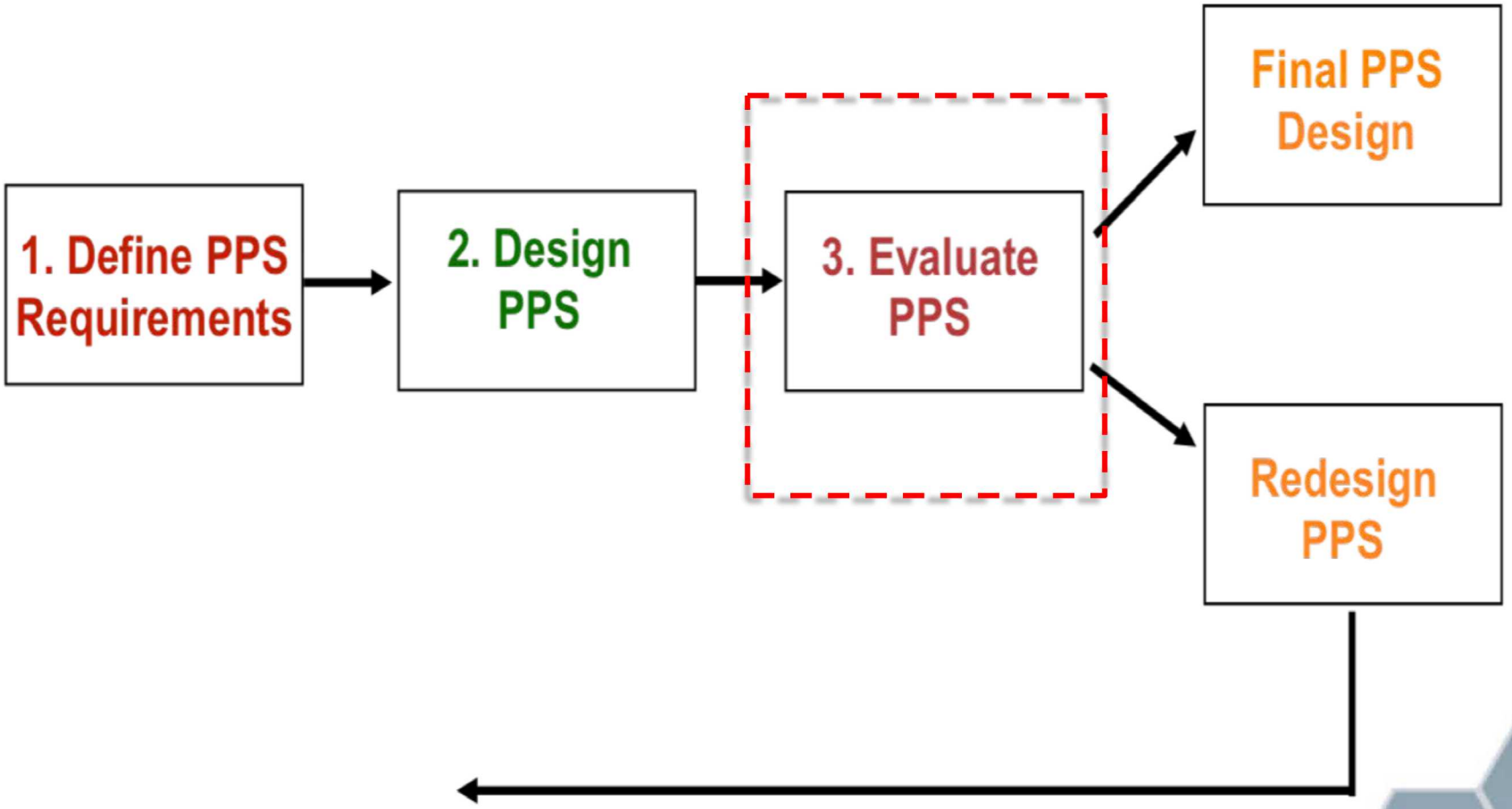
Module 16

# PPS EVALUATION OVERVIEW

# Lecture Outline

- Define three PPS performance metrics
- Identify the two basic PPS performance evaluation methodologies
- Recognize several PPS evaluation tools
- State two major factors affecting evaluation quality

# PPS Performance Metrics



# Security Risk Management

- The process of identifying and applying measures that reduce or mitigate the risk of an undesired event.
- The security risk equation is:

$$\mathbf{R = P_A\,(1 - P_E)\,C}$$

*Where* **R** = Risk of the undesired events theft or sabotage
**$P_A$** = Likelihood of adversary attack
**$P_E$** = Effectiveness of physical protection system
**C** = Consequences of undesired event

# Performance-Based Approach

- Recall, from the risk management and regulatory requirements module, the performance approach:
  - The Competent Authority specifies the required level of system effectiveness, $P_E$, against the DBT for the Operators
  - The Operator complies by designing and evaluating its physical protection system to achieve this $P_E$
  - The Competent Authority is responsible for verifying that the Operator's system satisfies the required performance against the potential adversary

# Evaluation Objectives

- Meet regulatory and operator requirements
  - Self-assessment by operators
  - 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

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

# Performance Evaluation Metrics

- Three metrics are commonly used for the evaluation of the performance of PPS:
  1. System Effectiveness ($P_E$)
  2. Probability of Interruption ($P_I$)
  3. Probability of Neutralization ($P_N$)

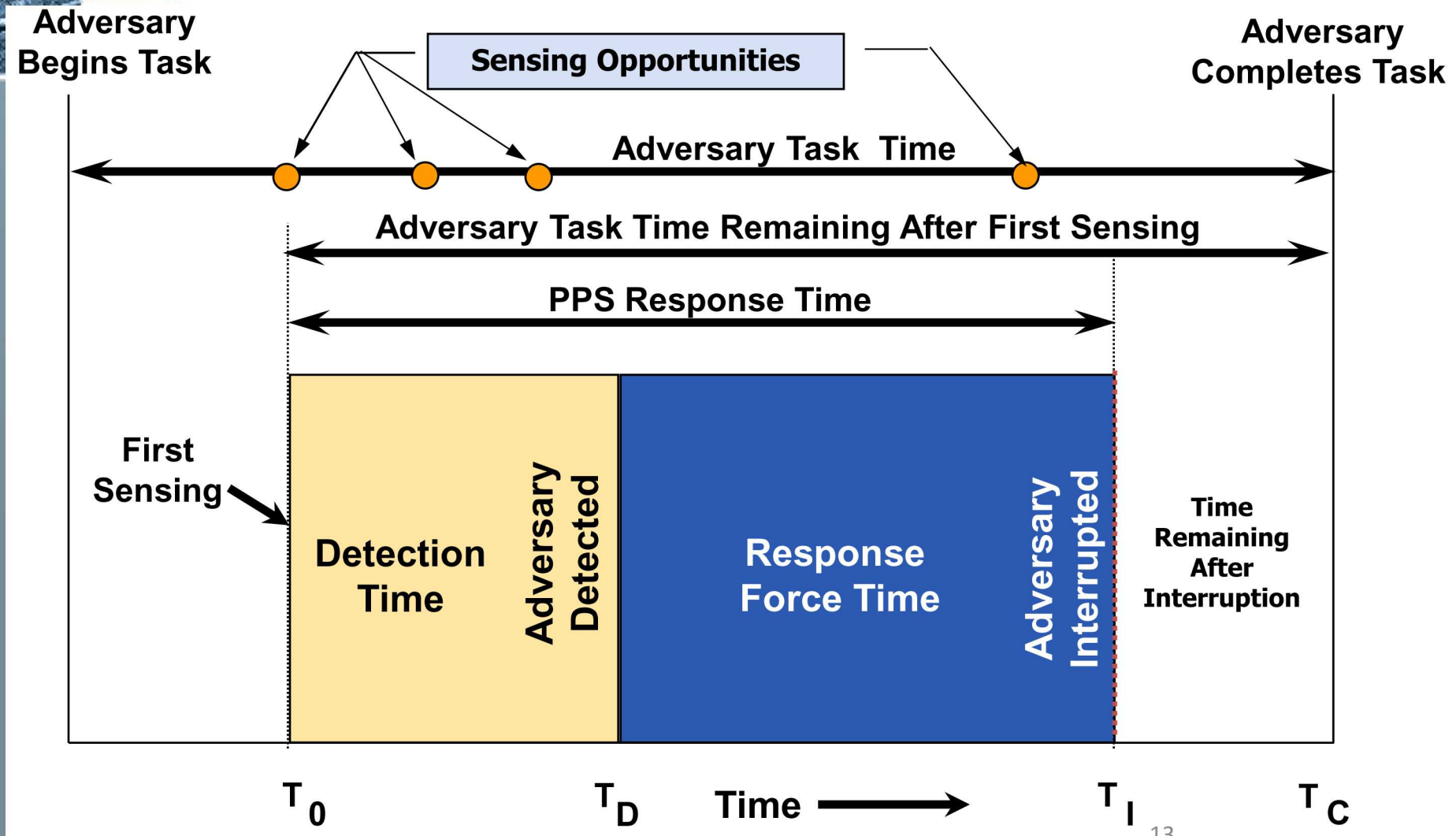
# System Effectiveness ($P_E$)

- The probability that the physical protection system will prevent the adversary from completing the undesired event

$$P_E = P_I * P_N$$

*Recall that we introduced the terms and concepts of interruption and neutralization during the introduction to the workshop*

# Adversary and PPS Timelines



# Review of Principles

- **Principle of Timely Detection:** To interrupt the adversary before the theft or sabotage task is completed, the PPS response time must be less than the adversary task time remaining after the first sensing
- **Critical Detection Point (CDP)**: The last sensing opportunity along an adversary path for which the PPS response time is less than the adversary task time remaining after the first sensing

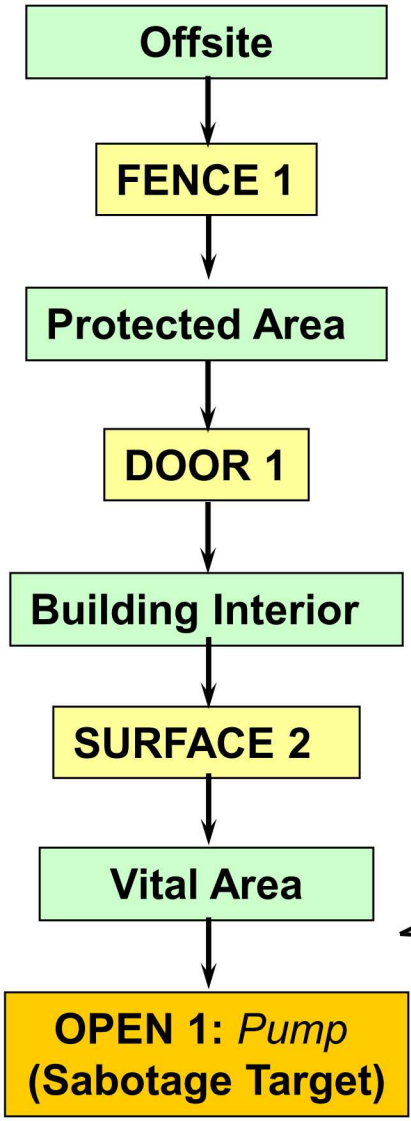
***To be an effective PPS, timely detection must be achieved against the DBT along all adversary paths***

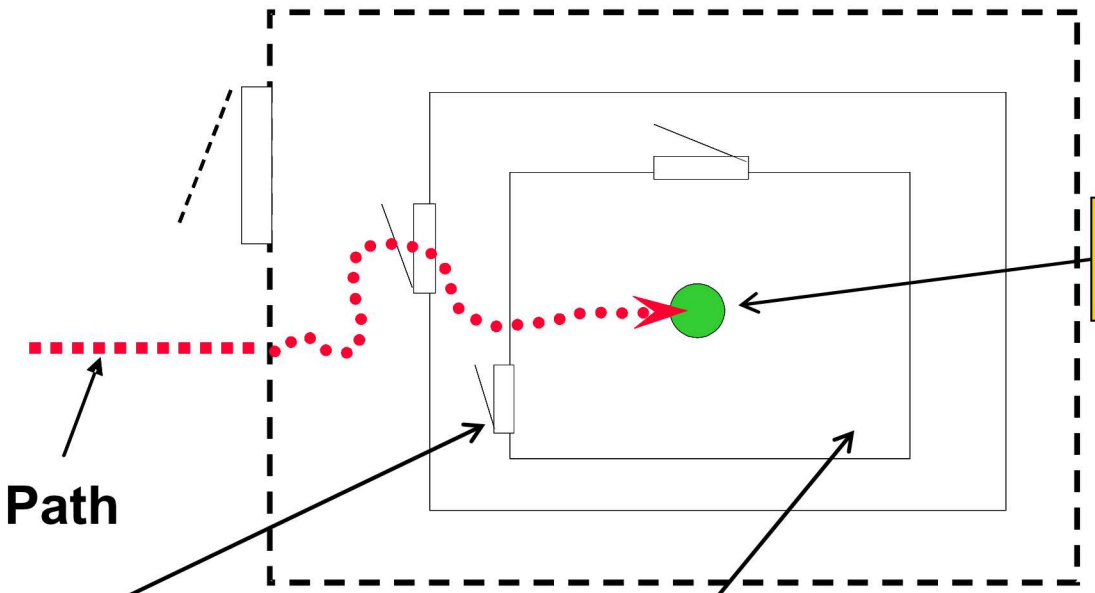
# Probability of Interruption ($P_I$)

- The cumulative probability of detection along a path up to and including the Critical Detection Point (CDP)
  - Based on principle of Timely Detection and concept of Critical Detection Point
  - Response force interrupts adversary task timeline

# Concept of an Adversary Path

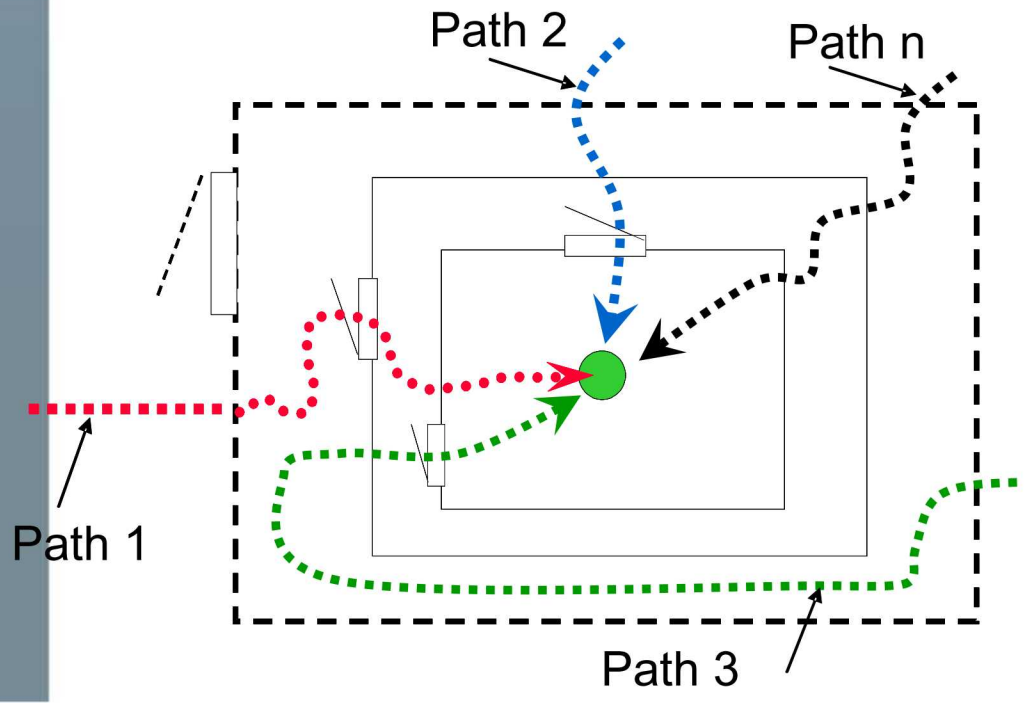
***Adversary Path:*** A time-ordered sequence of path elements, areas, and a target task that the adversary must traverse to complete an attack

