Learning Objectives

After completing this module, you should be able to:

- Recognize the motivation for multipath analysis
- Describe how force, stealth, and deceit tactics are used to set probabilities of detection and delay times
- Describe what MultiPath VEASI (MPVEASI) software is and its uses
- List and describe the three MPVEASI evaluation steps
- Determine input for MPVEASI for complex protection elements
Evaluations, including performance testing, of the physical protection measures and of the physical protection system, including timely response of the guards and response forces should be conducted regularly to determine reliability and effectiveness against the threat. 4.35 (Category I and II theft)

- Guards and response forces should provide an effective and timely response to prevent an adversary from completing the unauthorized removal. 4.49 (Category I theft)

- Evaluations, including performance testing, of the physical protection measures and of the physical protection system, including timely response of the guards and response forces, should be conducted regularly to determine reliability and effectiveness against the threat. 5.41 (Sabotage)

Motivation for Multipath Analysis

**Multipath analysis:** Identifies a path through the ASD with the lowest $P_1$ (Most Vulnerable Path)

- Motivation: Multipath Analysis is the approach taken for performing Path Interruption Analysis

  - **Path Interruption Analysis:** Determines whether detection and delay are sufficient along all adversary paths to provide an adequate level of Probability of Interruption, $P_1$

- Rationale: If the $P_1$ for the Most Vulnerable Path is adequate, then all the other paths have an adequate $P_1$
Motivation for Multipath Analysis (cont’d)

- Multipath analysis provides insight about other design considerations such as balanced protection and defense in depth
  - Balanced protection: Are there significant variations in Probability of Interruption between different paths?
  - Defense in depth: How many protection layers provide the following:
    - Significant timely detection before / at the CDP on the Most Vulnerable Path?
    - Significant delay after the CDP on the Most Vulnerable Path?
- Balanced protection and defense in depth can also be evaluated by reviewing the delay times and detection probabilities for each protection layer in the ASD

Two Evaluation Approaches Are Required to Perform Multipath Analysis

- Two approaches
  - One approach is to determine timeline information – \( P_D \) and delay times – for each element and area
  - Another approach is to examine all the paths through the ASD to determine the Most Vulnerable Path with the lowest \( P_I \)
- For this course:
  - The course participant determines the timeline \( P_D \) and delay times by considering force, stealth and deceit tactics at each element and area
  - Multipath VEASI (MPVEASI) determines the path with the lowest \( P_I \) (Most Vulnerable Path)
Three Types of Tactics Are Considered at Each Element and Area

- **Force**: An overt attempt to overcome a security system by violence, compulsion or constraint
- **Stealth**: An attempt to defeat a physical protection system by avoiding or inactivating its components in order to prevent detection
- **Deceit**: An attempt to defeat a security system using false identification or authorization

Consider all Tactics When Assigning $P_D$ and Delay Times ($T$) to Elements and Areas

- Set delay time based on minimum delays using force
- Set the $P_D$ based on the smaller of:
  - The minimum $P_D$ for an adversary using stealth
  - The minimum $P_D$ for an adversary using deceit (where possible)

Example: Setting $P_D$ and delay time for fence:

<table>
<thead>
<tr>
<th>Delay Time (sec) for adversary on foot</th>
<th>Fence fabric/outrigger (2.5m):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Climb over the fence?</td>
<td>10</td>
</tr>
<tr>
<td>Cut through fabric?</td>
<td>30</td>
</tr>
<tr>
<td>Go under the fence?</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detection $P_D$:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fence sensor: (Vibration)</td>
</tr>
<tr>
<td>Tamper?</td>
</tr>
<tr>
<td>Bridge over sensor?</td>
</tr>
<tr>
<td>Climb Fence?</td>
</tr>
<tr>
<td>Go under detection pattern?</td>
</tr>
<tr>
<td>Cut through fence carefully?</td>
</tr>
</tbody>
</table>

$P_D = 0.10$, Delay = 10 seconds
Example (Door): Setting $P_D$ and Delay Time ($T$)

- Delay Time = \(30\) seconds (Force: cutting through the door)
- $P_D$ is assigned as \(0\), as the smaller of
  - $P_D$ (Stealth) = \(0\) (cutting through the door)
  - $P_D$ (Deceit) = \(0.1\) (using a forged badge)

Door: $P_D = 0$
Delay = 30 seconds

Sensor for detecting cutting through the door: None – Stealth $P_D = 0$

Sensor for detecting unauthorized opening: Balanced Magnetic Switch – Stealth $P_D = 0.8$

Defeating Lock: Force Delay = 60 seconds
Penetrating Through Door: Force Delay = 30 seconds

Example Showing Approach for Determining Most Vulnerable Path: Facility and ASD
Approach for Determining Most Vulnerable $P_I$ Path*

