17. Evaluation of Physical Protection Systems

Abstract. Physical Protection System (PPS) effectiveness, \( P_E \), is defined as the product of the Probability of Interruption, \( P_I \), of the adversary by the response force and the Probability of Neutralization, \( P_N \), of the adversary by the response force. The third section of DEPO presents evaluation methods that are used to calculate \( P_I \) and \( P_N \) for the PPS effectiveness against the required DBT. This paper provides an introduction and overview of these evaluation techniques.

17.1 Introduction

Why Evaluate a PPS? The third major part of the DEPO process is the evaluation of physical protection system effectiveness, \( P_E \). There are several important reasons to evaluate the PPS design:

- Verify that the PPS designed or characterized in the second part of DEPO satisfies the requirements established in the first part of DEPO
- Identify any system deficiencies in the design or implementation that need to be addressed to meet the system requirements
- Analyze upgrade options that may be necessary to address identified deficiencies with regard to their improvement of system performance
- Compare the cost estimates of upgrade options to determine cost benefit in terms of improved system performance
- Repeat the PPS effectiveness evaluation on an annual or other regular basis to account for any changes in system performance or requirements

Analysis Tool Set

This evaluation section of DEPO addresses a set of analyses, models, algorithms, and computer codes that are used to determine system effectiveness:

- Path Interruption Analysis (18)
- Adversary Sequence Diagram (19)
- Multipath Analysis (20)
- Neutralization Analysis (21)
- Scenario Analysis (22)
- Tabletop Analysis (23)
- Insider Analysis (26)
- Information Security (28)
- Transportation Security (32)
17.2 System Effectiveness

**PPS Effectiveness**

For a PPS to be effective against theft and sabotage, the response force must both interrupt and neutralize the adversary. Interruption means the response force deploys before the adversary’s mission is complete and in adequate numbers so that the adversary must interrupt the mission and engage with the response force. Neutralization means that the response force stops or permanently interrupts the adversary, who either surrenders, attempts to flee, is captured, or is killed. Both interruption and neutralization are necessary for the PPS to be effective.

**Interruption Defined**

Neutralization Defined

The Probability of Interruption, $P_I$, is defined based on the principle of timely detection and a Critical Detection Point, or CDP. For any adversary path, the $P_I$ is the cumulative probability of detection along the path up to and including the CDP. The CDP is the last PPS detection component along that path for which the response force time is less than the remaining adversary task completion time.

**Probability of Neutralization, $P_N$**

The Probability of Neutralization, $P_N$, is the probability, given interruption of the adversary by the response force, that the response force will gain complete physical control of the adversary force. Then system effectiveness, $P_E$, along this path is defined as the product of these two probabilities, $P_I$ and $P_N$. The overall PPS effectiveness is conservatively defined as the lowest $P_E$ for all adversary paths, which is equivalent to the statement that a chain is only as strong as its weakest link.

17.3 Path Analysis

**Adversary Path**

To complete the objective of theft or sabotage, an adversary must select and follow some path from off-site to enter the nuclear facility and proceed to the theft or sabotage target, and in the case of theft, the adversary must also exit the site. This adversary path is defined both spatially and temporally, in terms of the physical route to the target and the time required passing along this route. This timeline also depends on the facility PPS, based on how the adversary chooses to avoid detection and penetrate barriers.

**Timeline**

The PPS also has a timeline in response to the adversary actions. The timeline for the response is a function of system performance and includes times for detection, alarm communication, assessment, communication to the response force, and response force deployment. The relationship between the adversary and response force timelines determines whether the response force can interrupt the adversary before the theft or sabotage mission is completed.

**Principle of Timely Detection**

The principle of timely detection is introduced to establish a quantitative metric for $P_I$. For the response force to be able to interrupt the adversary, the PPS must detect the adversary early enough along the adversary timeline that the response force has enough time to interrupt the adversary before theft or sabotage is completed. In this case, there is said to be timely
17. Evaluation of Physical Protection Systems

| detection of the adversary by the PPS. Without timely detection, the PPS is ineffective. |

17.4 Path Interruption Analysis

**P₁ Algorithm**

The quantitative P₁ can be calculated using a mathematical algorithm. The simplest model is for a single adversary path. The analyst identifies an adversary path with its associated tasks using task times and detection probabilities along the entire mission path for either theft or sabotage. Then the chosen algorithm and computer software calculate the P₁.

17.5 Adversary Sequence Diagrams Model

**Adversary Sequence Diagram Model**

An Adversary Sequence Diagram, or ASD, is used to model all adversary paths into and out of a facility. An ASD is a graphical representation of the adversary paths and the facility PPS. The facility is modeled as concentric areas around an adversary theft or sabotage target. The PPS is modeled as layers between two concentric facility areas. Each PPS layer is decomposed into a number of physical protection elements. Each PPS element has associated detection and delay components.

**Offsite to Target**

Any adversary path from offsite to the target must traverse each concentric area and each PPS layer between areas. For sabotage, the adversary path is one way from offsite to the target, and for theft, the adversary path is two-way, from offsite to the target and then back offsite.

Although the ASD is represented in two dimensions, it is easily adapted to model the three dimensions of facilities. Facility configurations that are not truly concentric can also be handled routinely by the ASD.

17.6 Multipath Analysis

**Calculate P₁ for All Adversary Paths**

Evaluation of PPS effectiveness against the outsider adversary includes calculating P₁ for all adversary paths. For complex facilities, this is done using the ASD to address all paths. This course uses the MPVEASI model and software. MPVEASI is a shortened form of Multipath Very-simplified Estimate of Adversary Sequence Interruption.