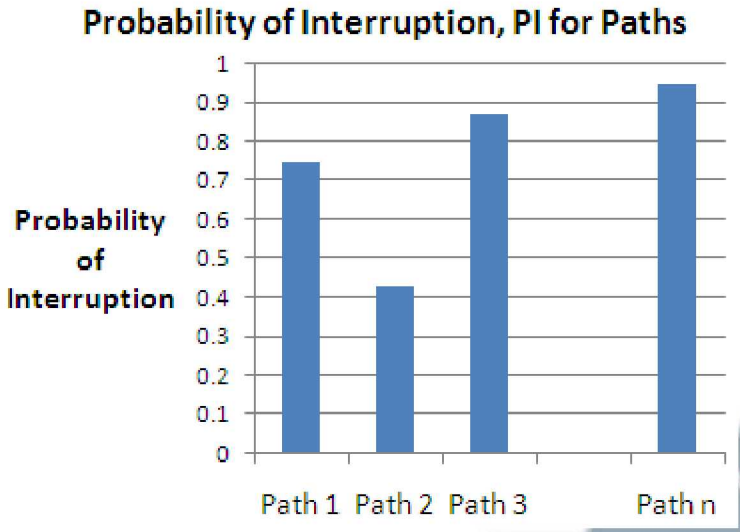


# Purpose of Path Interruption Analysis

- Determines whether detection and delay are sufficient along all adversary paths to provide an adequate level of Probability of Interruption, $P_I$, based on planned PPS Response Times

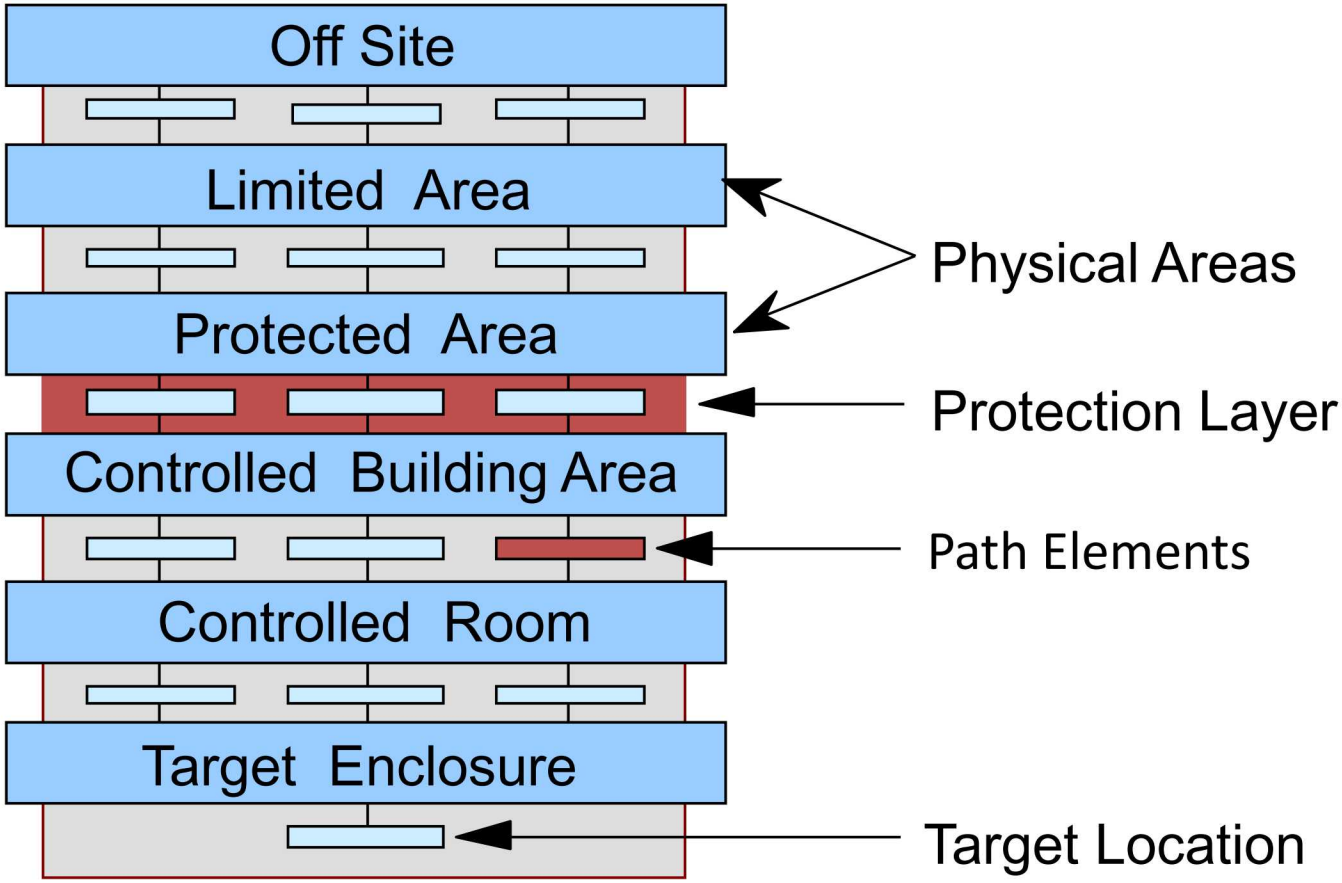


# Adversary Sequence Diagram (ASD)

- A graphical model used to help evaluate the effectiveness of the PPS at a facility
- ASD represents
  - Paths that adversaries can follow to accomplish sabotage or theft
  - PPS elements along paths
- ASD is used to determine the most vulnerable path for specific PPS and threat

# Concept of Adversary Sequence Diagram



# Probability of Neutralization ($P_N$)

- The probability that the response force can prevent an adversary from completing a malicious act such as theft of nuclear material or sabotage of a nuclear facility
  - Response force must neutralize adversary following interruption
  - Neutralize means response force arrests, captures, or kills adversary, or causes adversary to flee

# Neutralization Analysis Methods

- Expert judgment
- Simple numerical methods for $P_N$
- Simulations
  - Scenario analysis
  - Determines $P_N$ as part of $P_E$
- Actual engagements

# What Is Scenario Analysis?

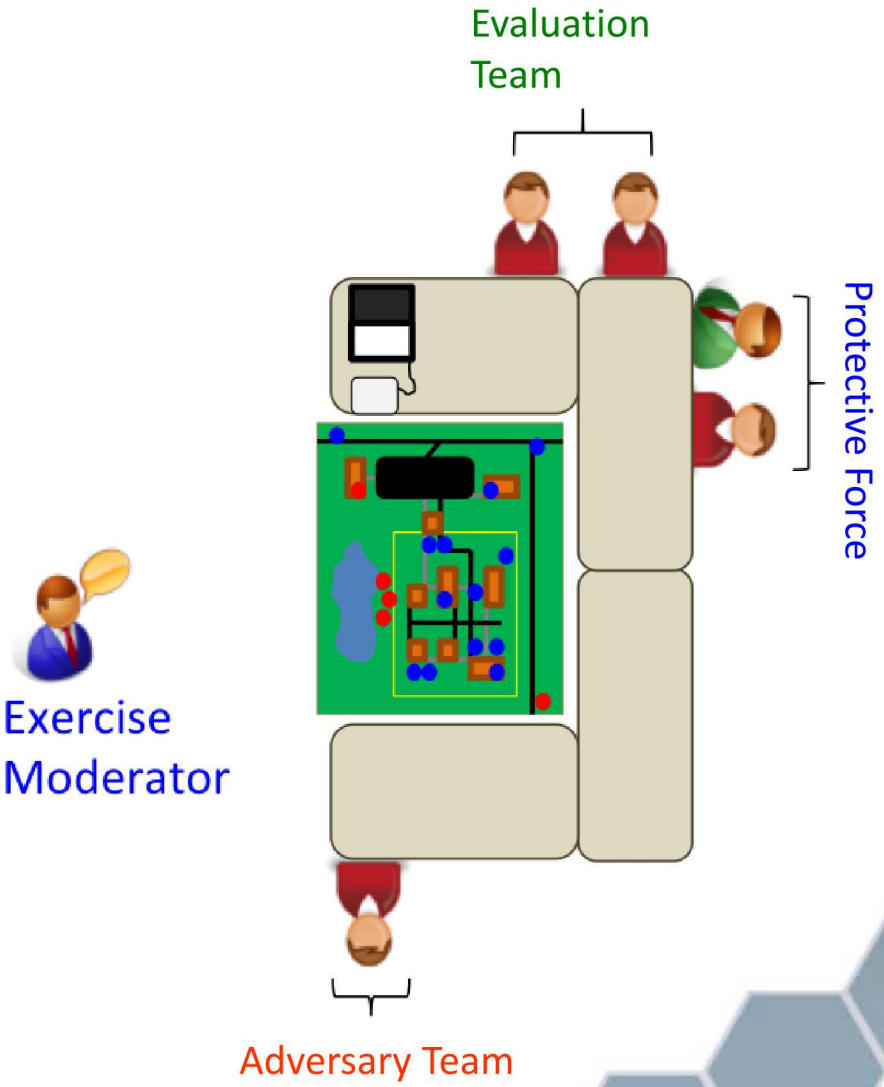
- A methodology for analyzing system effectiveness, PE, by considering several alternative possible adversary attacks (scenarios).
  - Allows more detailed analysis of the attack, the defense, and the results than path interruption analysis

# Simulation Techniques

- Several simulation techniques are used in scenario analysis to estimate PE or PN:
  - Structured and detailed tabletop exercise
  - Computer simulation of small force engagement
  - Force-on-Force exercises
- Performance test results are used as input to all simulation techniques
  - Security equipment tests
  - Limited scope performance tests

# What is a Table-Top Exercise?

- A method to simulate an adversary attack on a site's existing or proposed Physical Protection System (PPS).
- Analyzes PPS elements:
  - Detection
  - Delay
  - Response
- Provides insight into a PPS that can stand alone or be used in other analysis tools.



# Evaluation Methodologies

- Path Modeling and Analysis
  - Path interruption analysis determines whether detection and delay are sufficient along all potential adversary paths to provide an adequate level of Probability of Interruption ($P_I$), based on planned response times
- Scenario Development and Analysis
  - Scenario analysis determines whether the PPS effectiveness, $P_E$, is adequate across the range of detailed attack scenarios that might be credibly planned and conducted by adversaries within the Design Basis Threat

*Thee are two complementary methodologies typically used in the evaluation of PPS effectiveness*

# Current Evaluation Best Practice

- Use a combination of
  - Path Interruption Analysis
    - One of several analytical tools
  - Scenario Analysis
    - Several simulation techniques
- Look for consistency among results

# Evaluation Quality

- There are two major factors that determine the quality of the PPS performance evaluation:
  1. Subject matter experts
     - Expert knowledge and experience are involved in the application of all evaluation methodologies
  2. Performance test data
     - Security component (detection, delay, and response) performance data used in the system evaluation must be high quality
     - Component performance data should be based on current performance testing

# Summary

- The three PPS performance metrics are:
  - $P_I$, $P_N$, and $P_E$
- The two basic PPS evaluation methodologies are:
  - Path and scenario analyses
- PPS evaluation tools used are:
  - $P_I$ equation, simulation, $P_N$ numerical model, tabletop exercise
- Two major factors affecting evaluation quality are:
  - Subject matter experts and performance test data

Exercise

# ASD EXERCISE

Module 17

# CONTINGENCY PLAN OVERVIEW

# Lecture Outline

- Describe the INFCIRC/225 recommendations for contingency plans
- Distinguish between security plans, contingency plans, and emergency plans
- Identify recommendations for contingency planning
- Recognize various evaluation tools for contingency plans

# Plans - Definitions

- **Security Plans** – Based on design basis threat/threat assessment and include design, evaluation, implementation and maintenance of physical protection system and contingency plans
- **Contingency Plans** – Predefined sets of actions for response to **security events** such as unauthorized acts indicative of attempted unauthorized removal or sabotage designed to effectively counter such acts
- **Emergency Plans** - Predefined sets of actions for response to **safety events** or other emergency events

# Effective Contingency Plans

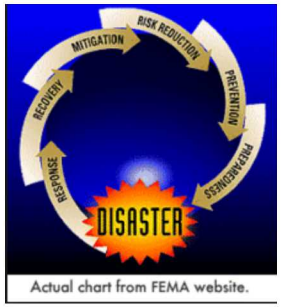
- Based on event type and prepared to counter or mitigate the event consequences.
- Includes – **what**, **who**, **when**, and **where**
- Should be well understood by all response forces
- Should include interfaces with safety (emergency plan)
- Should be periodically drilled/exercised such as
  - Security exercises
  - Fire drills
  - Evacuation drills
  - Shelter in place

# Contingency Plans - What

- Facility characterization
- Target consequence based response strategy (containment or denial)
- For each type response personnel involved:
  - On-site or Off-site
  - Procedures for what they must do including response area location, response time requirement, deployment tactics, rules of engagement
  - Communication protocols
  - Required Equipment (weapons, ammunition, support equipment, vehicles, radios)
  - Facility recapture procedures

# Contingency Plans - Who

- Response Personnel Duties
  - Central Alarm Station personnel or other recipient of alarm
  - Guards
  - On-site Response Force
  - Off-site Response Forces
- Incident Response Personnel – Safety, Emergency, and Operations personnel
- Site Personnel



Actual chart from FEMA website.

# Contingency Plans - When

- When to respond
- When to change tactics
- When to escalate use of force
- When to notify other agencies
- When to communicate to the public


EAS
Emergency Alert System

# Contingency Plans - Where

- Where are mustering/coordination points
  - Onsite?
  - Off-site coming onsite?
- Where are normal operations patrol areas?
- Where are primary response locations for security incident?
- Where should response move to as the situation progresses?

# Attacks and Other Considerations

- Unauthorized removal from the facility, the limited area, the protected area or from an inner area
- Sabotage of a vital area
- Locate and recover missing nuclear material (NM)
- Insider attacks
- Cyber attacks
- Other attacks – airborne, stand-off, hostage, active shooter
- Other events – natural disaster, medical, fire, evacuation, civil disturbance
- Bomb threat/bomb found

*The different types of attacks may be given code names and have checklists which outline responses, roles/responsibilities, people.*

# Overview - Other Decisions

- Can this malicious act lead to radiological consequences?
- What equipment or emergency personnel must be protected to minimize consequences?
- What are the overlaps between safety, security and operations and which has priority?
- When does the incident start and when is it over?

# Summary

- Both the State and Operator have CPs
- CPs are based on a event/incident type
- CPs cover various attack scenarios
- What should an effective CP enable the response force to do and areas it should address

Module 18

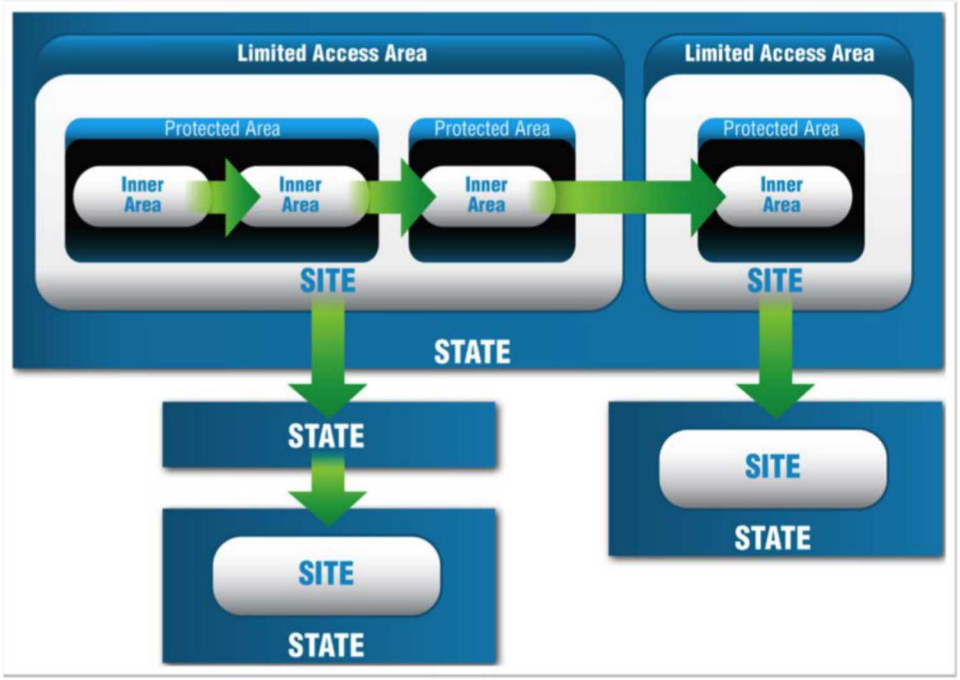
# TRANSPORTATION SECURITY

# Lecture Outline

- Identify the scope of transportation security
- Compare similarities and differences between fixed site and transportation security
- Identify specific issues associated with transportation security
- Identify methods for analyzing transportation security

