16. Evaluation of Physical Protection Systems

Abstract. *PPS system 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 chapter provides an introduction and overview of these evaluation techniques.*

16.1 Introduction

Why Evaluate a PPS?

As shown in Figure 2-2, the third major part of the DEPO process is the evaluation of physical protection system effectiveness. There are several important reasons to evaluate the PPS design.

- Verify that the PPS that was designed or characterized in the second part of DEPO satisfies the requirements that were established in the first part of DEPO.
- Identify any system deficiencies in the design or implementation that need to be addressed in order 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 take into account 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:

- Adversary Sequence Diagrams Model(17)
- Single Path Computer Tool (18)
- Multipath Computer Tool (19)
- Neutralization Analysis (20)
- Scenario Analysis (21)
- Tabletop Analysis (22)
- Insider Analysis (23)
- Transportation Security (24)

The student learning objectives for Chapter 16 are:

- Identify the physical protective system effectiveness measures:
  - Probability of Interruption, P_I
  - Probability of Neutralization, P_N
- Recognize PPS evaluation approaches for:
  - Scenario and Path Analysis
  - Neutralization Analysis
  - Insider Analysis

16.2 System Effectiveness

PPS Effectiveness

Interruption Defined

Neutralization Defined

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 mission is complete and in adequate numbers 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 killed. Both interruption and neutralization are necessary for the PPS to be effective.

Probability of Interruption P_I

The Probability of Interruption P_I is defined based on the Principle of Timely Detection and a Critical Detection Point. For any adversary path the P_I is the cumulative probability of detection along the path up to and including the Critical Detection Point 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 the 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. This is equivalent to the statement that a chain is only as strong as its weakest link.

16.3 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 is also dependent 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 the 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 time lines determines whether or not the response force is able to interrupt the adversary before the theft or sabotage mission is completed.

Principle of Timely Detection

The principle of timely detection is introduced in order to establish a quantitative metric for probability of interruption. In order 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 along its timeline to be able to interrupt the adversary before theft or sabotage is completed. In this case there is said to be timely detection of the adversary by the PPS. Without timely detection the PPS is ineffective.

16.4 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. It 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

16.5 Single Path Computer Tool

P_I Algorithm

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

EASI Software

This course uses VEASI as an adversary single path model and software. VEASI is an acronym for Very-simplified Estimate of Adversary Sequence Interruption. The current version uses a Microsoft Excel spreadsheet to enter data that define the adversary task delay times, task detection probabilities and response force time. VEASI assumes the delay times are fixed values while the response time is a reliable time taken from response plans. (VEASI is so named because it is adapted from the EASI (Estimate of Adversary Sequence Interruption) software code which has the same features as VEASI but adds in a guard communication probability; EASI also allows for uncertainties in delay and response times by using a Gaussian distribution with mean and standard deviation for these variables. VEASI was used instead because it is closer to the codes for calculating Probability of Interruption created for the U.S. Department of Energy.)

Data entry is relatively quick and this makes it easy to analyze multiple paths, one at a time, or to investigate the effect of different detection probabilities or delay times on P_I. This enables the skilled analyst to evaluate relatively simple facilities and security systems and consider upgrade options with VEASI.

16.6 Multi-path Computer Tool

Calculate P_I For All Adversary Paths

Evaluation of PPS effectiveness against the outsider adversary includes calculating P_I for all adversary paths. For complex facilities this is done using the ASD to address all paths. This course uses the PANL model and software. PANL is a shortened form of Path ANaLysis.

PANL Software

An analyst uses the PANL interface to define the ASD that is appropriate for a specific facility. After defining the areas and layers, the analyst selects from a library 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. PANL includes a numerical database of representative detection probabilities and delay times for typical sensors and barriers. It cannot be overemphasized that 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 third PPS function input of response force times is entered by the analyst. The analyst can also choose adversary tactics of force, stealth, and deceit that determine which detection and delay values are used in the calculation. The user also selects either theft (two-way paths) or sabotage (one-way paths) analysis. The PANL software then quickly calculates P_I for all adversary paths and provides the results ranked by the most vulnerable paths – the ones with the lowest P_I. A secondary metric calculated by PANL is the Time Remaining after Interruption and represents the time margin for the response force.

16.7 Neutralization Analysis

Probability of Neutralization P_N

The second factor in PPS effectiveness is the Probability of Neutralization P_N. There is a wide range of models and tools that 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 multipath P_I models. The input parameters are numbers, weapons, and arrival times for the adversary and response forces, taking into account that the response force generally deploys from different locations and thus arrives at different times and possibly with different weapons.

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

16.8 Insider Analysis

Insider Analysis

An insider adversary is a part of every DBT. In addition to considering insiders in collusion with outsiders during scenario analysis, 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 full 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.

16.9 Scenario Analysis

Postulate Adversary Attack Scenarios

Scenario analysis is a PPS effectiveness evaluation technique that is based on postulating adversary attack scenarios and determining PE directly without needing to calculate P_I 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 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.

16.10 Tabletop Exercise

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 and 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.

16.11 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 as 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 a major component 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.

Performance Analysis Tools

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

16.12 Summary

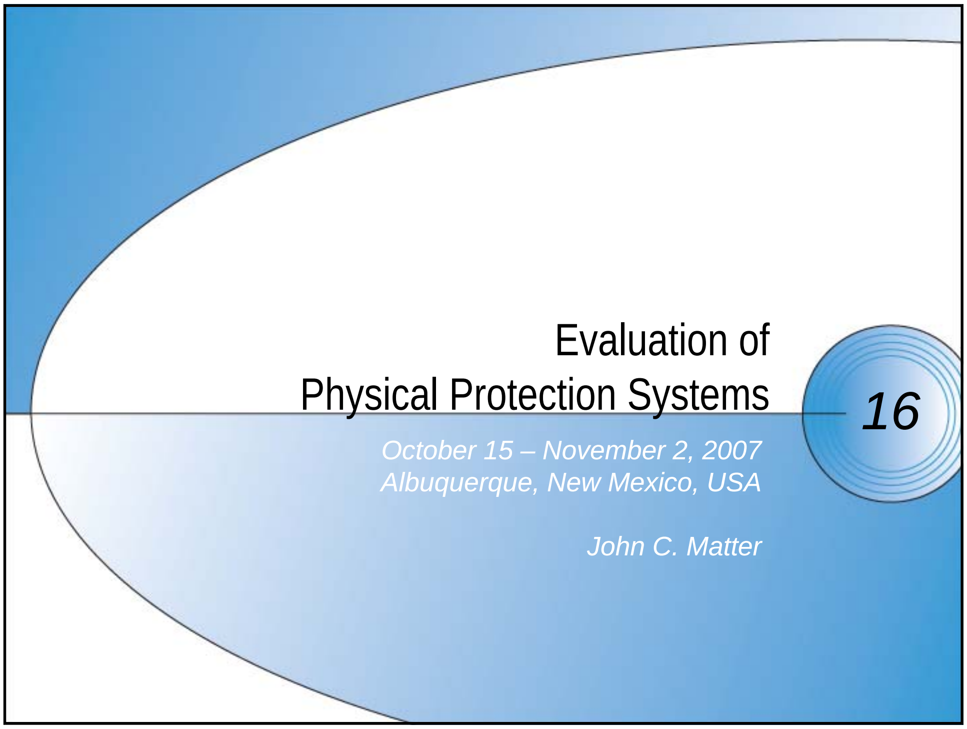
Evaluate PPS Effectiveness

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

- The metric for PPS effectiveness along paths is $P_E = P_I * P_N$, 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 PE estimates based on simulations

- Evaluations should be conducted for the full DBT that includes outsiders, insiders, and outsiders in collusion with insiders

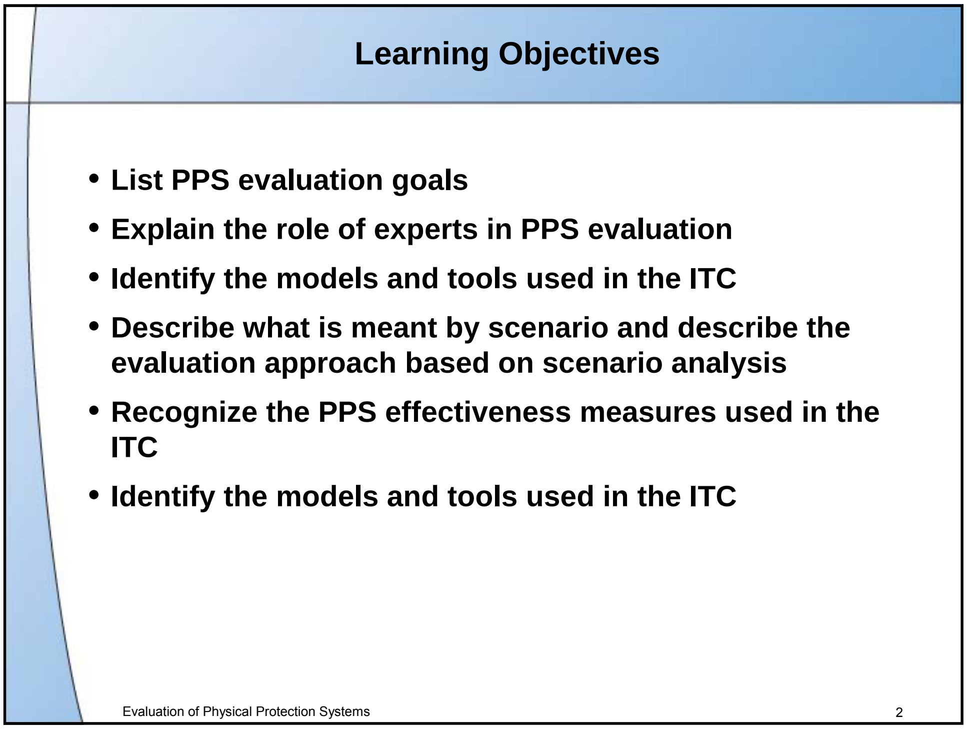


Evaluation of Physical Protection Systems

16

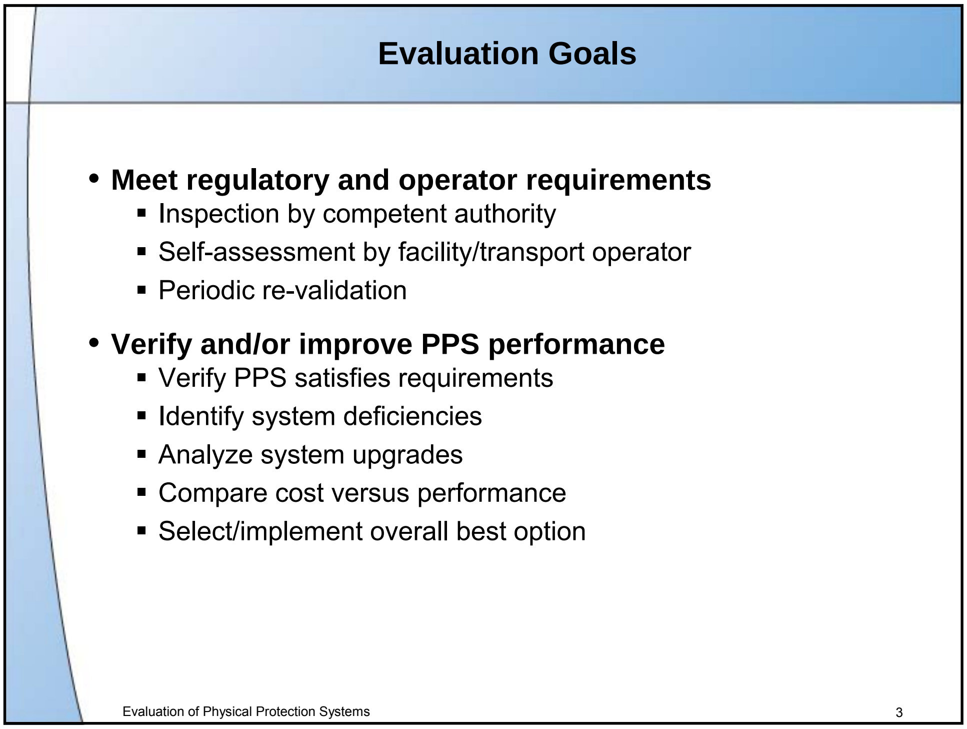
October 15 – November 2, 2007
Albuquerque, New Mexico, USA

John C. Matter



Learning Objectives

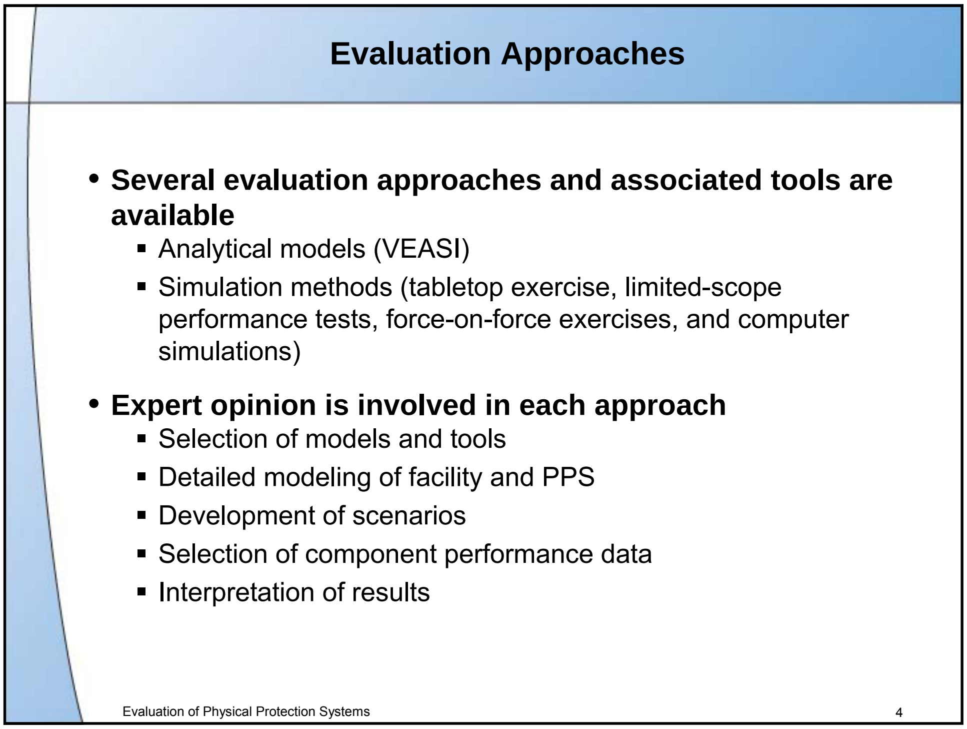
- List PPS evaluation goals
- Explain the role of experts in PPS evaluation
- Identify the models and tools used in the ITC
- Describe what is meant by scenario and describe the evaluation approach based on scenario analysis
- Recognize the PPS effectiveness measures used in the ITC
- Identify the models and tools used in the ITC



Evaluation Goals

- **Meet regulatory and operator requirements**
  - Inspection by competent authority
  - Self-assessment by facility/transport operator
  - 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

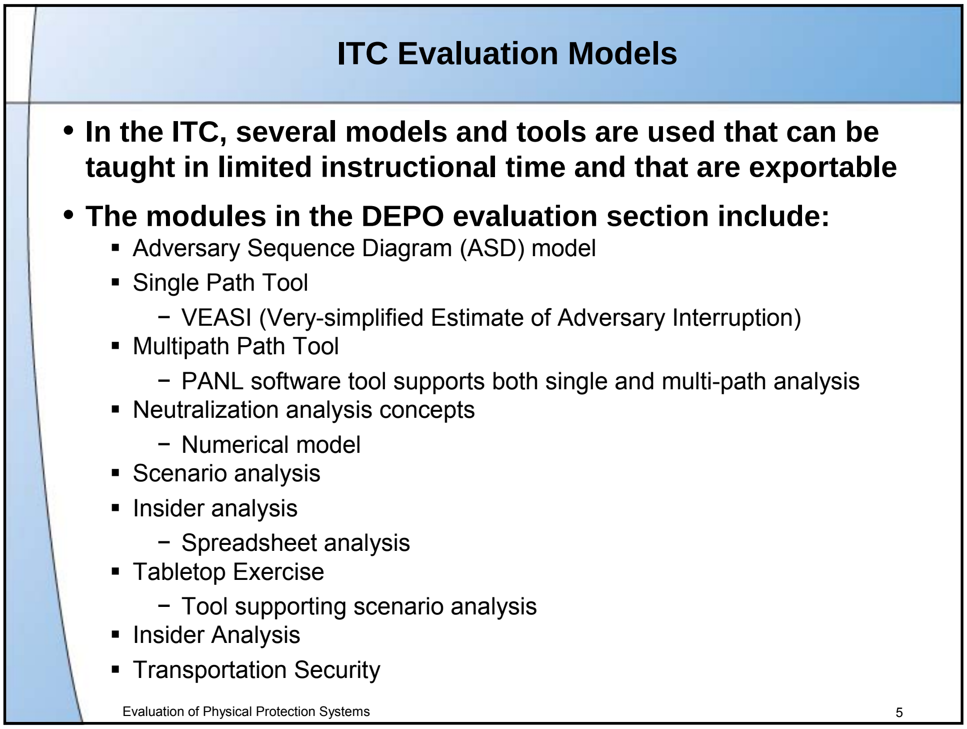
Evaluation of Physical Protection Systems 3



Evaluation Approaches

- **Several evaluation approaches and associated tools are available**
  - Analytical models (VEASI)
  - Simulation methods (tabletop exercise, limited-scope performance tests, force-on-force exercises, and computer simulations)
- **Expert opinion is involved in each approach**
  - Selection of models and tools
  - Detailed modeling of facility and PPS
  - Development of scenarios
  - Selection of component performance data
  - Interpretation of results

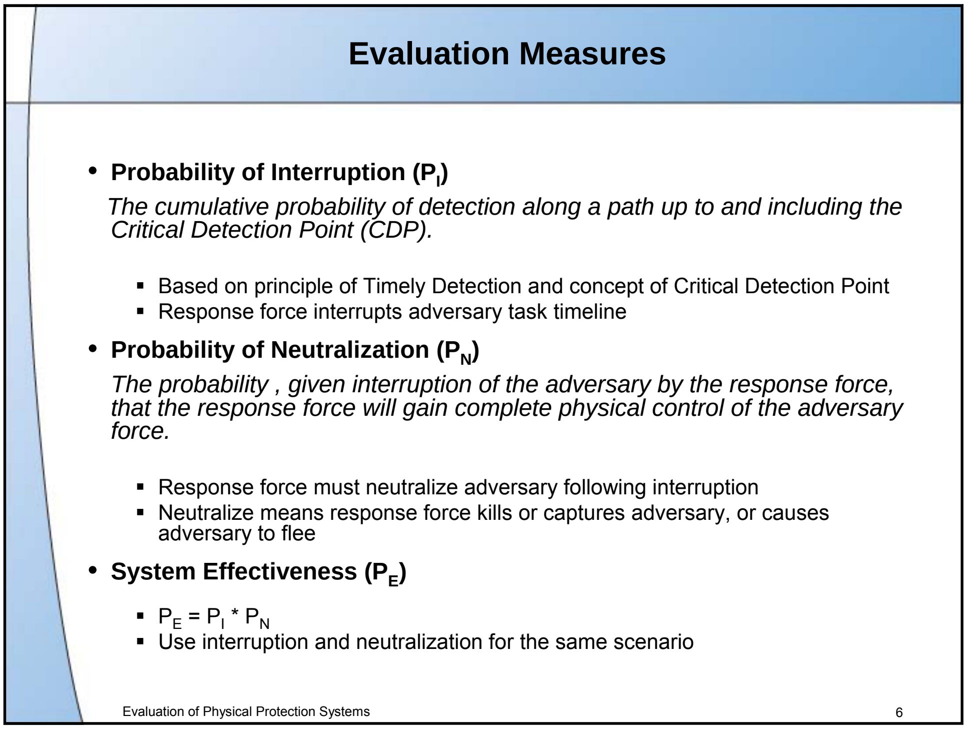
Evaluation of Physical Protection Systems 4



ITC Evaluation Models

- **In the ITC, several models and tools are used that can be taught in limited instructional time and that are exportable**
- **The modules in the DEPO evaluation section include:**
  - Adversary Sequence Diagram (ASD) model
  - Single Path Tool
    - VEASI (Very-simplified Estimate of Adversary Interruption)
  - Multipath Path Tool
    - PANL software tool supports both single and multi-path analysis
  - Neutralization analysis concepts
    - Numerical model
  - Scenario analysis
  - Insider analysis
    - Spreadsheet analysis
  - Tabletop Exercise
    - Tool supporting scenario analysis
  - Insider Analysis
  - Transportation Security

Evaluation of Physical Protection Systems 5



Evaluation Measures

- **Probability of Interruption (P_I)**

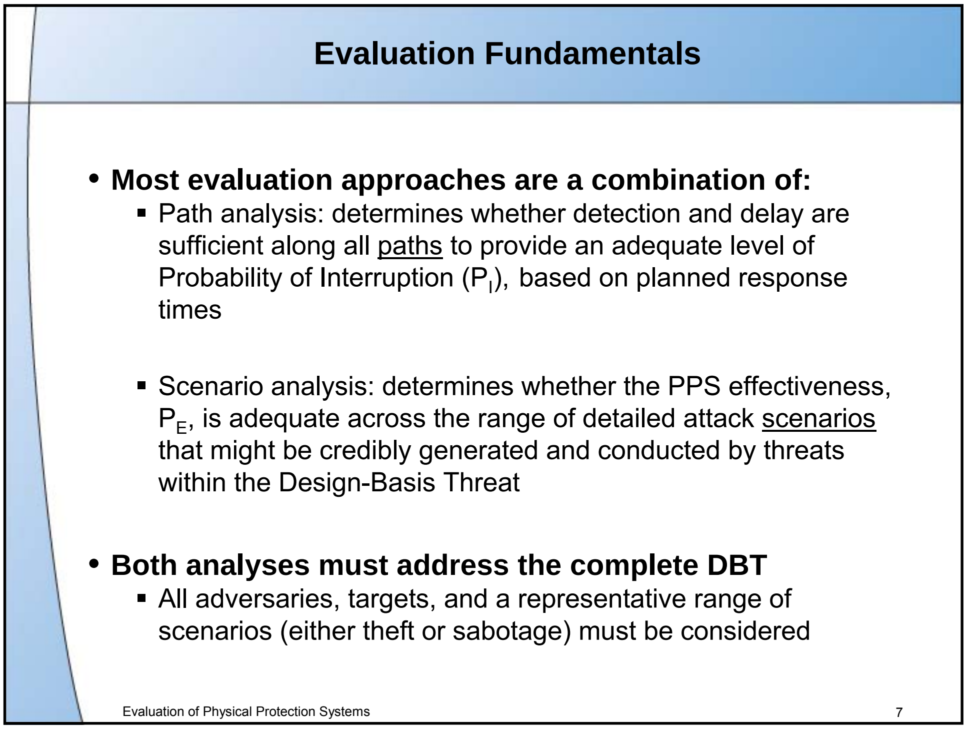
  The cumulative probability of detection along a path up to and including the Critical Detection Point (CDP).

  - Based on principle of Timely Detection and concept of Critical Detection Point
  - Response force interrupts adversary task timeline
- **Probability of Neutralization (P_N)**

  The probability , given interruption of the adversary by the response force, that the response force will gain complete physical control of the adversary force.

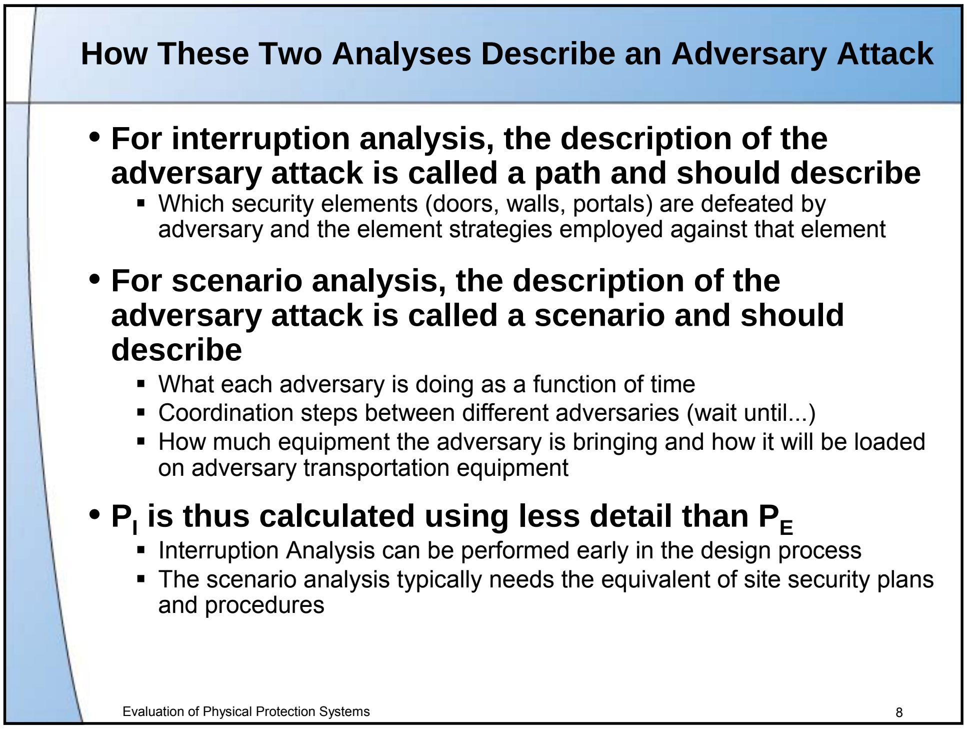
  - Response force must neutralize adversary following interruption
  - Neutralize means response force kills or captures adversary, or causes adversary to flee
- **System Effectiveness (P_E)**
  - $P_E = P_I * P_N$
  - Use interruption and neutralization for the same scenario

Evaluation of Physical Protection Systems 6



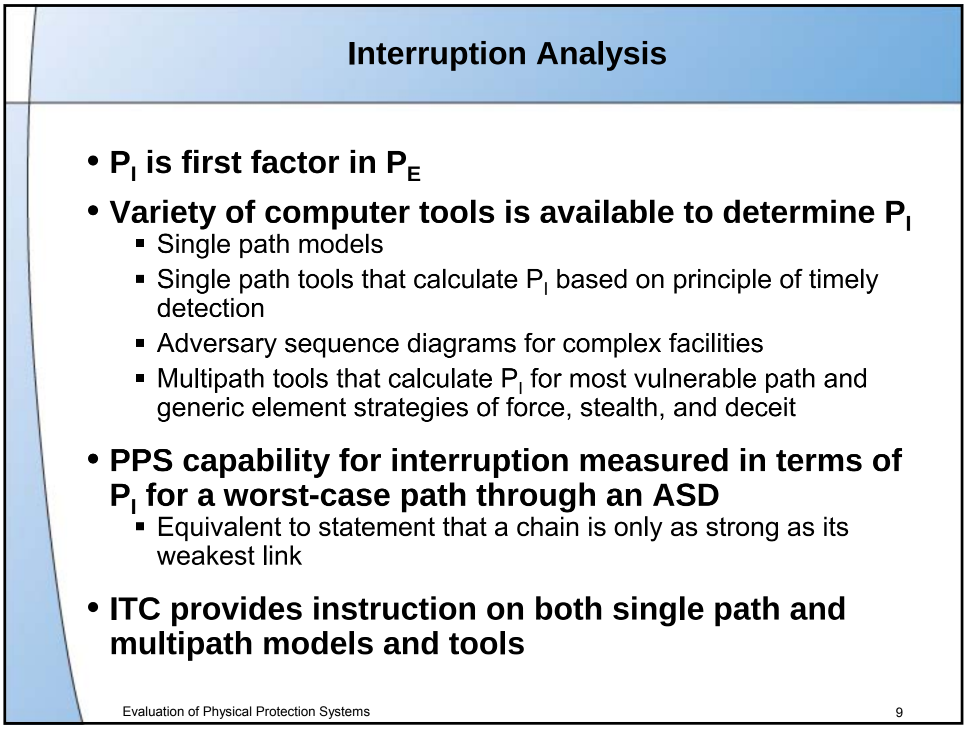
Evaluation Fundamentals

- **Most evaluation approaches are a combination of:**
  - Path analysis: determines whether detection and delay are sufficient along all paths to provide an adequate level of Probability of Interruption (P_I), based on planned response times
  - Scenario analysis: determines whether the PPS effectiveness, P_E, is adequate across the range of detailed attack scenarios that might be credibly generated and conducted by threats within the Design-Basis Threat
- **Both analyses must address the complete DBT**
  - All adversaries, targets, and a representative range of scenarios (either theft or sabotage) must be considered



How These Two Analyses Describe an Adversary Attack

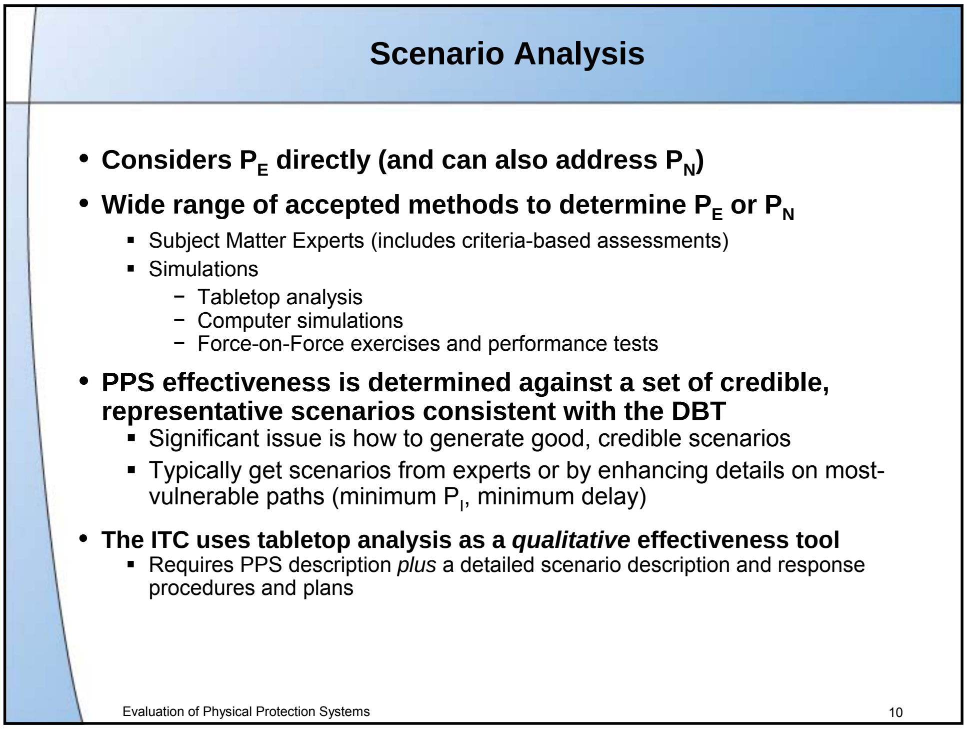
- **For interruption analysis, the description of the adversary attack is called a path and should describe**
  - Which security elements (doors, walls, portals) are defeated by adversary and the element strategies employed against that element
- **For scenario analysis, the description of the adversary attack is called a scenario and should describe**
  - What each adversary is doing as a function of time
  - Coordination steps between different adversaries (wait until...)
  - How much equipment the adversary is bringing and how it will be loaded on adversary transportation equipment
- **P_I is thus calculated using less detail than P_E**
  - Interruption Analysis can be performed early in the design process
  - The scenario analysis typically needs the equivalent of site security plans and procedures



