Learning Objectives

After completing this module, you should be able to:

• Recognize scenario recommendations from INFCIRC/225/Rev.5
• Describe the purpose of scenario analysis in the context of evaluating physical protection system (PPS) performance
• Discuss the four phases of the Scenario Analysis Process
• Create adversary attack scenarios
• Describe a process for selecting final attack scenarios
INCIRC/225/Revision 5 Guidance Scenario Development

- Using the DBT, the operator should define credible scenarios by which adversaries could carry out sabotage of nuclear facilities and nuclear materials.
- When defining scenarios, the operator should consider the location of the nuclear facility and all nuclear materials.
- Sabotage scenarios should consider external and/or insider adversaries who attempt to disperse nuclear material or to damage or interfere with equipment, systems, structure components or devices, including possible stand-off attack, consistent with the State's threat assessment or DBT.
- The operator should design a PPS that is effective against the defined sabotage scenarios and complies with the required level of protection for the nuclear facility and nuclear material.

What Is Scenario Analysis?

*Scenario analysis:* A methodology for analyzing physical protection system effectiveness (P_e) by considering several possible adversary scenarios.

- Allows more detailed analysis of the attack, defense, results of path analysis.
- Focuses on identifying vulnerabilities.
- Contributes to:
  - Overall PPS design
  - Contingency plans
  - Policies and procedures
  - Interagency coordination.
Purposes of Scenario Analysis

• Provide basis for level of confidence about PPS performance
• Create “robust” security plans to match and fully use the capabilities of the PPS design
  ▪ How?
    • Develop details of realistic adversary attack plan
      – Specific, coordinated tasks and timeline for all attackers
    • Develop detailed characterization of how PPS and response should behave, based on performance testing and site plans
    • Simulate how PPS and response behave during attempted adversary attack scenario
  ▪ **IMPORTANT**: Overall physical protection system effectiveness is represented by effectiveness against a few specific scenarios
    • No attempt to determine worst-case scenario

Scope of Scenario Analysis

• Identify key questions
  ▪ General analysis
    • How effective is the current PPS?
    • How effective is the existing response force strategy?
  ▪ Specific analysis
    • Procedure
    • Potential upgrade
• Identify major considerations
  ▪ What PPS configuration should be tested?
  ▪ What are the threat numbers and capabilities?
Scenario Analysis Process

1. Design
   - Identify Stakeholders
   - Create scoping agreement
   - Oversee scenario development

2. Develop
   - Determine attack scenario characteristics
   - Develop attack scenarios
   - Review and select attack scenarios

3. Implement
   - Gather and determine teams
   - Prepare for simulations
   - Simulate the attack
   - Record events

4. Evaluate
   - Conduct evaluation meeting
   - Determine vulnerabilities
   - Recommend changes and upgrades

Scenario Development
- Based on low probability of interruption/probability of neutralization (P1/P2) or delay paths
- By expert ‘Red Teams’

Scenario Evaluation
- Tabletop exercise
- Computer combat simulation
- Force-on-Force (FoF) exercises
Identify Stakeholders

- Identify people who are responsible for the design, implementation, evaluation, and risk acceptance of the PPS
  - Competent authority
  - Response force management
  - Vulnerability analysis team
  - Adversary planning subject-matter experts (SMEs)
  - Security management
  - Facility operations
  - Offsite response
  - Other required people

Scoping Agreement

**Scoping Agreement:** A contract among appropriate stakeholders that identifies parameters of scenario analysis

- Defines requirements
- Design basis threat (DBT) statement
- Characterizes facility
- Identifies targets (type of targets)
- Identifies credible SMEs for attack planning
- Determines types of attacks and numbers of scenarios (sabotage/theft)
- Identifies and agrees on assumptions
- Determines type of insider (passive/active, etc.)
- Determines picture-in-time
- Agrees on simulation tools and the process for using them
Oversee Scenario Development

- Stakeholder(s) familiar with the design and evaluation of the PPS should be included in scenario development.

- All participants should:
  - Agree to confidentiality of all site/adversary information.
  - Remain unbiased to site or adversaries.
  - Ensure the adversary scenarios are within the parameters of the scoping agreement.
  - Ensure accuracy of the PPS and target information:
    - Thickness of vault walls.
    - Assessment capability.
    - Response capability.

Scenario Characteristics

**Attack Scenario:** A time ordered, detailed description of an adversary attack used in analyzing $P_E$.

- For scenario analysis to be of maximum value, scenarios should be:
  - Detailed.
  - Credible.
  - Limited to threats within the DBT.
  - Well documented.

- Consider scenarios from Path Analysis:
  - Add scenario details to these paths.
  - Add supporting team plans to assist these attackers.
  - **IMPORTANT:** The most-vulnerable $P_j$ path from Path Analysis may be a poor basis for a scenario.
Adversary Scenario Definitions

**Adversary Strategy:** Short description of the scenario used to achieve the adversary’s objective

**Defeat Strategy:** General method used to defeat a path element or a PPS function

**Defeat Method:** Way to prevent a component within a path element from accomplishing its purpose or function

---

Adversary Strategy

- Two classes of adversary scenarios
  - Direct: Adversary follows a direct path to target
    - Adversary goal: Minimize $P_1$ by defeating system detection or delay elements
  - Indirect: Adversary attacks PPS infrastructure before attacking target
    - Adversary goal: Minimize $P_1$ or $P_N$ to:
      - Increase response time
      - Decrease response numbers
      - Disable critical systems
Defeat Strategies and Methods