# Scope of Transportation Security

- Transportation Security must consider all the factors involved during On-Site and Off-Site Transportation of Nuclear and Radioactive Material



# Modes of Transportation Security

Tractor Trailer

Plane

Ship

Railcar

# Threats to Transportation Security

Pirates

Hijacking

Ambush

Sabotage

# Fixed Site versus Transportation Security

| Fixed Site | Transportation Security |
|---|---|
| Fixed Protection Boundary | Moving Boundary |
| Stable Environment | Continuously Changing |
| Control Over Environment | Uncontrolled Environment |
| Operations Are Predictable | Opportunity to be Less Predictable |
| Protection System in Place | Protection System Must Be Transportable |

# Transportation Security Analysis

- Follows the same DEPO process as for a fixed site
  - Determine system objectives
  - Characterize existing system
    - Detection / Delay / Response
  - Analyze PPS

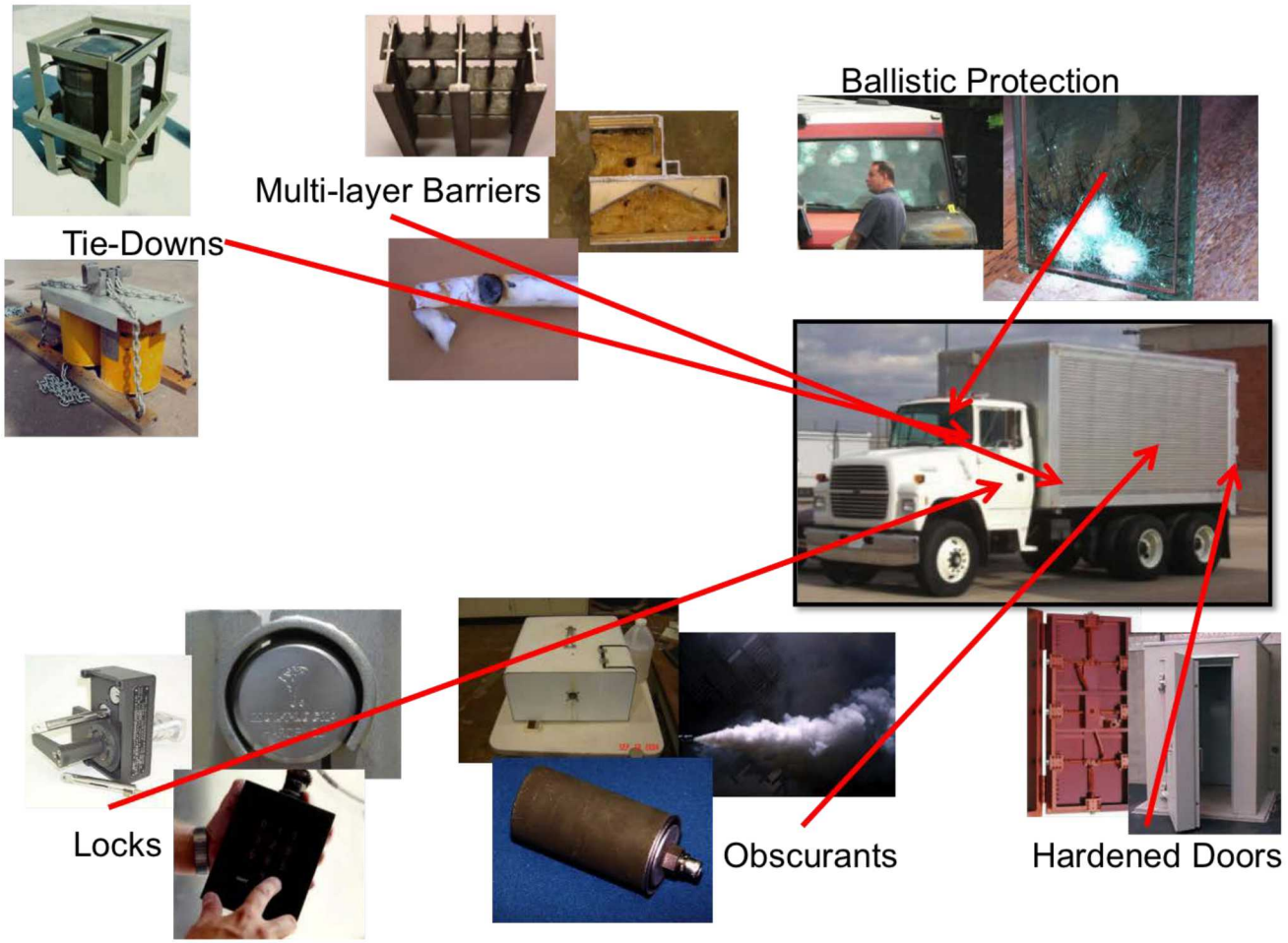
# Transportation Security Analysis

- Transportation Detection, Assessment, Communication
  - Response force provides detection
  - Response force performs visual assessment
  - Response force communicates alarm
  - Interior alarms for transportation vehicle vault
  - Access control
    - Two-person rule

# Transportation Security Delay

- Only other security element is vehicle access delay
  - Requires careful design of delay elements
  - Keep cargo secured to vehicle
  - Use vehicle immobilization
  - Hardened vehicle or vault provides delay
  - Interior activated dispensable barriers, entanglements, tie-downs, hardened containers, and response force can provide added delay

# Transportation Security Delay Features




**Transportation Delay Element - Examples**

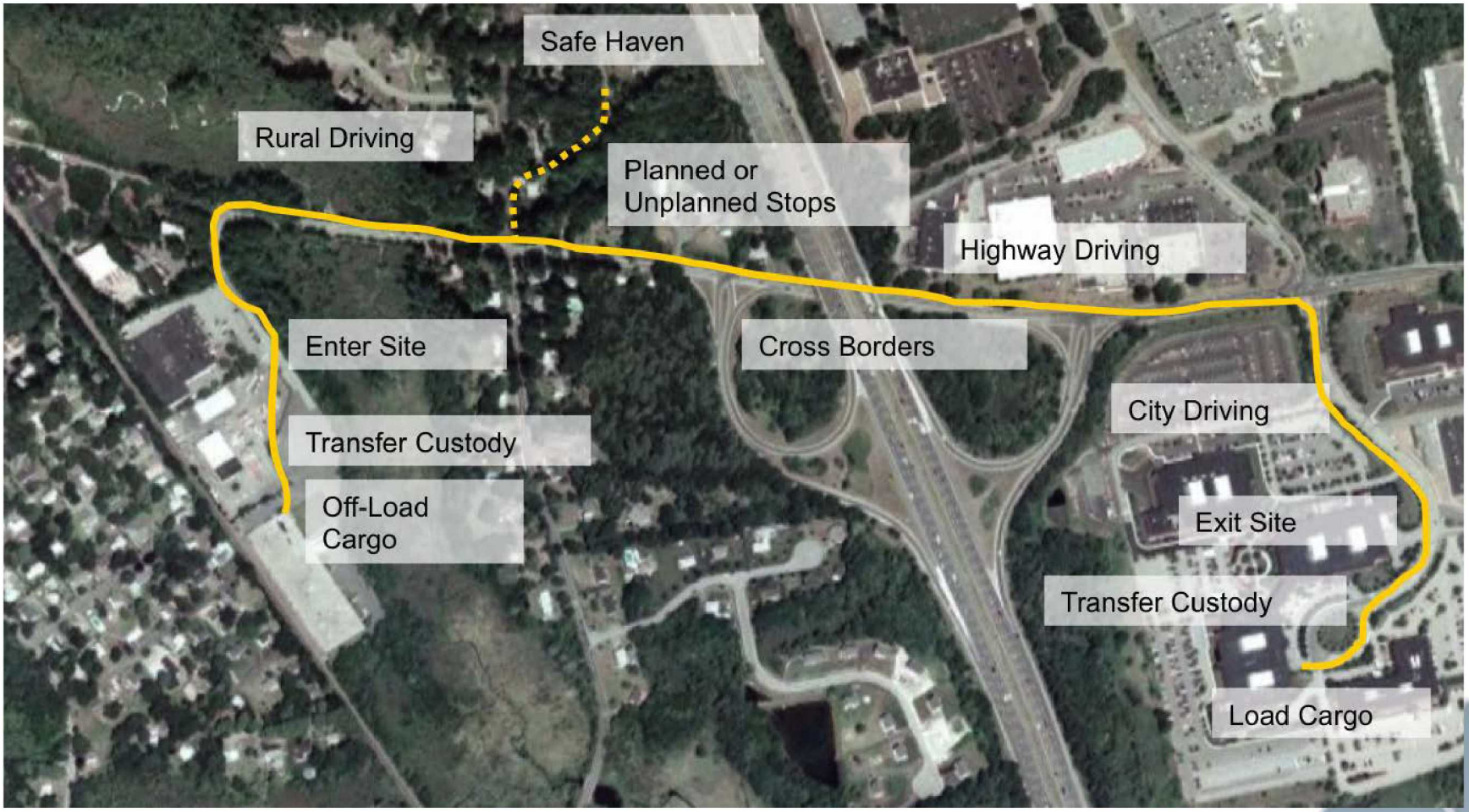
# Transportation Security Response

- Transportation Response
  - Response force numbers, equipment, and training required depend on the threat and operating environment
  - Continuous (secure) communications:
    - Each member of the response force & secondary responders
    - Transport Control Centre

# Transportation Response Considerations

- Transportation Response
  - Response force configuration
    - Number of responders and their location relative to target
    - Overt vs. Covert
    - Optimized based on terrain, time of day, vehicle state, other operating space conditions
  - Response Strategy/Contingency Plans
    - Individual response force responsibilities
    - Accident, vehicle trouble, sickness, weather, threat

# Possible Transportation Conditions



# Transportation Security Analysis Methods

- Requires scenario analysis instead of a path analysis
  - Travel through public areas with no protected area
  - Constantly changing surroundings
  - Adversary attack and first detection both begin at the target

# Summary: Transportation Security

- The scope of transportation security
- Similarities and differences between fixed site and transportation security
- Specific issues associated with transportation security
- Methods for analyzing transportation security

Module 19

# INSIDER OVERVIEW

# Lecture Outline

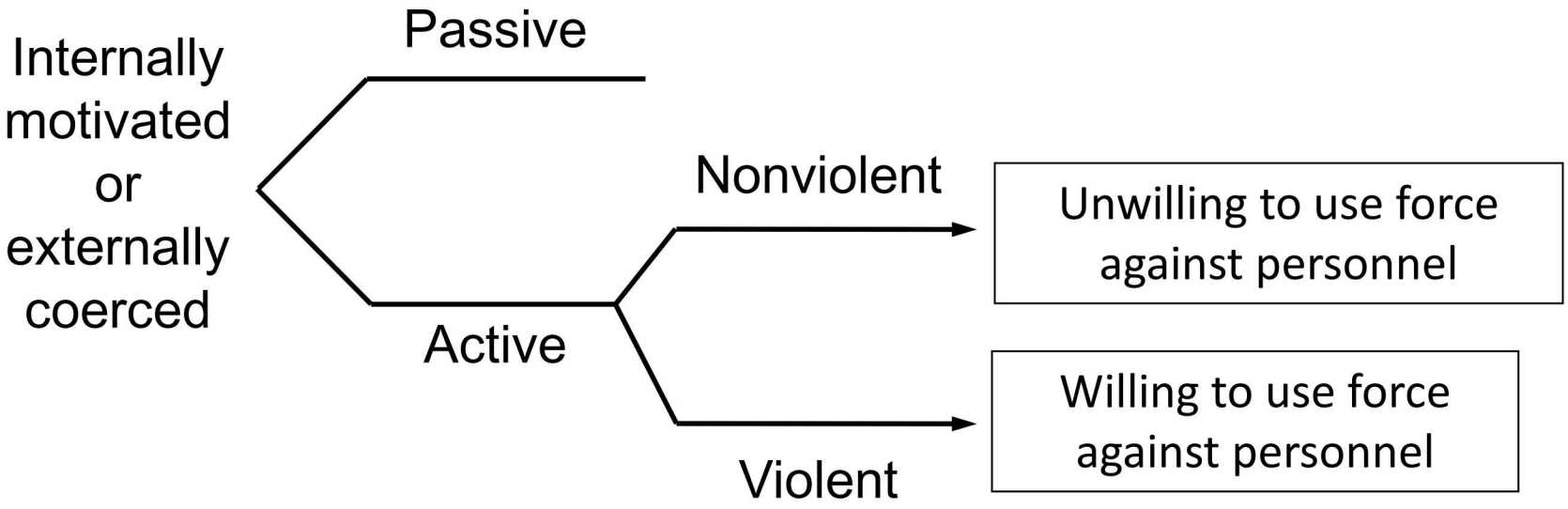
- Recognize an accepted description of an insider
- Identify insider unique issues and concerns
- Define potential insiders at a facility
- Discuss the insider analysis methodology

# Insider Definition

- One or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so. (From INFCIRC/225/Rev.5)

- Insiders might include, but are not limited to:
  - Management
  - Regular employees
  - Security personnel
  - Service providers
  - Visitors
  - Inspectors
  - Past employees

# Insider Categories




- All insiders can use stealth and deceit
- Violent insiders may be rational or irrational

# Insider Attributes

| Authorized access to nuclear facilities or transport (from definition) | Authority | Knowledge |
|---|---|---|
| Special/temporary/emergency access | Over people, tasks, and/or equipment (coercion) | Targets (location, characteristics, facility layout details, etc.) |
| Escorted vs. unescorted | Temporary/falsified authority | Security systems (response force details, operations, bypass info, etc.) |
| Access to special tools and/or knowledge | Exemption from procedures | Special tools/equipment (storage, access controls, etc.) |

# Insider Motivations

- Political
- Ideological – Fanatical conviction
  - Moscow Theater
- Financial – Wants/needs money
  - General Electric

***Note***: Motivation is an important indicator for both level of malevolence and likelihood of attempt

- Personal
  - Revenge – Disgruntled employee or customer
    - Idaho 1950s nuclear incident
  - Ego – "Look what I am smart enough to do"
    - Hackers
- Psychotic – Mentally unstable but capable
- Coercion – Family or self-threatened
  - 2006 London Robbery

# Factors Affecting Insider Attempt

Access

Knowledge

Authority

Insider Opportunity

and

Political

Ideological

Financial

Personal

Insider Motivations

~

Insider Attempt

# Insider Issues and Concerns

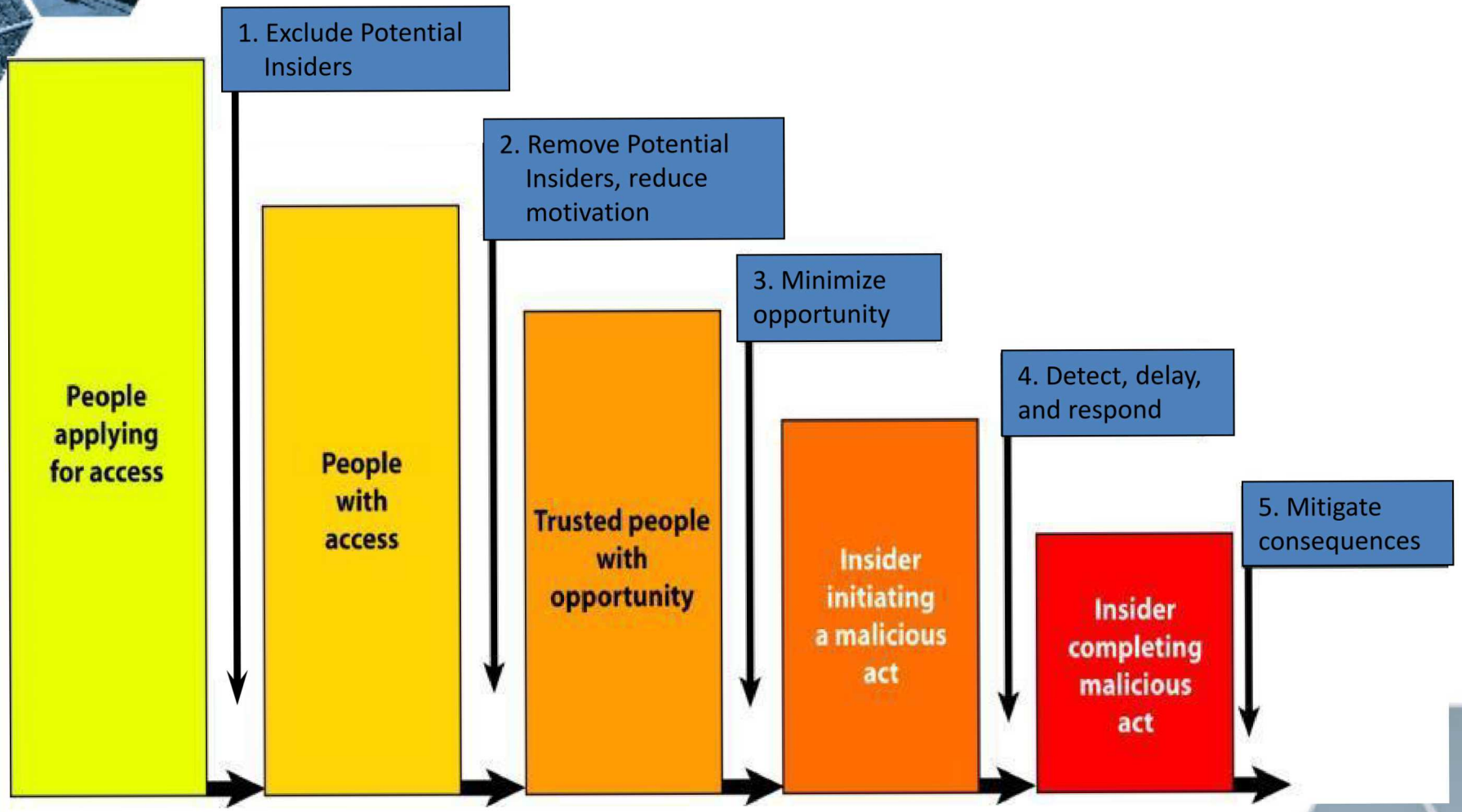
- Time
  - Can select optimum time to implement plan
  - Can extend actions over long periods of time
- Tools
  - Has knowledge of and capability to use tools already at work location
- Tests
  - Can test the system with normal “mistakes”
- Teamwork (Collusion)
  - May recruit/collude with others, either insiders or outsiders