Interruption Analysis

- P_I is first factor in P_E
- Variety of computer tools is available to determine P_I
  - Single path models
  - Single path tools that calculate P_I based on principle of timely detection
  - Adversary sequence diagrams for complex facilities
  - Multipath tools that calculate P_I for most vulnerable path and generic element strategies of force, stealth, and deceit
- PPS capability for interruption measured in terms of P_I for a worst-case path through an ASD
  - Equivalent to statement that a chain is only as strong as its weakest link
- ITC provides instruction on both single path and multipath models and tools

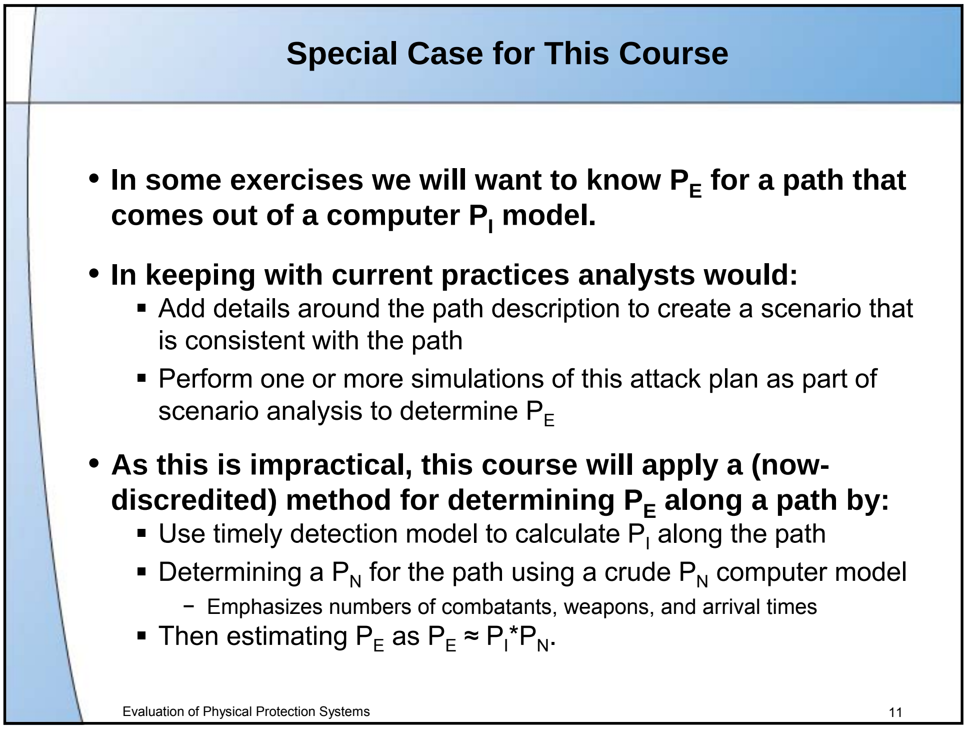
Evaluation of Physical Protection Systems 9



Scenario Analysis

- **Considers P_E directly (and can also address P_N)**
- **Wide range of accepted methods to determine P_E or P_N**
  - Subject Matter Experts (includes criteria-based assessments)
  - Simulations
    - Tabletop analysis
    - Computer simulations
    - Force-on-Force exercises and performance tests
- **PPS effectiveness is determined against a set of credible, representative scenarios consistent with the DBT**
  - Significant issue is how to generate good, credible scenarios
  - Typically get scenarios from experts or by enhancing details on most-vulnerable paths (minimum P_I, minimum delay)
- **The ITC uses tabletop analysis as a *qualitative* effectiveness tool**
  - Requires PPS description *plus* a detailed scenario description and response procedures and plans

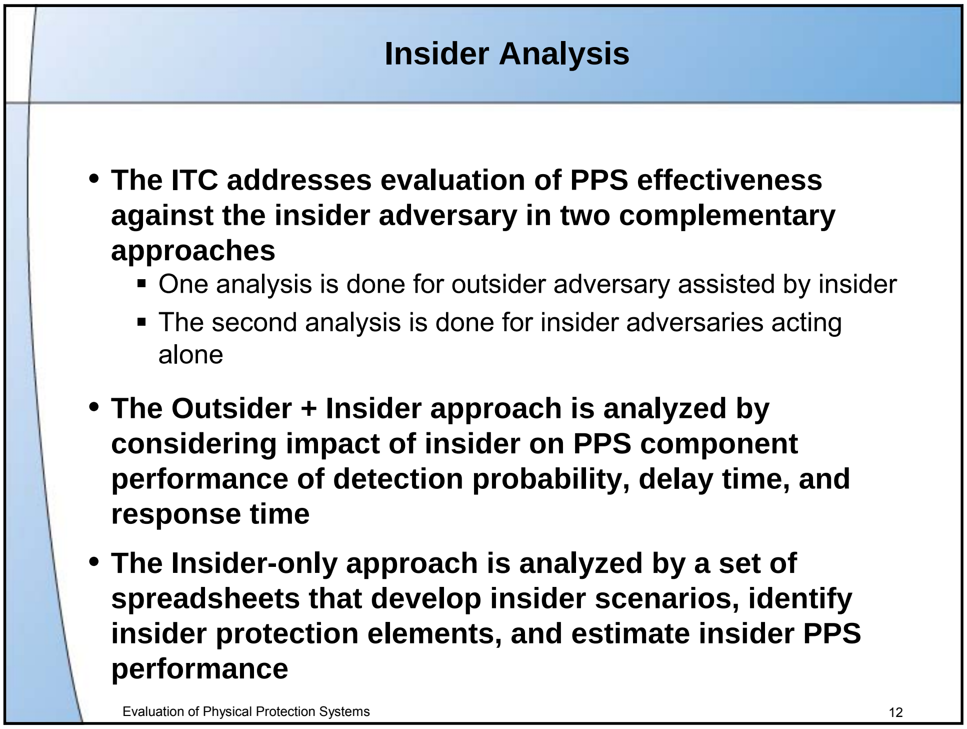
Evaluation of Physical Protection Systems 10



Special Case for This Course

- **In some exercises we will want to know P_E for a path that comes out of a computer P_I model.**
- **In keeping with current practices analysts would:**
  - Add details around the path description to create a scenario that is consistent with the path
  - Perform one or more simulations of this attack plan as part of scenario analysis to determine P_E
- **As this is impractical, this course will apply a (now-discredited) method for determining P_E along a path by:**
  - Use timely detection model to calculate P_I along the path
  - Determining a P_N for the path using a crude P_N computer model
    - Emphasizes numbers of combatants, weapons, and arrival times
  - Then estimating P_E as $P_E \approx P_I * P_N$.

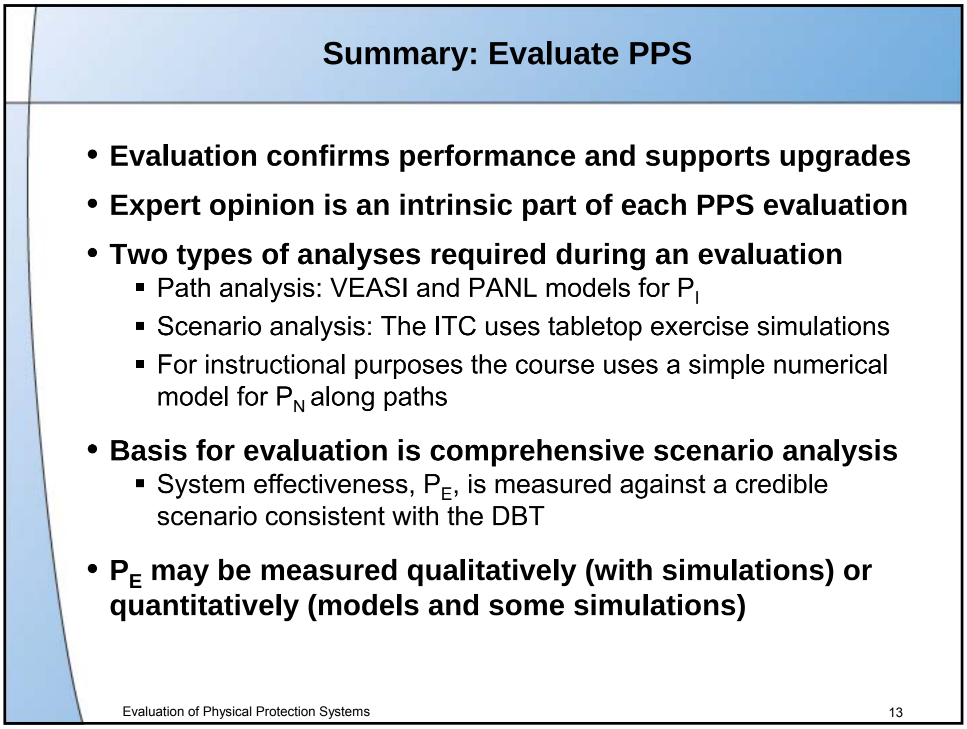
Evaluation of Physical Protection Systems 11



Insider Analysis

- **The ITC addresses evaluation of PPS effectiveness against the insider adversary in two complementary approaches**
  - One analysis is done for outsider adversary assisted by insider
  - The second analysis is done for insider adversaries acting alone
- **The Outsider + Insider approach is analyzed by considering impact of insider on PPS component performance of detection probability, delay time, and response time**
- **The Insider-only approach is analyzed by a set of spreadsheets that develop insider scenarios, identify insider protection elements, and estimate insider PPS performance**

Evaluation of Physical Protection Systems 12



Summary: Evaluate PPS

- **Evaluation confirms performance and supports upgrades**
- **Expert opinion is an intrinsic part of each PPS evaluation**
- **Two types of analyses required during an evaluation**
  - Path analysis: VEASI and PANL models for P_I
  - Scenario analysis: The ITC uses tabletop exercise simulations
  - For instructional purposes the course uses a simple numerical model for P_N along paths
- **Basis for evaluation is comprehensive scenario analysis**
  - System effectiveness, P_E, is measured against a credible scenario consistent with the DBT
- **P_E may be measured qualitatively (with simulations) or quantitatively (models and some simulations)**

Evaluation of Physical Protection Systems 13

17. Adversary Sequence Diagram (ASD) Model

Abstract. *The adversary sequence diagram (ASD) graphically models the PPS at a facility. It identifies paths which adversaries can follow to accomplish sabotage or theft. The most vulnerable path can be determined and used to measure the effectiveness of the entire PPS. There are five steps in developing an adversary sequence diagram for a specific site. The first step is to model the facility by separating it into adjacent physical areas. Next, the protection layers are defined between the adjacent areas. Each protection layer includes one or more path elements which are the basic building blocks of a PPS. Examples of path elements are doors, fences, surfaces, and portals. The third step is to identify targets. The fourth step is to reduce the size of the ASD by, for example, combining path elements and target locations that have identical security features. Finally, each element is assigned a 3-letter code (such as SUR), an index (so it is SUR 1 or SUR 2).*

17.1 Introduction

Definition of Adversary Sequence Diagram (ASD)

Adversaries accomplish their objective by moving along a path through a facility and defeating elements of the Physical Protection System (PPS) encountered along the path. The adversary sequence diagram (ASD) is a graphic representation that is used to help evaluate the effectiveness of the PPS at a facility. It identifies the paths which adversaries can follow to accomplish sabotage or theft. For a specific PPS and a specific threat, the most vulnerable path (or the path with least PPS effectiveness) can be determined. This path establishes the effectiveness of the total PPS.

Using Models with Path Analysis

A previous session, Evaluation of Physical Protection Systems, mentioned two evaluation computer tools, VEASI and PANL. VEASI models one path selected by the user. PANL models all paths by using an ASD to graphically represent the paths. This session discusses the ASD and demonstrates how an ASD can be developed for a specific facility.

17.2 The Model

Anticipating the Adversary

Adversaries must be detected and an alarm must be received by the response force in time to assess the alarm, initiate a response, and interrupt the adversary before they complete their task. Adversary sequence diagrams can be used to model all possible adversary paths through a facility.

17.2.1 Paths

Sabotage vs. Theft Paths

Figure 17-1 shows two representative paths that adversaries might take to attack a sabotage target. For a theft attack, paths must be drawn both into the facility to the target and from the target out of the facility.

Path Defines the Set of Adversary Actions

In a typical facility, there are usually hundreds of alternative paths an adversary might take to reach a target that he wants to steal or sabotage. Further, each path can be traveled in many ways using force, deceit, or stealth tactics to defeat the various detection and delay components located along a path. Thus, each path consists of a specific set of adversary actions that, if accomplished, will result in the achievement of the adversary’s objective.

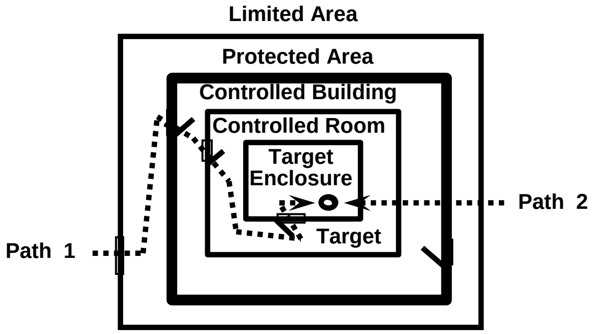


Figure 17-1. Possible Adversary Paths for a Sabotage Threat

17.2.2 Creating an ASD

Steps for Creating the ASD

The five basic steps in creating an ASD for a specific site include:

1. Modeling the facility by separating it into adjacent physical areas separated by a protection layer controlling movement between areas.
2. Defining path elements that make up the protection layers between the adjacent areas.
3. Identifying targets where nuclear material or vital components are located.
4. Reduce the size of the ASD by combining paths elements and target location elements that have identical security features (and are therefore duplicates) or by removing protection layers that are expected to afford little protection.
5. Assigning each path/target location element on the diagram a 3-letter code (such as SUR or DOR) and a unique index (so it is SUR 1 or DOR 2), and adding path segments attaching that element to adjacent areas.

These steps will allow development of an ASD that can be used by the PANL computer model.

17.2.3 Physical Areas

A Facility Is a Set of Adjacent Physical Areas

The ASD models a facility by separating it into adjacent physical areas. Figure 17-2 is a facility sketch of an example facility.

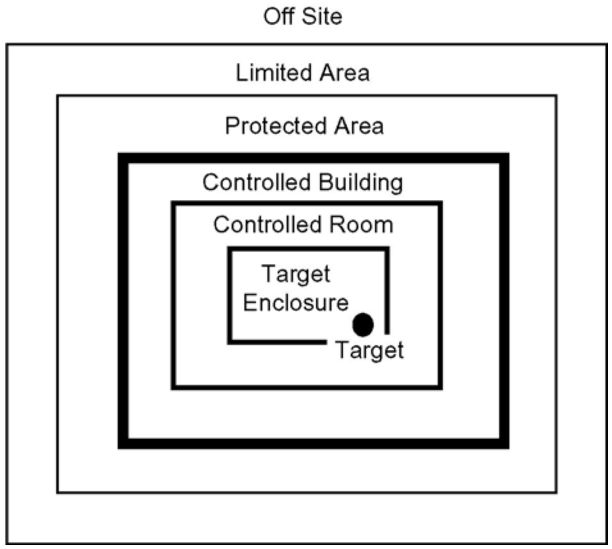


Figure 17-2. Basic Areas At An Example Facility

General Types of Physical Areas

Figure 17-3 describes the adjacent physical areas of the example facility. The ASD represents areas by sequential rectangles. The names of these areas can be changed to model a specific site.

Off Site
Limited Area
Protected Area
Controlled Building
Controlled Room
Target Enclosure
Target

Figure 17-3. Adjacent Physical Areas—Example Facility

17.2.4 Protection Layers and Path Elements

Path Elements Are the Building Blocks

The ASD models a PPS by identifying the path elements composing protection layers between adjacent areas (Figure 17-4). Each protection layer consists of a number of path elements (Figure 17-5) such as doors, or fences. Path elements (PE) are the basic building blocks of a PPS. During this step the analyst describes the complete set of elements making up a protection layer in plain language, such as “Protected Area Vehicle Portal” or “Vital Area Wall.”

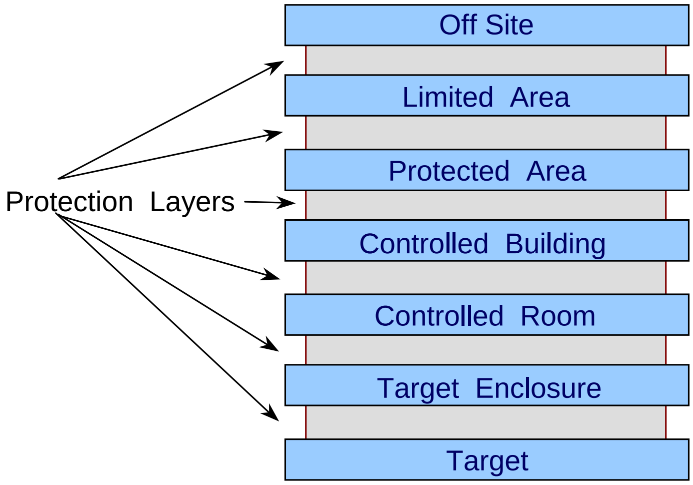


Figure 17-4. Protection Layers Between Adjacent Areas

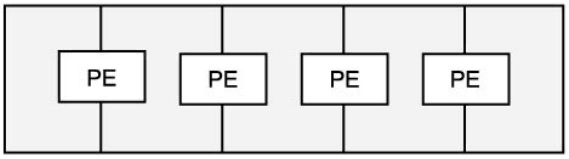


Figure 17-5. Protection Layers Consist of Path Elements

17.2.5 Target Location Elements

Target locations are special elements describing detection and delay at targets

The protection layer between the Target Enclosure and the Target (see Figure 17-4) consists of specialized path elements called target location elements. These elements need to be defined for this layer to describe detection and delay associated with either completing a sabotage task or acquiring cross a target for theft. Target elements have no distance across them.

17.2.6 Reducing the Size of the ASD

Combining similar elements reduces the time required to analyze the site using multipath analysis software

The larger the number of elements included in the ASD the longer it will take the user to describe the facility and the longer it will take software, such as PANL, to complete desired analysis. For this reason it is a good idea to combine identical protection elements. Elements are said to be identical if they 1) are on the same protection level separating the same two areas and 2) have identical performance values (e.g., similar detection and delay as well as similar sequencing of detection with delay). This process of combining elements should be documented so it is clear that all the original elements are covered.

ASD's do not model variations in widths across areas

Adversary Sequence Diagrams do not consider take into account that some elements on one protection layer are closer to those on the next layer due to variations in area width along the perimeter of that area. In practice, for example, different portal elements on a perimeter may have different distances to various building doors and surfaces. This variation is typically ignored in creating an ASD and either an average or minimum distance is used. For this reason, elements can and should be combined even if they fall at different distances from surrounding protection layers.

Remove protection layers that provide little security by combining the areas on either side of them.

Another way to reduce the size of the ASD is to remove protection layers that afford little security now and are not expected to be improved by much during any security upgrade process. Protection layers are typically removed by combining the areas on either side of the protection layer into one area. An example of this would be to combine Offsite with the Limited Area in Figure 17-4 into one area called Offsite.

17.2.7 Assigning 3-Letter Element Codes and Adding Path Segments

Path elements and target locations are assigned 3-letter codes and index numbers to name each one uniquely

Each element is then assigned a 3-Letter Element code and an index number to identify each element uniquely, resulting in SUR 1 or DOR 2. The types of path elements and target locations used in the PANL ASD are shown below along with their 3-letter code:

Path Elements:

DUC	-	Duct
EMC	-	Emergency Evacuation Corral
EMX	-	Emergency Exit
EMP	-	Emergency Portal
FEN	-	Fenceline
GAT	-	Gateway
HEL	-	Helicopter Flight Path
ISO	-	Isolation Zone
PST	-	Material Passthrough
MAT	-	Material Portal
OVP	-	Overpass
DOR	-	Personnel Doorway
PER	-	Personnel Portal
SHD	-	Shipping/Receiving Doorway
SHP	-	Shipping/Receiving Portal
SUR	-	Surface
TUN	-	Tunnel
VHD	-	Vehicle Doorway
VEH	-	Vehicle Portal
WND	-	Window

Target Locations:

BPL	-	Bulk Process Line
CGE	-	Cage
FLV	-	Floor Vault
GNL	-	Generic Location
GBX	-	Glovebox
IPL	-	Item Process Line
OPN	-	Open Location
TNK	-	Storage Tank

ASD's use segments to represent connections between each element and the surrounding areas

The ASD represents path segments between areas, through the PEs, by lines. Both entry and exit parts of a path can be modeled. The entry part is from off site to the target, and the exit is from the target back to off site (Figure 17-6). A given PE may be traversed once (either on entry or exit), or it may be traversed twice, on entry and in the opposite direction on exit.

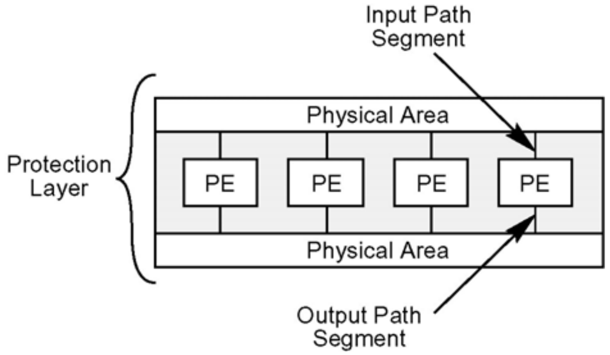


Figure 17-6. Path Element—Input and Output Path Segments

ASD Shows All Paths

The basic concept for an ASD is shown in Figure 17-7. The adversary attempts to defeat an element in each protection layer as he moves along a path through the facility to the target. The ASD represents all of the realistic paths that an adversary might take to reach a target.

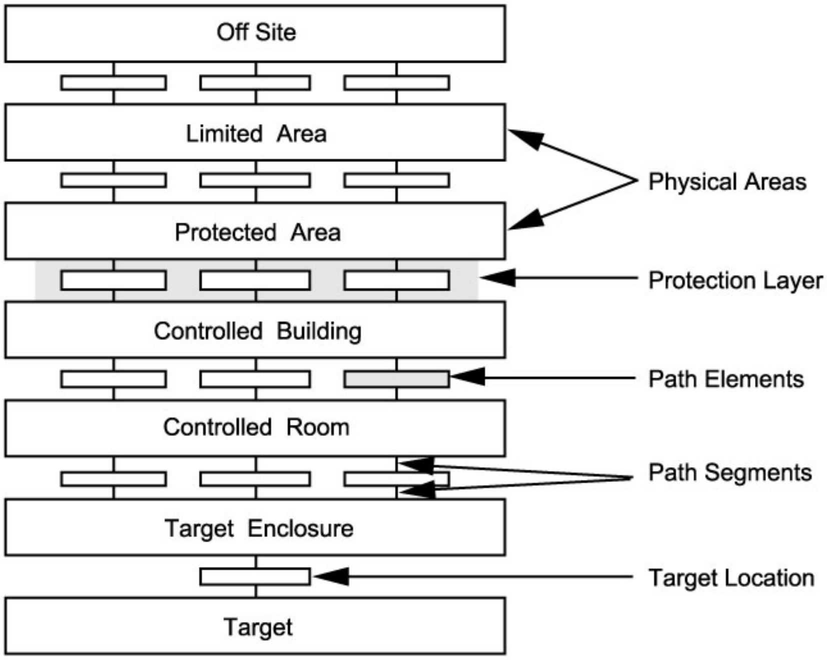


Figure 17-7. ASD Concept

Sabotage versus Theft Analysis

For sabotage analysis, only the entry paths would be evaluated, and the path elements would be assumed to be traversed in only one direction.

- For theft analysis, the ASD shown would be considered to be traversed twice—on entry to the target and on exit from the target.

- A more conservative protection goal, to interrupt the adversary before he removes the target from its location, requires only that entry be considered. When the entry and exit case is evaluated, the number of possible paths shown on the ASD is the square of the number of entry paths.

17.2.8 Site-Specific ASD

Use a Site-Specific ASD to Model the Facility

A site-specific ASD is constructed for each target, or set of targets having a common location. The objective is to correctly model the PPS that exists at a site. This site-specific ASD is created by identifying the path elements that are present at the facility. Figure 17-8 shows a simplified example facility and PPS layout. Figure 17-9 shows the resulting site-specific ASD that is constructed by using the example facility information.

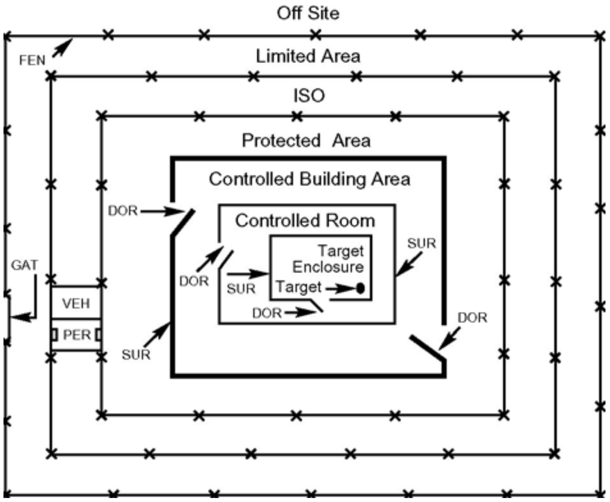


Figure 17-8. Sample Facility

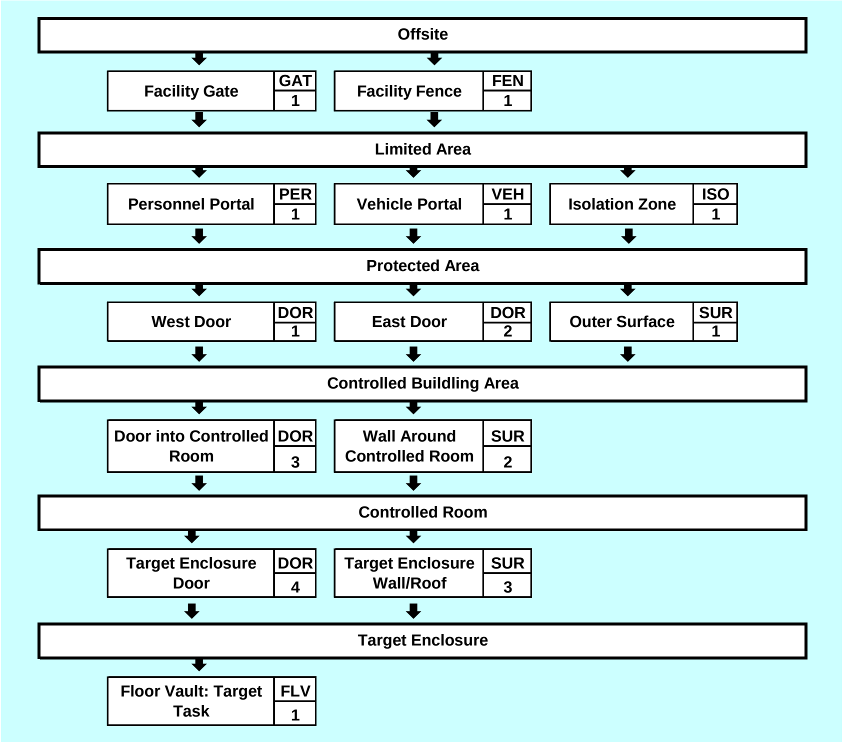


Figure 17-9. Site-Specific ASD for Sample Facility

17.2.9 ASD Jump

A “Jump” in an ASD Reflects Site-Specific Conditions

Sometimes it is necessary to deviate from the orderly sequence of physical areas and protection layers of the generic ASD in order to create an accurate site-specific ASD. A “jump” is used to model a site element that does not directly connect to the adjacent area shown on the generic ASD.

Example of a Jump

As shown in Figure 17-10, there is a wall common to the controlled building area and to the target enclosure. This situation is correctly modeled by including a SUR jump element from the controlled building area to model this portion of the common surface. As shown in Figure 17-11, the site-specific ASD then shows a direct path that jumps from the controlled building area to the target enclosure (without passing through the controlled room) in addition to all other selected indirect paths.