- Start at Win Point – Point on the adversary path where they “win” and response force plan is considered to fail
- Work backwards through the ASD, selecting the path elements with the least delay times at each protection layer and adding delay times
- Once the adversary task time remaining after first sensing exceeds the PPS Response Time, you have found a CDP
- Select the element with the minimum $P_D$ on each layer down to and including the CDP

*Path with minimum $P_I$, given the adversary type, target, and facility state

Example: Start at Target, and Enter Target Time on Path Timeline

<table>
<thead>
<tr>
<th>Timeline Section</th>
<th>Probability (P)</th>
<th>Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offsite</td>
<td>$P_D = 0.35$</td>
<td>25 s</td>
</tr>
<tr>
<td>Portal</td>
<td>$P_D = 0.5$</td>
<td>45 s</td>
</tr>
<tr>
<td>Protected Area</td>
<td>$P_D = 0.1$</td>
<td>10 s</td>
</tr>
<tr>
<td>Door</td>
<td>$P_D = 0.9$</td>
<td>60 s</td>
</tr>
<tr>
<td>Surface</td>
<td>$P_D = 0.99$</td>
<td>480 s</td>
</tr>
<tr>
<td>Vital Area</td>
<td>$P_D = 0.0$</td>
<td>30 s</td>
</tr>
<tr>
<td>Pump</td>
<td>$P_D = 0.5$</td>
<td>50 s</td>
</tr>
</tbody>
</table>

PPS Response Time = 70 sec

Win Point
Example Using Approach: Once CDP is found, choose elements and areas above it that have the smallest $P_D$ and determine $P_I$.

$$P_I = 1 - (1-0.35)(1-0.1)(1-0.9)$$
$$= 1 - (0.65)(0.9)(0.1)$$
$$= 1 - 0.0585$$
$$= 0.9415 \approx 0.94$$

Adversary uses defeat methods and elements that minimize detection probability.

Adversary chooses defeat methods and elements that minimize delay.

Relationship of Multipath Algorithm to Assumed Adversary Planning Preferences:

- **Start Path**
- **Complete Path**
- **PPS Response Time**
- **Time Remaining Along Path**
- **Probability of Interruption, $P_I$**
- **Critical Detection Point**

**Adversary Task Time**

- **Adjacent Task Time**
- **Elemental/Area**
- **Detection Opportunity**
- **Probability of Detection, $P_D$**
- **Mean Time Delay (seconds)**
Containment Response: Make Worst-Case Assumptions for Exit and Count Area Delay Times

- Find Win Point* on Exit (typically an area)
- Add just area delays from target to part of the Win Point closest to target (consider using a vehicle)
- Add delay to Exit Area defined just after the Target
- Set $P_D = 0$.

* Win Point—point in the exit path where the adversary is expected to “break” containment and be outside the response force’s ability to prevent the theft of material.

### Description of MPVEASI Software

- MPVEASI determines the Most Vulnerable Path through the ASD and its Probability of Interruption ($P_I$)
  - Cumulative probability of detection up to and including the Critical Detection Point (CDP)
- MPVEASI does not calculate Probability of Neutralization
- MPVEASI is NOT used by US DOE to analyze PPS effectiveness or support licensing
  - Codes actually used take too long to learn for this course
  - MPVEASI concepts and algorithms are similar to those used by DOE
DEPO Can Be Matched to MPVEASI Steps

MPVEASI Evaluation Steps

1. Enter ASD data for each target including a minimum Probability of Detection, \( P_D \), and delay, \( T \), value for each element and area
2. Enter response data—response strategy and PPS Response Time (referred to as Response Force Time in MPVEASI)
3. Analyze and review results in MPVEASI
1. Enter ASD Data for Each Target: Assign Delay (T) and Probability of Detection (P_D) Values

- Extracts from Component Class Tables in Section 27 and 28 of Data Book

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Component Description</th>
<th>No Equipment (sec)</th>
<th>Hand Tools (sec)</th>
<th>Power Tools (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walls</td>
<td>60 cm reinforced concrete wall</td>
<td>Infinite</td>
<td>Infinite</td>
<td>900</td>
</tr>
<tr>
<td></td>
<td>30 cm reinforced concrete wall</td>
<td>Infinite</td>
<td>Infinite</td>
<td>840</td>
</tr>
<tr>
<td></td>
<td>20 cm reinforced concrete wall</td>
<td>Infinite</td>
<td>Infinite</td>
<td>600</td>
</tr>
<tr>
<td>Wood studs and sheetrock</td>
<td>60</td>
<td>30</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Component Description</th>
<th>No Equipment (P(D))</th>
<th>Hand Tools (P(D))</th>
<th>Power Tools (P(D))</th>
<th>High Explosives (P(D))</th>
<th>Land Vehicle (P(D))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exterior Sensors</td>
<td>Seismic Buried Cable</td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>Electric field</td>
<td>0.5</td>
<td>0.3</td>
<td>0.3</td>
<td>0.5</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>Infrared</td>
<td>0.8</td>
<td>0.4</td>
<td>0.4</td>
<td>0.5</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>Microwave</td>
<td>0.8</td>
<td>0.7</td>
<td>0.7</td>
<td>0.7</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>Video motion</td>
<td>0.8</td>
<td>0.6</td>
<td>0.6</td>
<td>0.7</td>
<td>0.9</td>
</tr>
<tr>
<td></td>
<td>Multiple non-complementary</td>
<td>0.9</td>
<td>0.8</td>
<td>0.8</td>
<td>0.8</td>
<td>0.99</td>
</tr>
<tr>
<td></td>
<td>Multiple complementary</td>
<td>0.99</td>
<td>0.95</td>
<td>0.95</td>
<td>0.99</td>
<td>0.99</td>
</tr>
</tbody>
</table>