# Insider Definition RECAP

- Categories
  - Passive
  - Active Nonviolent
  - Active Violent
- Facility insider characteristics:
  - Access, authority, knowledge
  - Motivation

- Insider advantages
  - Time
  - Tools
  - Tests
  - Teamwork

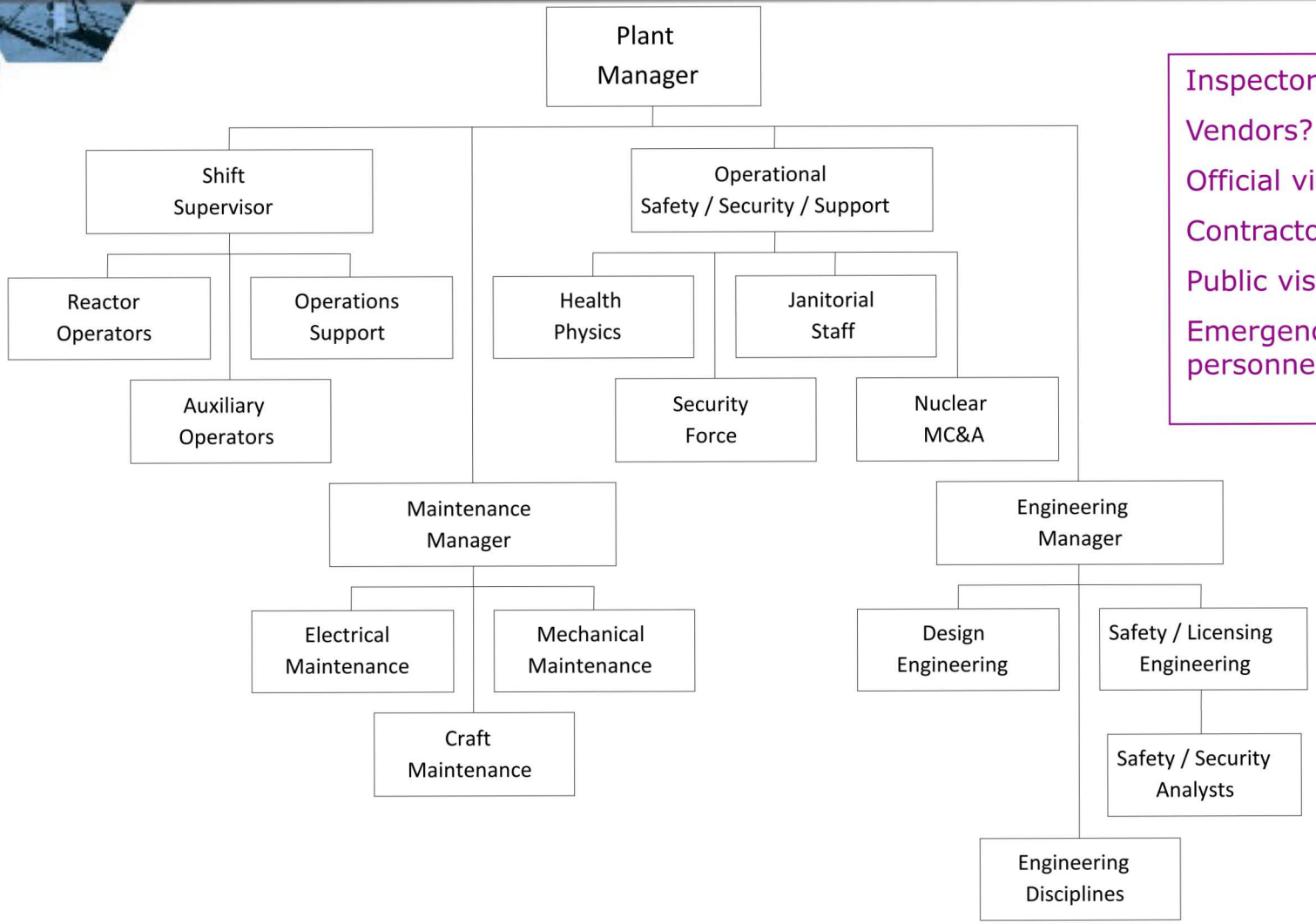
# System Approach to Prevent and Protect Against Insiders



# Facility-Specific Insider Analysis Methodology

- Collect facility or transport information
- Identify targets of interest
  - Abrupt unauthorized removal
  - Protracted unauthorized removal
  - Single-event sabotage
  - Protracted multiple-event sabotage
- Define facility-specific threat (insider groups)
- Evaluate the preventive and protective measures
- Summarize target/threat results

# Facility-Specific Threat Definition: Example




- Inspectors?
- Vendors?
- Official visitors?
- Contractors?
- Public visitors?
- Emergency personnel?

# Guidelines and Methods for Grouping

- Personnel should be grouped whenever:
  - Types have identical access, knowledge and authority
  - Access, knowledge and authority, of one type is completely a subset of another,

    -or-
  - Access, knowledge and authority are nearly identical—create a composite group to cover both (conservative).
- Groups may be:
  - Target-dependent
  - Indicative of potential level of insider problem
  - Based on Expert judgment
    - Preliminary grouping
    - Limited site access
    - Incomplete data
  - Based on Data-Based grouping
    - Job descriptions
    - Site access data
    - Personnel discussions

# Attributes to Consider During Grouping

**Access**

- Limited areas
- Protected areas
- Vital areas
- Nuclear materials
- Central alarm station
- Alarms
- Keys
- Badging
- Information management of access system
- Nuclear material records
- Nuclear material forms
- Site vehicles
- Tools
- Controlled information

**Authority**

- Supervisory
- Supervisory over guards
- Personal vehicle
- Exempt searches
- Exempt metal detector
- Exempt nuclear material detector
- Authorize nuclear material transfers
- Prepare nuclear material transfers
- Verify nuclear material transfers
- Verify inventory
- Assess alarms
- Issue badges
- Issue codes
- Prepare access lists
- Equipment maintenance

**Knowledge**

- Procedures
- Processes
- Locations
- Site details
- Physical protection system
- Frequency of events
- Potential vulnerabilities
- Tools, equipment
- Procedure violations

# Scenario Development

- Develop action sequence for each target
- Identify protection measures
- Define insider defeat strategies
- Determine protection measure effectiveness
- Develop most vulnerable scenarios

***Later, evaluate ALL targets!

# Analyze: Consider Response Issues and Compute $P_i$

- Consider response for an active non-violent insider
  - Detection usually occurs as soon as he goes active
  - Delay may be at end of pathway – need rapid response
  - Containment strategy for theft
  - Denial strategy for sabotage
  - Generally gives up if confronted: $P_N = 1.0$
- Assume $P_i$ equals combined $P_D$ (combined probabilities)
- Compute $P_N$ for active violent insider
- Calculate system effectiveness
- Include consequence mitigation

# Summary: Insider Analysis

- Insider:  Any individual with authorized access to nuclear facilities or transport who might attempt unauthorized removal or sabotage, or who could aid outsiders to do so.
- Such as, management, regular employees, security personnel, service providers, visitors, inspectors, past employees
- Insider issues and concerns
  - Time, Tools, Tests, and Teamwork

- Analysis process for insider:
  - Target Identification for Insiders
  - Facility-Specific Insider Threat Definition
  - Scenario Development
  - Protection System Evaluation
  - Summarize Insider/Target Results

Exercise

# INSIDER EXERCISES

# Day 4 Summary

- PPS Evaluation Overview
- Contingency Plan Overview
- Transportation Security
- Insider Analysis

Module 20

# NUCLEAR SECURITY PHYSICAL PROTECTION SUMMARY

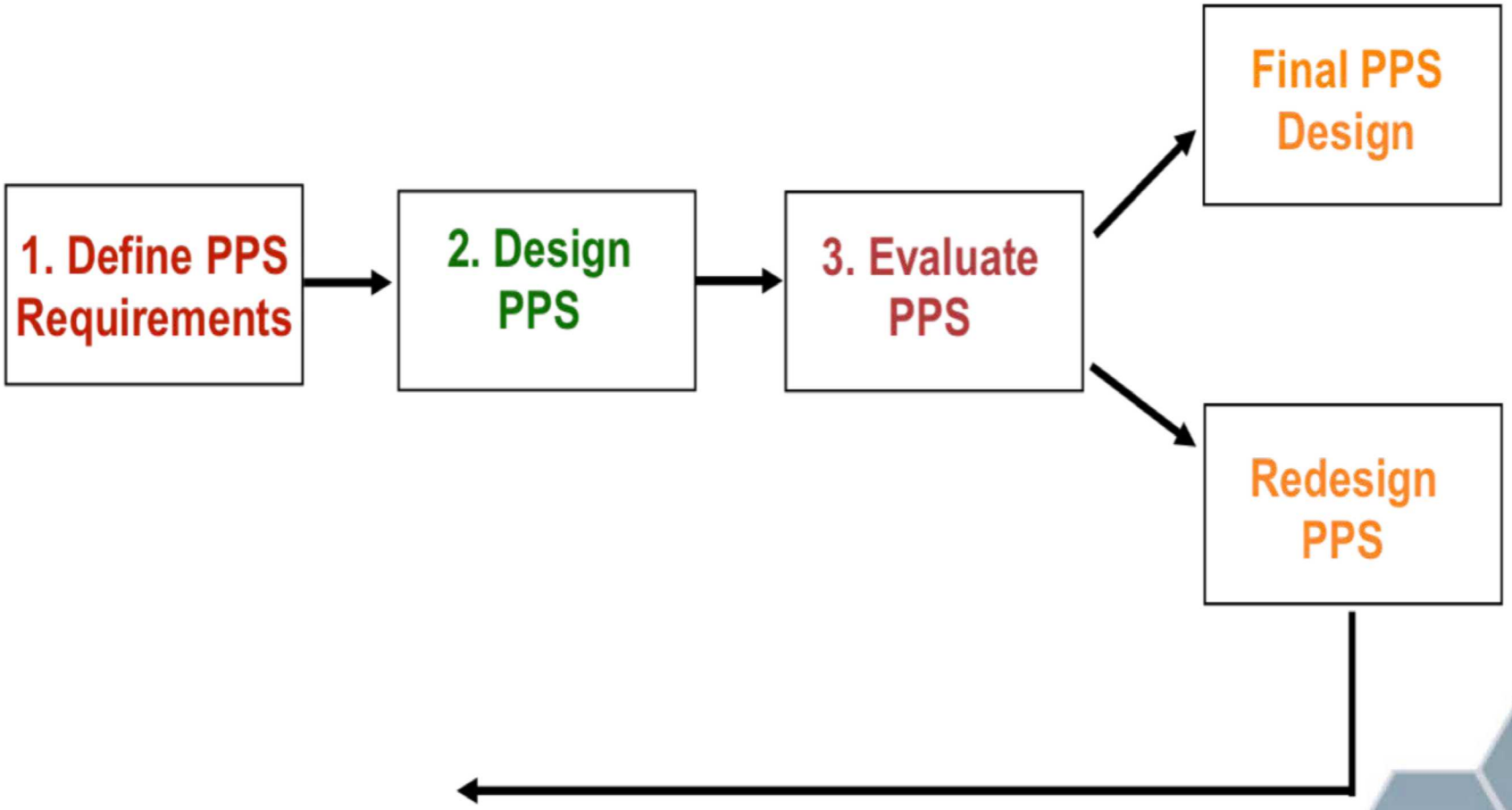
# Lecture Outline

- Discuss international legal instruments
- Review the DEPO Process

# International Legal Instruments

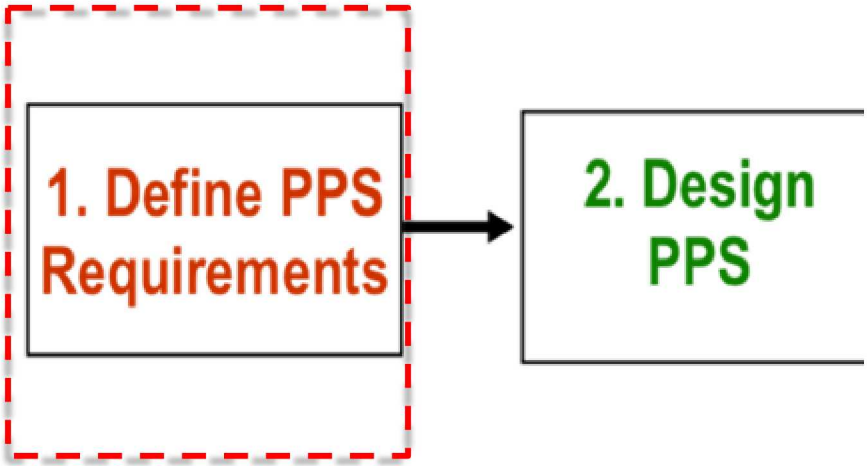
- Convention on the Physical Protection of Nuclear Material (CPPNM)
- Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM)
- UN Security Council Resolution 1373
- UN Security Council Resolution 1540
- Convention on the Suppression of Acts of Nuclear Terrorism
- INFCIRC 225 Document and other NSS documents

# DEPO Process

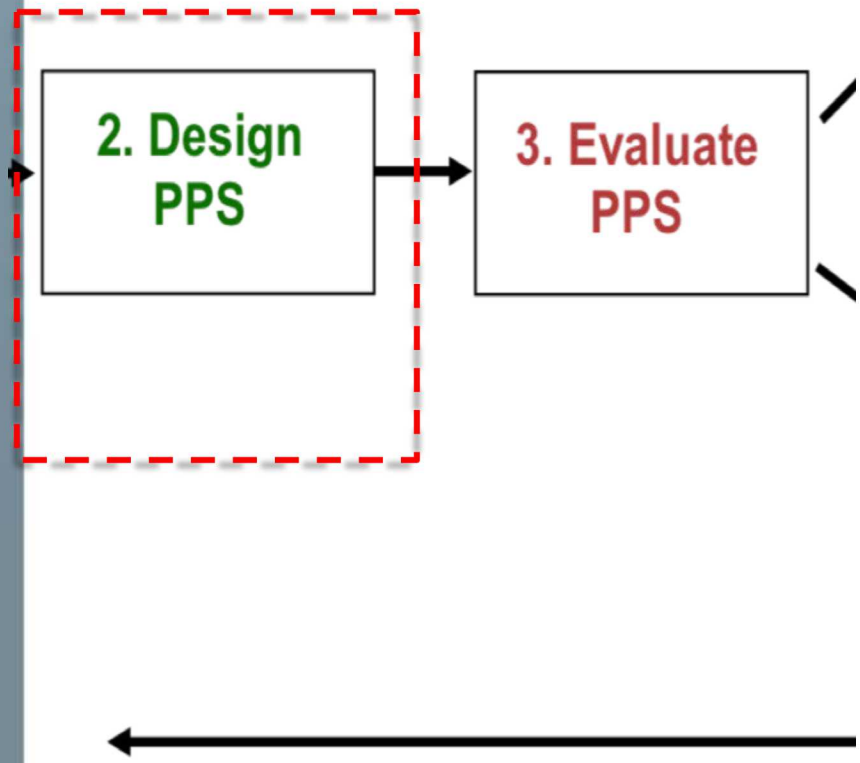


# DEPO Process

- Define PPS:
  - Inputs of PPS system including facility characterization, target identification, threat definition, risk management and regulatory requirements