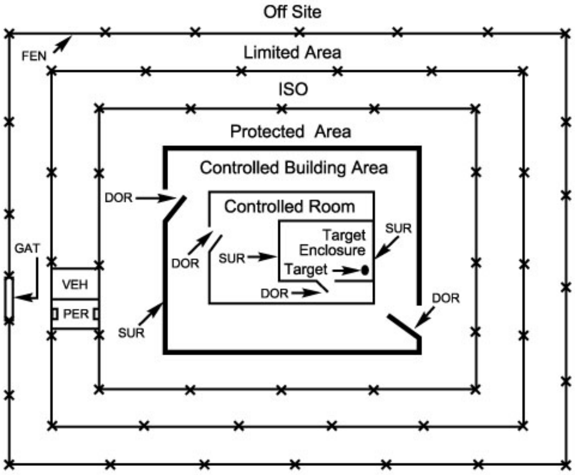


Figure 17-10. Sample Facility with Jump

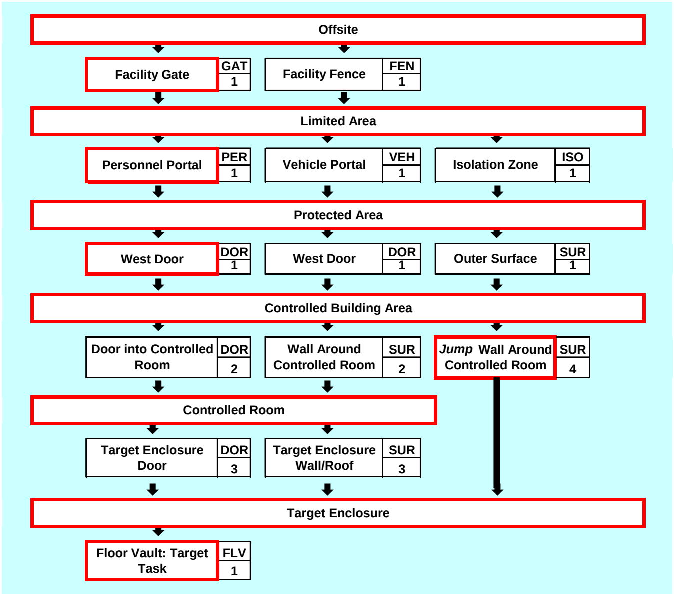
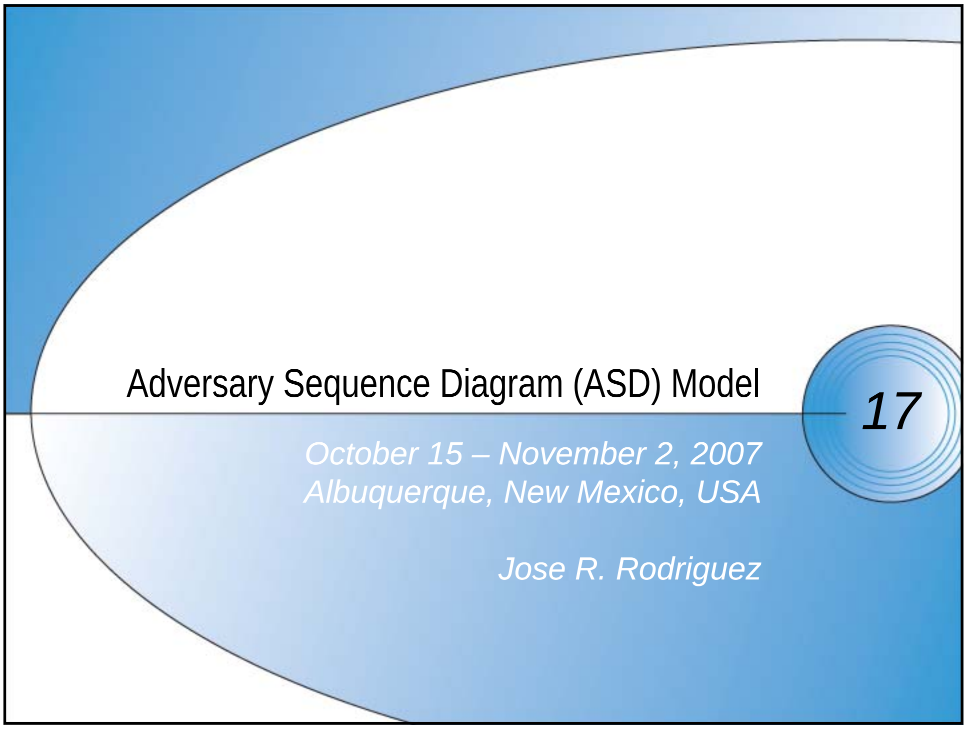


Figure 17-11. Site-Specific ASD for Sample Facility with Jump and Path Indicated in Red

17.3 Summary

ASDs Represent Adversary Paths

The Adversary Sequence Diagram (ASD) represents the paths that adversaries can follow to accomplish sabotage or theft and the PPS elements along the paths. This session describes a procedure to construct an ASD for a specific site. In following sessions, we will see how the ASD is used to evaluate the effectiveness of the PPS at a facility.

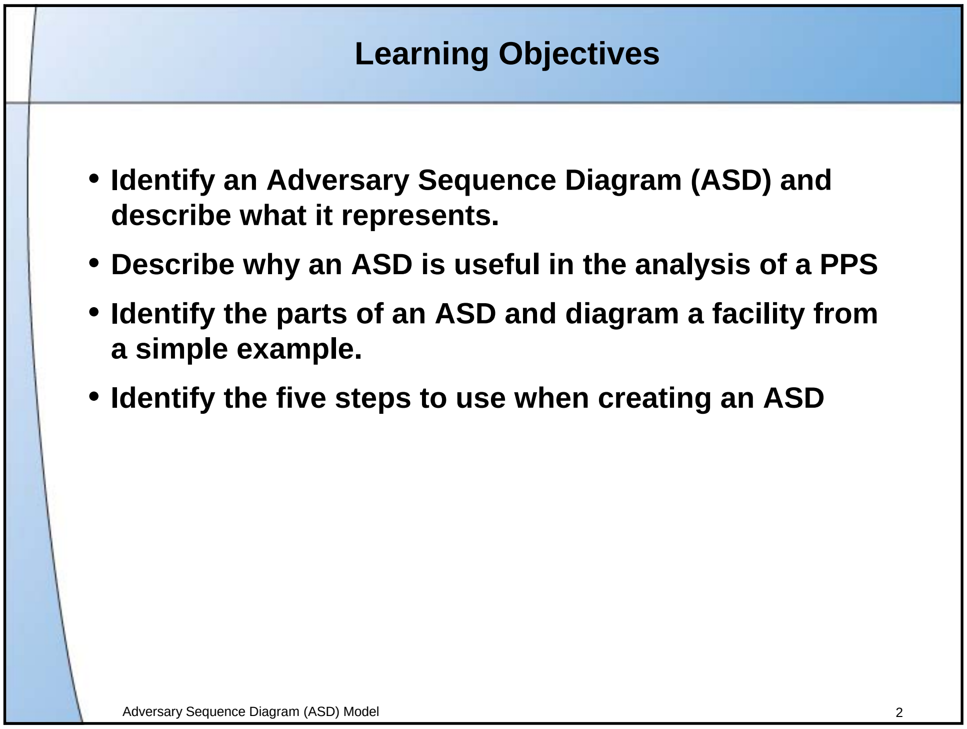


Adversary Sequence Diagram (ASD) Model

17

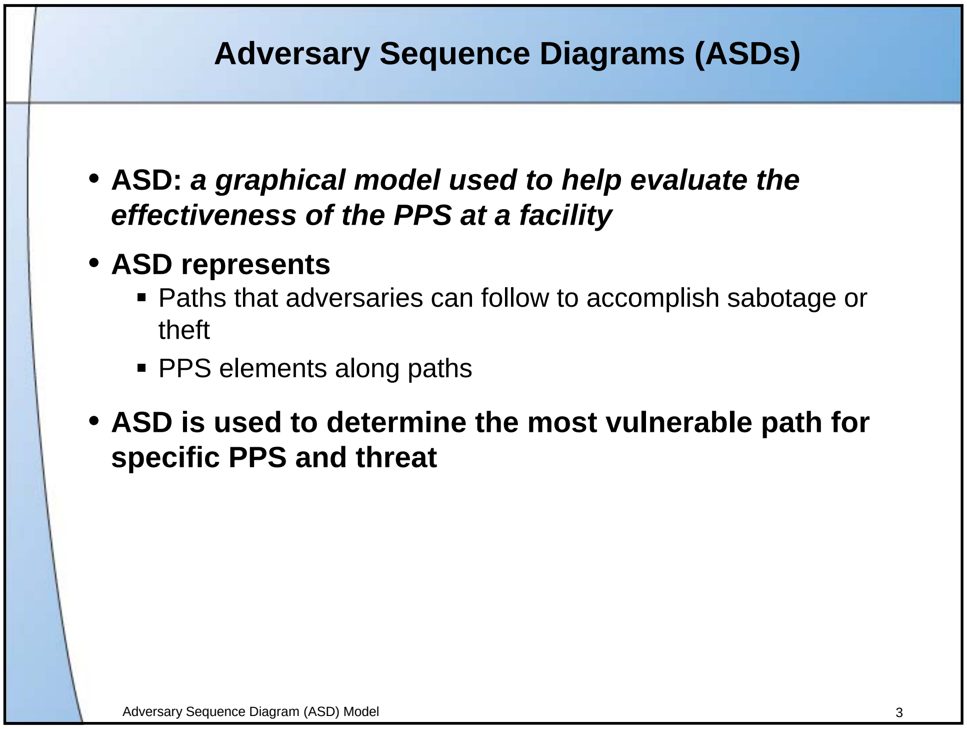
October 15 – November 2, 2007
Albuquerque, New Mexico, USA

Jose R. Rodriguez



Learning Objectives

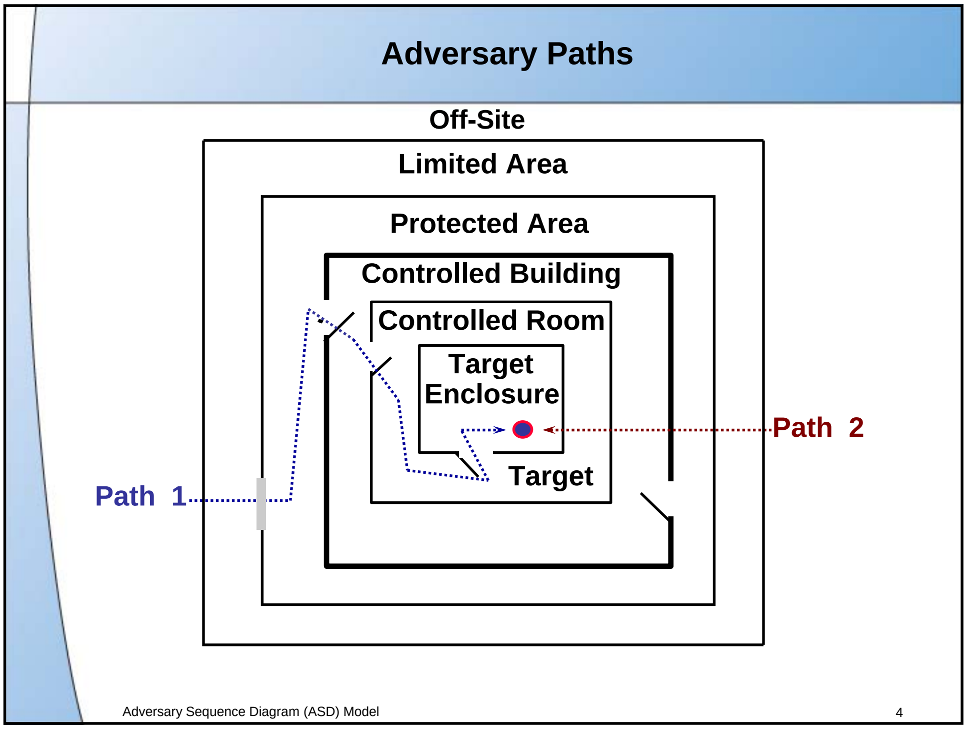
- Identify an Adversary Sequence Diagram (ASD) and describe what it represents.
- Describe why an ASD is useful in the analysis of a PPS
- Identify the parts of an ASD and diagram a facility from a simple example.
- Identify the five steps to use when creating an ASD



Adversary Sequence Diagrams (ASDs)

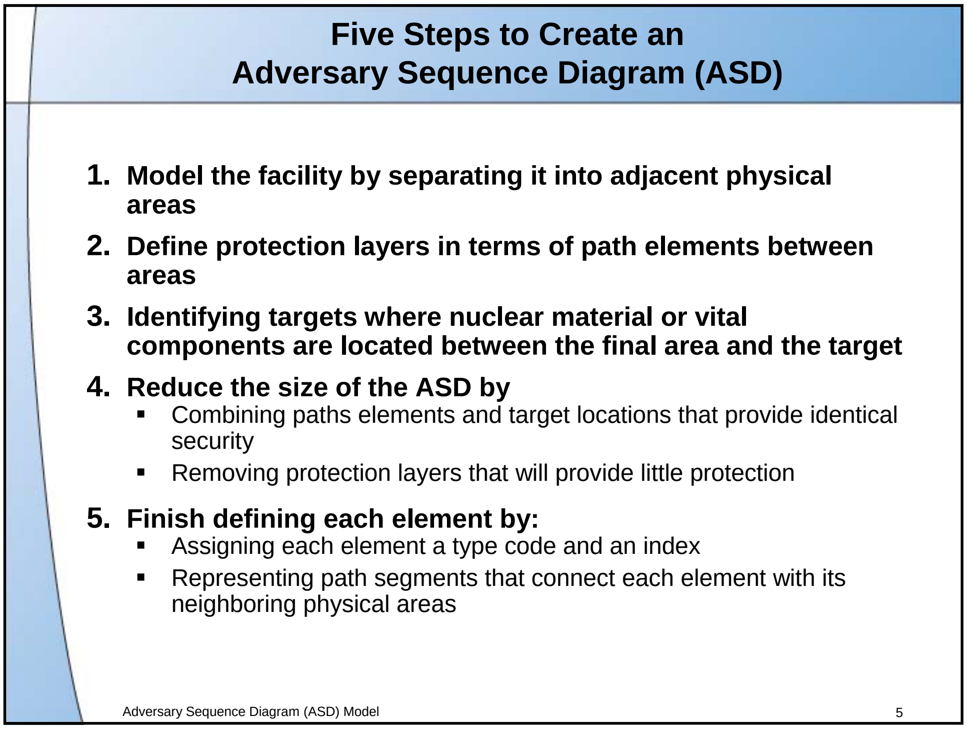
- **ASD: *a graphical model used to help evaluate the effectiveness of the PPS at a facility***
- **ASD represents**
  - Paths that adversaries can follow to accomplish sabotage or theft
  - PPS elements along paths
- **ASD is used to determine the most vulnerable path for specific PPS and threat**

Adversary Sequence Diagram (ASD) Model 3



Adversary Paths

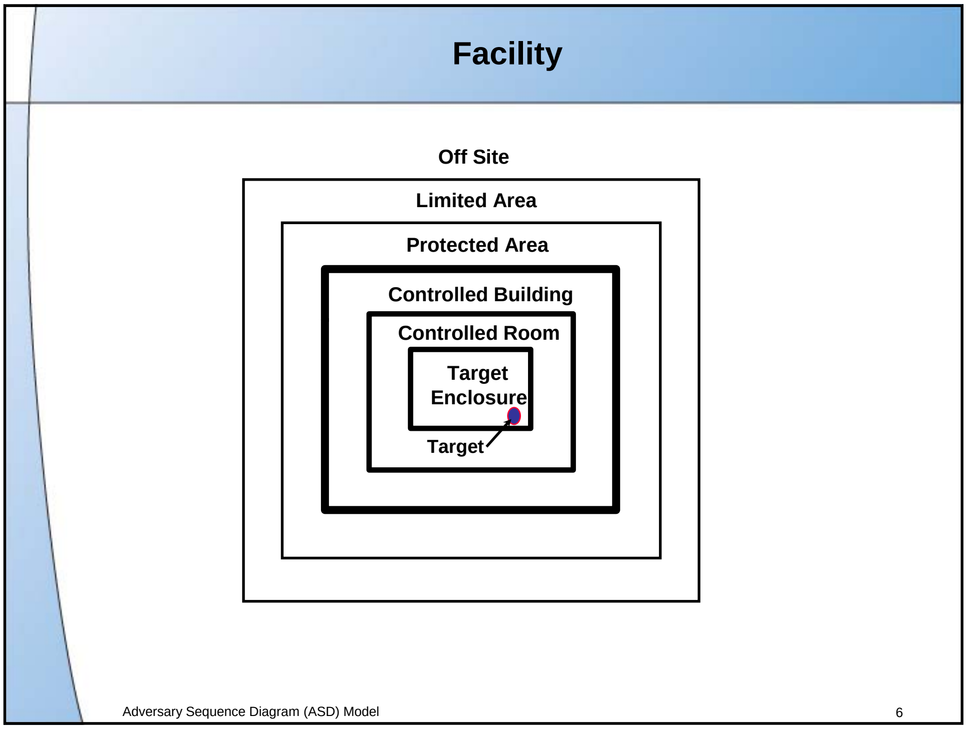
Adversary Sequence Diagram (ASD) Model 4



Five Steps to Create an Adversary Sequence Diagram (ASD)

1. **Model the facility by separating it into adjacent physical areas**
2. **Define protection layers in terms of path elements between areas**
3. **Identifying targets where nuclear material or vital components are located between the final area and the target**
4. **Reduce the size of the ASD by**
   - Combining paths elements and target locations that provide identical security
   - Removing protection layers that will provide little protection
5. **Finish defining each element by:**
   - Assigning each element a type code and an index
   - Representing path segments that connect each element with its neighboring physical areas

Adversary Sequence Diagram (ASD) Model 5



Facility

Off Site

Limited Area

Protected Area

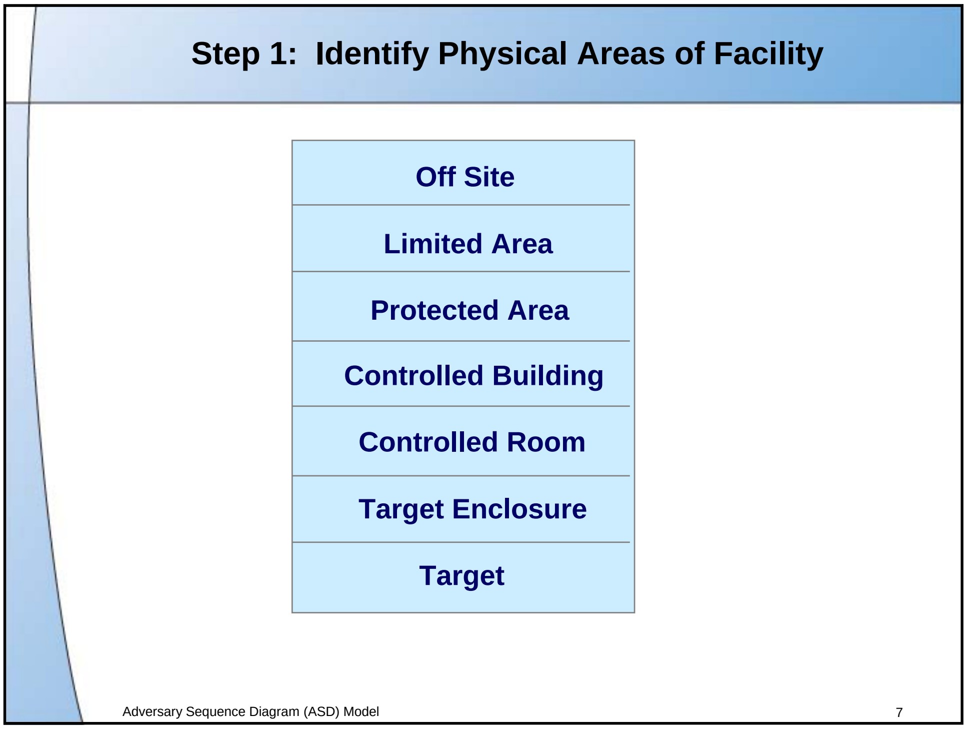
Controlled Building

Controlled Room

Target Enclosure

Target

Adversary Sequence Diagram (ASD) Model 6



Step 1: Identify Physical Areas of Facility

Off Site

Limited Area

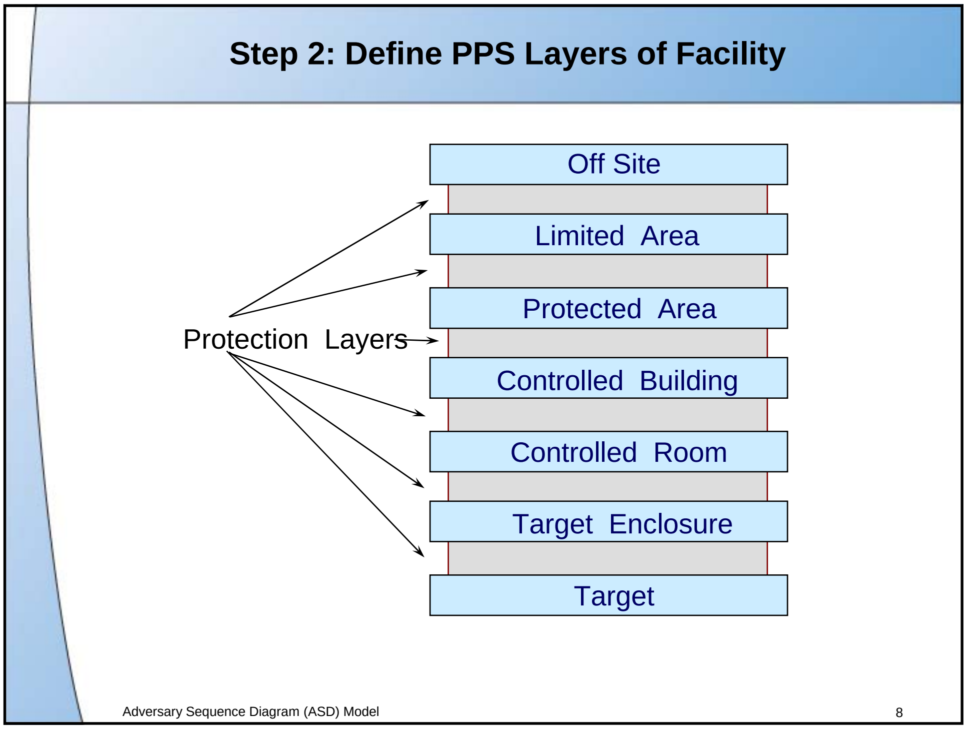
Protected Area

Controlled Building

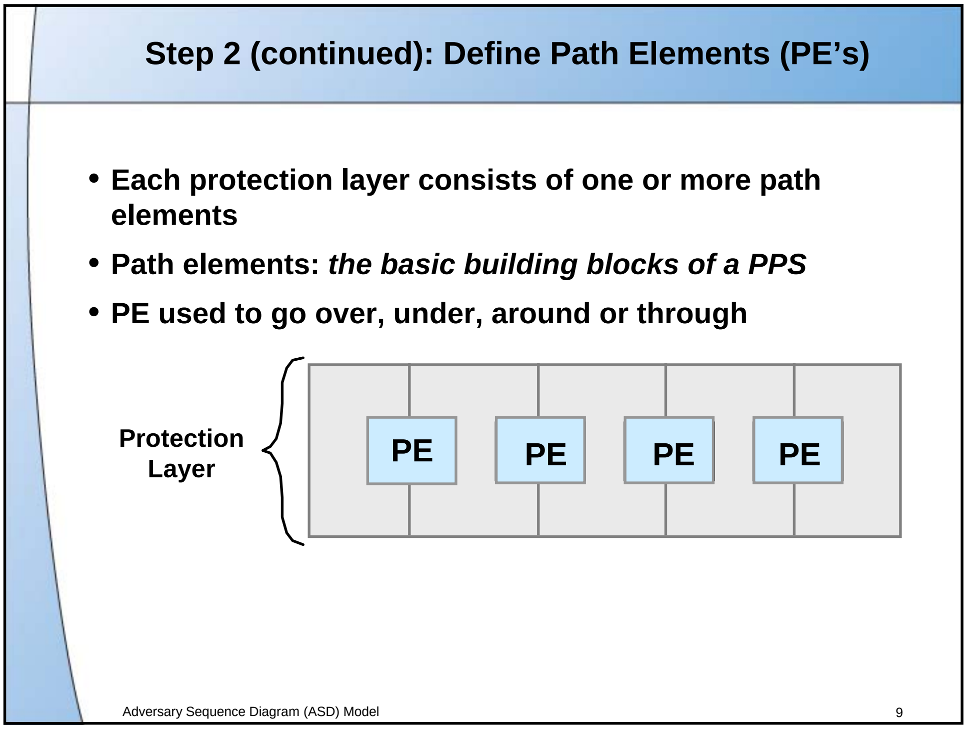
Controlled Room

Target Enclosure

Target



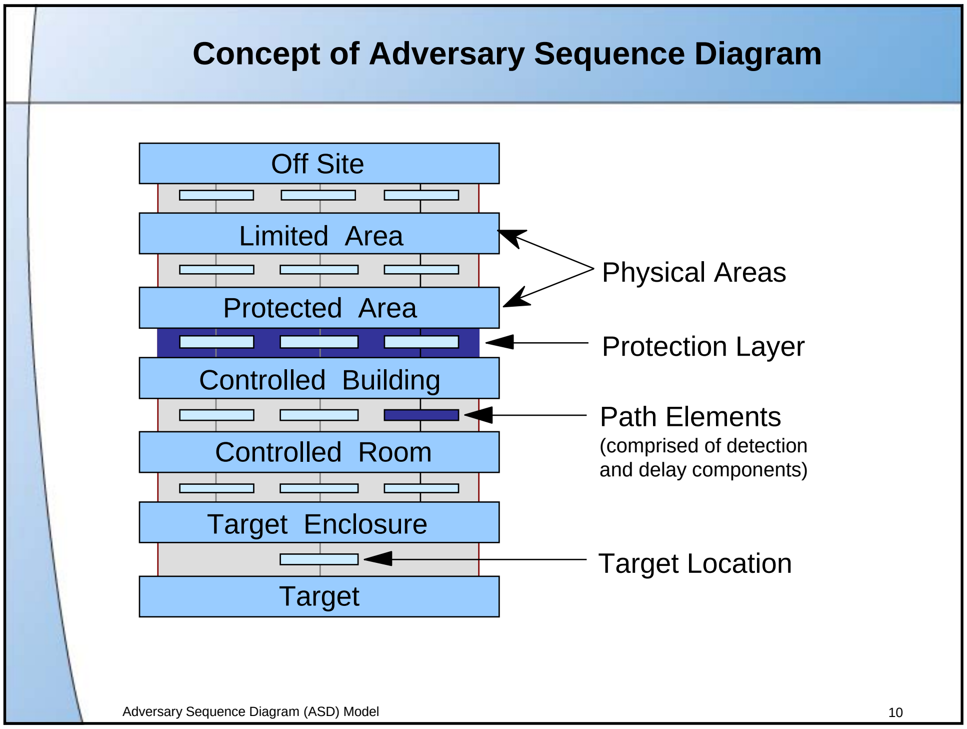
Step 2: Define PPS Layers of Facility



Step 2 (continued): Define Path Elements (PE's)

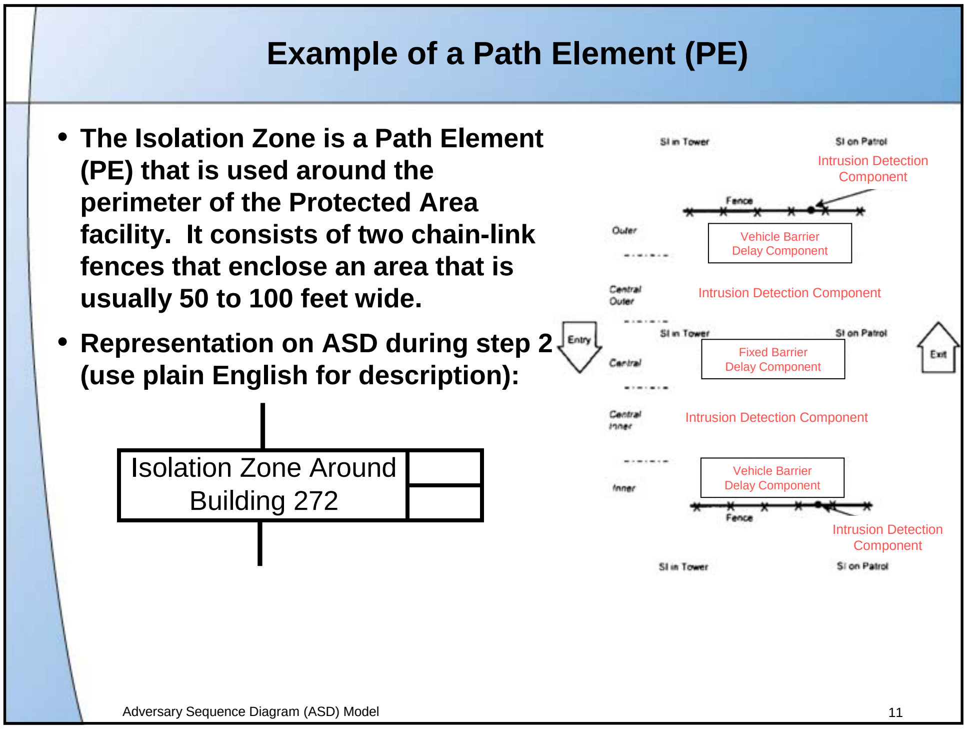
- **Each protection layer consists of one or more path elements**
- **Path elements: *the basic building blocks of a PPS***
- **PE used to go over, under, around or through**

Adversary Sequence Diagram (ASD) Model 9



Concept of Adversary Sequence Diagram

Adversary Sequence Diagram (ASD) Model 10

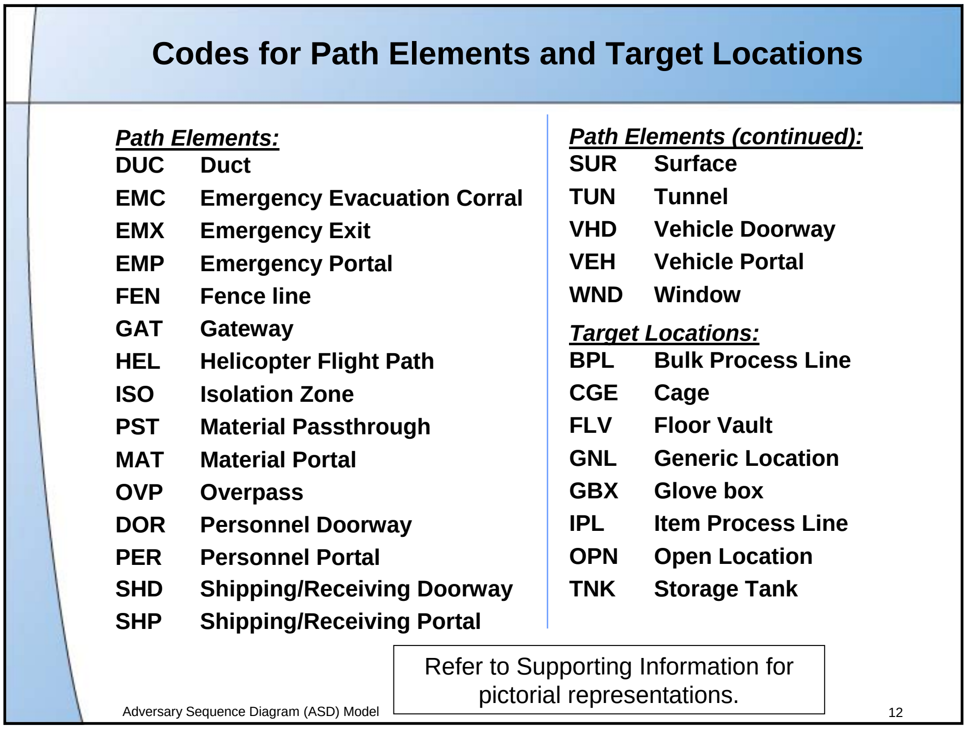


Example of a Path Element (PE)