**Path Analysis Software**

An analyst uses the MPVEASI interface to define the ASD as appropriate for a specific facility. After defining the areas and layers, the analyst enters the protection elements in each PPS layer. The next step is to define the detection and delay values for each component in each protection element. The responsible analyst *must* use site-specific detection and delay values for the results to be accurate for that facility.

**Response Times and Tactics**

The analyst enters response force time for the site. The analyst can also choose adversary tactics of force, stealth, and deceit, which determine the detection and delay values to be used in the calculation. The analyst also selects either theft (two-way paths) or sabotage (one-way paths) analysis.
Next, the analyst identifies the path beginning with the elements that have the least delay; when a CDP is identified, the analyst then chooses the elements with the least detection. Once the path is identified, the tool calculates \( P_1 \) for the identified path. A secondary metric calculated by MPVEASI is Time Remaining after Interruption, which represents the time margin for the response force.

17.7 Neutralization Analysis

**Probability of Neutralization, \( P_N \)**
The second factor in PPS effectiveness is the Probability of Neutralization, \( P_N \). A wide range of models and tools can be used to estimate \( P_N \). These include expert opinion, simple calculations, complex simulations, and force-on-force exercises. They vary in the number of variables that are considered and thus in the fidelity of the model to an actual adversary and response engagement. The basic tradeoff in the use of these models is accuracy versus cost.

**Input Parameters**
Due to time constraints, this course uses a relatively simple model and calculation for estimating \( P_N \) for paths determined from single- or multi-path \( P_1 \) models. The model is built on a conservative estimate that approximately three response force members for every attacker results in a very high \( P_N \). This method can account for uncertainties with other factors (e.g., use of surprise or force multipliers). When using this model, the following assumptions are made:

- Table is based on a discrete time Markov chain
- Firing rates and PH/PK are the same on both sides
- Firing rate is proportional to the number of combatants on a side

In actual practice for nuclear facilities in the U.S., \( P_N \) is estimated using a combination of adversary and response force simulations and force-on-force exercises as part of scenario analysis.

17.8 Scenario Analysis

**Postulate Adversary Attack Scenarios**
Scenario analysis is a PPS effectiveness evaluation technique that is based on postulating adversary attack scenarios and determining \( P_E \) directly without the need to calculate \( P_1 \) in one tool and \( P_N \) in another. The emphasis is on selecting adversary paths that take advantage of possible PPS vulnerabilities. The process involves identifying PPS components that may be susceptible to defeat due to installation specifics or operational procedures. This includes defeat methods for sensors, barriers, and communication systems, and possible diversion or elimination of part of the response force. This is a place to consider the role of possible insiders in collusion with an outsider adversary.

**Credible Scenarios**
For scenario analysis, the analyst must be careful to ensure that the scenarios are credible. The primary way to ensure credibility is to revisit the capabilities of the adversary in the approved DBT and to realize that
the adversary must complete the entire mission to be successful, and not just defeat a specific PPS component.

### 17.9 Tabletop Analysis

**Tabletop Exercise**

Scenario analysis is typically conducted as a tabletop exercise with a facility model or map, and using a set of experts, including facility operators, security managers, response force, and system analysts. The results of the scenario analysis are the impact of the specific attack scenarios on system effectiveness. The results are used to augment the results of the path analysis, which only addressed timely detection. A methodology for conducting tabletops is described in this course.

### 17.10 Insider Analysis

**Insider Analysis**

An insider adversary is a part of every DBT. During scenario analysis, in addition to considering insiders colluding with outsiders, insiders acting alone must be analyzed as part of PPS effectiveness.

**Insider Characteristics**

The insider adversary is generally a formidable one. That is because the insider can be any of the employees or persons with facility access. Thus, the insider has some combination of knowledge, access, and authority that typically provides the capability of bypassing some of the PPS components. Insider characteristics can vary widely as defined in the DBT. The spectrum of insider characteristics includes number, passive or active, nonviolent or violent, and irrational or rational.

**Manual Analysis Process**

In this course, insider analysis methodology uses the DEPO process to characterize the facility, define the threat, develop insider strategies, evaluate security components and measures, and summarize and analyze the results. This is currently a manual process using worksheets rather than computer models and codes.

### 17.11 Transportation Security

**Moving Facility**

The DEPO process is also applied to the transportation of nuclear materials, with some modifications. The nuclear material transportation system can be considered a moving facility. The PPS objectives are the same as for a fixed facility: prevent theft and sabotage.

**Differences Between Fixed and Moving Sites**

Although the PPS design includes detection, delay, and response, there are design differences for transportation systems compared to fixed facilities. Although there may be onboard intrusion sensors, the vehicle drivers and escorts are major components of the detection system. The delay function is provided by a combination of the transport escort response force and by the construction features of the truck or trailer, which by necessity must be relatively compact and lightweight. The response force is provided by the drivers and escorts that are both onboard and in separate vehicles.
Cooperation agreements with local law enforcement agencies are an important consideration.

The analysis of transport PPS effectiveness also tends to have a different emphasis. Path analysis is used less because the number of adversary paths is limited. Scenario analysis and force-on-force exercises are commonly used for transport security performance analysis.

17.12 Summary

The third section of the DEPO process is to evaluate PPS effectiveness. The major points to keep in mind are:

- The metric for PPS effectiveness along paths is $P_E = P_I \times P_N$, i.e., the product of the probabilities for interruption and neutralization
- Adversary sequence diagrams and PPS models are used by path analysis codes to calculate $P_I$
- Expert opinion, calculations, simulations, and force-on-force exercises are used to determine $P_N$
- Scenario analysis postulates adversary attacks that exploit vulnerabilities and can produce qualitative $P_E$ estimates based on simulations
- Evaluations should be conducted for the full DBT, including outsiders, insiders, and outsiders in collusion with insiders