- Three basic adversary defeat strategies and methods can be used
  - Avoid, degrade, or disable detection systems
    - Include entry control and contraband detection systems
  - Degrade, disable, or circumvent delay systems
  - Degrade or eliminate response
    - Identify
      - Weak links
      - Single points of failure

Scenario Development Planning and Complexity Factors

- The best attack scenario for the adversary does not always use all of the equipment allowed within the design basis threat
  - Not all of the equipment will provide an advantage to the adversary
  - Adding equipment may increase the complexity of the attack scenario
- Coordinating actions and synchronizing time between groups increases difficulty
Adversary’s Perspective for Main and Supporting Teams

Structured Approach to Create Scenarios

- Create a range of scenarios
  - Identify site vulnerabilities
  - Exploit the identified site vulnerabilities
    1. Build scenarios
    2. Review and select final scenarios based on criteria
Identify Site Vulnerabilities

• Collect Site Specific PPS Data
  ▪ Passive insider information
  ▪ Site surveillance
  ▪ Outside sources (Internet, libraries, etc.)
• Identify site vulnerabilities across various operational conditions and states:
  ▪ Operational conditions (operational versus non-operational)
  ▪ Target material configurations (reactor refueling versus operations)
  ▪ Response force alert levels
• Identify sources of vulnerabilities
  ▪ Experts (site personnel, police)
  ▪ Path analysis
  ▪ Previous vulnerability studies and performance tests

Example: Identify Site Vulnerabilities

Vulnerability: At times the guard force is divided

• Scenario conditions:
  ▪ 2 guards at entry portal
  ▪ 3 guards at guard house

Results from Path Analysis
Adversaries = 5 (DBT)
Guard Force = 7

Expected Results from vulnerability based scenario

Task Plan A:
3 Adversaries vs. 2 Guards
Surprise advantage to adversaries

Task Plan B:
3 Adversaries vs. 3 Guards
Surprise advantage to adversaries
Exploit Identified Site Vulnerabilities

- Determine how an adversary could exploit site identified vulnerabilities
- Create a list of essential tasks that must be accomplished for the attack to succeed
- Create task plans describing how an adversary team can perform each task within resource constraints
  - Who is involved?
  - What are they doing as a function of time?
  - How are they performing each step?
  - What equipment are they using?
  - How are they transporting the equipment?

Example: **Exploit** Site Vulnerabilities

- Example
  - Vulnerability: At times the response force is divided
  - List of tasks to exploit vulnerability
    A. Ambush Guard Post
    B. Attack remaining Response Force
    C. Enter Material Storage Building and remove material
    D. Escape to safe house
### Task Plan A

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Activity</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00</td>
<td>A1, A2, and A3 drives vehicle up to the gate</td>
<td>00:40</td>
</tr>
<tr>
<td>00:40</td>
<td>A1 waits until P1 and P2 arrive at vehicle</td>
<td>00:50</td>
</tr>
<tr>
<td>00:50</td>
<td>A1 engages P1 while A2 and A3 exit vehicle</td>
<td>00:55</td>
</tr>
<tr>
<td>00:55</td>
<td>A2 and A3 engage P2</td>
<td>01:00</td>
</tr>
<tr>
<td>01:00</td>
<td>A2 and A3 breach gate</td>
<td>01:30</td>
</tr>
<tr>
<td>01:30</td>
<td>A1 drives vehicle through gate and picks up A2 and A3</td>
<td>01:45</td>
</tr>
</tbody>
</table>

### Task Plan B

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Activity</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:45</td>
<td>A1 drives to guardhouse and A1, A2, and A3 dismount</td>
<td>03:00</td>
</tr>
<tr>
<td>03:00</td>
<td>A1, A2 and A3 surround guardhouse and wait for guards to exit</td>
<td>03:30</td>
</tr>
<tr>
<td>03:30</td>
<td>Adversary team engages guards in guardhouse</td>
<td>04:00</td>
</tr>
</tbody>
</table>
Exploit Identified Site Vulnerabilities (cont’d.)

- Combine task plans into a master attack plan / scenario description, adjusting task activities to:
  - Meet DBT and other constraints
  - Determine how to get adversary team from offsite to the target
  - Achieve synchronization between teams
  - Coordinate progress at key steps (e.g., the point of detection)
  - Refine task time estimates
  - Identify key locations for chance encounters with security or site personnel
  - Consider ambushes and diversions as ways of delaying/defeating the guards and response force
  - Identify:
    - Target selection, minimum delay path, and breaching techniques

Review and Select Final Scenarios

- Include stakeholders in the review and selection process
- Review and select final scenarios based on scoping agreement criteria
  - Are all analysis objectives covered?
    - Are conditions and states covered adequately?
    - Do the scenarios address several means of adversary approach (on foot, in land vehicles, on water, or by air) that apply, based on the DBT?
  - Are scenarios credible, limited by threats within the DBT, etc.?
Review and Select Final Scenarios (cont’d)

- Consider impact of colluding insider
  - Modify appropriate detection, delay, response force time, or response force numbers to reflect what insider can accomplish
  - Examples of collusion scenarios
    - Detection: Insider tampers with alarm communication lines
    - Delay: Insider opens vault door at time of attack
    - Response:
      - Insider activates an emergency alarm in a different location to divert response force
      - Insider detonates explosive at armory

Summary

- Scenario analysis is a methodology for analyzing system effectiveness, $P_E$, by considering several alternative possible adversary attacks (scenarios)
- System effectiveness, $P_E$, of PPS is represented by effectiveness against several distinct adversary scenarios