- The Isolation Zone is a Path Element (PE) that is used around the perimeter of the Protected Area facility. It consists of two chain-link fences that enclose an area that is usually 50 to 100 feet wide.
- Representation on ASD during step 2 (use plain English for description):

Isolation Zone Around Building 272

SI in Tower
SI on Patrol
Intrusion Detection Component
Fence
Outer
Vehicle Barrier Delay Component
Central Outer
Intrusion Detection Component
Entry
SI in Tower
SI on Patrol
Central
Fixed Barrier Delay Component
Exit
Central Inner
Intrusion Detection Component
Inner
Vehicle Barrier Delay Component
Fence
Intrusion Detection Component
SI in Tower
SI on Patrol



Codes for Path Elements and Target Locations

Path Elements:

DUC	Duct
EMC	Emergency Evacuation Corral
EMX	Emergency Exit
EMP	Emergency Portal
FEN	Fence line
GAT	Gateway
HEL	Helicopter Flight Path
ISO	Isolation Zone
PST	Material Passthrough
MAT	Material Portal
OVP	Overpass
DOR	Personnel Doorway
PER	Personnel Portal
SHD	Shipping/Receiving Doorway
SHP	Shipping/Receiving Portal

Path Elements (continued):

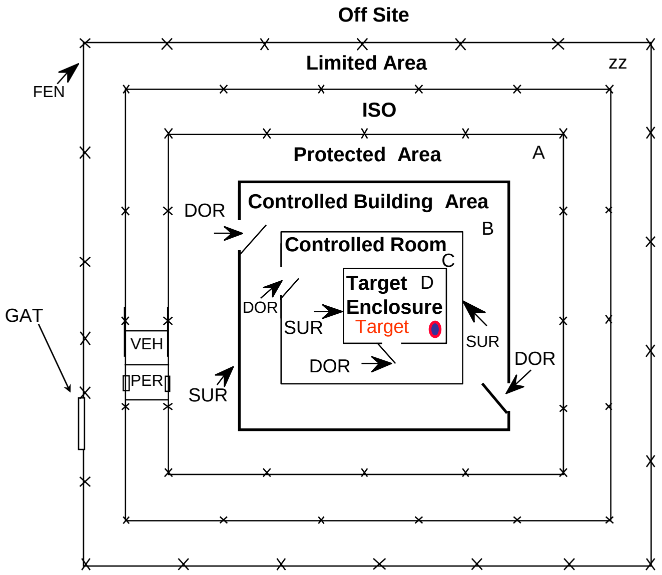
SUR	Surface
TUN	Tunnel
VHD	Vehicle Doorway
VEH	Vehicle Portal
WND	Window

Target Locations:

BPL	Bulk Process Line
CGE	Cage
FLV	Floor Vault
GNL	Generic Location
GBX	Glove box
IPL	Item Process Line
OPN	Open Location
TNK	Storage Tank

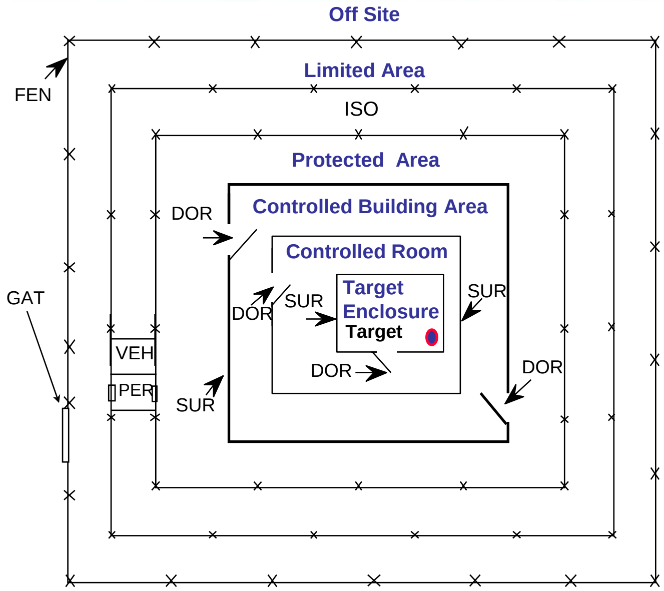
Refer to Supporting Information for pictorial representations.

Sample Facility

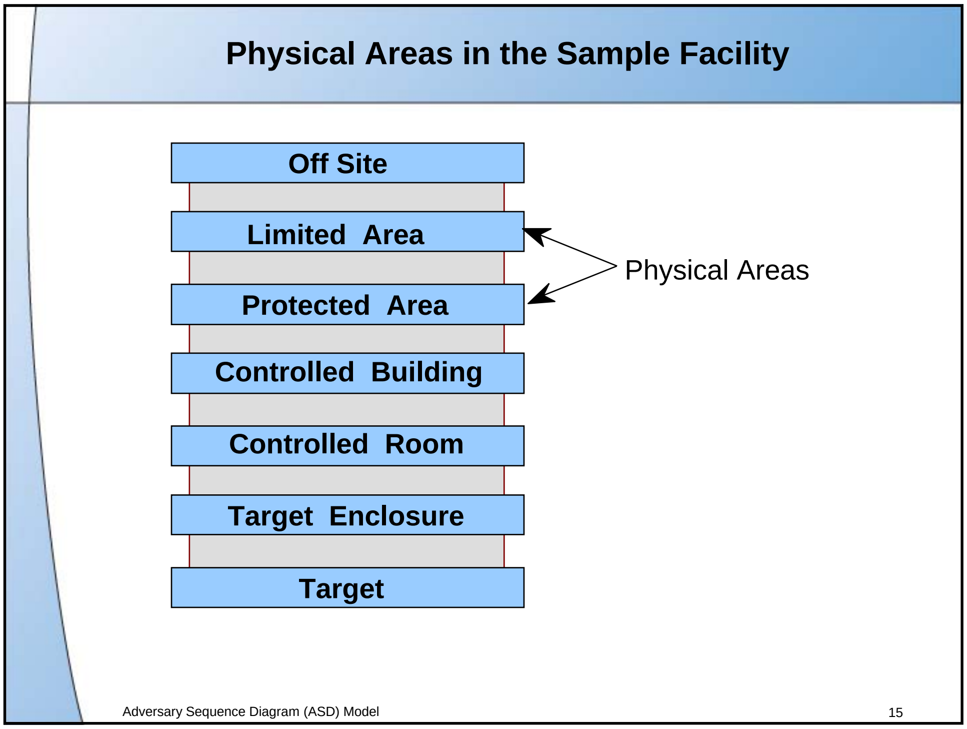


Adversary Sequence Diagram (ASD) Model 13

Sample Facility - Areas



Adversary Sequence Diagram (ASD) Model 14



Physical Areas in the Sample Facility

Off Site

Limited Area

Protected Area

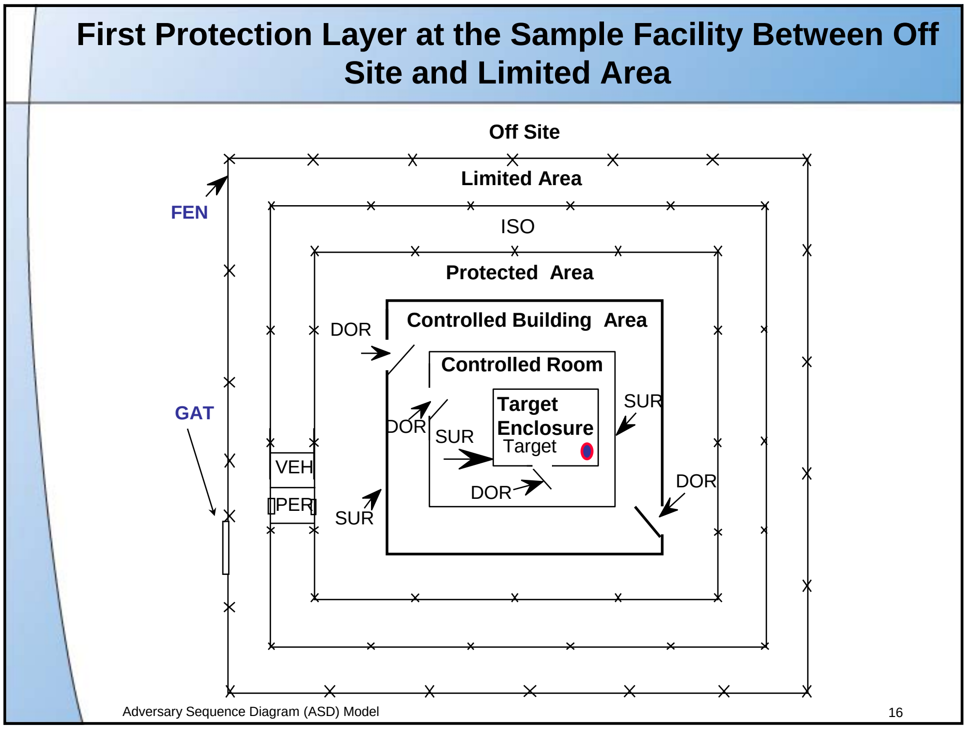
Controlled Building

Controlled Room

Target Enclosure

Target

Physical Areas



First Protection Layer at the Sample Facility Between Off Site and Limited Area

Off Site

Limited Area

FEN

ISO

Protected Area

DOR

Controlled Building Area

Controlled Room

GAT

Target Enclosure

Target

SUR

DOR

SUR

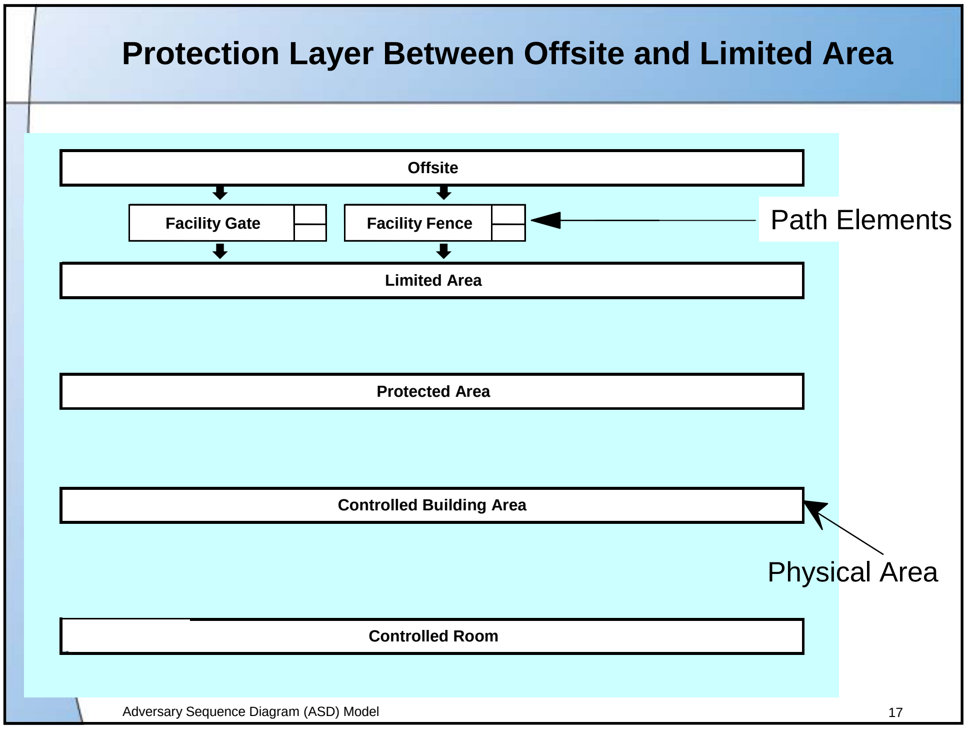
VEH

PER

DOR

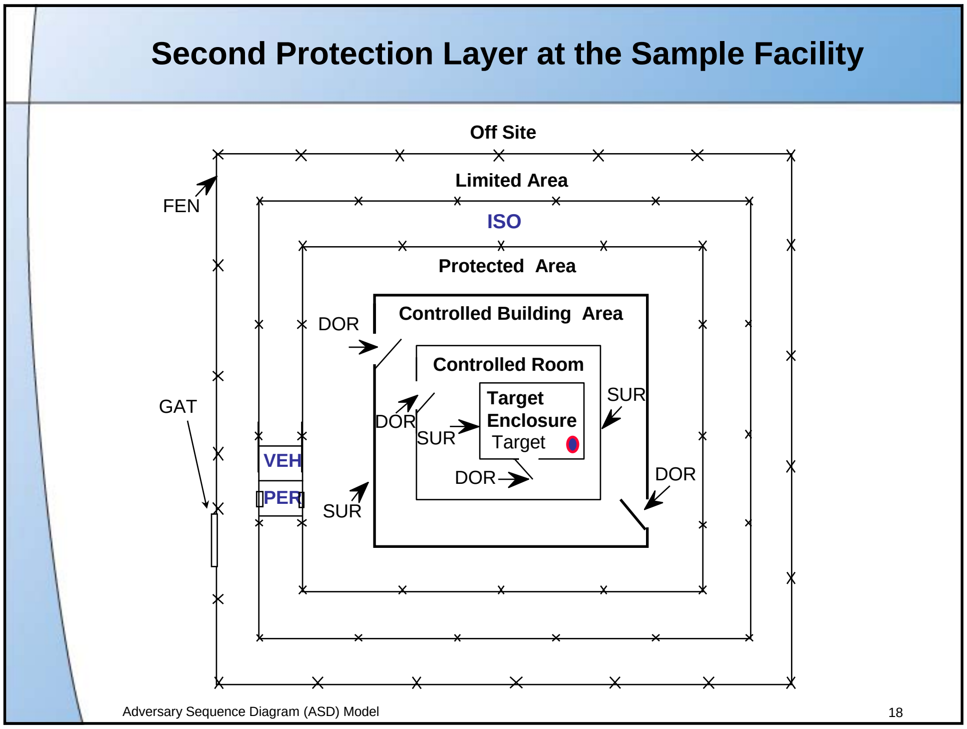
DOR

SUR



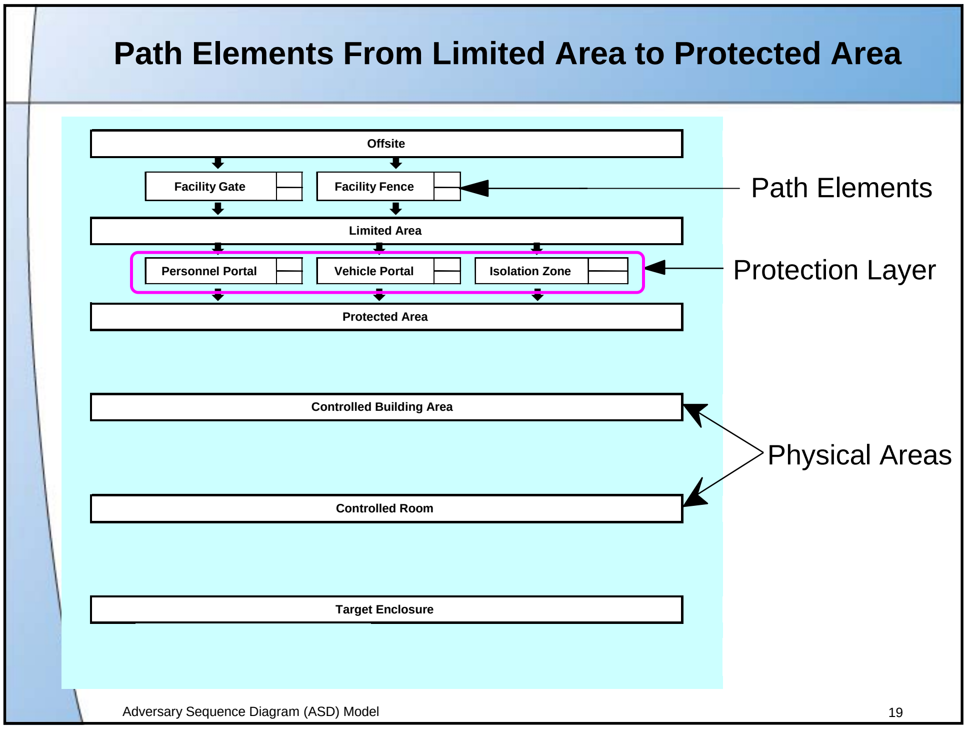
Protection Layer Between Offsite and Limited Area

Adversary Sequence Diagram (ASD) Model 17



Second Protection Layer at the Sample Facility

Adversary Sequence Diagram (ASD) Model 18



Path Elements From Limited Area to Protected Area

Offsite

Facility Gate

Facility Fence

Limited Area

Personnel Portal

Vehicle Portal

Isolation Zone

Protected Area

Controlled Building Area

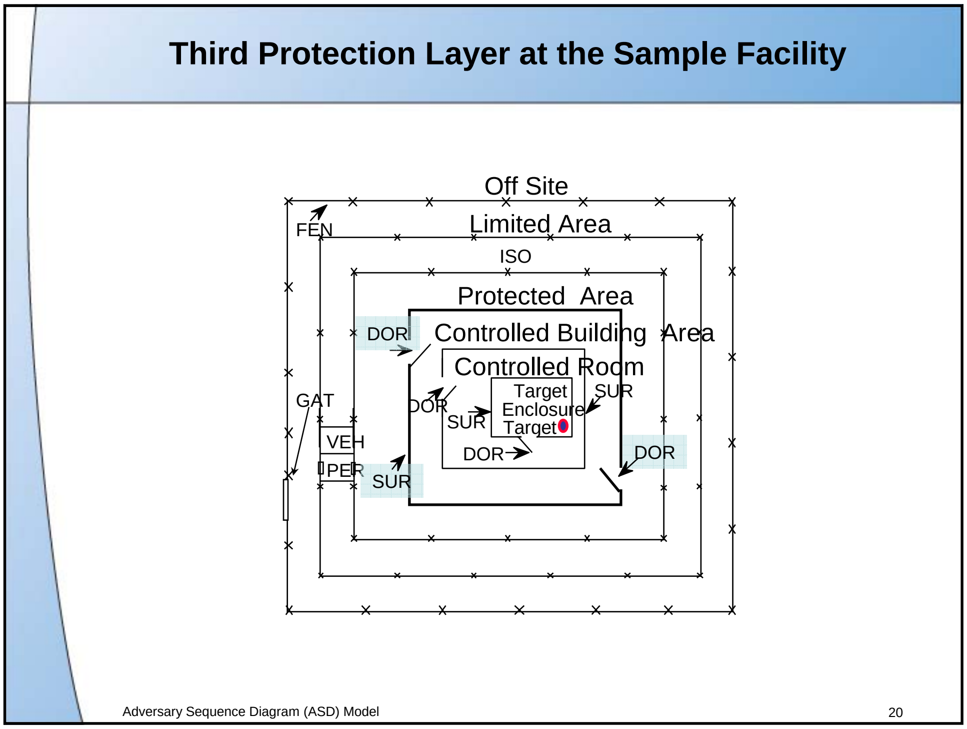
Controlled Room

Target Enclosure

Path Elements

Protection Layer

Physical Areas



Third Protection Layer at the Sample Facility

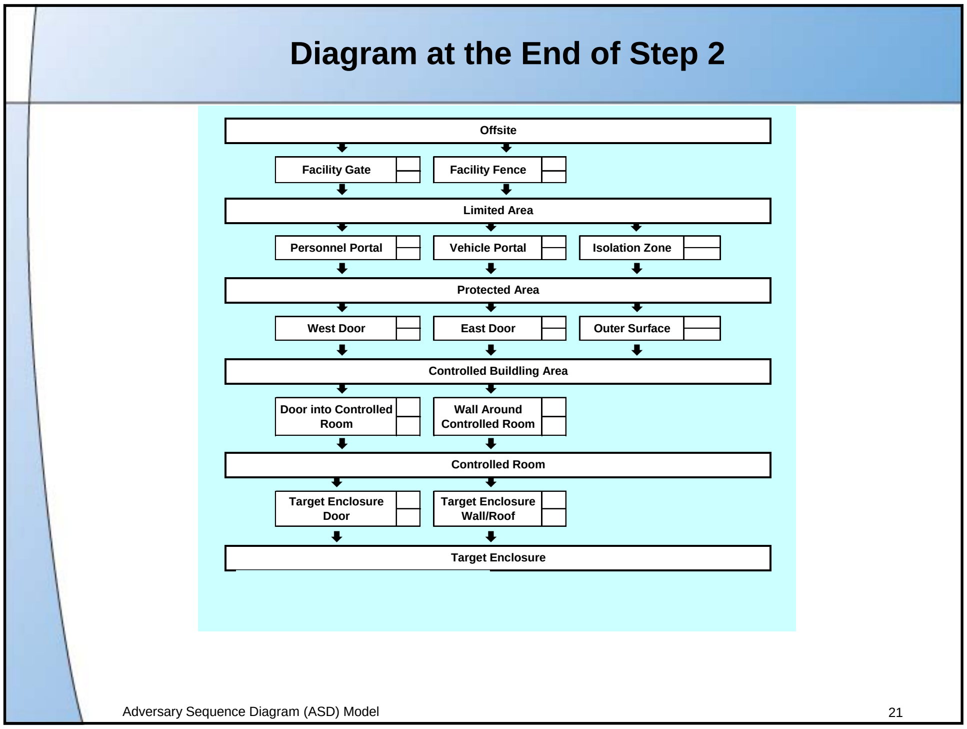


Diagram at the End of Step 2

Offsite

Facility Gate | Facility Fence

Limited Area

Personnel Portal | Vehicle Portal | Isolation Zone

Protected Area

West Door | East Door | Outer Surface

Controlled Buildling Area

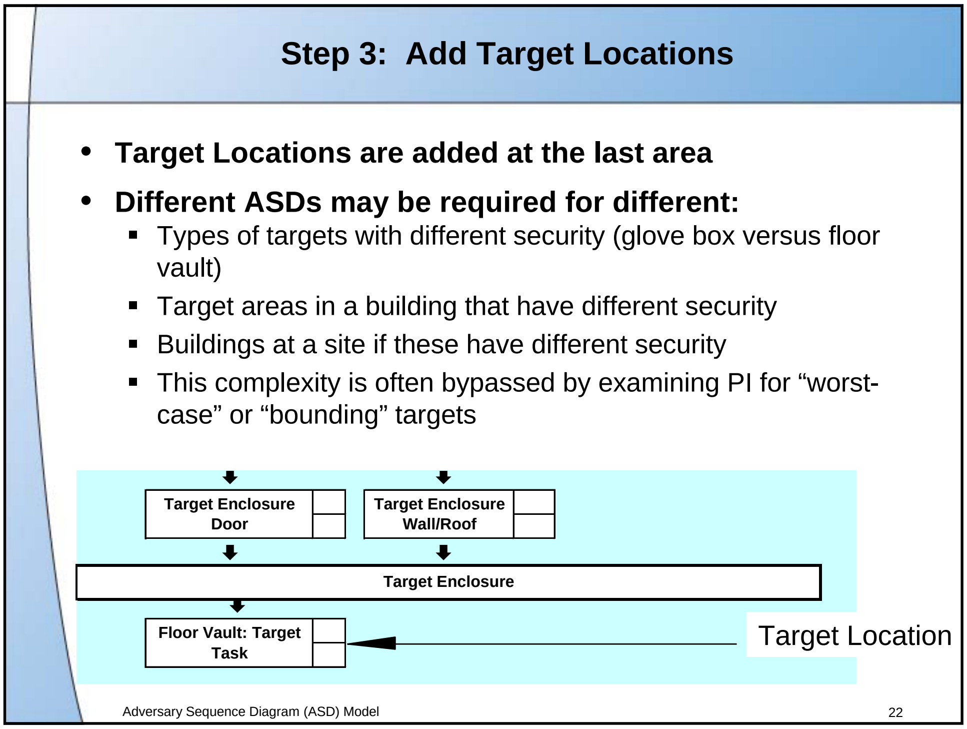
Door into Controlled Room | Wall Around Controlled Room

Controlled Room

Target Enclosure Door | Target Enclosure Wall/Roof

Target Enclosure

Adversary Sequence Diagram (ASD) Model 21



Step 3: Add Target Locations

- **Target Locations are added at the last area**
- **Different ASDs may be required for different:**
  - Types of targets with different security (glove box versus floor vault)
  - Target areas in a building that have different security
  - Buildings at a site if these have different security
  - This complexity is often bypassed by examining PI for “worst-case” or “bounding” targets

Target Enclosure Door | **Target Enclosure Wall/Roof**

Target Enclosure

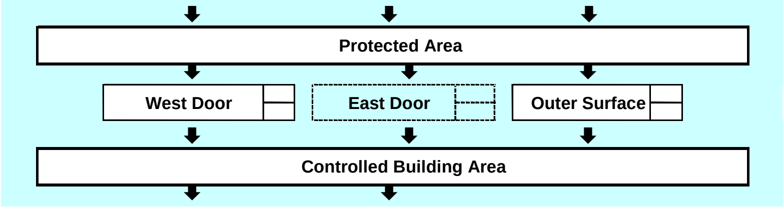
Floor Vault: Target Task

Target Location

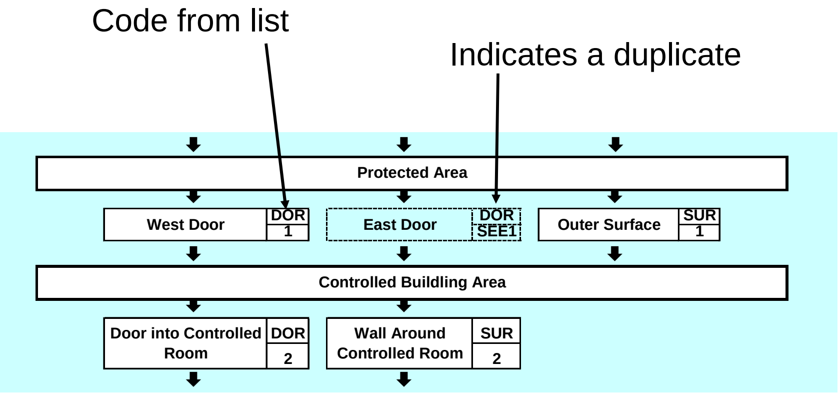
Adversary Sequence Diagram (ASD) Model 22

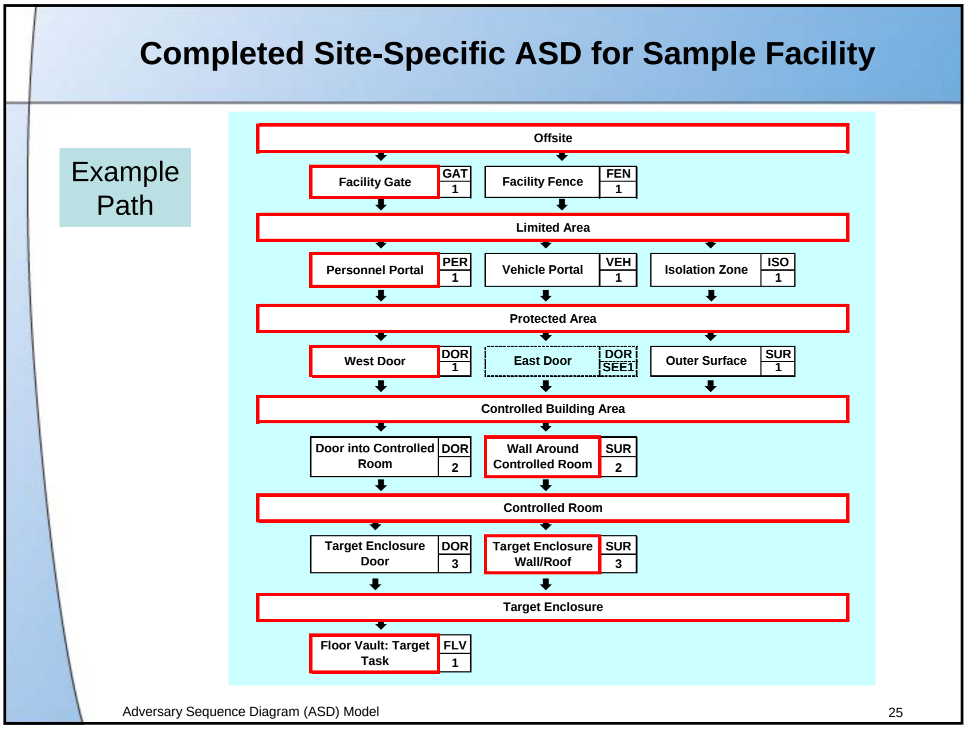
Step 4: Reduce the Size of The ASD, if Possible

- **Remove elements with identical security**
- **Remove protection layers that provide little protection**



Step 5: Finish Defining Each Element by Assigning A Three Letter Code, A Unique Index, and Segments