1. Enter ASD Data for Each Target: Data as Entered into MPVEASI

ASD Data for Example Site shown in MPVEASI
2. Enter Response Data

- Response Strategy
  - Denial: Entry only
  - Containment: Entry and exit
- Response Force Time (PPS Response Time)
  - Reflect deployment time associated with sufficient number of responders to successfully interrupt adversary attack
  - You can also enter Response Force Time = -1 and Response Force Time = 9999 seconds to determine a minimum $P_0$ and a minimum delay time through the facility

<table>
<thead>
<tr>
<th>Step 2: Enter Response Data</th>
<th>Step 3: P(E ) Calculations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Strategy</td>
<td>Analyze</td>
</tr>
<tr>
<td>Denial</td>
<td></td>
</tr>
<tr>
<td>Response Force Time(sec)</td>
<td>70</td>
</tr>
</tbody>
</table>

3. Analyze and Review Results

- Analysis addresses a number of questions
  - How does worst-case $P_1$ vary as a function of Response Force Time?
  - What does the most vulnerable path look like and what is its $P_0$?
    - Results shown on ASD
- MPVEASI determines the most-vulnerable path using the “Analyze” function
Examining Balance on Each Protection Layer

- Balanced Protection: Compare both $P_D$ and delay times for elements within a protection layer
  - Values do not have to be identical but there should not be any big differences

<table>
<thead>
<tr>
<th>Door</th>
<th>Fence</th>
<th>Gate</th>
</tr>
</thead>
<tbody>
<tr>
<td>PD</td>
<td>0.8</td>
<td>PD</td>
</tr>
<tr>
<td>Ti</td>
<td>80</td>
<td>Ti</td>
</tr>
<tr>
<td>Jump</td>
<td>Jump</td>
<td>Jump</td>
</tr>
</tbody>
</table>

- Protection in Depth: Compare detection probabilities and delay times across multiple layers
  - Consider where the CDP is located

Perform Upgrade Analysis

- Determine if your system has adequate performance
  - Is $P_i$ for your system greater than or equal to the $P_i$ required from your regulator?
  - Does the system provide balanced protection and defense in depth?
- If performance is not adequate, look for improvements
  - Look for weak elements across each layer with low minimum $P_i$ through them
  - Change Response Force Time to affect all paths (sensitivity analysis)
- Reanalyze the improved system
- Note: Study PPS upgrade effectiveness before implementation
Demonstration of MPVEASI

Projected Demonstration of MPVEASI

Note: This demo covers identifying the most vulnerable path, looking at balance and defense in depth, finding minimum delay and detection probabilities, and performing upgrade analysis.

Modeling More Complex Elements, Such as Portals

A sensor on each door of a portal.
Modeling an Element with More than One Delay or Detection Feature in MPVEASI

- Sometimes useful to model an element with more than one delay or detection feature in MPVEASI.
- Combining detection across several sensors.
  - Combined $P_D = 1 - (1 - P_{D1}) \times (1 - P_{D2}) \times \ldots \times (1 - P_{Dm})$.
    - Example: 0.5 sensor on each of two doors.
    - $P_D = 1 - (1 - 0.5)^2 = 0.75$.
- Combined Delay $= Delay_1 + Delay_2 + \ldots + Delay_m$.
  - Example: 2–20 second doors + 10 second transit time.
  - Delay $= 20s + 10s + 20s = 50s$.

Summary

- MPVEASI uses the ASD to evaluate PPS effectiveness.
  - ASD represents all paths that adversaries can follow to accomplish sabotage or theft and the PPS elements along paths.
  - MPVEASI can be used to find Most Vulnerable Path.
- Most Vulnerable Path $P_I$ establishes adequacy for the PPS.
- Probabilities of detection and delay times for areas and elements are set as minimum values considering force, stealth, and (where appropriate) deceit tactics.
- Probabilities of detection and delay times are combined to model complex elements.