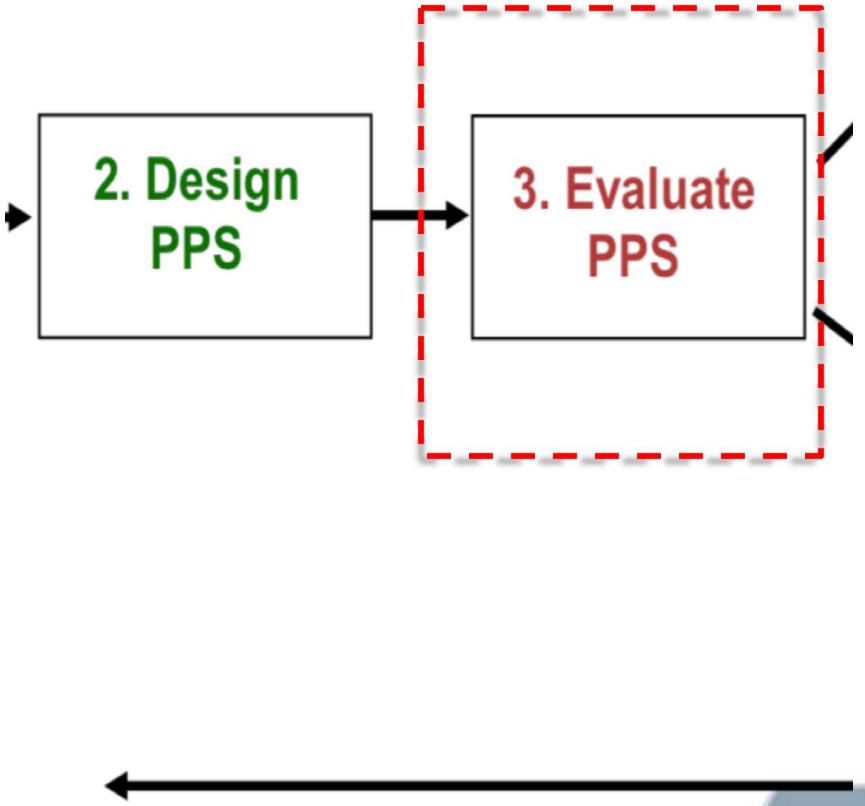
# DEPO Process




- Design PPS:
  - Variable of the PPS system including detection, delay and response force

# DEPO Process

- Evaluate PPS:
  - Testing of the PPS system including path analysis, ASDs, transportation security, neutralization analysis and insider analysis



# Summary: Nuclear Security Physical Protection Summary

- International legal instruments
- DEPO Process

# INFCIRC225 EXERCISE

1. What category of nuclear material would most likely be used at most nuclear power plants?

2. What category of nuclear material do you think would be used at most nuclear research reactors?

3. Is the physical security and nuclear security at universities sufficient to support a nuclear research reactor?

4. What requirements are written by your government for nuclear security?

5. You are moving nuclear fuel into your research reactor, what type of compensatory measures could you apply?

6. Three zones in your outer perimeter detection system are currently not working, what type of compensatory measures are needed?

7. Provide some examples of how to incorporate security by design?

8. How are Security Plans, Contingency Plans and Emergency Plans different and who should be responsible for each document? How often should these plans be exercised?

**Part 2:** Name the associated responsible organization in your country for the following physical protection regime legislative and regulatory framework elements.

| Legal and Regulatory Framework Element | Responsible Organization |
|---|---|
| International transportation | |
| What organization/entity assigns the responsibilities within each level of the involved governmental entities | |
| Formulation for defining a threat assessment and, if needed, a design basis threat | |
| Requirements for physical protection | |
| Requirements for licensing | |
| Requirements for evaluating elements of a physical protection system | |
| Specification of a trustworthiness policy | |
| Requirements for enforcing physical protection regulations | |
| Sanctions against the unauthorized removal and against sabotage | |

Who is your competent authority for the following:

a. Threat Assessment/Definition of DBT? _____
b. Licensing?_____
c. Regulations?_____
d. Inspections? _____
e. Response? _____
f. Emergency Response? _____

Additional discussion questions:

1. Should the regulator have inspectors on-site at all times? If so, what are the advantages and disadvantages?
2. Should regulators be allowed to conduct no-notice inspections?
3. Who should the competent authority report to in the government?
4. Should the competent authority be the same for a nuclear power plant and a nuclear research reactor?

## NUCLEAR SECURITY CULTURE EXERCISE

PAUL SMITH

Phone: 555-513-5484
E-mail: paulsmith28@gmail.com

### Objectives

Leverage expertise in nuclear design, safety, and project management.

### Education

**Masters** (August 2010)

- Civil Engineering degree from Five Star University
- GPA: 4.0
- President of Engineering Society

### Experience

Senior Engineer (December 2010 –September 2013)
ABC Nuclear Company
Incorporated design requirements into analysis and design documents
Provided technical guidance and mentoring to less experienced engineers
Lead engineer on new water pump design
Led the safety team through 5 successful safety audits

### Skills

- Experience with 6 Sigma Black Belt events
- Project Management Professional
- Plant Design
- Mechanical System Design
- Safety initiative lead

**Group Exercise: Case Study (20min)**
*Recruitment and Hiring*

Paul is a smart engineer with impressive accomplishments. Managers at Lagassi Nuclear Research Institute were eager to interview Paul after reviewing his resume. Paul skillfully interviewed with several managers and staff. Everyone was enthusiastic with the idea of hiring Paul as soon as possible.

Before an employment offer could be extended, a required, thorough background investigation would need to be completed. The background investigators were diligent, uncovered some interesting facts about Paul.

## Background Report – Resume

There a few small inconsistencies on Paul's resume:

- His university reported an overall GPA 3.5, not 4.0. Paul performed poorly on a few non-engineering classes that he did not include in the GPA on his resume.
- As a member of his university's Engineering Society he coordinated a small seminar with several guest speakers on behalf of the President during the President's medical absence, but he was not the President.
- Although Paul took some project management and 6 Sigma classes, he is not a 6 Sigma black belt or a certified project management professional.
- Paul, as designated Deputy Project Manager, coordinated the audit meetings and activities for the safety team at ABC Nuclear Company, but he was not the lead technical contributor

When asked about these inconsistencies during his investigation interview, Paul was open and honest, explaining that a typical resume formats are not conducive to long explanations best discussed during an interview.

## Background Report – Family History

Paul grew up in a very poor family, but through his own hard work was able to do well in school and get a full scholarship to Five Star University. Now that Paul is working, he supports his parents financially. Sometimes his siblings ask for loans that are never repaid. This puts Paul under considerable financial strain.

Paul's older brother, Michael, is currently in prison on gang related charges. Michael will be released from prison in 3 months and will be looking for a job.

During Paul's investigation interview, he confessed that his sister, Rachel, has a skillset in cyber hacking. She has been known to put her skills to use for criminal purposes if the price is right.

1. Would you hire Paul Smith for an Engineering Support position? Why or Why not?

2. How would your facility address this scenario?

3. Is Paul Smith a potential security risk?

*During Employment*

Time: 20 minutes

Paul is met at the LNRI PTR gate by a coworker who says he has left his badge on his desk. He asks Paul to let him in so he can go get it.

Paul recognizes the coworker as someone he works daily with so lets him in and goes to his own office.

Later, Paul sees the employee with a toolbox in an area he does not normally work in and notices that he is still not wearing his badge. Paul is unsure whether to challenge the coworker or go talk to his manager.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

# TARGET IDENTIFICATION EXERCISE

| Facility | Location | Form of Material | Amount of Material on Site (wt% enrichment) | Total Isotope Amounts | Level of Radiation |
|---|---|---|---|---|---|
| PTR Research Reactor | Reactor | $BeO-UO_2$ Fuel Rods (236 in reactor) | 67.5 kg U (36% $^{235}U$) | 24.3 kg $^{235}U$ | High >1 Gy/hr at 1m |
| | R090 Fresh Fuel Vault | $BeO-UO_2$ Fresh Fuel Rods (50 in storage) | 14.3 kg U (36% $^{235}U$) | 5.2 kg $^{235}U$ | Low |
| | Irradiated Fuel Pool | $BeO-UO_2$ irradiated fuel Rods (100 in pool) | 28.6 kg U (35% $^{235}U$ | 10.0 kg $^{235}U$ | High 0.02-0.03 Gy/hr at 1m |
| | R091 Product Vault | Pu Experiments<br><br>HEU metal<br>Other Sources | 9.3 kg $^{239}PuO_2$ (100% $^{239}Pu$)<br>23 Kg U (95% $^{235}U$)<br>Cs, Am, Sr | 8kg $^{239}Pu$<br><br>22 Kg $^{235}U$<br>3 kg total | Low<br><br>Low<br>High |
| NBR Reactor Facility | R100 | Fuel in Reactor Core (10 discs) | 14 kg U (93% $^{235}U$) | 13 kg $^{235}U$ | Low |
| | R102 | HEU-metal Fresh Fuel (9 discs) | 12.6 kg U (93% $^{235}U$) | 11.7 kg $^{235}U$ | Low |
| | R102 | Used Fuel (1 discs) | 1.4 kg U (93% $^{235}U$) | 1.3 kg $^{235}U$ | Low <0.003 Gy/hr contact |

1. Identify the category of nuclear material according to the table in INFCIRC/225/Revision 5:

   ____ 12 Kg of Uranium-235 Enriched to 7%

   ____ 3 Kg of Uranium-235

   ____ 15 Kg of Unirradiated Uranium-233

   ____ 12 Kg of Uranium-235 Enriched to 15%

   ____ 16 g of Plutonium

   ____ 15 g of Plutonium

   ____ 14 g of Plutonium

## Manual Listing of Targets and Theft Categorization

1. Develop an itemized target list for nuclear material at the PTR and NBR facility. Include location, material form, element (U or Pu) and % enrichment ($^{235}$U or $^{239}$Pu), element quantity (all isotopes), and radiation level.

2. Next, on the basis of INFCIRC/225 Categorization of Nuclear Material table given in the text §3.7.3.1, categorize the targets.

| Location | Form of Material(s) | Element and %Enrichment ($^{235}$U or $^{239}$Pu) | Element Quantity (kg) | Radiation Level (Gy/hr at 1 m) | Theft or SAB Target? | Category |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## DESIGN BASIS THREAT EXERCISE

The following Threat Assessment is prepared to assist the Development of the State Design Basis Threat (DBT). The Threat Assessment is organized into threats from two ideological terrorist groups and one activist group. As you review the Threat Assessment, consider the following policy issues for the State of Lagassi when developing the DBT:

- Lagassi is a developing state with limited economic resources. Significant increase in protection costs could strain the fragile economy.
- Lagassi has evolved from a somewhat unknown state on the world stage to an emerging economic state. This emergence has quickly increased the crime rate and a recently growing interest from terrorist groups.
- The people of Lagassi are proud of the historical accomplishments and their intellectual contribution to science. This includes the many accomplishments of the research reactor, including the recently awarded Nobel Prize for Physics.
- The state is politically democratic but has several political factions. The current government struggles to maintain its power base.
- A DBT review is scheduled for every 3 years.
- The people of Lagassi trust their government to make the appropriate decisions to protect them; any breach of that trust will greatly undermine the government's ability to maintain power.

### *International Ideological Terrorist Groups:*

There are two ideological terrorist groups assessed in this report: The Antarctics and Peoples Liberation Movement.

#### The Antarctics

The Antarctics are founded, and continue to be a lead by Adrian Baker, a former professor of global economics. His deputy is Jose Digger, a former nuclear scientist and committed revolutionary. Baker embraced anarchist politics as a graduate student and developed a distinctive academic stance. He was dismissed from his academic post for his revolutionary views. He spent time working with various rebel groups before he put his thoughts into print. His most famous book, "The Antarctic Economy," was published in 1985. In it he argued that global trade is responsible for all environmental degradation and that the major economic blocks deny the opportunity for the rest of the world to develop environmentally sustainable local economies. In the book he develops his arguments by theorizing how an anarchist terrorist group might return the world to a

pre-trade era. He chose the name the Antarctics because, he said, it had symbolic value. It was white, pure, and pristine.

Baker disappeared until 1998 when a small explosion occurred on a pipe-line north east of the Republic of Varnado. The explosion was commonly thought to be the work of a local terrorist group, but they denied it. Noticed only by one or two of the world's intelligence agencies – and dismissed as a hoax – was a claim on a website in the name of the Antarctics.

Less is known about Jose Digger. After national service in a nuclear submarine, he trained as an engineer and has worked at nuclear power plants. He is believed to have spent some time on a research project designing novel small nuclear reactors. He was a committed revolutionary. It has been suggested that he blames western capitalism for the world's poverty and for this purpose he has allied himself with Baker.

Digger came to official notice after a second explosion at an oil refinery in Northern Stoyia. The explosive was placed on sensitive processing equipment within the controlled area of the refinery. It was again attributed to, but denied by, a local political terrorist group. Again, the Antarctics, claimed responsibility and included a description of the device, confirmed months later by forensic analysis, on their website.

The whereabouts of Baker and the Digger are typically unknown but recent highly sensitive intelligence reports them being in the mountains just north of Lagassi. They are thought to move easily among a number of separatist groups (Uplanders), and because of their intelligence and competence as well as their anti-everybody stance, are trusted by serious criminals. The latter are believed to offer them protection, and in exchange for small favors, operational support such as false documentation and small arms. These criminals, however, will not risk prejudicing their lucrative lifestyles by becoming too closely identified with the Antarctics.

The Antarctics originally believed that they should only have two members. However, the numbers of plausible Antarctic claims have risen substantially in the last 18 months and it is clear that they have recruited some dedicated support. It is estimated that there are up to five capable operatives involved. Forensic evidence suggests that there is now more than one bomb maker, although it is likely that they are all trained by the Digger. Analysis of the metals used suggests that he has created a sophisticated workshop or small factory. The metal case of one device contained minute quantities of $CO_{60}$ but it was not possible to say whether this was from contaminated scrap metal or had been picked up in the factory.

It is believed that Baker is feeling older, he may even be terminally ill. If so, the fear is, he will want to do as much damage as he can before he dies. He cannot be confident that his beliefs and passion will outlive him. Based on this belief, his greatest desire

would be to cause a nuclear winter and Digger's explosive expertise may be designed to support this effort. The intelligence consensus is that he now has no constraints other than to avoid capture. That too may end as he nears death and he may be prepared to risk arrest to achieve one final victory.

The most common means of attack used by the Antarctics is the improvised explosive device (IED). Improvised is something of a misnomer. These are sophisticated, highly reproducible devices built to precision. There is a preference for plastic explosives but black powder as well as a variety of non-commercial explosive mixtures have been used.

To supplement their income, the Antarctics have been accused of several bank robberies in a series of central continental states. This is unproven, but the professional planning and use of sophisticated, light equipment and weapons tends to point to the group. The method of operation for the robberies was three Individuals enter the bank, take control of the employees, customers, and guards and complete the robbery, while one of two others provided cover and escape. In each case, the alarm communications systems of the bank had been disabled just before the robbery and the video cameras diverted.

It is unlikely that the Antarctics will turn to suicide attacks. There is no evidence that they are even willing to risk their life, but their ultimate motivation, and Baker's health may change that.

### The People's Liberation Movement

The People's Liberation Movement (PLM) was founded in 1994 by their religious messiah, know publically as Reverend X. The group's goal is to lead the world to the pious way prior to the end of the earth through dialogue, proselytism, and, if necessary, intimidation. They view governments as the barrier to the path to piety and are therefore, staunchly anti-government. They are also competitively anti-other religious beliefs, believing their theology, which is a mixture of the world's major religions, is the only true approach. The group's objective was announced publically on Dec 31, 1999 when they claimed responsibility for a truck bomb made of fertilizer and diesel fuel, which leveled the Evanistan parliament building. There were no casualties, but the announcement came with a warning to head the way or else.