Completed Site-Specific ASD for Sample Facility

Example Path

Offsite

Facility Gate GAT 1 | Facility Fence FEN 1

Limited Area

Personnel Portal PER 1 | Vehicle Portal VEH 1 | Isolation Zone ISO 1

Protected Area

West Door DOR 1 | East Door DOR SEE1 | Outer Surface SUR 1

Controlled Building Area

Door into Controlled Room DOR 2 | Wall Around Controlled Room SUR 2

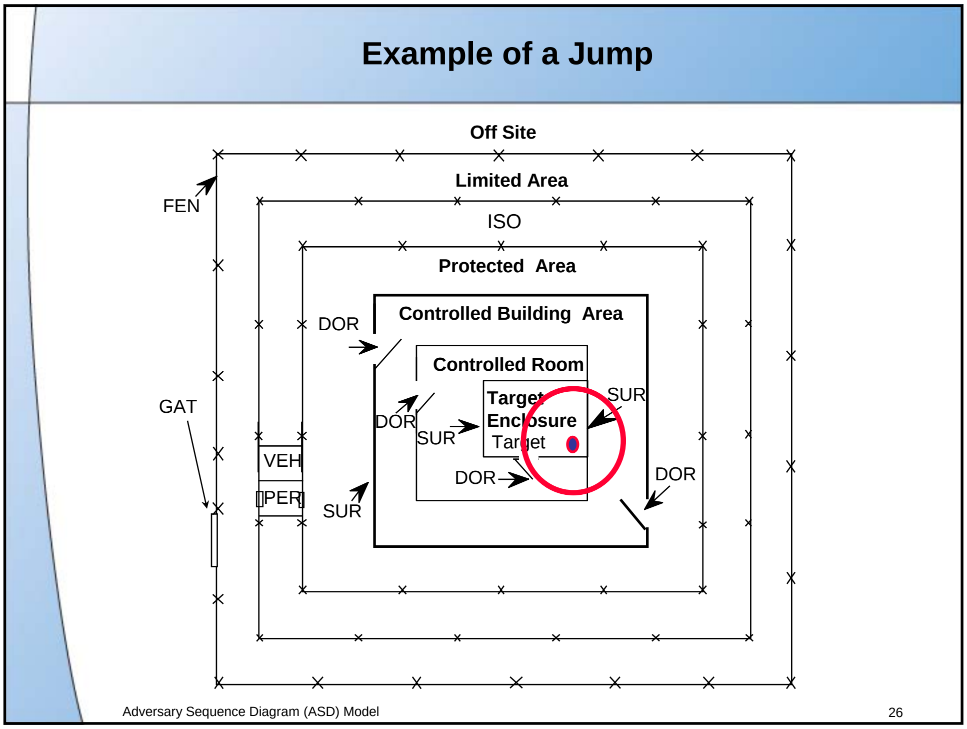
Controlled Room

Target Enclosure Door DOR 3 | Target Enclosure Wall/Roof SUR 3

Target Enclosure

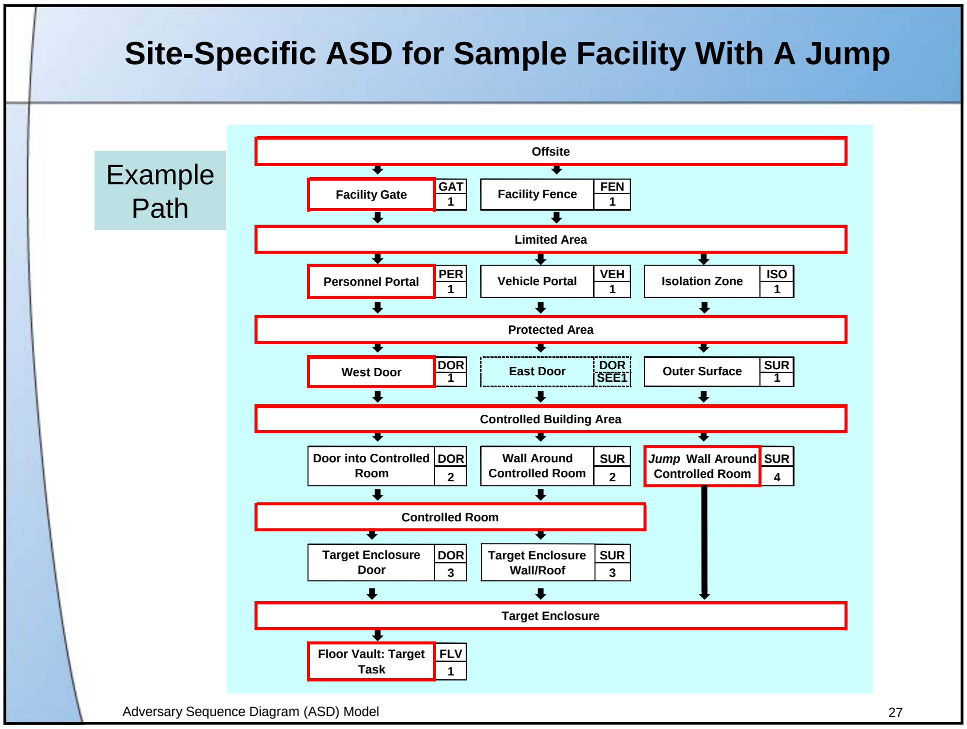
Floor Vault: Target Task FLV 1

Adversary Sequence Diagram (ASD) Model 25



Example of a Jump

Adversary Sequence Diagram (ASD) Model 26



Site-Specific ASD for Sample Facility With A Jump

Example Path

Offsite

Facility Gate GAT 1 | Facility Fence FEN 1

Limited Area

Personnel Portal PER 1 | Vehicle Portal VEH 1 | Isolation Zone ISO 1

Protected Area

West Door DOR 1 | East Door DOR SEE1 | Outer Surface SUR 1

Controlled Building Area

Door into Controlled Room DOR 2 | Wall Around Controlled Room SUR 2 | *Jump* Wall Around Controlled Room SUR 4

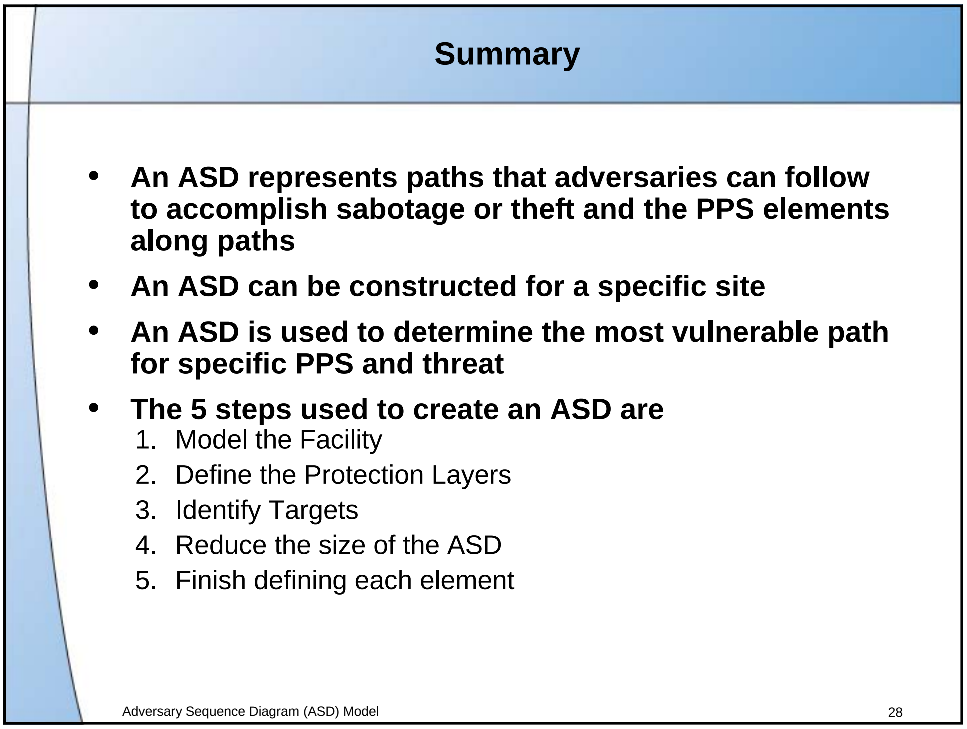
Controlled Room

Target Enclosure Door DOR 3 | Target Enclosure Wall/Roof SUR 3

Target Enclosure

Floor Vault: Target Task FLV 1

Adversary Sequence Diagram (ASD) Model 27



Summary

- **An ASD represents paths that adversaries can follow to accomplish sabotage or theft and the PPS elements along paths**
- **An ASD can be constructed for a specific site**
- **An ASD is used to determine the most vulnerable path for specific PPS and threat**
- **The 5 steps used to create an ASD are**
  1. Model the Facility
  2. Define the Protection Layers
  3. Identify Targets
  4. Reduce the size of the ASD
  5. Finish defining each element

Adversary Sequence Diagram (ASD) Model 28

Subgroup 17S
Adversary Sequence Diagram (ASD) Model

Session Objectives

After the session, the participants will be able to do the following:

1. Construct a site-specific ASD.
2. Demonstrate that the Adversary Sequence Diagram (ASD) represents credible paths that adversaries can follow to accomplish sabotage or theft and the path elements along the path

Exercise 1 - Identify Adjacent Physical Areas

The purpose of this subgroup session is to construct an ASD. Using the Exercise Data Book (Sections 6, 10, 12 through 15, Response for the PTR, Building Floor Plan, Wall Thicknesses and Distances, Exterior Physical Protection Elements, Interior Physical Protection Elements, Access Control Plan), for the Lagassi Institute for Medicine and Physics, construct an ASD for the PTR reactor, beginning with OFFSITE and ending at the TARGET. Separate the Institute into seven adjacent physical areas and name each one by filling its name into the following graphic.

It is suggested that the example answers be reviewed as each exercise is completed before proceeding with the next exercise.

1.

2.

3.

4.

5.

6.

7.

Path Elements:

DUC	-	Duct
EMC	-	Emergency Evacuation Corral
EMX	-	Emergency Exit
EMP	-	Emergency Portal
FEN	-	Fenceline
GAT	-	Gateway
HEL	-	Helicopter Flight Path
ISO	-	Isolation Zone
PST	-	Material Passthrough
MAT	-	Material Portal
OVP	-	Overpass
DOR	-	Personnel Doorway
PER	-	Personnel Portal
SHD	-	Shipping/Receiving Doorway
SHP	-	Shipping/Receiving Portal
SUR	-	Surface
TUN	-	Tunnel
VHD	-	Vehicle Doorway
VEH	-	Vehicle Portal
WND	-	Window

Target Locations:

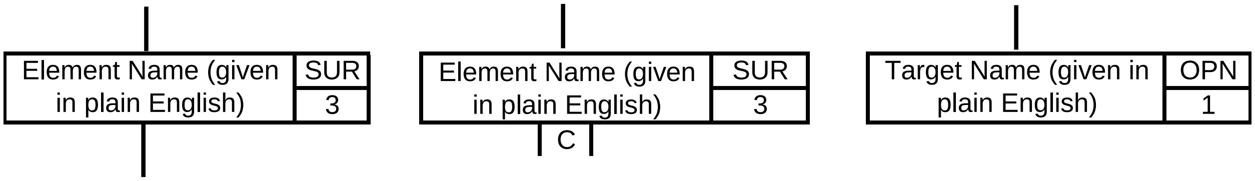
BPL	-	Bulk Process Line
CGE	-	Cage
FLV	-	Floor Vault
GNL	-	Generic Location
GBX	-	Glovebox
IPL	-	Item Process Line
OPN	-	Open Location
TNK	-	Storage Tank

Exercise 2 – Define Protection Layers, Path Elements, Target Locations, and Path Segments

The ASD represents potential adversary pathways into and out of the facility. Paths travel through path elements and target locations that make up protection layers between each concentric area. The path segments connect each element with its surrounding physical areas.

Use information about the PTR reactor (Exercise Data Book, Sections 7, 10, 12 through 15, Response for the PTR, PTR Research Reactor, Wall Thicknesses and Distances, Building Floor Plan, Exterior Physical Protection Elements, Interior Physical Protection Elements, Access Control Plan) perform the other four steps for creating an ASD.

- Defining path elements that make up the protection layers between the adjacent areas. *(Use colored marking pens to indicate protection layers on your site maps. Identify elements on each protection layer and label these with plain English names.)*
- Identifying targets where nuclear material or vital components are located. *(Indicate on map and label these with plain English names.)*
- Reduce the size of the ASD by combining paths elements and target location elements that have identical security features (and are therefore duplicates) or by removing protection layers that are expected to afford little protection. *Note: do not remove any areas but answer the question: What would be a rationale for eliminating the first layer (between the Offsite area and the Limited Area) and its path elements?*
- Assigning each path/target location element on the diagram a 3-letter type code (such as SUR or DOR) and a unique index (so it is SUR 1 or DOR 2), and adding path segments attaching that element to adjacent areas. *It may be convenient to give represent each element on a label with three parts as shown below (note the middle figure is a jump):*


Element Name (given in plain English)
SUR
3
Element Name (given in plain English)
SUR
3
C
Target Name (given in plain English)
OPN
1

During your construction, begin your ASD at the Offsite area and end at the target. The result of this exercise is an ASD for the PTR reactor. This ASD will be analyzed in Subgroup 17S, *Multipath Computer Model,* and if time permits, enter it into PANL as an exercise.

PTR ASD

1.

2.

3.

4.

5.

6.

7.

Boundary Barrier and Penetration Elements

SUR	Surface	Represents walls, floors, and roofs
WIN	Window	
DUC	Duct	Represents Penetrations above Grade
TUN	Tunnel	Represents Penetrations below Grade

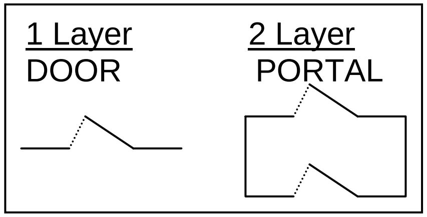
Miscellaneous Elements

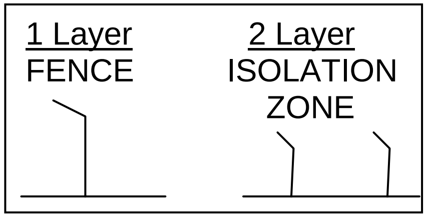
HEL	Helicopter Flight Path	Represents Transit Delay onto Site and Delays Unloading Personnel

Single Layer/Double Layer Elements

This category includes element types that occur in pairs:

- One of the pair represents a single-layer barrier;
- The other includes 2 copies of the same barrier (hence double-layer barriers)





Single Layer Elements		Double Layer Elements		Comments
FEN	Fenceline	ISO	Isolation Zone	Surrounds exterior area eg: Protected Area
		OVP	Overpass	Like Isolation Zone but over Buildings
GAT	Gateway			For Human and Vehicle Movement
DOR	Personnel Doorway	PER	Personnel Portal	For Human Movement
MAP	Material Passthrough	MAT	Material Portal	For Material Movement Only
VHD	Vehicle Doorway	VEH	Vehicle Portal	For Vehicle Movement
SHD	Shipping/Receiving Doorway	SHP	Shipping/ Receiving Portal	For Vehicle Movement-restricted to building boundaries – ex: S/R docks
EMX	Emergency Exit	EMP	Emergency Portal	
		EMC	Emergency Evacuation Corral	

Application Considerations

1. Can an ASD be constructed for any facility?
   a) always
   b) sometimes
   c) maybe
   d) seldom

2. An ASD represents:
   a) every possible path in and out of a facility
   b) every credible path in and out of a facility
   c) most of the credible paths in and out of a facility
   d) none of the credible paths in and out of a facility

3. ASDs can be used to determine:
   a) minimum detection pathways
   b) detection balance between areas
   c) detection protection in depth
   d) all of the above
   e) none of the above

4. ASDs can be used to determine:
   a) shortest delay pathways
   b) delay balance between areas
   c) delay protection in depth
   d) all of the above
   e) none of the above

5. An ASD is:
   a) an analysis tool
   b) a design tool
   c) a single solution for PPS defects
   d) both a and b
   e) none of the above

6. An ASD
   a) must always be developed on a computer
   b) must sometimes be developed on a computer
   c) can never be developed on a computer
   d) can always be developed by hand (on paper)
   e) can never be developed by hand (on paper)

7. An ASD is:
   a) only as good as the analyst who created it
   b) only as good as the computer it runs on
   c) independent of the analyst
   d) independent of the computer

8. An ASD
   a) always predicts the most vulnerable path
   b) may predict the most vulnerable path
   c) never predicts the most vulnerable path
   d) may predict a non-credible most vulnerable path

18. Single Path Computer Tool

Abstract. *This session begins describing the principles behind path analysis. It describes how models of Physical Protection System (PPS) performance may be based on the interrelation of three system functions: detect, delay, and response. A path is defined as an ordered series of actions against a target, which, if completed, results in successful theft or sabotage. The timing relationships between security functions and the adversary attack are then described on a timing diagram. The principle of timely detection is discussed next, along with its performance measure, Probability of Interruption or P_I. Finally, the purpose of path analysis is then explained, namely to determine what the minimum P_I is across all targets, threats, and facility operating conditions to determine if time after detection is sufficient to respond and interrupt the attack before the adversary completes his task timeline. The session then describes the Very Simplified Estimate of Adversary Sequence Interruption (VEASI) model. It uses detection, delay, and response time values to compute the P_I. VEASI is a simple-to-use calculational tool that quantitatively illustrates how P_I is affected when physical protection parameters are changed along a single, specific path. Even so, VEASI is able to perform sensitivity analyses and analysis of physical protection system interactions and time trade-offs along that path. The input for the model requires (1) detection inputs as probabilities that the total detection function will be successful, (2) delay inputs as mean times for each element, and (3) where detection occurs with respect to the delay, as well as (4) a value for Response Force Time from the security response plans. The output is the probability of interruption, or the probability of intercepting the adversary before any theft or sabotage occurs. After obtaining the output, any part of the input data can be changed to determine the effect on the output. However, since VEASI is a single path-level model, it may be necessary to use another model to observe all possible paths to determine which are the most vulnerable.*

18.1 Introduction

Discussion of basic aspects of path analysis

This section of the course discusses the following basic features of the path analysis approach to the design of physical protection systems (PPS):

- Basic security functions of detection, delay, and response
- Concept of the adversary path
- Timing relationship between the intruder and the PPS
- Measures of security effectiveness for paths
- The purpose of path analysis

Later, the VEASI code is discussed

After this introduction, the session discusses a single path computer code called Very Simplified Estimate of Adversary Sequence Interruption (VEASI) that can be used for P_I calculations.

18.2 Basic Physical Protection System Model

PPS System Functions

The module titled Design of Physical Protection Systems presented the development of a basic PPS model, which is based on the defense-in-depth concept. Three system functions were identified:

- **Detect.** An intelligence function that must sense the presence of an intrusion into a protected area (to include discrimination from authorized presences), assess the nature of the intrusion, and communicate such information to the response function (and to the delay function, especially when active elements are used).
- **Delay.** A barrier-like function that must be overcome by adversaries before intrusion mission (theft or sabotage) can be completed.
- **Response.** An offensive force function responsible for interrupting and neutralizing intruders before they can complete their mission.

Decompose Detect Function

From a design perspective, it would be ideal to relate these three functions together in a mathematical relationship. A problem occurs, however, in defining appropriate, compatible metrics. As mentioned previously, delay and response are generally discussed in terms of function time, and so are easily related. But how is detect characterized? Usually, when discussing sensors, it is possible to talk about detection probabilities. But what, for example, about the assessment and communications sub-functions? How can detection be related to the delay and response functions? One way to approach this issue is through decompositions, by describing the detect function in more detail through decomposition. This is illustrated in Figure 18-1, along with partial decomposition of response. (Note that it is possible to decompose the delay and response functions further, if required.[1])

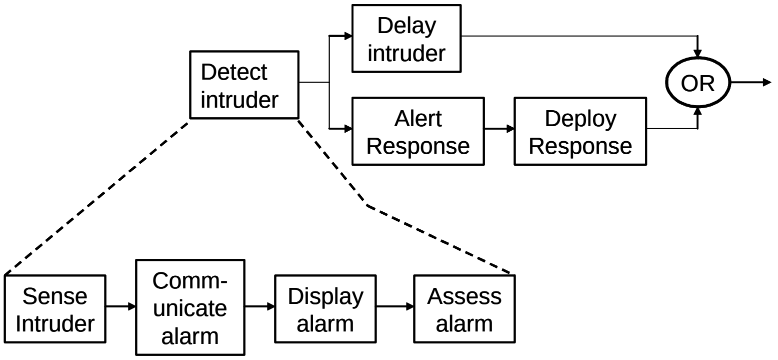


Figure 18-1. PPS Functional Flow Block Diagram Showing Decomposed Detect Function

[1] For example, the response function includes sub-functions such as muster, preparation, travel, deployment, and communications. If active delay elements are used, the delay function would include command, control and communications sub-functions.

Describe Detection Subfunctions

This view suggests that it is possible to describe many of the detect sub-functions in terms of time as well—this fact is used below. Alternatively, it is equally valid to talk about function or sub-function success probabilities. For example, in addition to the probability that the detector will sense the intruder (P_S), other system effectiveness measures might be the probability of accurate communication (of alarm, P_T, or to response P_C), the probability of accurate assessment (P_A), or even the probability of deployment by response forces to the adversary location. Such probabilities can also be combined based on the basic laws of probability (e.g., probability of detection $P_D = P_S * P_T * P_A$ and the probability of response force notification of an alarm $P_R = P_D * P_C$).

As seen in Figure 18-1, recognizing the temporal behavior inherent in the delay function allows for the possibility of taking credit for additional delay features that may exist in the system. However, note that this delay is conditional on completing the detect function. Just because a sensor activates does not necessarily mean that the system can take credit—from a performance standpoint—for the delay an intruder is experiencing; only upon successful assessment and activation of the response function does it count. Another important implication is that this conditional delay sub-function can only be fulfilled by in-place, pre-deployed delay features; active delay elements require command and control support which can only take place after completing the delay function, as represented by the link between the detect and delay functions in Figure 18-1.

18.3 Adversary Path

Adversary Path

To evaluate how well these functions are performed in path analysis, we need some way to describe adversary actions against the PPS. The concept used is that of the adversary path.

An adversary path is an ordered series of actions, called element strategies, against a target, which, if completed, result in successful theft or sabotage. Figure 18-2 illustrates a single sabotage path of an adversary who wishes to destroy a pump in a high security area. The element strategies, such as "Penetrate Outer Door" or "Destroy Pump" are short descriptions of how each path element are defeated by the adversary. Each element consists of a number of detection and delay components. For example, the door element provides delay because it has hardness and provides detection due to the noise of it being attacked. Figure 18-3 describes one set of element strategies for this path.

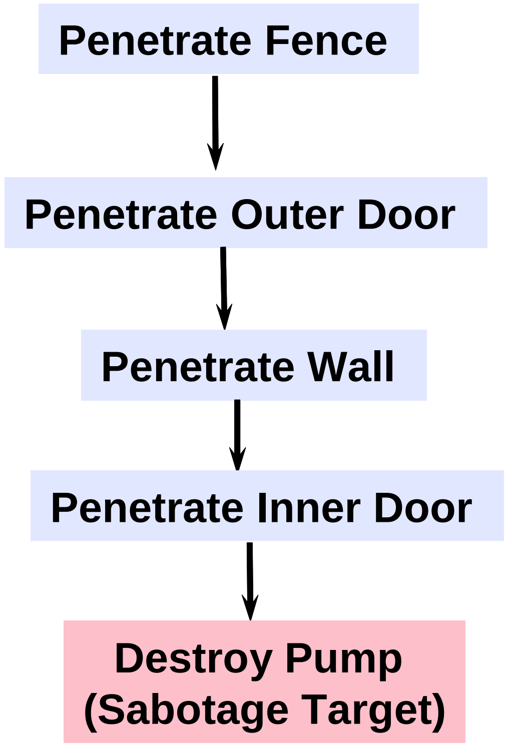


Figure 18-2. An Adversary Path

Element Strategy	Delay Component	Detection Component
Penetrate Fence	Fence Fabric	Fence Sensor
Penetrate Outer Door	Door Hardness	Sensors on Door
Penetrate Wall	Wall Hardness	Personnel Hear Noise
Penetrate Inner Door	Door Hardness	Sensors on Door
Destroy Pump	Time Required to Sabotage Target	Loss of Pump

Figure 18-3. Delay and Detection Components along the Path

Knowing the sequence of actions the adversary is trying to perform, we can overlay the timeline of PPS functions alongside the entire adversary timeline on the same timing diagram (see Figure 18-4 below) to see whether response can interrupt the adversary before they complete their task.

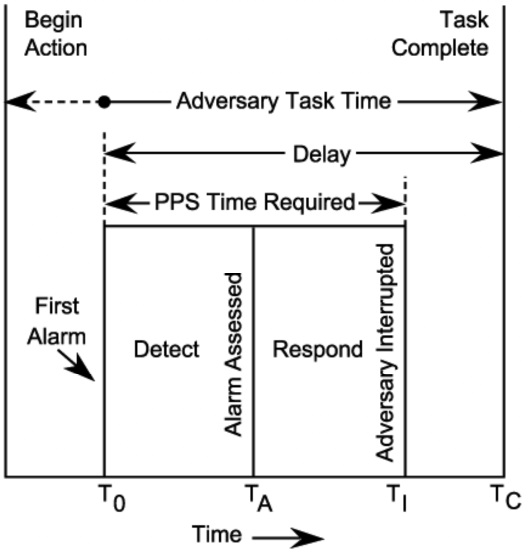


Figure 18-3. PPS Timing Diagram

PPS Timing Diagram Explanation	To help explain the diagram, the following descriptions are provided: • *First Alarm* is the first alarm that results in a correct assessment of the intrusion and communication to the response force – T_0 is the time of first alarm • *Detect* is the time required to complete the detect function (see Figure 18-2) – T_A is the time the detect function is successfully completed • *Respond* is the time required to complete the response function – T_I is the time required for the response force to muster, prepare, travel, and deploy a sufficient number of response personnel to interrupt the adversary from completing his task • *PPS Time Required* is the sum of the *Detect* and *Respond* times • *Delay* is the sum of the intruder delay times associated with the ‘mayhap delay intruder’ sub-function and ‘delay intruder’ function (see Figure 18-2) • *Adversary Task Time* is the total amount of time required for an adversary to complete his tasks (theft or sabotage) • *Begin Action* is the point in time when an adversary actually begins his

task by intruding into a controlled (e.g., alarmed) area

- *Task Complete* and T_C is that point in time when an adversary's task will be completed

Cumulative Path Delay Deficiency

The differences between PPS Time Required and delay are sometimes referred to as the cumulative path delay deficiency (for delay < PPS Time Required) or the time remaining after interruption (or TRI for delay > PPS Time Required).

Clearly, in order for the PPS to accomplish its objective, T_I must occur before T_C. It is equally clear that detection (First Alarm) should occur as early as possible and T_0 (as well as T_A and T_I) should be as far to the left on the time axis as possible.

18.4 Measures of Security Effectiveness for Paths

Security Effectiveness measures for Paths

This section discusses and compares three measures of effectiveness that address how well security performs along an adversary path:

- Minimum Delay
- Minimum Cumulative Probability of Detection
- Minimum Timely Detection/Probability of Interruption

18.4.1 Delay Model

Compare Minimum Cumulative Time Delay to PPS Time Required

One measure of PPS effectiveness is the comparison of the minimum cumulative time delay along an adversary path (T_{min}) compared to the PPS Time Required[2] (T_{RFT}) as defined in Figure 18-3. This is illustrated in Figure 18-4 below, where the length of each bar is intended to illustrate the length of time associated with a particular adversary task time t_{ai} .

[2] *PPS Time Required* is also referred to as *Response Force Time*. However, it must be recognized that such use includes all of the time-based **detect** sub-functions as well as the time associated with the response function.

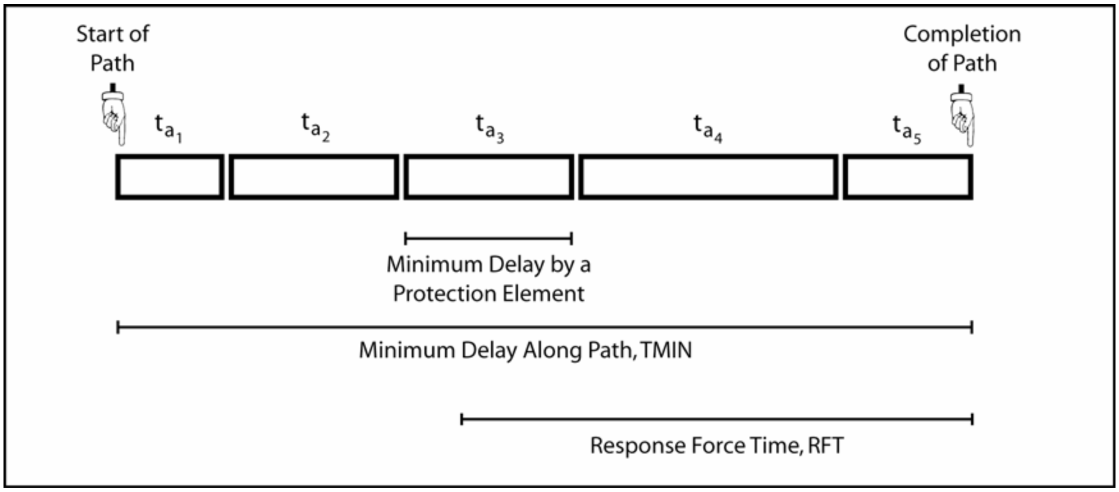


Figure 18.4. Minimum Path Delay as a measure of PPS effectiveness

Calculate Total Delay Time

In terms of PPS elements, total minimum delay time, T_{min}, for some set of elements is calculated as a sum of the element delays. So we have:

$$T_{\min} = \sum_{i=1}^{m} t_{ai}$$

where m is the total number of delay elements along the path of concern and t_{ai} is the time delay[3] provided by i^{th} element. And, for an effective PPS, the following condition must hold true (where T_{RFT} is the response force time):

$$T_{RFT} < T_{\min}$$

The disadvantage of this measure is that no consideration of detection is involved. As has been shown, delay without prior detection is not meaningful (except possibly as a deterrent, an effect which we are not modeling) because the response force must be alerted in order to deploy and interrupt the adversary. However, unless T_{min} is greater than $T_{RFT,}$ the PPS has no chance of success.

18.4.2 Detection Model

Detection System Performance

Another measure of effectiveness is the cumulative probability of detecting the adversary before their mission is completed. An effective protection system must provide a high probability of detection. To assess detection system performance, then, we must turn to some basic probability theory.

First some definitions:

- Two events are *independent* if the occurrence or nonoccurrence of one event in no way affects the probability of occurrence of the other.