A break up in 2002 greatly weakened the group's organization, and many leaders—not including Reverend X—were arrested. Since this time, PLM members have dispersed, gone underground, and infiltrated many other organizations. They await instruction from Reverend X. As a result, they are viewed as very resourceful, highly educated, very dangerous, and potentially suicidal.

A recent PLM member was captured during a foiled attempt to disable a military airport traffic control station using a home-concocted lethal gas in Dianistan. Interrogation of the member by a military officer at the air traffic center provided great insight into the mindset of the membership at large. From what was learned, it appears that members work alone and have little communication with each other. The PLM received instruction and the recipe for the lethal gas from an unknown (to him) source.

### *Activist Group:*

#### Yellow-Green League

Although vehemently denied by its official spokesman, the Yellow-Green League is the political front for the **Environmental Defenders (ED),** one of the oldest environmental activist groups. The Yellow-Green League stands in elections and currently holds about 15% of the seats in the Regional Assembly. It came in a close second in four of the National Parliamentary seats at the last election.

The ED has historically pursued aggressive and even violent means to achieve its ends, which are to protect the environment from damage for future generations. The approach has included protests, sabotage of facilities and transport, and physical violence against workers and government officials related to the research reactor. There is reported to be vigorous debate within the League and ED about future strategy. A younger leadership is emerging that believes that any hint of violence may be counter-productive to the desire to pursue a national anti-nuclear stance, whereas older members are more inclined to pursue methods that have worked in the past.

The last large activity of the group was a demonstration two years ago that turned violent. A group of 300 protesters advanced on the reactor at dawn on a Sunday morning and climbed the fences in unison. The guards were called out but were quickly overwhelmed by the mob who came to paint a slogan on the reactor building. A few guards tried to use force to repel the protestors, and the confrontation turned violent. One guard was killed, and two were hospitalized. It is thought that a few violent instigators were responsible for inciting the violence. There is some evidence that the group may have been infiltrated by local terrorist groups.

**Miscellaneous intelligence thought to be relevant**

1) **Yellow-Green League**

Intelligence

A source has reported that the YGL leadership plans to buy land adjacent to the site of the research reactor. The land includes the road over which fuel shipments are transported. The intention is to resell the land in lots of 1 sq. m.

Assessment

The source volunteered this information to us. The source is new and unproven but is known to have direct access to the ED leadership. We believe the source to have been motivated by personal vengeance and assess the intelligence to be credible.

## Part 1 – Compile a Table of Threat Entity Capabilities based on the Threat Assessment

The purpose of this exercise is to familiarize the team and interpret the threat assessment in a format that will simplify the development of a DBT. For this exercise, assume your sub-group is the national task force, assigned by the government to undertake the development of a DBT for Lagassi. From the threat assessment information in the data book, organize the data for each threat entity into one consolidated matrix. Rate the Likelihood of Potential Action and Motivation using "High", "Medium", or "Low". For Capabilities, write a statement.

| | 1<br>Antarctics | 2<br>PLM | 3<br>YGL |
|---|---|---|---|
| **Likelihood of Potential Action** | | | |
| Theft | | | |
| Sabotage | | | |
| Other _____ | | | |
| **Motivations** | | | |
| Ideological | | | |
| Economic | | | |
| Personal | | | |
| **Capabilities** | | | |
| Number of attackers | | | |
| Type of weapons | | | |
| Explosives (type and quantity) | | | |
| Transportation | | | |
| Power and hand tools | | | |
| Technical skills | | | |
| Level of funding | | | |
| Infrastructure | | | |
| Collusion with Insider (passive or active support) | | | |

## Part 2 – Use DBT Process to Develop CBT from Threat Assessment for Hypothetical Facility

The purpose of this exercise is to define a DBT that the facility will be expected to protect against.

**Task 1:** Review the threat entities in the threat matrix, and set aside any that do not appear relevant for the DBT because:

- The capability (assuming no PPS) is insufficient to initiate an unacceptable consequence
- The motivation and intention is incompatible with an unacceptable consequence with the material.

YGL will be set aside due to having no motivation for theft or release of rad material

**Task 2:** Develop a composite adversary from the capabilities of the remaining threat entities. Use the table on the next page to develop the composite adversary. Provide a rationale for how your group decided on each composite characteristic.

**Composite Based Threat**

| | Composite Adversary | Justification for decision |
|---|---|---|
| **Likelihood of Potential Action** | | |
| Theft | | |
| Sabotage | | |
| Other _____ | | |
| **Motivations** | | |
| Ideological | | |
| Economic | | |
| Personal | | |
| **Capabilities** | | |
| Number of attackers | | |
| Type of weapons | | |
| Explosives (type and quantity) | | |
| Transportation | | |
| Power and hand tools | | |
| Technical skills | | |
| Level of funding | | |
| Infrastructure | | |
| Collusion with Insider (passive or active support) | | |

**Part 3:** Apply policy considerations to the composite adversary and either increase, decrease or include capabilities as appropriate.

The policy considerations include:

- Degree of conservatism either because there is low confidence in the data, or the desire for robustness considering uncertainty into the future.
- Cost-Benefit-consequence Trade-offs understanding the costs of protection, the severity of consequences, and the benefit of nuclear industry to society. Consider protection provided to other industries with similar consequence severity.
- Political factors which would cause the State to assume threat characteristics with no other supporting information, such as public concerns, or neighboring States.

| ***Policy Consideration*** | ***Changes in Composite Based Threat*** |
|---|---|
| Degree of Conservatism | |
| Robustness into the future | |
| Capabilities included for prudence | |
| Costs of Physical Protection | |
| Public Confidence | |
| Other | |

**Part 4:** Separate the remaining threat description into those capabilities assigned to the DBT, and those other threats for which Protection is required. All remaining threats should be part of DBT or other threats.

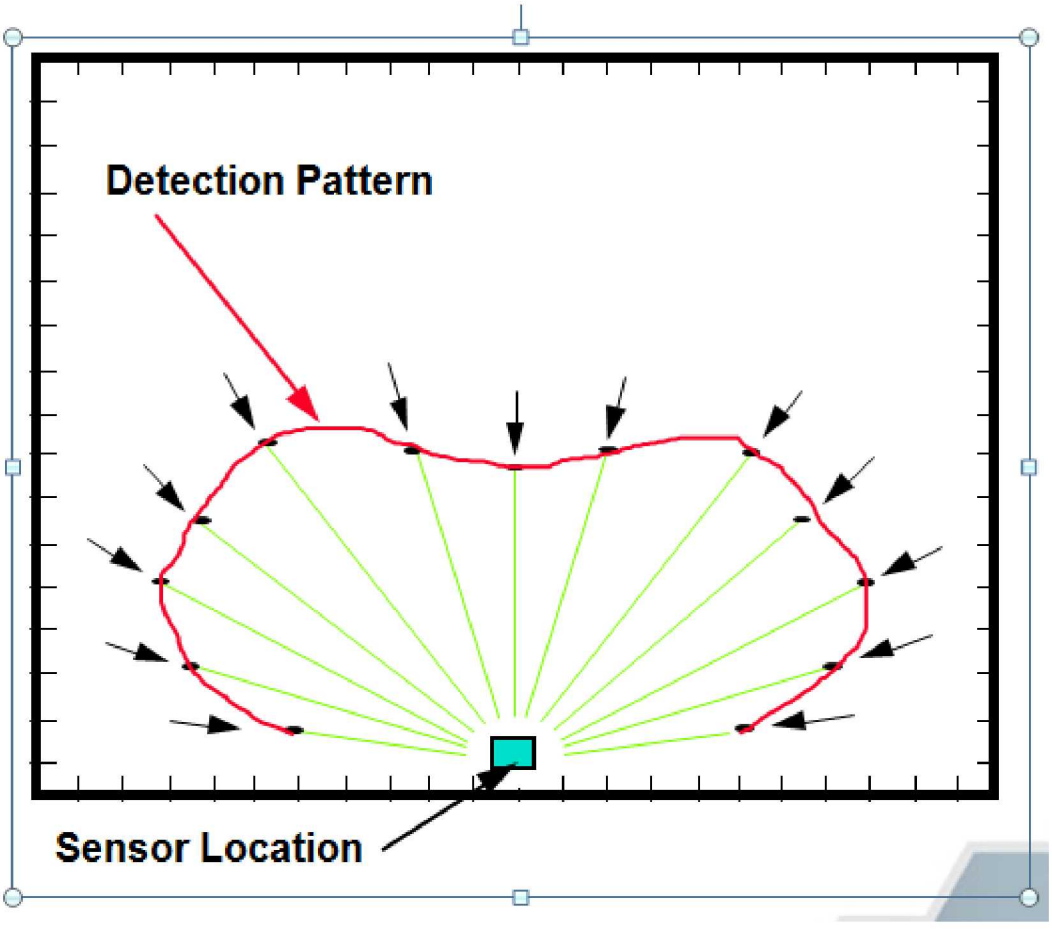
**STATE DBT**

| | DBT | Other Threats |
|---|---|---|
| **Likelihood of Potential Action** | | |
| Theft | | |
| Sabotage | | |
| Other _____ | | |
| **Motivations** | | |
| Ideological | | |
| Economic | | |
| Personal | | |
| **Capabilities** | | |
| Number of attackers | | |
| Type of weapons | | |
| Explosives (type and quantity) | | |
| Transportation | | |
| Power and hand tools | | |
| Technical skills | | |
| Level of funding | | |
| Infrastructure | | |
| Collusion with Insider (passive or active support) | | |

# SENSOR PERFORMANCE TESTING EXERCISES

**Exercise 1 – Discuss  plan for sensor testing**

Develop a plan of the sensor to be tested and distance of detection pattern.  This includes distances, speed, location, area, markers used, and detection methods that would be considered.  The question you should be asking as a group is how do I want to test this sensor and what am I trying to achieve.



### Exercise 2: Test Preparation and Planning

Prepare the test and conduct planning of the actual test. This will include preparing worksheets, preparing the location, and roles and responsibilities of the team members. You should also have a goal of what you are trying to accomplish and what safety measures need to be considered. At this point, you will list assumptions for the test, consider any constraints, and how the data will be collected.

### Exercise 3: Conduct Test

Conduct the test as per the exercise plan you previously created. Remember, that you are testing per the plan. There should be no deviations and any changes should be noted and explained. Collect the data and make sure that you have sufficient information. It is better to have too much information than not having enough information.

### Exercise 4: Analyze Data and Prepare Presentation

Analyze the data and create presentation for the rest of the participants. The presentation should show the process you used and the information above. Don't forget to list goals, assumptions, results and lessons learned.

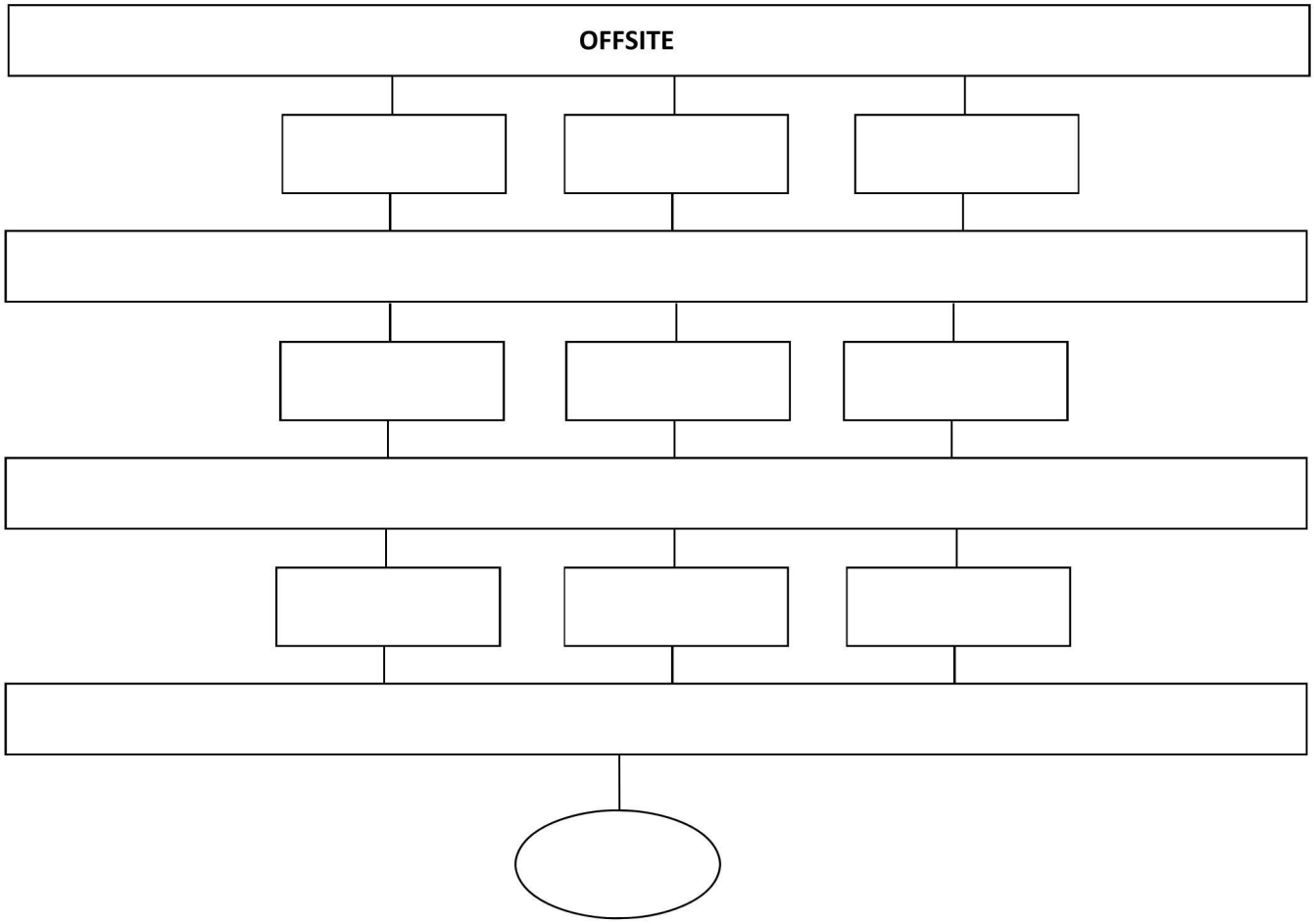
### Exercise 5: Present Results

Present the results. The presentation should be about 10 minutes and you can use electronic (PowerPoint) or paper (flip charts and manual measures.

# ADVERSARY SEQUNCE DIAGRAM EXERCISE

Develop an Adversary Sequence Diagram for this facility. Start from OFFSITE and proceed to the target enclosure. Define physical areas, protection layers, path elements, and target location. Using the slide from the presentation as an example, complete the following steps:

- Identify the physical areas and define the path elements that make up each protection layer between the adjacent physical areas
- Identify target location and other vital areas



# INSIDER THREAT EXERCISE

**Small Group Exercise: Case Study #1**

*Insider*

For the past year, Paul shared an office with Jim. Jim had been with the company for 20 years and always seems over-worked. He never seemed to have time to go out for lunch with the other coworkers or talk about sports in the hallways. The only time that he would take a break from his work was to complain about "stupid company policies" or "incompetent managers". Although Jim's rants were annoying at times, Paul didn't mind sharing an office with him because he mostly kept to himself and focused on his work. Over the course of a few short weeks, Paul began to notice some pretty big differences in Jim's behavior. Jim not only started going out to lunch, but he offered to pay for everyone. He was always smiling and laughing, things he never seemed to do before. One day after work Paul saw Jim leave work in a very expensive sports car. This didn't make any sense to Paul because Jim had always complained about not having enough money.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

**Small Group Exercise: Case Study #2**

*Insider*

Paul's family routinely asks him for loans that they never pay back. He would feel guilty saying no to them because after all they are family. Until now the requests have been manageable, but Paul's mother has been going through some expensive health procedures. Paul had to put these extra expenses on his credit cards, but he is reaching his credit limit and running out of options. His mother's health is the highest priority so he needs to find another way to find money quickly.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

**Small Group Exercise: Case Study #3**

*Insider*

Paul wanted to see if he could do some freelance work on nights and weekends so he posted his resume on a social media site. His resume was very detailed about the type of projects he worked on, how he impacted those projects, and it even stated that he had an active security clearance. Just a few days after posting his resume, he was contacted by someone interested in his work. The contact told him that if he downloaded all of the project files onto a CD he would give him a large amount of money. Although these documents were classified, Paul thought there would be not much harm in sharing the information because the projects had long been finished. Paul went to work the next day and secretly download the files. He sent the CD to the contact and received the large amount of money.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

**Small Group Exercise: Case Study #1**

*Management*

Paul has seen Robert driving a new luxury sports car to work. Paul had recently heard Robert discuss some financial difficulties. Paul reports his concerns to management, but no action seems to have been taken.

Paul also observes his manager yelling at a co-worker who has reported a security concern. Paul is hesitant to report anything to his manager now and is not sure who to report his concerns to.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

**Small Group Exercise: Case Study #2**

*Management*

Time: 20 minutes

Paul observes that the PTR facility manager is driving his vehicle into the PRN protected area. Because of his security training, Paul recognized the potential security risk of this behavior. He tries to discuss it with his manager and is told that it is one of the privileges of being a manager. Paul lets the matter drop.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

**Small Group Exercise: Case Study #3**

*Management*

Time: 20 minutes

The manager notices that Alice, a material balance custodian, is routinely late for work. The manager asks Paul, who also works in the PTR, if he knows of a reason for this before confronting Alice. When the manager talks to Alice, she states she just doesn't like to be in the morning rush. However, after this meeting, he also notices that Alice appears to be taking long lunches and tends to leave before her coworkers. He decides that disciplinary actions are needed. During subsequent meetings, Alice states how important she is to facility operations and jokes that she just might take some material.

**Small Group Discussion:**

1. What are the good or bad indicator(s) of nuclear security culture in this case?

2. How would your facility address this scenario?

3. What improvements would enhance nuclear security culture in this case?

# BACK UP EXERCISES

**Threat Definition Discussion Exercise**

Discuss what factors might change the state provided DBT

- Degree of conservatism
- Robustness into the future
- Costs of physical protection
- Public confidence
- Other

Discuss how to use the DBT to protect the site and to help develop policy

**Intrusion Detection - Exterior**

Sensor Placement: For a single fence perimeter around the facility, list the positive and negative aspects of applying the following types of exterior sensors:

| Sensor | Positive | Negative |
|---|---|---|
| Microwave | | |
| Infrared | | |
| Tautwire | | |

**Intrusion Detection - Interior**

Sensor Selection: For the facility, indicate which sensors should be chosen to best accomplish the specified task and explain why:

| Sensing Task | Sensor Type | Explanation |
|---|---|---|
| Boundary penetration for wall or ceiling or floor | | |
| Motion detection within the classroom | | |
| Door penetration | | |
| Window penetration | | |

**Entry Control**

Selection of personnel identification equipment: Using the information provided below, select the personnel identification equipment that satisfies the following requirements:

- The personnel identification equipment must be very user friendly
- The equipment must have a user throughput rate of at least 6 persons/minute
- The equipment will be used at an exterior fence gate

**Selected Equipment: _____**

**Reasons: _____**

**What type (if any) environmental protection is required? _____**

| Technology | Verification Time [s] | False Reject Rate | False Accept Rate | User Acceptability | Adverse Conditions |
|---|---|---|---|---|---|
| Iris Pattern | 10** | Medium | Very low | High | Reflections (e.g., glasses) |
| Face | 4* | Medium | Medium | High | Ambient light changes |
| Hand Geometry | 4* | Low | Low | High | Direct sunlight on platen; dust/dirt |
| Fingerprint | 4* | Medium | Very low | Medium | Dust/dirt, dry fingers |
| Voice | 10* | Medium | Medium | High | High noise |

* Includes time to enter PIN or read a card
** Recognition time (no PIN or card read)

**Contraband Detection**

Indicate where the following types of contraband detectors should be located and for which direction of personnel flow (entering or exiting):

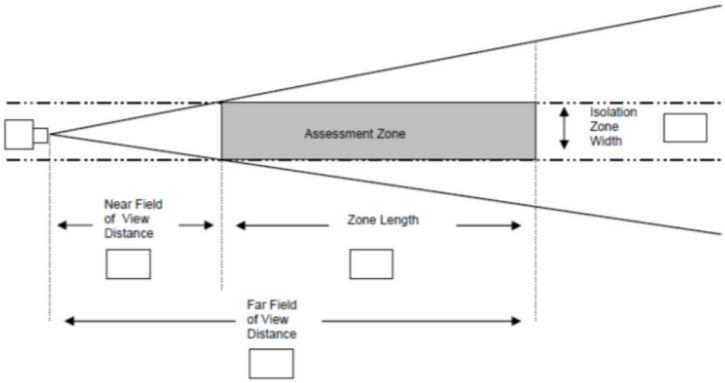
*Please use "E" for entering and "X" for exiting

| Situation | Metal Detector | Explosive Detector | Radiation Portal | Explanation |
|---|---|---|---|---|
| Entrance into the main gate a large nuclear power plant complex | | | | |
| At a PPS control console which allows putting detection equipment into access or secure mode | | | | |
| Entry into the accounting Paymaster's office | | | | |

**Alarm Assessment**

**(OPTIONAL)** Exercise #1: Camera Placement: Assuming the perimeter of the facility runs approximately 125m by 200m and has two parallel fences 12m apart, using the camera information provided below, suggest proper placement of exterior cameras for assessment. Keep in mind the cost associated with each installed camera.

| Camera Focal Length | Near field of view distance [m] | Far field of view distance [m] | Assessment Zone Length [m] |
|---|---|---|---|
| 12mm | 23 | 56 | 23 |
| 25mm | 47 | 118 | 71 |
| 35mm | 66 | 164 | 98 |



**Alarm Communication & Display**

Display Comparisons: The table below contains examples of information that can be displayed on computer display monitors and CCTV monitors mounted in a display console. The information displayed would aid the response force in the event of an alarm. A reasonably sized console is limited in the amount of information it can display at one time. As a result, many alarm display consoles are designed to so that some crucial information is displayed at all times while other information is displayed only when requested, usually by a single keystroke or mouse click, or when an alarm is received. For each item below, write "ALWAYS," "REQUESTED," or "WHEN ALARM" beside it depending on whether you feel the item should be displayed on the screen always, only when requested by the operator, or automatically when an alarm occurs.

| | |
|---|---|
| | The alarm status (secure or access) of the zones |
| | Telephone numbers of persons to call in emergencies |
| | The geographic location of the zones |
| | The time of the alarm |
| | Supplementary text providing additional information such as special hazards or material associated with the zones |
| | Instructions describing special actions to be taken |
| | Maps of each secure area |
| | CCTV coverage of the instrumented areas |

**Response**

Answer the following questions:

- What is the relative effectiveness of each wave of response?

- How can the response effectiveness of the response be improved?

- Describe **five** specific improvements that could be made to the response forces on your site to make them more effective. Please describe the level of effort required for each potential improvement.

1.

2.

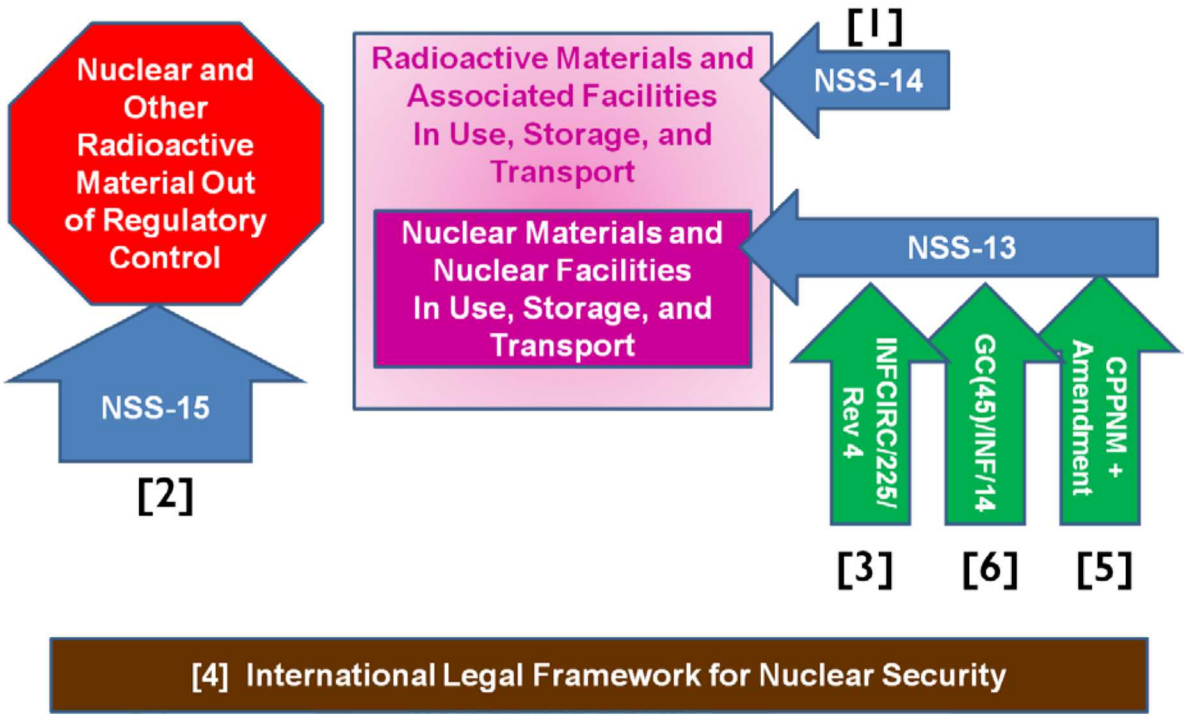
3.

4.

5.

# REFERENCE 1

## Nuclear and Radioactive Security: Supporting Resources





1. NSS 14 – "Nuclear Security Recommendations on Radioactive Material and Associated Facilities," IAEA Nuclear Security Series No. 14, IAEA. Vienna (2011).

2. NSS 15 – "Nuclear Security Recommendations on Nuclear and other Radioactive Material out of Regulatory Control," IAEA Nuclear Security Series No. 15, IAEA. Vienna (2011).

3. Physical Protection of Nuclear Material and Nuclear Facilities. (INFCIRC/225/Rev.4) (Corrected). IAEA, Vienna (1999).

4. "The International Legal Framework for Nuclear Security," IAEA International Law Series No. 4. IAEA. Vienna (2011).

5. "Convention on the Physical Protection of Nuclear Material," (CPPNM). INFCIRC/274/Rev. 1. IAEA. Vienna (1980): Amendment to the Convention on the Physical Protection of Nuclear Material. GOV/INF12005/10—GC(49)1NF/6, IAEA, Vienna (2005).

6. "Measures to Improve the Security of Nuclear Materials and other Radioactive Materials," GC(45)/1NF/14. IAEA. Vienna (14 September 2001).

# REFERENCE 2
# Definitions: Terms Used in NSS-13

Red indicates terms added to Rev. 5; Blue indicates terms that have changed from Rev. 4 to Rev.5;
Terms in black are unchanged

| No. | Term | Definition | Notes | √ |
|---|---|---|---|---|
| 1 | **Access delay** | The element of a *physical protection system* designed to increase adversary penetration time for entry into and/or exit from the *nuclear facility* or *transport*. | | |
| 2 | **Central alarm station** | An installation which provides for the complete and continuous alarm monitoring, assessment and communication with *guards*, facility management and *response forces* | | |
| 3 | **Competent authority** | Governmental organization(s) or institution(s) that has(have) been designated by a State to carry out one or more nuclear security functions. | | |
| 4 | **Contingency plan** | Predefined sets of actions for response to unauthorized acts indicative of attempted *unauthorized removal* or *sabotage*, including *threats* thereof, designed to effectively counter such acts. | | |
| 5 | **Conveyance** | For *transport* (a) by road or rail: any vehicle used for carriage of nuclear material cargo; (b) by water: any seagoing vessel or inland waterway craft, or any hold, compartment, or defined deck area of a seagoing vessel or inland waterway craft used for carriage of nuclear material cargo; and (c) by air: any aircraft used for carriage of nuclear material cargo. | | |
| 6 | **Defense-in-depth** | The combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised. | | |

| No. | Term | Definition | Notes | √ |
|---|---|---|---|---|
| 7 | **Design basis threat** | The attributes and characteristics of potential *insider* and/or external adversaries, who might attempt *unauthorized removal* or *sabotage*, against which a *physical protection system* is designed and evaluated. | | |
| 8 | **Detection** | A process in a *physical protection system* that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm. | | |
| 9 | **Force-on-force exercise** | A *performance test* of the *physical protection system* that uses designated trained personnel in the role of an adversary force to simulate an attack consistent with the *threat* or the *design basis threat*. | | |
| 10 | **Graded approach** | The application of *physical protection measures* proportional to the potential consequences of a *malicious act*. | | |
| 11 | **Guard** | A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or *transport*, controlling access and/or providing initial response. | | |
| 12 | **Inner area** | An area with additional protection measures inside a *protected area*, where Category I *nuclear material* is used and/or stored. | | |
| 13 | **Insider** | One or more individuals with authorized access to *nuclear facilities* or *nuclear material* in *transport* who could attempt *unauthorized removal* or *sabotage*, or who could aid an external adversary to do so. | | |

| No. | Term | Definition | Notes | √ |
|---|---|---|---|---|
| 14 | **Limited access area** | Designated area containing a *nuclear facility* and *nuclear material* to which access is limited and controlled for physical protection purposes. | | |
| 15 | **Malicious act** | An act or attempt of *unauthorized removal* or *sabotage*. | | |
| 16 | **Nuclear facility** | A facility (including associated buildings and equipment) in which *nuclear material* is produced, processed, used, handled, stored or disposed of and for which a specific license is required. | | |
| 17 | **Nuclear material** | Material listed in Table 1, in Section 4 of this publication, including the material listed in its footnotes. | | |
| 18 | **Nuclear security culture** | The assembly of characteristics, attitudes and behaviors of individuals, organizations and institutions which serves as means to support, enhance and sustain nuclear security. | | |
| 19 | **Nuclear security event** | An event that is assessed as having implications for physical protection. | | |
| 20 | **Operator** | Any person, organization, or government entity licensed or authorized to undertake the operation of a *nuclear facility*. | | |
| 21 | **Performance testing** | Testing of the *physical protection measures* and the *physical protection system* to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements. | | |

| No. | Term | Definition | Notes | √ |
|---|---|---|---|---|
| 22 | **Physical barrier** | A fence, wall or similar impediment which provides *access delay* and complements access control. | | |
| 23 | **Physical protection measures** | The personnel, procedures, and equipment that constitute a *physical protection system*. | | |
| 24 | **Physical protection regime** | A State's regime including:<br>- The legislative and regulatory framework governing the physical protection of *nuclear material* and *nuclear facilities*;<br>- The institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework;<br>- Facility and transport *physical protection systems.* | | |
| 25 | **Physical protection system** | An integrated set of *physical protection measures* intended to prevent the completion of a *malicious act*. | | |
| 26 | **Protected Area** | Area inside a *limited access area* containing Category I or II *nuclear material* and/or *sabotage* targets surrounded by a *physical barrier* with additional *physical protection measures*. | | |
| 27 | **Response forces** | Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted *unauthorized removal* or an act of *sabotage*. | | |

| No. | Term | Definition | Notes | √ |
|---|---|---|---|---|
| 28 | **Sabotage** | Any deliberate act directed against a *nuclear facility* or *nuclear material* in use, storage or *transport* which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances. | | |
| 29 | **Shipper** | Any person, organization or government that prepares or offers a consignment of *nuclear material* for *transport* (i.e. the consignor). | | |
| 30 | **Stand-off attack** | An attack, executed at a distance from the target *nuclear facility* or *transport*, which does not require adversary hands-on access to the target, or require the adversary to overcome the *physical protection system*. | | |
| 31 | **System for nuclear material accountancy and control** | An integrated set of measures designed to provide information on, control of, and assurance of the presence of *nuclear material*, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of *nuclear material*, and ensure the integrity of those systems and measures. | | |
| 32 | **Threat** | A person or group of persons with motivation, intention and capability to commit a *malicious act.* | | |
| 33 | **Threat Assessments** | An evaluation of the *threats* — based on available intelligence, law enforcement, and open source information — that describes the motivations, intentions, and capabilities of these *threats*. | | |

| No. | Term | Definition | Notes | √ |
|---|---|---|---|---|
| 34 | **Transport** | International or domestic carriage of *nuclear material* by any means of transportation, beginning with the departure from a *nuclear facility* of the *shipper* and ending with the arrival at a *nuclear facility* of the receiver | | |
| 35 | **Transport control centre** | A facility which provides for the continuous monitoring of a *transport* conveyance location and security status and for communication with the *transport* conveyance, *shipper*/receiver, carrier and, when appropriate, its *guards* and the *response forces*. | | |
| 36 | **Two person rule** | A procedure that requires at least two authorized and knowledgeable persons to be present to verify that activities involving *nuclear material* and *nuclear facilities* are authorized in order to detect access or actions that are unauthorized. | | |
| 37 | **Unacceptable radiological consequences** | A level of radiological consequences, established by the State, above which the implementation of *physical protection measures* is warranted. | | |
| 38 | **Unauthorized removal** | The theft or other unlawful taking of *nuclear material*. | | |
| 39 | **Vital area** | Area inside a *protected area* containing equipment, systems or devices, or *nuclear material*, the *sabotage* of which could directly or indirectly lead to high radiological consequences. | | |