[3] Use of the minimum delay here will provide a conservative approach. As noted earlier, it would also be possible to use other measures, such as a median or average delay value.

- Two events are *mutually exclusive* if the occurrence of one precludes the occurrence of the other.

  – The symbol $\cup$ indicates the union (and/or) of two sets, the symbol $\cap$ indicates the intersection (and) of two sets, and the letter P or function notation P() is used to indicate probability.

A useful basic statistical relationship governing independent but *non*-mutually exclusive events, E_n, states that:

$$P\left(E_1 \cup E_2 \cup \ldots \cup E_n\right) = 1 - \left(1 - P\left(E_1\right)\right)\left(1 - P\left(E_2\right)\right)\ldots\left(1 - P\left(E_n\right)\right)$$

In terms of PPS elements, this law applies to the minimum cumulative detection probability, $P_{\min}$, for some set of sensors as:

$$P_{\min} = 1 - \prod_{i=1}^{m} \overline{P_i}$$

where m is the total number of detection elements along the path of concern and $\overline{P_i}$ is the non-detection probability[4] (which is one minus the detection probability) provided by i^{th} element. And, for an effective PPS, the following condition must hold true:

$$P_{\min} \geq P_{acceptable}$$

Acceptable Probability of Detection

The acceptable probability of detection value, $P_{\text{acceptable}}$, must be established as part of the system requirements. The disadvantage of this measure is that no consideration of delay is involved. Detection without sufficient subsequent delay is not meaningful; the response force may have insufficient time to interrupt the adversary.

18.4.3 Critical Detection Point Models

Integrate Detection Probability with System Timing

Neither minimum path delay nor minimum probability of detection provides a complete model of system behavior along some adversary path. As noted earlier, some means must be provided to integrate sensor behavior with system timing considerations. Such a measure of effectiveness would take into account and combine measures like $T_{\min}$, T_{RFT}, and $P_{\min}$, and will be referred to as timely detection. The basic concept is that the adversary will be detected while there is enough time remaining for the response force to deploy and prevent the adversary from completing their theft or sabotage task, as illustrated in Figure 18-7.

[4] Use of the minimum detection probability here will provide a conservative approach. It would also be possible to use other measures, such as a median or average non-detection probability.

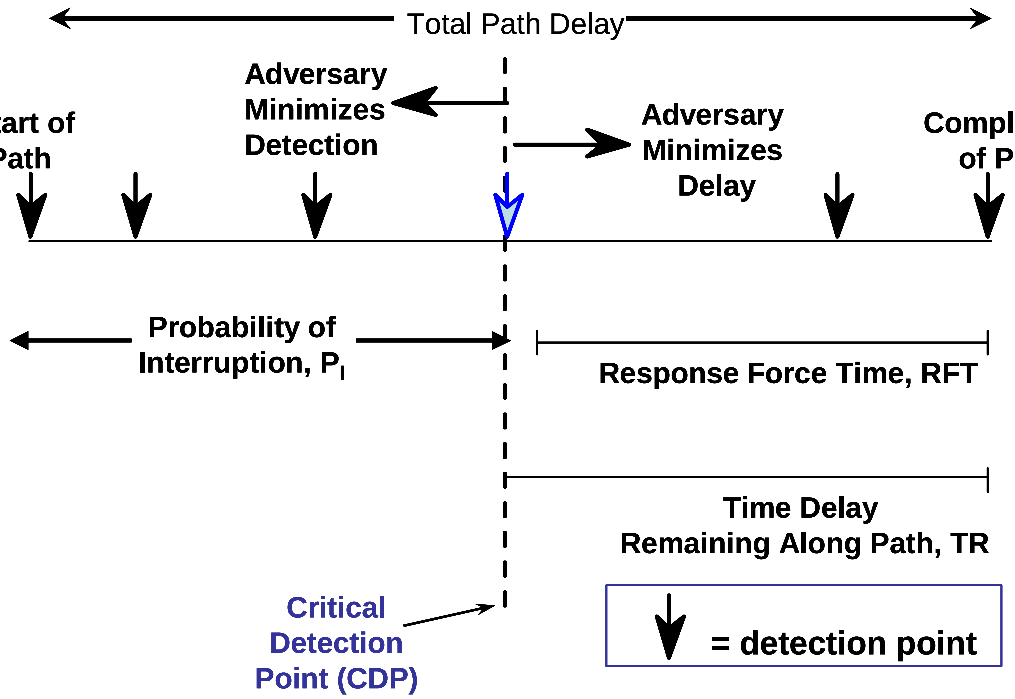

Total Path Delay
Adversary Minimizes Detection
Adversary Minimizes Delay
Start of Path
Completion of Path
Probability of Interruption, P$_I$
Response Force Time, RFT
Time Delay Remaining Along Path, TR
Critical Detection Point (CDP)
= detection point

Figure 18-5. ***Timely Detection*** **as a measure of PPS effectiveness**

Determine Response Force Time

The path analysis for this system approach proceeds by first determining the response force time, T$_{RFT}$ (but see earlier caution in Delay Model section). Then, working outward from the protected asset, the minimum delays associated with each protection element encountered along the path are summed (and thus represent the minimum delay remaining along a path at any point, represented as T$_R$) until T$_{RFT}$ is just exceeded. This is represented mathematically as:

$$T_R > T_{RFT}$$

and:

$$T_R = \sum_{i=k}^{m} t_{a_i}$$

Probability of Interruption

where m is the total number of delay elements along the path of concern, k is the point at which T$_R$ just exceeds T$_{RFT}$, and t$_{ai}$ is the time delay provided by ith element. The critical detection point (CDP) is then defined to be the first sensor located prior to this point (relative to the outside). Finally, the analysis proceeds from the outside in along the chosen path in order to develop the probability of interruption, P$_I$; this metric is calculated as the minimum cumulative probability of detection from the start of the path up to the CDP, or (using the same basic relationship presented earlier):

$$P_I = 1 - \prod_{i=1}^{k-1} \overline{P_i}$$

where k-1 is the total number of detection elements along the path of concern up to and including that at the CDP, and where $\overline{P}_i$ is the non-detection probability provided by i^{th} element. For an effective PPS, the following condition must also hold true:

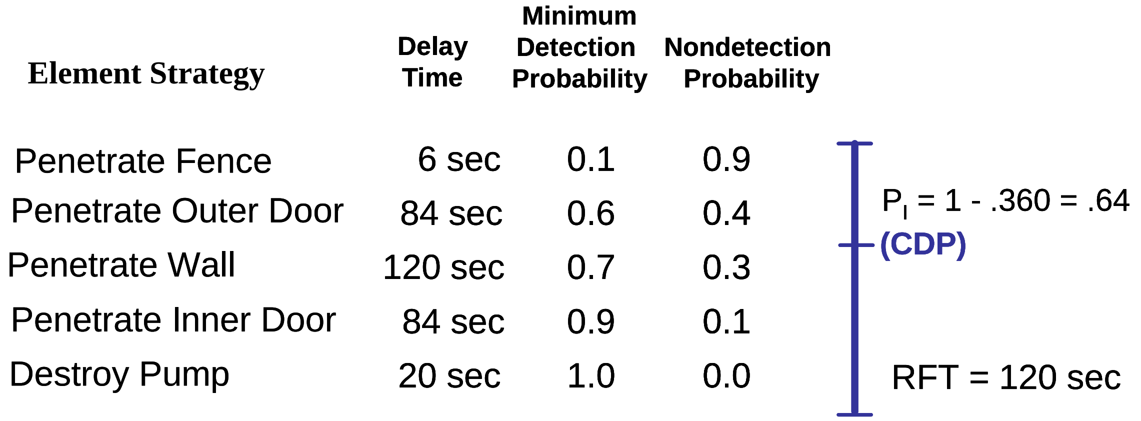
$$P_I \geq P_{I\ acceptable}$$

The acceptable probability of interruption value, $P_{I\ acceptable}$, must be established as part of the system requirements. The disadvantage of this measure is that it does not consider the results of an actual force-on-force engagement between the response and the adversaries.

Example

Figure 18-6 illustrates the concept of timely detection. Assume protection system elements provide the time delays and detection probabilities shown in Figure 18-6. If the guard response time is 120 seconds, the designer/evaluator must find a detection point on the adversary path where the adversary is more than 120 seconds away from his goal. In this example, the time remaining is 224 seconds after he has penetrated the outer door (for this example, we assume detection at an action occurs at the end of the delay time). The 224-second total is the sum of 120 seconds for the wall, 84 seconds for the inner door, and 20 seconds for attacking the pump. Since two detectors have been passed, the probability of detection is calculated as

P_I = 1- (1-.1)(1-.6) = .64; TR = 120+84+20 = 224 seconds



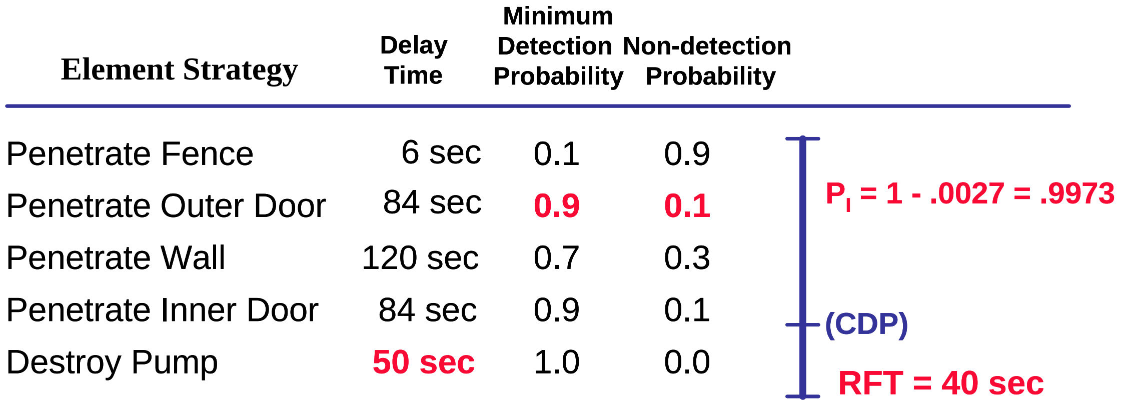
Element Strategy	Delay Time	Minimum Detection Probability	Nondetection Probability
Penetrate Fence	6 sec	0.1	0.9
Penetrate Outer Door	84 sec	0.6	0.4
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Destroy Pump	20 sec	1.0	0.0

Figure 18-6. Example of Timely Detection

Example path upgraded

The designer/evaluator must decide whether P_I = .64 is satisfactory. If it is not, the system must be improved.

Three types of system improvements are shown in Figure 18-7: (1) a reduction in guard response to 40 seconds from 120 seconds, (2) a delay improvement where the pump delay time has increased from 20 to 50 seconds, and (3) an improvement in detection at the outer door, from probability of detection of .60 to .90. P_I in this case reaches .9973. Not all upgrades probably need to be implemented.



Element Strategy	Delay Time	Minimum Detection Probability	Non-detection Probability
Penetrate Fence	6 sec	0.1	0.9
Penetrate Outer Door	84 sec	0.9	0.1
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Destroy Pump	50 sec	1.0	0.0

P_I = 1 - .0027 = .9973
(CDP)
RFT = 40 sec

Figure 18-7*.* Timely Detection for Upgraded Example

18.5 Path Analysis

Path analysis considers all adversary paths

The last section merely considered one adversary path. To have an effective system, from the perspective of timely detection, all paths to all targets need to provide Probability of Interruption against threats in the design basis threat (DBT) that are sufficiently high enough to meet either design or security plan requirements. Path analysis performs such a search.

The path with the lowest probability of interruption for a given target, threat, and operation condition is called the critical path. The Probability of Interruption along the critical path is taken as the performance of the facility or site. This is in keeping with a "weak-link" approach to security where it is presumed that the adversary can discover this path while looking for weak security.

Unless the facility being evaluated is small, not all such critical paths can be identified manually. Multipath analysis tools, such as PANL, are typically used to search through all the paths in an ASD to identify the critical paths.

18.5.1 Path Analysis Response Models

How Effective Is the Response Force in Overcoming the DBT?

Commonly, there is an interest in seeing how effectively the PPS interrupts and neutralizes the adversary. This is addressed currently in the United States by creating a detailed scenario around that path and performing a scenario analysis involving simulations to determine P_N and P_E for that path. To characterize the overall PPS performance, it is necessary to take into account both the probability of interruption and the expectation of response force capabilities in overcoming or neutralizing the DBT. This can be expressed as:

$$P_E = P_I \times P_N$$

where P_I is the probability of interruption, P_N is the probability of neutralization, and P_E is the overall system measure of probability of effectiveness. The challenge is, of course, to determine P_N. Possible options include the use of exercise data, historical engagement data, tabletop exercises, and computerized force-on-force modeling and simulation tools. Investigation of P_N is, however, beyond the scope of this module. Given a DBT definition, it is conceivably possible to size, equip, and train a response force such that, for analytical purposes, P_N can be assumed to approach a value of one.

18.6 Path Analysis Models

Path Analysis Models Used in the Course to Show how to Evaluate PPS along a single path

Several analytical computer models have been developed to help the analyst evaluate the effectiveness of a PPS. This course introduces VEASI and PANL:

- VEASI (Very-simplified Estimate of Adversary Sequence Interruption)—A simple, easy-to-use method of evaluating a PPS's performance along a specific path and under specific conditions of threat and system operation. This model computes a probability of interruption (P_I) from an analysis of the interactions of detection, delay, and response.
- PANL (Path ANaLysis)—This model conducts a comprehensive analysis of paths defined by adversary sequence diagrams (ASD). Once data on the threat, target, facility state, site-specific PPS, and response force response time are entered, the PANL code computes and ranks the most vulnerable paths for up to 10 response force times. While PANL has not been used for security analyses per se, it is based on research performed for several multipath analysis tools

Changing Parameters Changes the Outcome

VEASI is simple to use, easy to change, and it quantitatively illustrates the effect of changing physical protection parameters. This session briefly explains the model, the input, and the output and then describes the best way to use the model.

18.7 The VEASI Model

VEASI Model Uses One Path or Scenario

VEASI is a path-level analytical model of PPS performance in carrying out the detection, delay, and response functions. "Path-level" means that the model analyzes the protection system performance along only one possible adversary path or one adversary scenario.

To defeat theft or sabotage attempts, the response force must be notified while enough time remains for that force to respond and interrupt the adversary. An adversary interruption occurs in the VEASI model if the PPS works properly, resulting in confronting the adversary with a response force large enough to prevent them from proceeding further along their path.

Advantages and Limitations

Table 18-1 summarizes the advantages and limitations of VEASI.

Table 18-1. VEASI Analysis

Advantages • Allows analysis of PPS interactions and time trade-offs • Uses uncomplicated, numeric techniques • Qualitatively illustrates vulnerability • Used to perform sensitivity analyses
Limitations • Analyzes only a single path • Does not readily show lack of vulnerability • Is a simplified model using estimates of detection, delay, and responses • Does not model the neutralization of adversaries

18.8 The Input

Parameters Represent Detection, Delay, and Response

In the VEASI model, input parameters representing the physical protection functions of detection, delay, and response are required. Detection inputs are in the form of probabilities that the total detection function will be performed successfully. Delay inputs are in the form of mean times and standard deviations for each element. The location of detection—before, in the middle of, or after the delay—is also required. A value for response time is selected from the security response plans and used for input. All inputs refer to a specific adversary path, and depend on the specific skills of the adversary (usually the DBT).

18.8.1 Detection

Factors for Determining the Probability of Detection

The VEASI input for the detection function is the probability of detection for each sensor encountered by an adversary along a specific path and where that delay occurs with respect to the delay (at the beginning, middle, or end of the delay). Note that this probability depends on the capabilities of the adversary. The probability of detection is a product of the following three factors:

- probability that the detector will sense abnormal or unauthorized activities of the DBT or mix of threats,

- probability that this indication will be transmitted to an evaluation point, and

- probability that a valid signal will be declared valid when evaluated.

18.8.2 Delay

Adversary Task Time Includes Time to Travel to the Next Location

The time required by an adversary to travel a given path to a target can be thought of as the sum of the times required to perform certain tasks or travel distinct path segments. For the sake of simplicity, both task times and travel times are referred to as adversary task times. In general, it is not possible to predict the exact time interval necessary for the adversary to perform these tasks or proceed across these path segments, yet typically not enough data are generated to predict the distribution of the delay time. As a result, these delay times are represented in VEASI as “mean” or average times of whatever distribution the delay comes from.

18.8.3 Guard Response Time

How VEASI Looks at Response

Response is modeled in VEASI as the time between the generation of an alarm signal by a sensing device and the confrontation of the adversary by a response force adequate to halt the progress of the adversary along the path. In VEASI, the guard response time includes the times required for both detection and response. This time consists of successive time increments listed below:

How Time Is Counted in Detection and Response

Detection
- alarm communication time
- time required for alarm assessment

Response
- guard communication time (taking into account communications failures)
- time required for guards to prepare, to gather arms, to start vehicles, etc.
- guard travel time
- time required for the guard force to muster and deploy.

A response time input to VEASI should represent a response time taken from site security response plans that the response can reliably meet a high percentage of the time (thus it should normally exceed the mean or 50th percentile response time). This response time should represent the sum of all the elements shown on Figure 18-9. Up to 5 values can be entered.

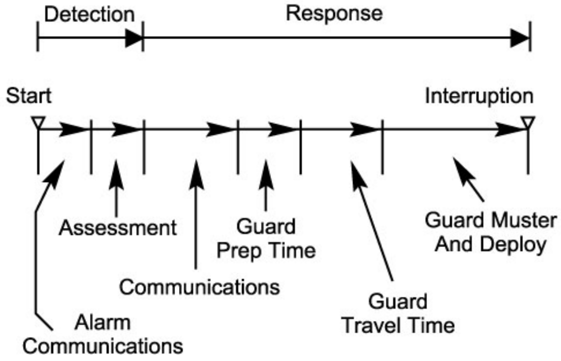


Figure 18-9. Guard Response Time

18.9 The Output

VEASI Estimates the Probability of Interruption (P_I) and the Critical Detection Point

The output of the VEASI model is an estimate of the probability that a sufficient team of response force personnel will interrupt the adversary at some point before the adversary completes an act of theft or sabotage. The output is referred to as the probability of interruption (P_I). It does not include an estimate of the likelihood of adversary neutralization. A value of P_I is shown for each of the response times entered.

VEASI also indicates the Critical Detection Point (CDP)

The critical detection point, CDP, is the first detection point encountered on the line prior to TR* (equal to the response force time or RFT). The CDP is considered critical because detection must occur either before or at this point to achieve interruption. The CDP for the path shown in Figure 18-10 is the point labeled p3.

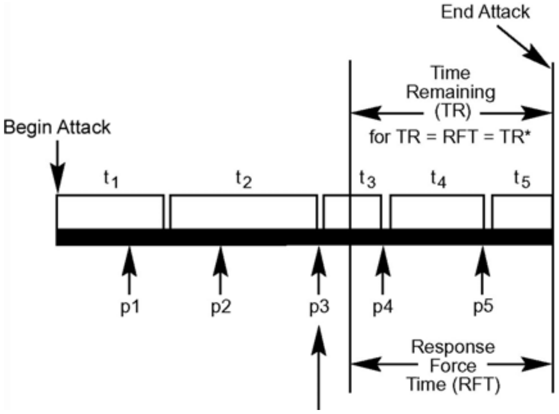


Figure 18-10. Critical Detection Point Indicated on a Path Event Timeline

18.10 Using the Model

Overview of Data Entry Process

To use VEASI, the initial step is the selection of an adversary action sequence. The selection should be based on a good knowledge of the facility and reasonable assumptions about the adversary. Next, select a physical path to the target corresponding to the chosen sequence and this should be the worst path (for you). Visualize the adversary tasks along that path, and determine the location of sensors. Then, obtain the required data: (1) the probabilities of detection, (2) the mean task times, (3) the location of detection with respect to delay (either E = at the end of the delay, M = in the middle of delay, or B = at the beginning of delay) and (4) the planned response times. Finally, enter the data into the computer and obtain the results. The real value of the VEASI model does not end there, however, because the analyst now has the opportunity to change the input data and see what effect this has on the output.

18.11 VEASI Example

Sabotage Target

Consider the example where the adversary intends to sabotage a target in a vital area as shown in Figure 18-11.

Path of the Adversary

The adversary intends to penetrate the fence, travel to the building, force open the door, travel to the vital area, open that door, and detonate an explosive device. The input to VEASI would be as shown in Table 18-2. Assume the planned RFT is 4 time units (in this case, minutes).

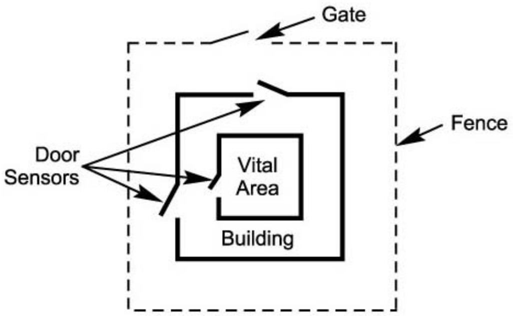
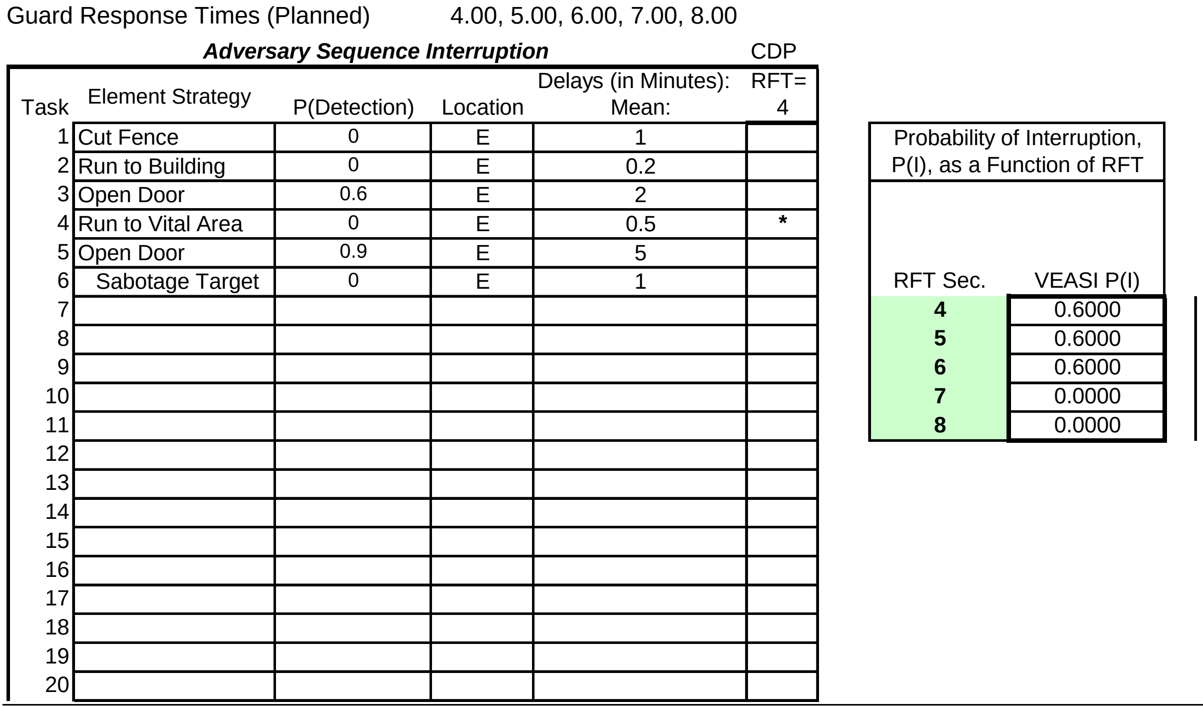


Figure 18-11. Example Facility

Table 18-2. VEASI Example



Guard Response Times (Planned) 4.00, 5.00, 6.00, 7.00, 8.00

Adversary Sequence Interruption

Task	Element Strategy	P(Detection)	Location	Delays (in Minutes): Mean:	CDP RFT= 4
1	Cut Fence	0	E	1	
2	Run to Building	0	E	0.2	
3	Open Door	0.6	E	2	
4	Run to Vital Area	0	E	0.5	*
5	Open Door	0.9	E	5	
6	Sabotage Target	0	E	1	
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Probability of Interruption, P(I), as a Function of RFT

RFT Sec.	VEASI P(I)
4	0.6000
5	0.6000
6	0.6000
7	0.0000
8	0.0000

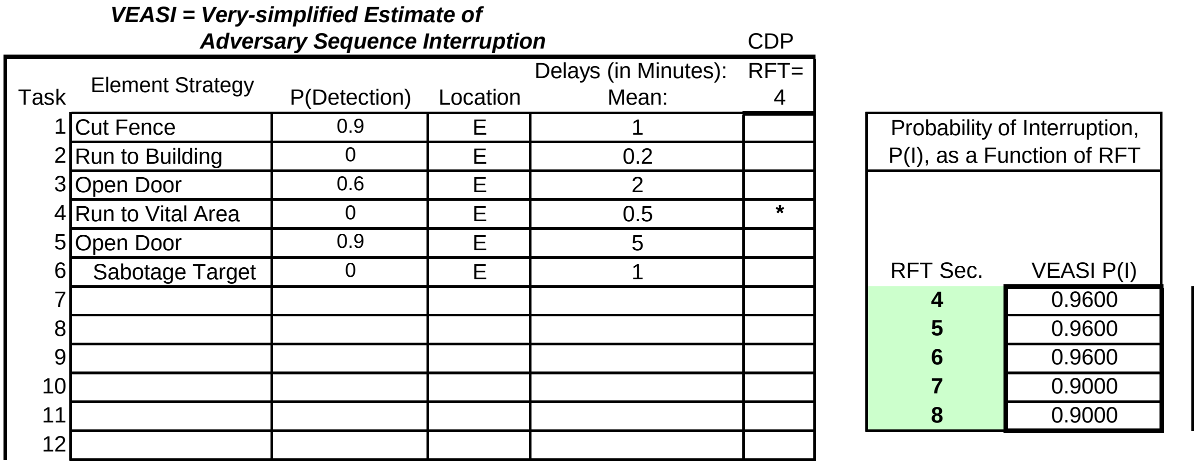
Analyst Uses Outcome to Suggest Ways to Improve PI

After this data is entered into VEASI, the result shows the probability of interruption is 0.6 with the CDP at the fourth task. (Note that the CDP is located here even though the probability of detection is zero because detection added here would, in fact, be timely.) On the right-hand side, note that the P_I remains at 0.6 until response time equals 7 seconds and P_I then drops to zero. This occurs as the CDP moves from the Open Door task (where PI = 0.6) to tasks 1 and 2 that have no associated detection.

The analyst may decide that this probability of interruption is too low and that something should be done to improve this probability. If a decision were made to put a series of vibration sensors on the fence with a probability of detection of 0.9, the input would be as shown in Table 18-3.

Table 18-3. VEASI Upgrade

Guard Response Times (Planned) 4.00, 5.00, 6.00, 7.00, 8.00



VEASI = Very-simplified Estimate of Adversary Sequence Interruption

Task	Element Strategy	P(Detection)	Location	Delays (in Minutes): Mean:	CDP RFT= 4
1	Cut Fence	0.9	E	1	
2	Run to Building	0	E	0.2	
3	Open Door	0.6	E	2	
4	Run to Vital Area	0	E	0.5	*
5	Open Door	0.9	E	5	
6	Sabotage Target	0	E	1	
7					
8					
9					
10					
11					
12					

Probability of Interruption, P(I), as a Function of RFT

RFT Sec.	VEASI P(I)
4	0.9600
5	0.9600
6	0.9600
7	0.9000
8	0.9000

Results of Upgrade

The probability of interruption in this upgraded case is 0.96, which may be satisfactory and may justify the installation of the fence vibration sensor.

18.12 Summary

Definition of VEASI

VEASI is a simple method of evaluating the adequacy of a PPS against a defined adversary utilizing a specific path and specific scenario. The analyst must enter the data as shown on Table 18-4.

VEASI Outcome: Probability of Interruption and Critical Detection Point

The VEASI model then performs the calculation and displays a probability of interruption. This says nothing about who will win in a battle, just what the chances are that a sufficiently large contingent of the response force will arrive in time to interrupt the adversary. If this probability is not satisfactory, additional PPS measures can be planned and subsequent analyses run to determine the most cost-effective solutions.

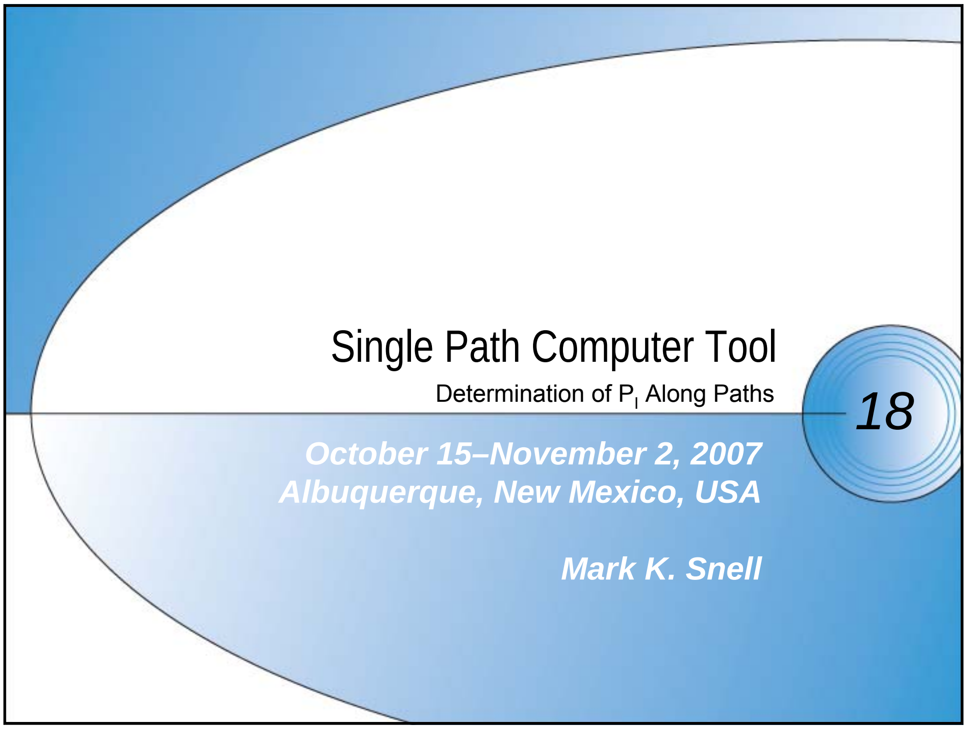
VEASI Analyzes Only One Path

It must be remembered that VEASI only analyzes one specific path, and other paths may have an even lower probability of interruption. Because of this limitation, an exhaustive program, like PANL, is valuable for looking at all possible paths and displaying only the most vulnerable.

Participants in this course will receive a disk copy of EXCEL™ VEASI that can accommodate up to 30 path segments.

Table 18-4. Input Summary for VEASI

Detection • Probability of detection
Delay • Mean Delay time
Location of Detection with Respect to Delay • B = at the beginning *or* • M = in the middle of delay *or* • E = at the end of delay;
Guard Response • Planned response time



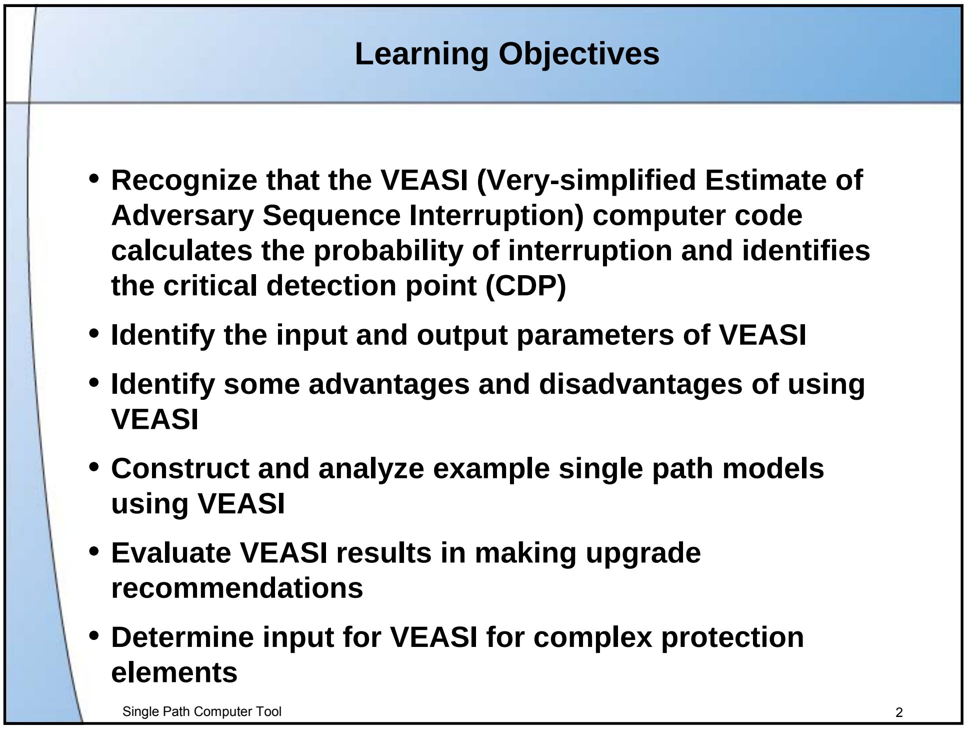
Single Path Computer Tool

Determination of P_I Along Paths

18

October 15–November 2, 2007
Albuquerque, New Mexico, USA

Mark K. Snell



Learning Objectives

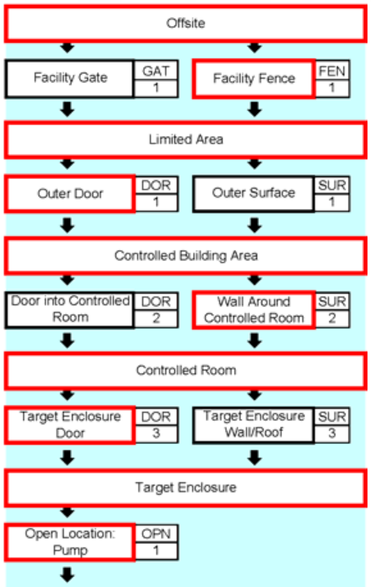
- Recognize that the VEASI (Very-simplified Estimate of Adversary Sequence Interruption) computer code calculates the probability of interruption and identifies the critical detection point (CDP)
- Identify the input and output parameters of VEASI
- Identify some advantages and disadvantages of using VEASI
- Construct and analyze example single path models using VEASI
- Evaluate VEASI results in making upgrade recommendations
- Determine input for VEASI for complex protection elements

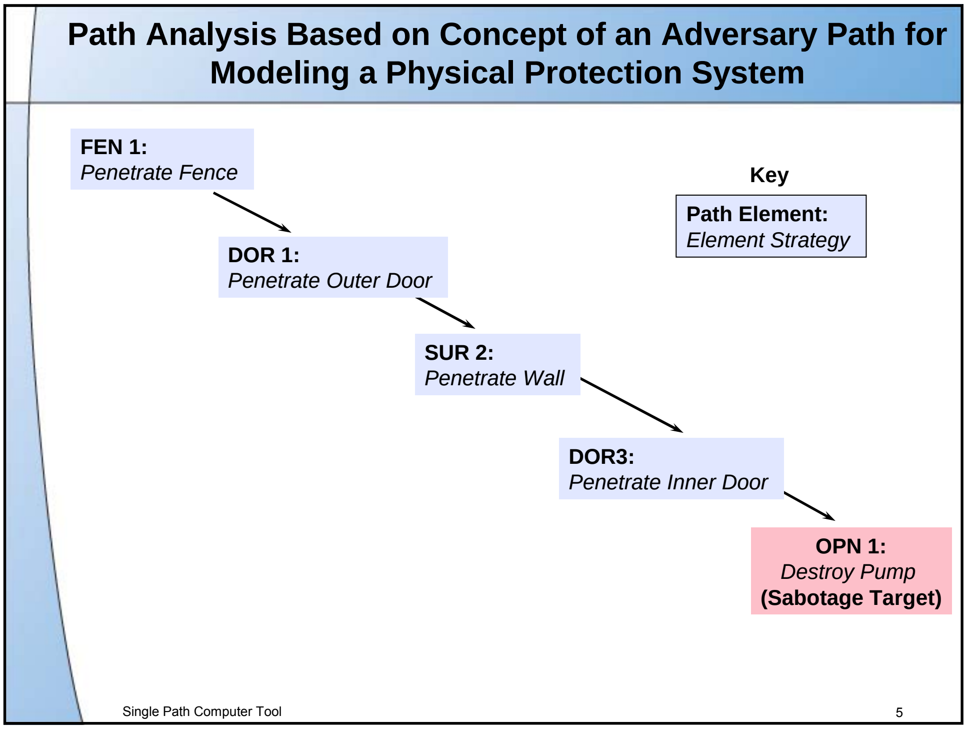
Context for VEASI

- **Path analysis: determines whether detection and delay are sufficient along all <u>paths</u> to provide an adequate level of Probability of Interruption, P_I, based on planned response times**
  - Addresses three basic functions of a physical security system: detection, delay, and response
- **VEASI calculates P_I for a <u>single</u> path and up to five response times**
  - Shows total delay and cumulative probability of detection on the path
  - Determines the CDP

Pump Sabotage Path from Site-Specific ASD

Example Path





Path Analysis Based on Concept of an Adversary Path for Modeling a Physical Protection System

FEN 1:
Penetrate Fence

DOR 1:
Penetrate Outer Door

SUR 2:
Penetrate Wall

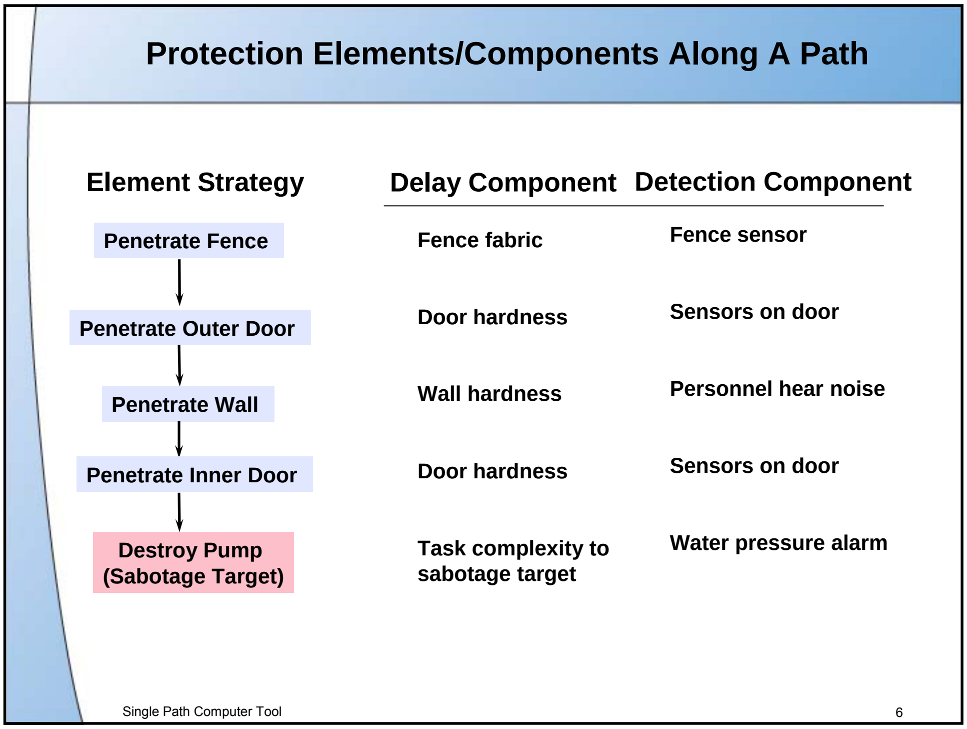
DOR3:
Penetrate Inner Door

OPN 1:
Destroy Pump
(Sabotage Target)

Key

Path Element:
Element Strategy

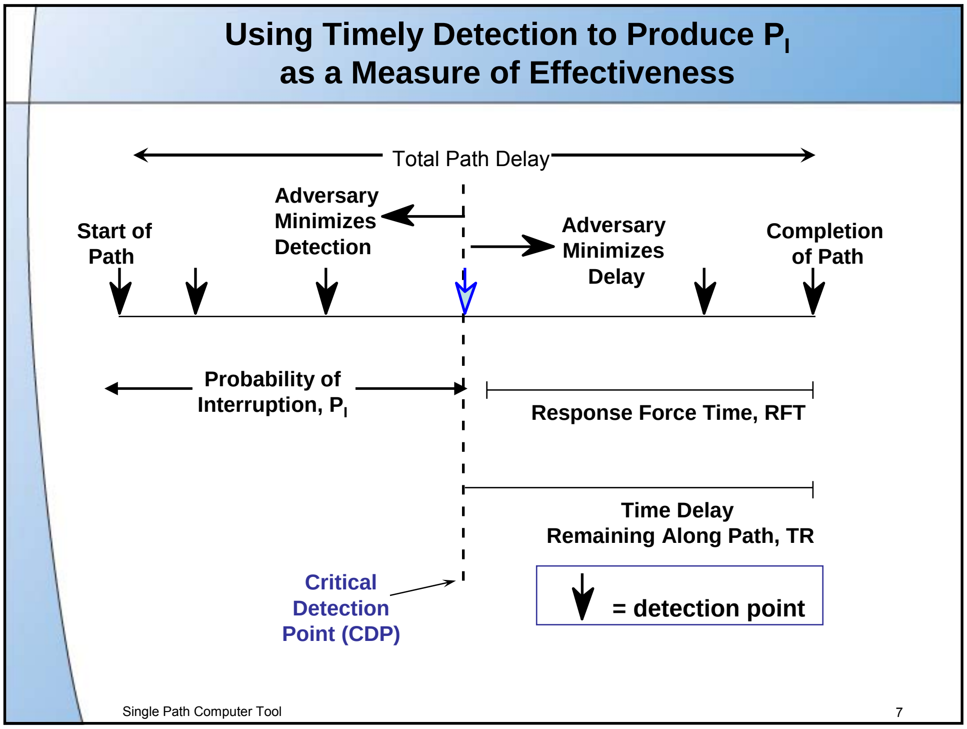
Single Path Computer Tool 5



Protection Elements/Components Along A Path

Element Strategy	Delay Component	Detection Component
Penetrate Fence	Fence fabric	Fence sensor
Penetrate Outer Door	Door hardness	Sensors on door
Penetrate Wall	Wall hardness	Personnel hear noise
Penetrate Inner Door	Door hardness	Sensors on door
Destroy Pump (Sabotage Target)	Task complexity to sabotage target	Water pressure alarm

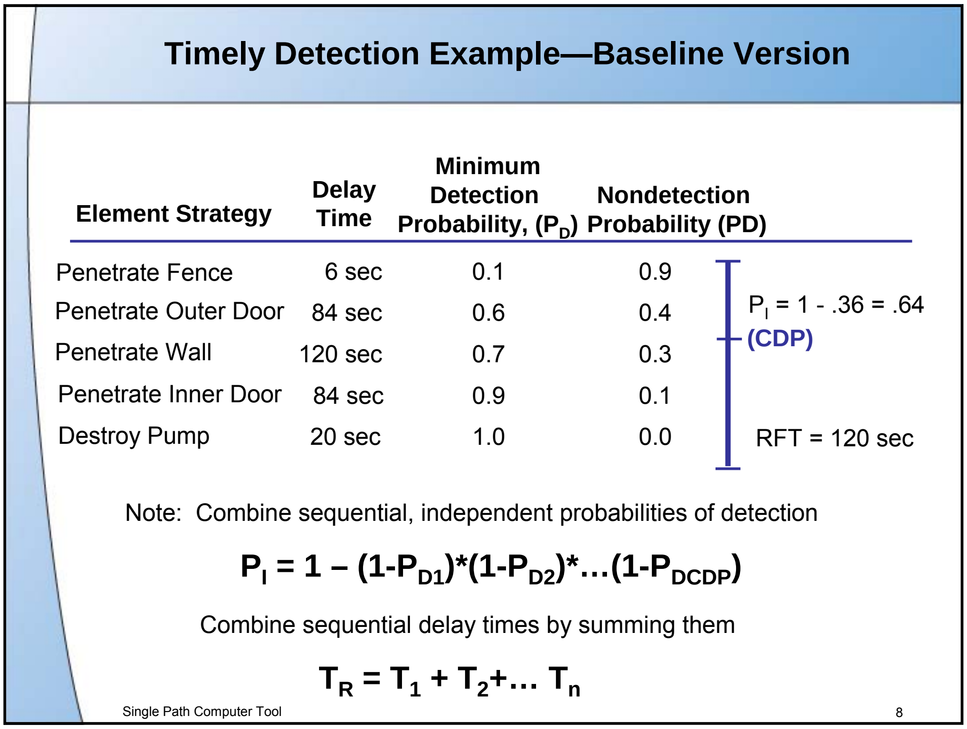
Single Path Computer Tool 6



Using Timely Detection to Produce P_I as a Measure of Effectiveness

Total Path Delay
Start of Path
Adversary Minimizes Detection
Adversary Minimizes Delay
Completion of Path
Probability of Interruption, P_I
Response Force Time, RFT
Time Delay Remaining Along Path, TR
Critical Detection Point (CDP)
= detection point

Single Path Computer Tool 7



Timely Detection Example—Baseline Version

Element Strategy	Delay Time	Minimum Detection Probability, (P_D)	Nondetection Probability (PD)
Penetrate Fence	6 sec	0.1	0.9
Penetrate Outer Door	84 sec	0.6	0.4
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Destroy Pump	20 sec	1.0	0.0

P_I = 1 - .36 = .64

(CDP)

RFT = 120 sec

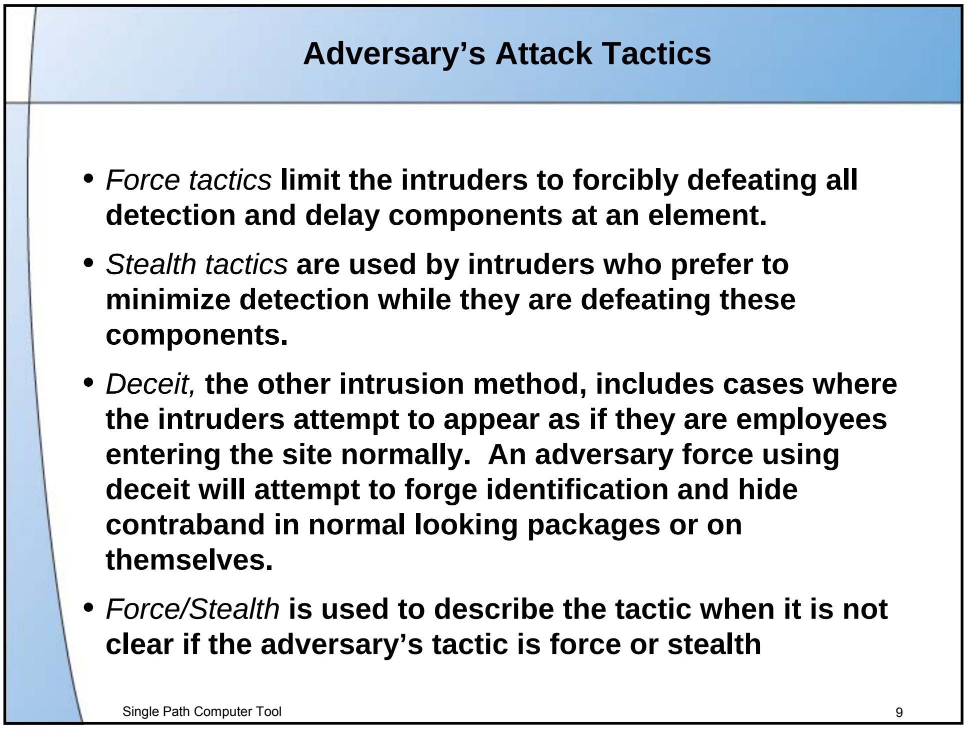
Note: Combine sequential, independent probabilities of detection

$$P_I = 1 – (1-P_{D1})*(1-P_{D2})*…(1-P_{DCDP})$$

Combine sequential delay times by summing them

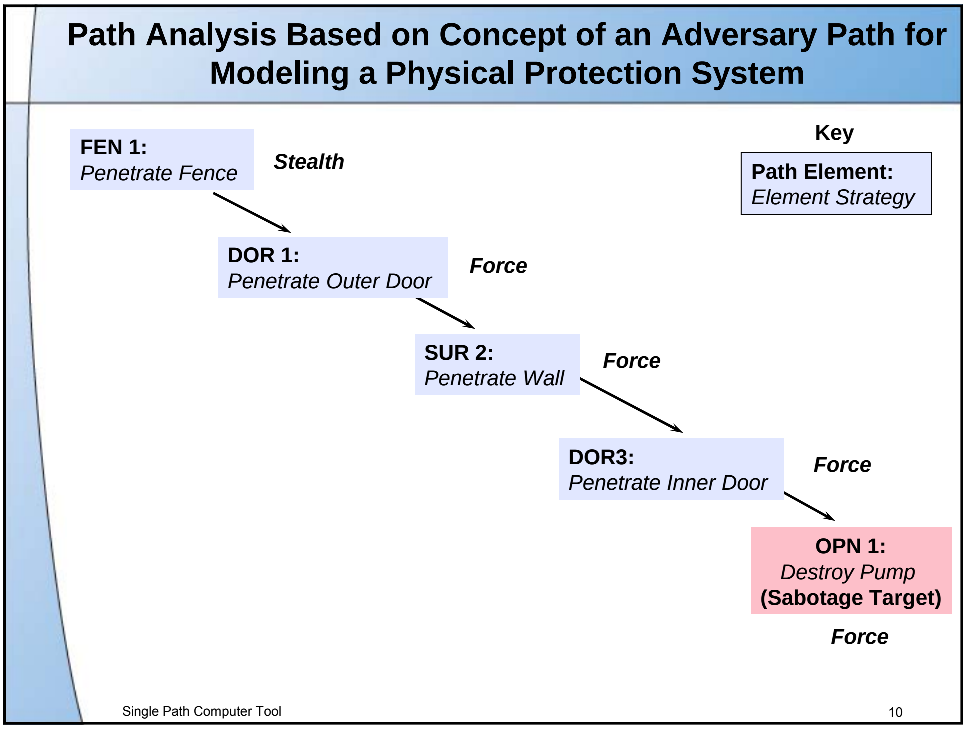
$$T_R = T_1 + T_2+… T_n$$

Single Path Computer Tool 8



Adversary’s Attack Tactics

- *Force tactics* **limit the intruders to forcibly defeating all detection and delay components at an element.**
- *Stealth tactics* **are used by intruders who prefer to minimize detection while they are defeating these components.**
- *Deceit,* **the other intrusion method, includes cases where the intruders attempt to appear as if they are employees entering the site normally. An adversary force using deceit will attempt to forge identification and hide contraband in normal looking packages or on themselves.**
- *Force/Stealth* **is used to describe the tactic when it is not clear if the adversary’s tactic is force or stealth**



Path Analysis Based on Concept of an Adversary Path for Modeling a Physical Protection System

FEN 1:
Penetrate Fence
Stealth

DOR 1:
Penetrate Outer Door
Force

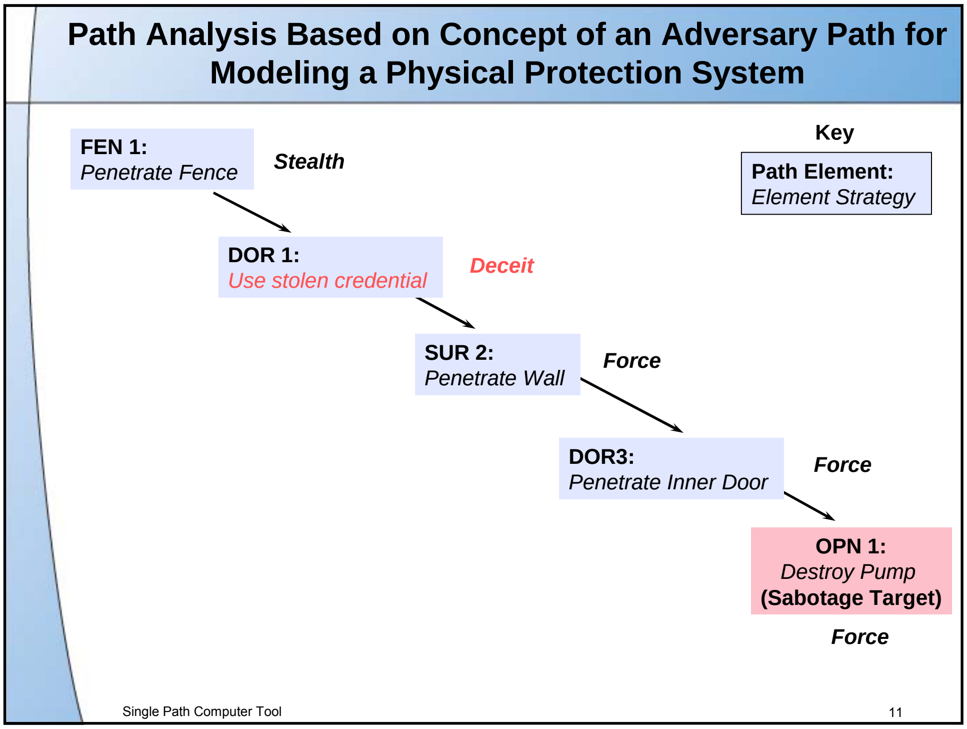
SUR 2:
Penetrate Wall
Force

DOR3:
Penetrate Inner Door
Force

OPN 1:
Destroy Pump
(Sabotage Target)
Force

Key

Path Element:
Element Strategy



Path Analysis Based on Concept of an Adversary Path for Modeling a Physical Protection System

FEN 1:
Penetrate Fence

Stealth

DOR 1:
Use stolen credential

Deceit

SUR 2:
Penetrate Wall

Force

DOR3:
Penetrate Inner Door

Force

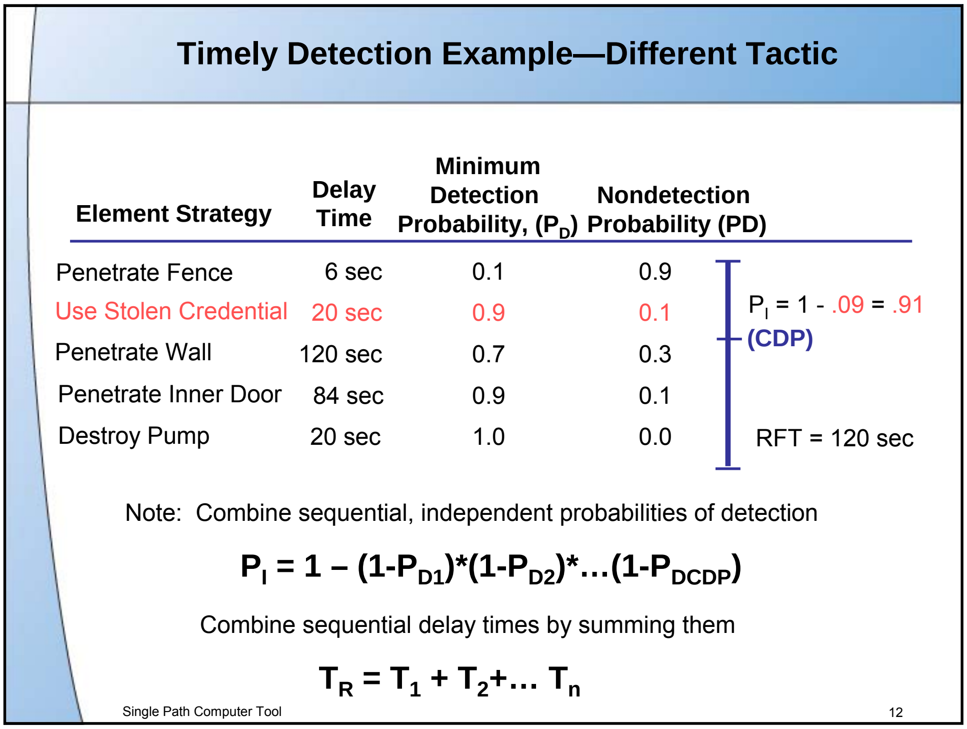
OPN 1:
Destroy Pump
(Sabotage Target)

Force

Key

Path Element:
Element Strategy

Single Path Computer Tool 11



Timely Detection Example—Different Tactic

Element Strategy	Delay Time	Minimum Detection Probability, (P_D)	Nondetection Probability (PD)
Penetrate Fence	6 sec	0.1	0.9
Use Stolen Credential	20 sec	0.9	0.1
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Destroy Pump	20 sec	1.0	0.0

P_I = 1 - .09 = .91
(CDP)

RFT = 120 sec

Note: Combine sequential, independent probabilities of detection

$$P_I = 1 - (1-P_{D1})*(1-P_{D2})*\ldots(1-P_{DCDP})$$

Combine sequential delay times by summing them

$$T_R = T_1 + T_2 + \ldots T_n$$

Single Path Computer Tool 12

Timely Detection Example—Baseline Version

Element Strategy	Delay Time	Minimum Detection Probability, (P_D)	Nondetection Probability (PD)
Penetrate Fence	6 sec	0.1	0.9
Penetrate Outer Door	84 sec	0.6	0.4
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Destroy Pump	20 sec	1.0	0.0

P_I = 1 - .36 = .64

(CDP)

RFT = 120 sec

Note: Combine sequential, independent probabilities of detection

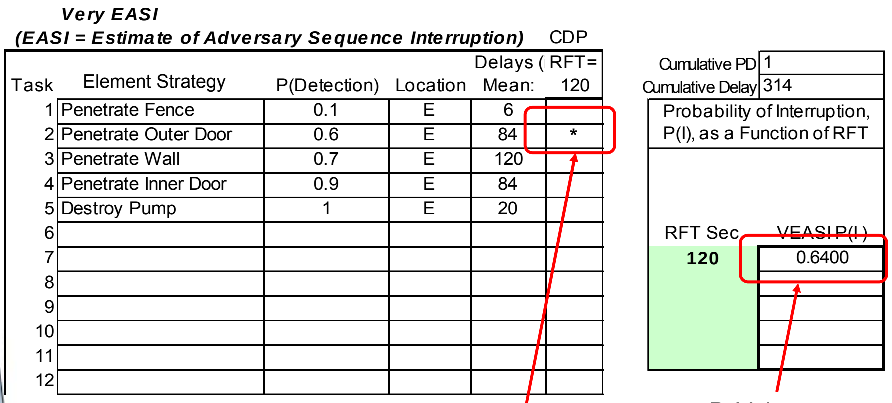
$$P_I = 1 - (1-P_{D1})*(1-P_{D2})*\ldots(1-P_{DCDP})$$

Combine sequential delay times by summing them

$$T_R = T_1 + T_2 + \ldots T_n$$

Single Path Computer Tool 13

VEASI Computer Code Performs the Same Calculations



Very EASI

(EASI = Estimate of Adversary Sequence Interruption) CDP

Task	Element Strategy	P(Detection)	Location	Delays (Mean:	RFT= 120
1	Penetrate Fence	0.1	E	6	
2	Penetrate Outer Door	0.6	E	84	*
3	Penetrate Wall	0.7	E	120	
4	Penetrate Inner Door	0.9	E	84	
5	Destroy Pump	1	E	20	
6					
7					
8					
9					
10					
11					
12					

Cumulative PD	1
Cumulative Delay	314

Probability of Interruption, P(I), as a Function of RFT

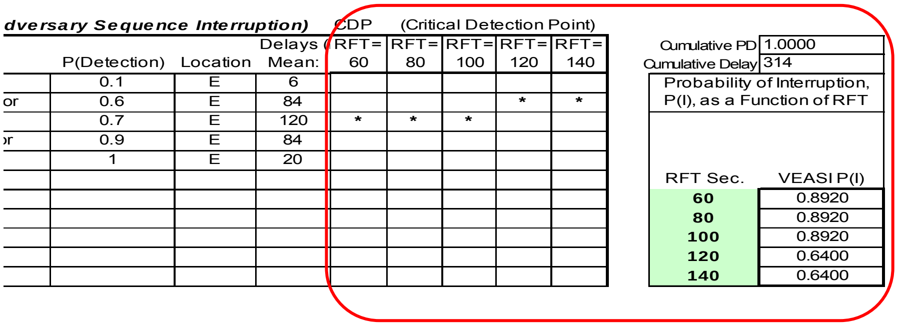
RFT Sec	VEASI P(I)
120	0.6400

CDP Location

P_I Value

Single Path Computer Tool 14

VEASI Computer Code



dversary Sequence Interruption) CDP (Critical Detection Point)

			Delays (	RFT=	RFT=	RFT=	RFT=	RFT=
	P(Detection)	Location	Mean:	60	80	100	120	140
	0.1	E	6					
or	0.6	E	84				*	*
	0.7	E	120	*	*	*		
›r	0.9	E	84					
	1	E	20					

Cumulative PD	1.0000
Cumulative Delay	314

Probability of Interruption, P(I), as a Function of RFT

RFT Sec.	VEASI P(I)
60	0.8920
80	0.8920
100	0.8920
120	0.6400
140	0.6400

VEASI allows you to determine P_I for up to five RFTs as a sensitivity analysis.