# REFERENCE 3

## Fixed Facility Physical Protection Measures in INFCIRC/225/Rev. 5

| **Material State** | **In Use and Storage** | | | **Sabotage for High Consequence Facilities** |
|---|---|---|---|---|
| **Material Category** | **Category III** | **Category II** | **Category I** | |
| **Protection Layer** | **Limited Access Area** | **Protected Area** | **Inner Area** | **Vital Area** |
| PP Measure | | | | |
| Intrusion Detection | 4.12, 4.15 | 4.12, 4.15, 4.23, 4.31 | 4.12, 4.15, 4.23, 4.31, 4.38, 4.46, 4.48 | 5.14, 5.21, 5.26, 5.29, 5.33, 5.36, 5.37 |
| Alarm Assessment | | 4.23, 4.30 | 4.23, 4.30, 4.47 | 5.21, 5.36 |
| Entry Control | 4.17 | 4.24, 4.25, 4.26, 4.27, 4.28, 4.30 | 4.24, 4.25, 4.26, 4.27, 4.28, 4.30, 4.38, 4.40, 4.42, 4.44, 4.45 | 5.14, 5.22, 5.23, 5.24, 5.25, 5.26, 5.28, 5.31, 5.32, 5.34, 5.35, 5.36 |
| Contraband Detection | | 4.25 | 4.43 | 5.23 |
| Alarm Control & Display | | 4.30, 4.31, 4.32 | 4.30, 4.31, 4.32, 4.47 | 5.36, 5.37, 5.38 |
| Access Delay | | 4.23 | 4.23, 4.38, 4.39, 4.41, 4.46 | 5.14, 5.21, 5.26, 5.27, 5.30 |
| Response | 4.19, 4.20 | 4.19, 4.20, 4.30, 4.32, 4.33, 4.34 | 4.19, 4.20, 4.30, 4.32, 4.33, 4.34, 4.49 | 5.14, 5.36, 5.38, 5.39, 5.40, 5.42 |
| Evaluation | | | | |
| Performance Testing | 4.20 | 4.20, 4.35 | 4.20, 4.35, 4.49 | 5.15, 5.16, 5.41 |

# REFERENCE 4

## Responsibilities for Physical Protection Regime Entities

| Topic | INFCIRC/225/Revision 5 Reference |
|---|---|
| **STATE** | |
| Physical Protection Regime | 3.1-3.62 |
| Unauthorized Removal | 4.1-4.49 |
| Locate and Recover | 4.50-4.56 |
| Sabotage | 5.1-5.8 |
| Mitigate/Minimize Consequences | 5.45-5.53 |
| Transport | 6.6-6.69 |
| **COMPETENT AUTHORITY** | |
| Fundamental Responsibilities | 3.18-3.22 |
| Legislative and Regulatory Framework | 3.9 |
| Pertaining to Licence Holders | 3.23-3.33 |
| Threats | 3.34-3.40 |
| Nuclear Security Events | 3.58-3.59 |
| Unauthorized Removal | 4.8, 4.35 |
| Locate and Recover | 4.50-4.56 |
| Sabotage | 5.1, 5.9, 5.15, 5.41 |
| Mitigate/Minimize Consequences | 5.45-5.53 |
| Transport | 3.7, 6.22, 6.27, 6.33-34 |
| **LICENCE HOLDER** | |
| General Responsibilities | 3.24-3.30 |
| Unauthorized Removal* | 4.1-4.49 |
| Locate and Recover | 4.57-4.63 |
| Sabotage | 5.1-5.42 |
| Mitigate/Minimize Consequences | 5.54-5.58 |
| Transport* | 6.1-6.43, 6.52-6.59, 6.70-6.73 |

*Depends on Category of Nuclear Material

**Category-Based Physical Protection Requirements**

| Topic | Category 1 | Category II | Category III |
|---|---|---|---|
| Unauthorized Removal | 4.1-4.49 | 4.1-4.35 | 4.1-4.20 |
| Transport | 6.1-6.43 | 6.1-6.31 | 6.1-6.18 |

1. acilities.

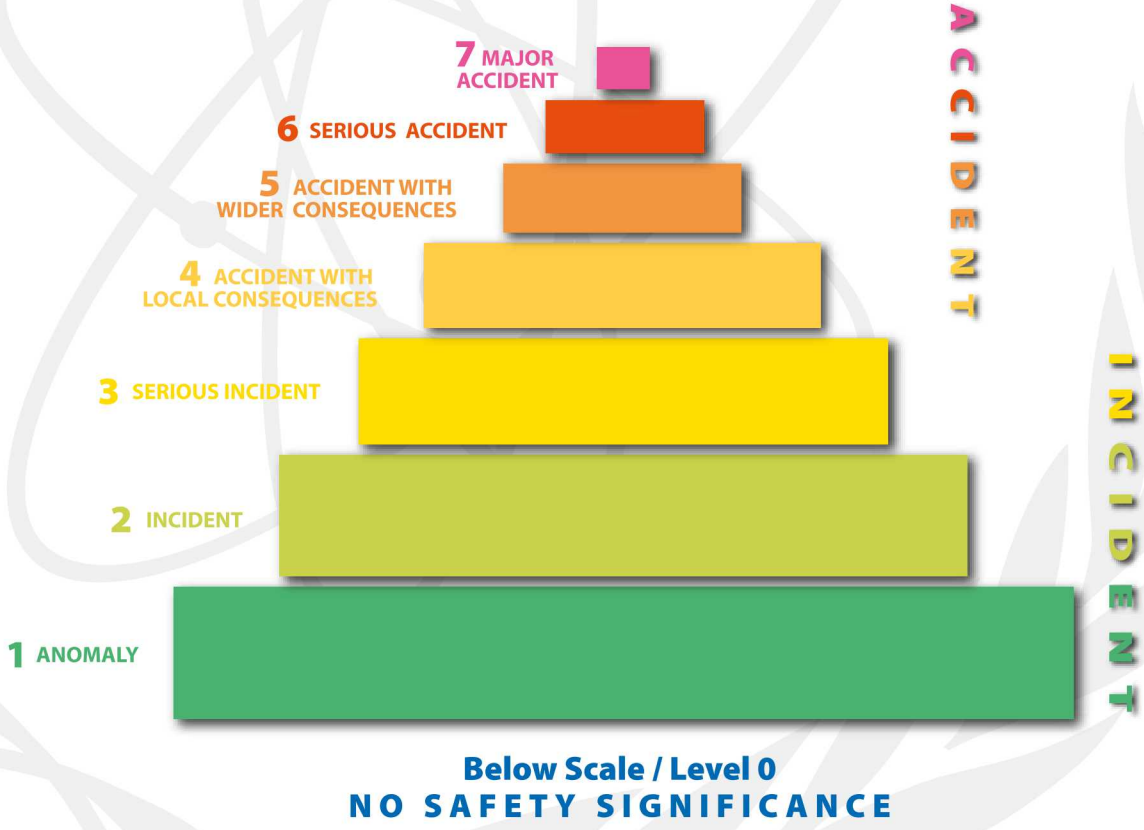
# INES

*THE INTERNATIONAL NUCLEAR AND RADIOLOGICAL EVENT SCALE*

The INES Scale is a worldwide tool for communicating to the public in a consistent way the safety significance of nuclear and radiological events.

Just like information on earthquakes or temperature would be difficult to understand without the Richter or Celsius scales, the INES Scale explains the significance of events from a range of activities, including industrial and medical use of radiation sources, operations at nuclear facilities and transport of radioactive material.

Events are classified on the scale at seven levels: Levels 1–3 are called "incidents" and Levels 4–7 "accidents". The scale is designed so that the severity of an event is about ten times greater for each increase in level on the scale. Events without safety significance are called “deviations” and are classified Below Scale / Level 0.




IAEA
International Atomic Energy Agency
*Atoms For Peace*

OECD
Nuclear Energy Agency

For more information: *www-news.iaea.org*


**INES** classifies nuclear and radiological accidents and incidents by considering three areas of impact:

***People and the Environment*** considers the radiation doses to people close to the location of the event and the widespread, unplanned release of radioactive material from an installation.

***Radiological Barriers and Control*** covers events without any direct impact on people or the environment and only applies inside major facilities. It covers unplanned high radiation levels and spread of significant quantities of radioactive materials confined within the installation.

***Defence-in-Depth*** also covers events without any direct impact on people or the environment, but for which the range of measures put in place to prevent accidents did not function as intended.

## Communicating Events

Nuclear and radiological events are promptly communicated by the INES Member States, otherwise a confused understanding of the event may occur from media or from public speculation. In some situations, where not all the details of the event are known early on, a provisional rating may be issued. Later, a final rating is determined and any differences explained.

To facilitate international communications for events attracting wider interest, the IAEA maintains a web-based communications network that allows details of the event to immediately be made publicly available.

The two tables that follow show selected examples of historic events rated using the INES scale, ranging from a Level 1 anomaly to a Level 7 major accident; a much wider range of examples showing the rating methodology is provided in the INES Manual.

## Scope of the Scale

**INES** applies to any event associated with the transport, storage and use of radioactive material and radiation sources, whether or not the event occurs at a facility. It covers a wide spectrum of practices, including industrial use

## EXAMPLES OF EVENTS AT NUCLEAR FACILITIES

| | People and Environment | Radiological Barriers and Control | Defence-in-Depth |
|---|---|---|---|
| 7 | *Chernobyl, 1986* — Widespread health and environmental effects. External release of a significant fraction of reactor core inventory. | | |
| 6 | *Kyshtym, Russia, 1957* — Significant release of radioactive material to the environment from explosion of a high activity waste tank. | | |
| 5 | *Windscale Pile, UK, 1957* — Release of radioactive material to the environment following a fire in a reactor core. | *Three Mile Island, USA, 1979* — Severe damage to the reactor core. | |
| 4 | *Tokaimura, Japan, 1999* — Fatal overexposures of workers following a criticality event at a nuclear facility. | *Saint Laurent des Eaux, France, 1980* — Melting of one channel of fuel in the reactor with no release outside the site. | |
| 3 | *No example available* | *Sellafield, UK, 2005* — Release of large quantity of radioactive material, contained within the installation. | *Vandellos, Spain, 1989* — Near accident caused by fire resulting in loss of safety systems at the nuclear power station. |
| 2 | *Atucha, Argentina, 2005* — Overexposure of a worker at a power reactor exceeding the annual limit. | *Cadarache, France, 1993* — Spread of contamination to an area not expected by design. | *Forsmark, Sweden, 2006* — Degraded safety functions for common cause failure in the emergency power supply system at nuclear power plant. |
| 1 | | | Breach of operating limits at a nuclear facility. |

## EXAMPLES OF EVENTS INVOLVING RADIATION SOURCES AND TRANSPORT

| | People and Environment | Defence-in-Depth |
|---|---|---|
| 7 | | |
| 6 | | |
| 5 | *Goiânia, Brazil, 1987* — Four people died and six received doses of a few Gy from an abandoned and ruptured highly radioactive Cs-137 source. | |
| 4 | *Fleurus, Belgium, 2006* — Severe health effects for a worker at a commercial irradiation facility as a result of high doses of radiation. | |
| 3 | *Yanango, Peru, 1999* — Incident with radiography source resulting in severe radiation burns. | *Ikitelli, Turkey, 1999* — Loss of a highly radioactive Co-60 source. |
| 2 | *USA, 2005* — Overexposure of a radiographer exceeding the annual limit for radiation workers. | *France, 1995* — Failure of access control systems at accelerator facility. |
| 1 | | Theft of a moisture-density gauge. |

such as radiography, use of radiation sources in hospitals, activity at nuclear facilities, and transport of radioactive material.

It also includes the loss or theft of radioactive sources or packages and the discovery of orphan sources, such as sources inadvertently transferred into the scrap metal trade.

When a device is used for medical purposes (e.g., radiodiagnosis or radiotherapy), INES is used for the rating of events resulting in actual exposure of workers and the public, or involving degradation of the device or deficiencies in the safety provisions. Currently, the scale does not cover the actual or potential consequences for patients exposed as part of a medical procedure.

The scale is only intended for use in civil (non-military) applications and only relates to the safety aspects of an event. INES is not intended for use in rating security-related events or malicious acts to deliberately expose people to radiation.

### What the Scale is Not For

It is not appropriate to use INES to compare safety performance between facilities, organizations or countries. The statistically small numbers of events at Level 2 and above and the differences between countries for reporting more minor events to the public make it inappropriate to draw international comparisons.

### History

Since 1990 the scale has been applied to classify events at nuclear power plants, then extended to enable it to be applied to all installations associated with the civil nuclear industry. By 2006, it had been adapted to meet the growing need for communication of the significance of all events associated with the transport, storage and use of radioactive material and radiation sources.

The IAEA has coordinated its development in cooperation with the OECD/NEA and with the support of more than 60 Member States through their officially designated INES National Officers.

The current version of the INES manual was adopted 1 July 2008. With this new edition, it is anticipated that INES will be widely used by the Member States and become the world-wide scale for putting into the proper perspective the safety significance of nuclear and radiation events.

INES

THE INTERNATIONAL NUCLEAR AND RADIOLOGICAL EVENT SCALE

# INES

*THE INTERNATIONAL NUCLEAR AND RADIOLOGICAL EVENT SCALE*

## GENERAL DESCRIPTION OF INES LEVELS

| INES Level | People and Environment | Radiological Barriers and Control | Defence-in-Depth |
|---|---|---|---|
| Major Accident<br>Level 7 | • Major release of radioactive material with widespread health and environmental effects requiring implementation of planned and extended countermeasures. | | |
| Serious Accident<br>Level 6 | • Significant release of radioactive material likely to require implementation of planned countermeasures. | | |
| Accident with Wider Consequences<br>Level 5 | • Limited release of radioactive material likely to require implementation of some planned countermeasures.<br>• Several deaths from radiation. | • Severe damage to reactor core.<br>• Release of large quantities of radioactive material within an installation with a high probability of significant public exposure. This could arise from a major criticality accident or fire. | |
| Accident with Local Consequences<br>Level 4 | • Minor release of radioactive material unlikely to result in implementation of planned countermeasures other than local food controls.<br>• At least one death from radiation. | • Fuel melt or damage to fuel resulting in more than 0.1% release of core inventory.<br>• Release of significant quantities of radioactive material within an installation with a high probability of significant public exposure. | |
| Serious Incident<br>Level 3 | • Exposure in excess of ten times the statutory annual limit for workers.<br>• Non-lethal deterministic health effect (e.g., burns) from radiation. | • Exposure rates of more than 1 Sv/h in an operating area.<br>• Severe contamination in an area not expected by design, with a low probability of significant public exposure. | • Near accident at a nuclear power plant with no safety provisions remaining.<br>• Lost or stolen highly radioactive sealed source.<br>• Misdelivered highly radioactive sealed source without adequate procedures in place to handle it. |
| Incident<br>Level 2 | • Exposure of a member of the public in excess of 10 mSv.<br>• Exposure of a worker in excess of the statutory annual limits. | • Radiation levels in an operating area of more than 50 mSv/h.<br>• Significant contamination within the facility into an area not expected by design. | • Significant failures in safety provisions but with no actual consequences.<br>• Found highly radioactive sealed orphan source, device or transport package with safety provisions intact.<br>• Inadequate packaging of a highly radioactive sealed source. |
| Anomaly<br>Level 1 | | | • Overexposure of a member of the public in excess of statutory annual limits.<br>• Minor problems with safety components with significant defence-in-depth remaining.<br>• Low activity lost or stolen radioactive source, device or transport package. |

NO SAFETY SIGNIFICANCE *(Below Scale/Level 0)*

*Photo Credits: Chilean Nuclear Energy Commission, Genkai Nuclear Power Plant, Genkai, Japan/Kyushu Electric Power Co., J. Mairs/IAEA*

International Atomic Energy Agency
Information Series / Division of Public Information
08-26941 / E