Timely Detection Example—Upgraded Version

Element Strategy	**Delay Time**	**Minimum Detection Probability**	**Non-detection Probability**
Penetrate Fence	6 sec	0.1	0.9
Penetrate Outer Door	84 sec	**0.9**	**0.1**
Penetrate Wall	120 sec	0.7	0.3
Penetrate Inner Door	84 sec	0.9	0.1
Destroy Pump	**50 sec**	1.0	0.0

P_I = 1 - .0027 = .9973

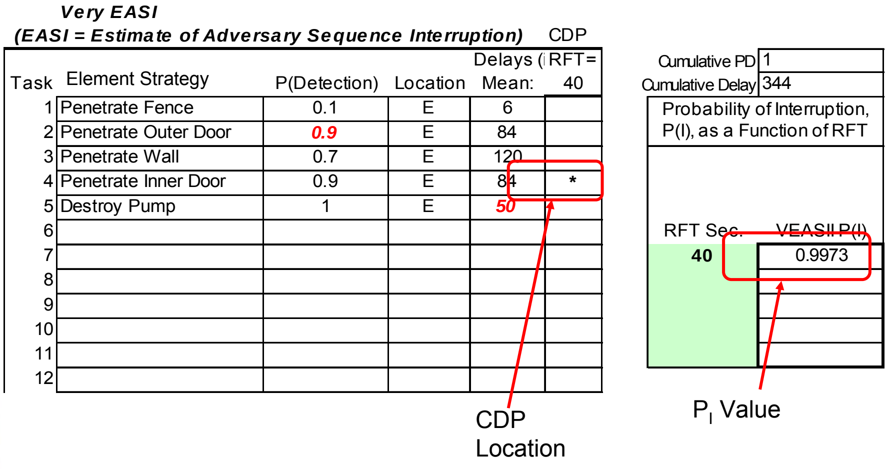
(CDP)

RFT = 40 sec

Note: Combine sequential, independent probabilities of detection

$$P_I = 1 - (1-P_{D1})*(1-P_{D2})*\ldots(1-P_{D\text{-}CDP})$$

VEASI Computer Code Version of Upgrade



Very EASI

(EASI = Estimate of Adversary Sequence Interruption)

Task	Element Strategy	P(Detection)	Location	Delays (Mean:	CDP RFT= 40
1	Penetrate Fence	0.1	E	6	
2	Penetrate Outer Door	***0.9***	E	84	
3	Penetrate Wall	0.7	E	120	
4	Penetrate Inner Door	0.9	E	84	*
5	Destroy Pump	1	E	***50***	
6					
7					
8					
9					
10					
11					
12					

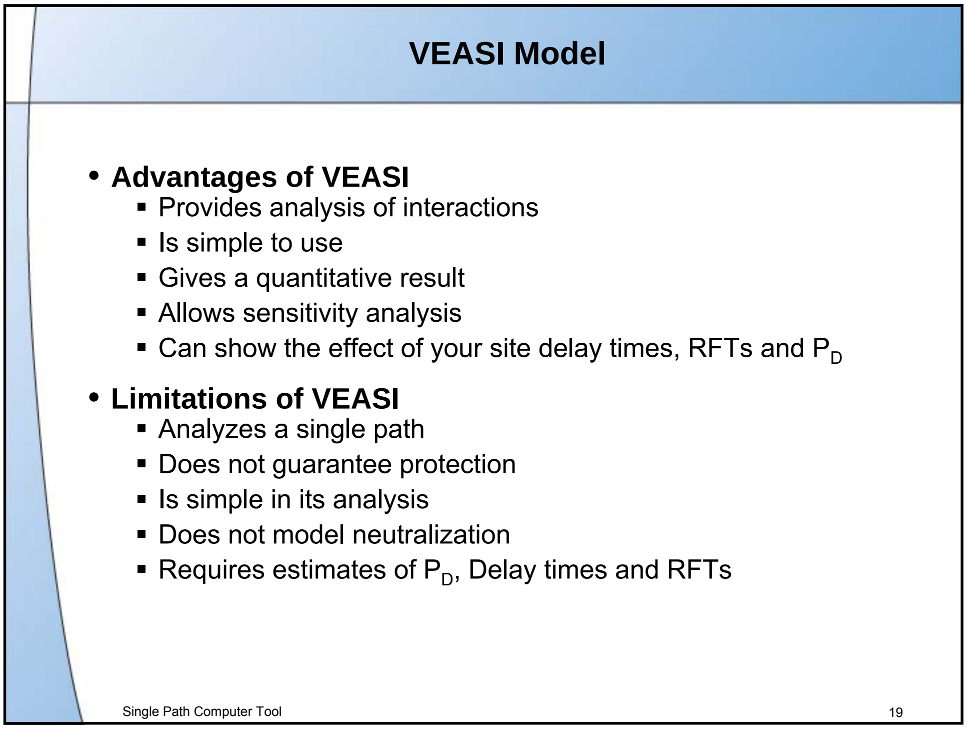
Cumulative PD	1
Cumulative Delay	344

Probability of Interruption, P(I), as a Function of RFT

RFT Sec.	VEASI P(I)
40	0.9973

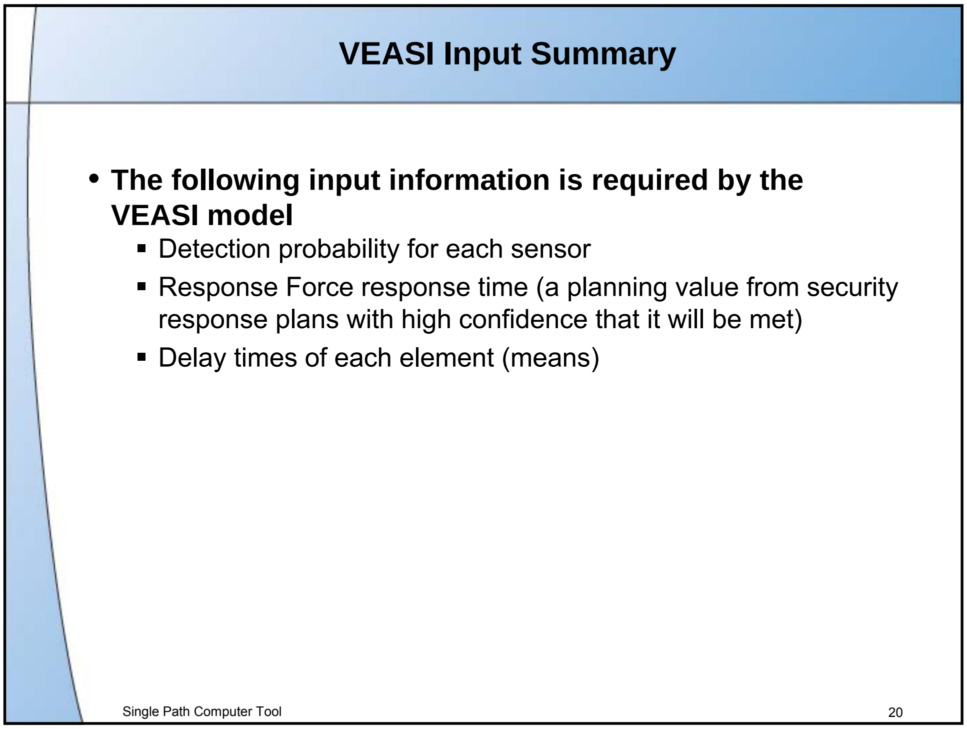
VEASI Model

- **This section of the presentation will cover:**
  - Model description
    - Advantages
    - Limitations
  - Input
    - Detection
    - Delay
    - Response
  - Output
    - Probability of interruption (P_I)
    - Critical Detection Point (CDP)
  - Uses of the output



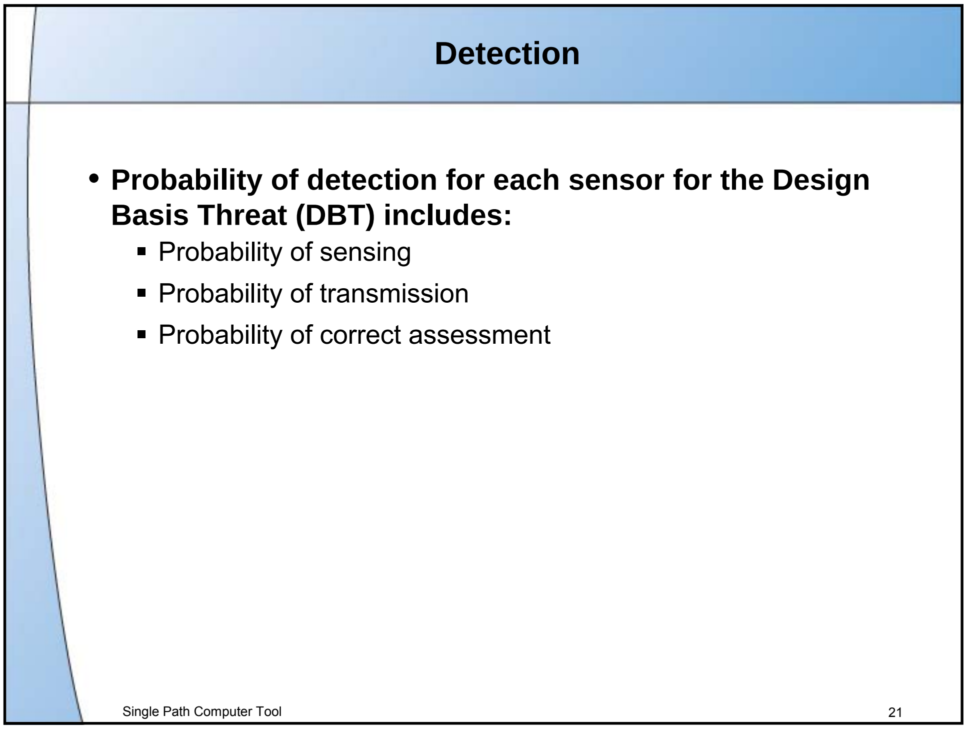
VEASI Model

- **Advantages of VEASI**
  - Provides analysis of interactions
  - Is simple to use
  - Gives a quantitative result
  - Allows sensitivity analysis
  - Can show the effect of your site delay times, RFTs and P_D
- **Limitations of VEASI**
  - Analyzes a single path
  - Does not guarantee protection
  - Is simple in its analysis
  - Does not model neutralization
  - Requires estimates of P_D, Delay times and RFTs



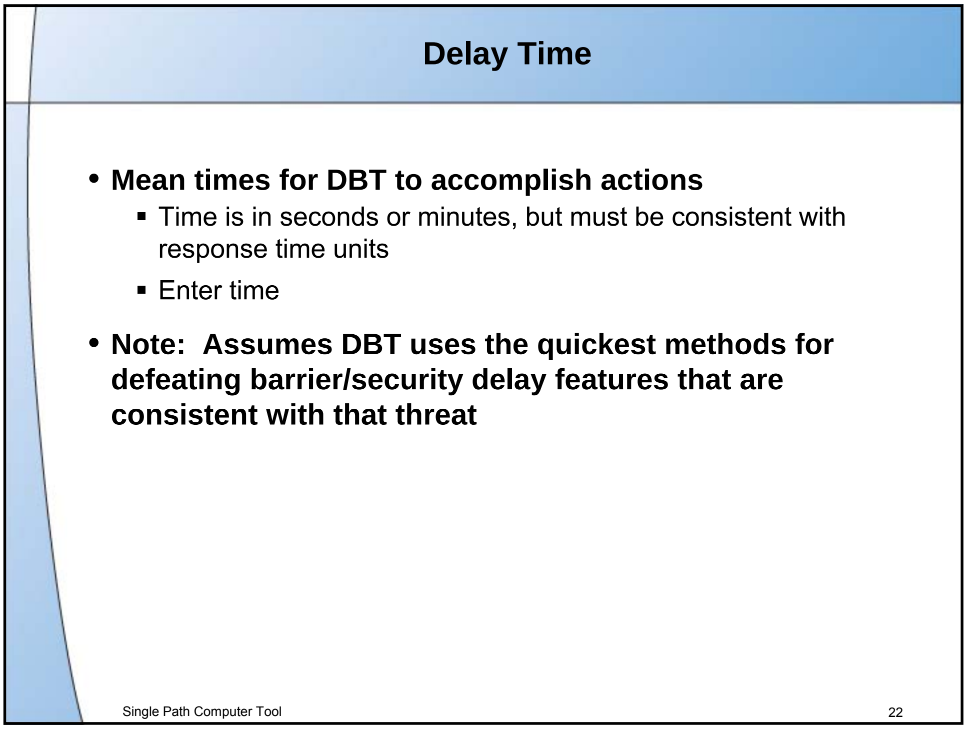
VEASI Input Summary

- **The following input information is required by the VEASI model**
  - Detection probability for each sensor
  - Response Force response time (a planning value from security response plans with high confidence that it will be met)
  - Delay times of each element (means)



Detection

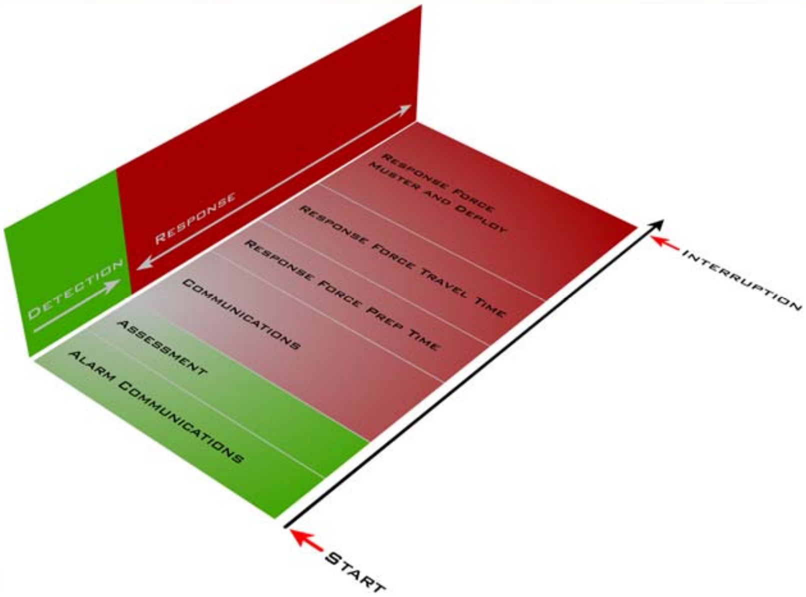
- **Probability of detection for each sensor for the Design Basis Threat (DBT) includes:**
  - Probability of sensing
  - Probability of transmission
  - Probability of correct assessment



Delay Time

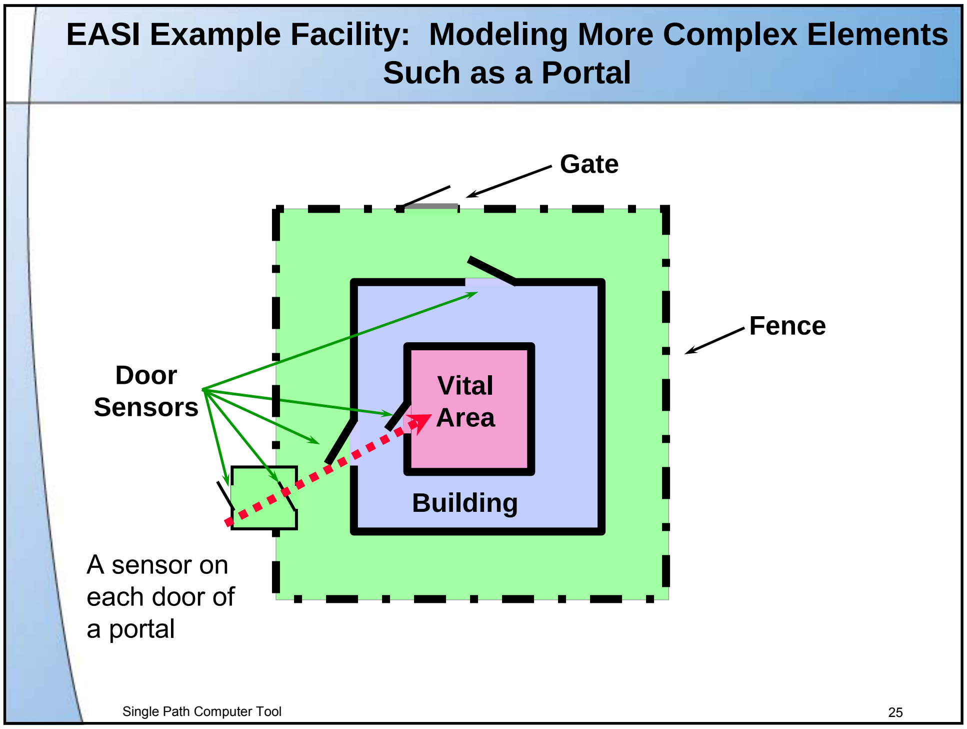
- **Mean times for DBT to accomplish actions**
  - Time is in seconds or minutes, but must be consistent with response time units
  - Enter time
- **Note: Assumes DBT uses the quickest methods for defeating barrier/security delay features that are consistent with that threat**

Response Force Time



VEASI Input Summary

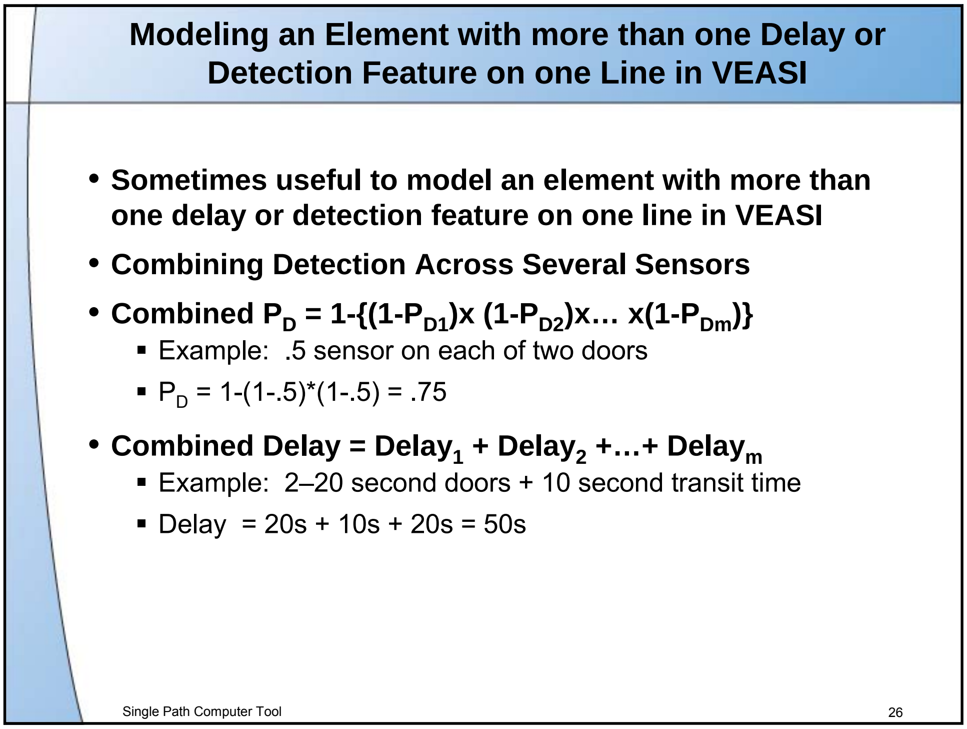
- **The following input information is required by the VEASI model**
  - Detection probability for each sensor
  - Response Force response time that can be met with high confidence
  - Mean delay times of each element



EASI Example Facility: Modeling More Complex Elements Such as a Portal

A sensor on each door of a portal

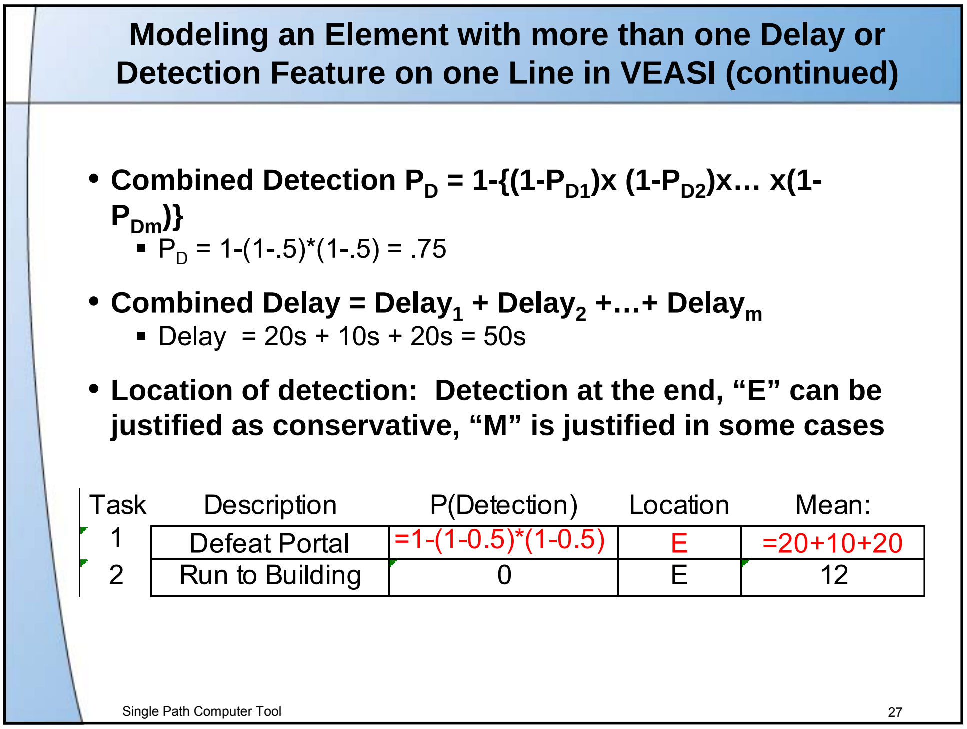
Single Path Computer Tool 25



Modeling an Element with more than one Delay or Detection Feature on one Line in VEASI

- **Sometimes useful to model an element with more than one delay or detection feature on one line in VEASI**
- **Combining Detection Across Several Sensors**
- **Combined $P_D = 1-\{(1-P_{D1})x\ (1-P_{D2})x\dots\ x(1-P_{Dm})\}$**
  - Example: .5 sensor on each of two doors
  - $P_D = 1-(1-.5)*(1-.5) = .75$
- **Combined Delay = $\text{Delay}_1 + \text{Delay}_2 +\dots+ \text{Delay}_m$**
  - Example: 2–20 second doors + 10 second transit time
  - Delay = 20s + 10s + 20s = 50s

Single Path Computer Tool 26

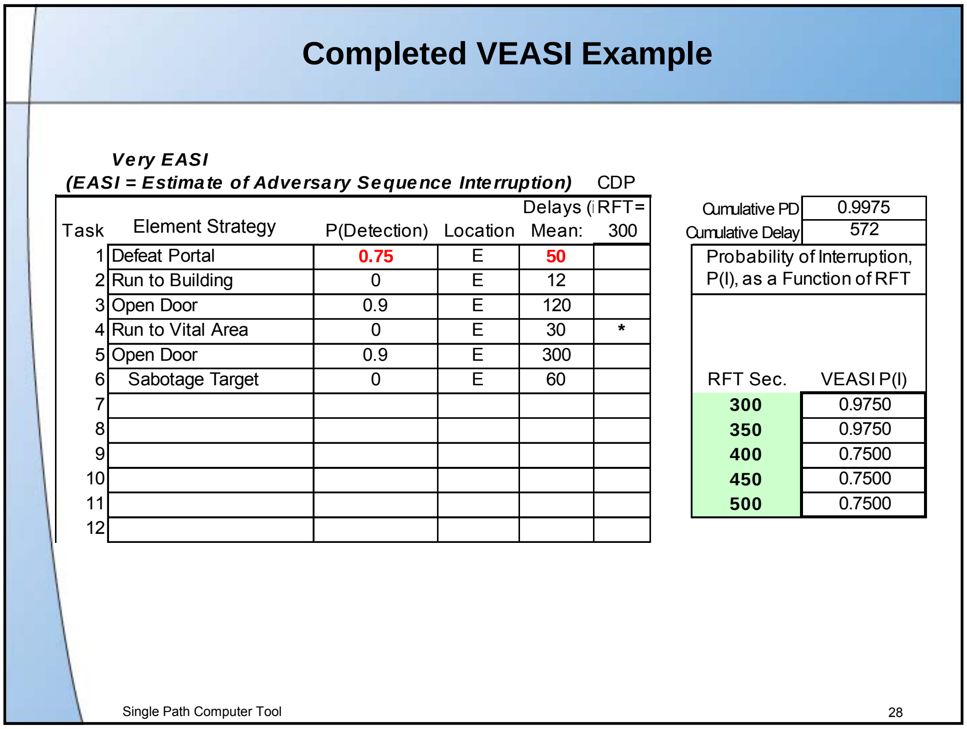


Modeling an Element with more than one Delay or Detection Feature on one Line in VEASI (continued)

- **Combined Detection P_D = 1-{(1-P_{D1})x (1-P_{D2})x… x(1-P_{Dm})}**
  - P_D = 1-(1-.5)*(1-.5) = .75
- **Combined Delay = $Delay_1$ + $Delay_2$ +…+ $Delay_m$**
  - Delay = 20s + 10s + 20s = 50s
- **Location of detection: Detection at the end, “E” can be justified as conservative, “M” is justified in some cases**

Task	Description	P(Detection)	Location	Mean:
1	Defeat Portal	=1-(1-0.5)*(1-0.5)	E	=20+10+20
2	Run to Building	0	E	12

Single Path Computer Tool 27



Completed VEASI Example

Very EASI

(EASI = Estimate of Adversary Sequence Interruption) CDP

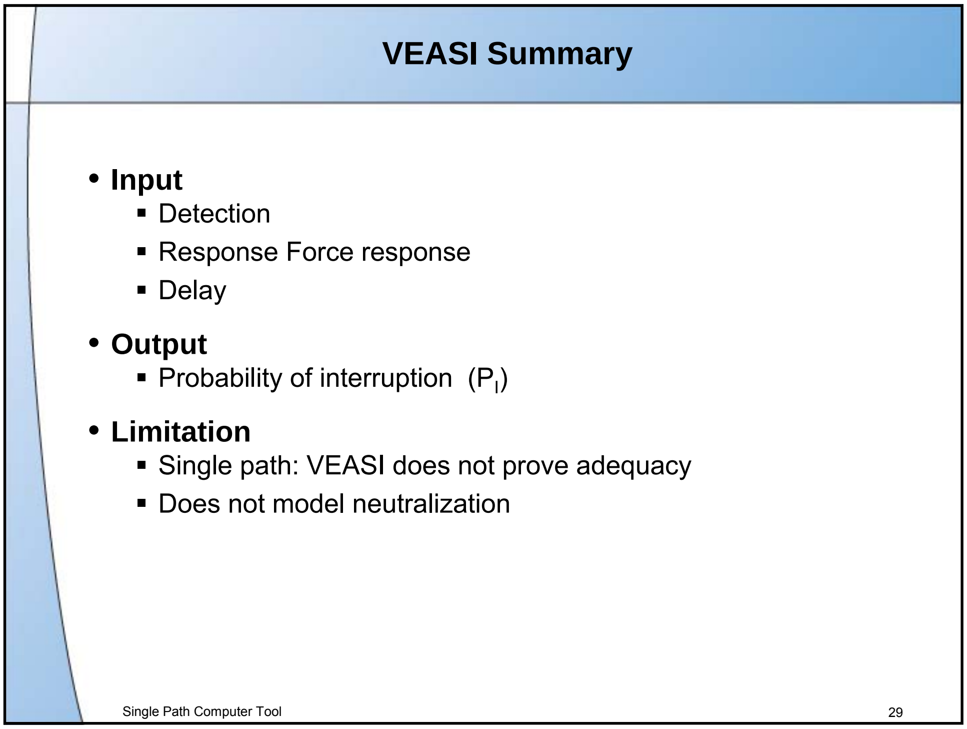
Task	Element Strategy	P(Detection)	Location	Delays (i Mean:	RFT= 300
1	Defeat Portal	**0.75**	E	**50**	
2	Run to Building	0	E	12	
3	Open Door	0.9	E	120	
4	Run to Vital Area	0	E	30	*
5	Open Door	0.9	E	300	
6	Sabotage Target	0	E	60	
7					
8					
9					
10					
11					
12					

Cumulative PD	0.9975
Cumulative Delay	572

Probability of Interruption, P(I), as a Function of RFT

RFT Sec.	VEASI P(I)
300	0.9750
350	0.9750
400	0.7500
450	0.7500
500	0.7500

Single Path Computer Tool 28



VEASI Summary

- **Input**
  - Detection
  - Response Force response
  - Delay
- **Output**
  - Probability of interruption (P_I)
- **Limitation**
  - Single path: VEASI does not prove adequacy
  - Does not model neutralization

Single Path Computer Tool 29

Subgroup 18S
Single Path Computer Tool

Session Objectives

After the session, the participants will be able to do the following:

1. Apply VEASI to evaluate the physical protection system of the research reactor.
2. Use a computerized EXCEL^{TM} version of VEASI.
3. Interpret the results of VEASI.

Exercise 1 - VEASI Analysis of Fence Intrusion

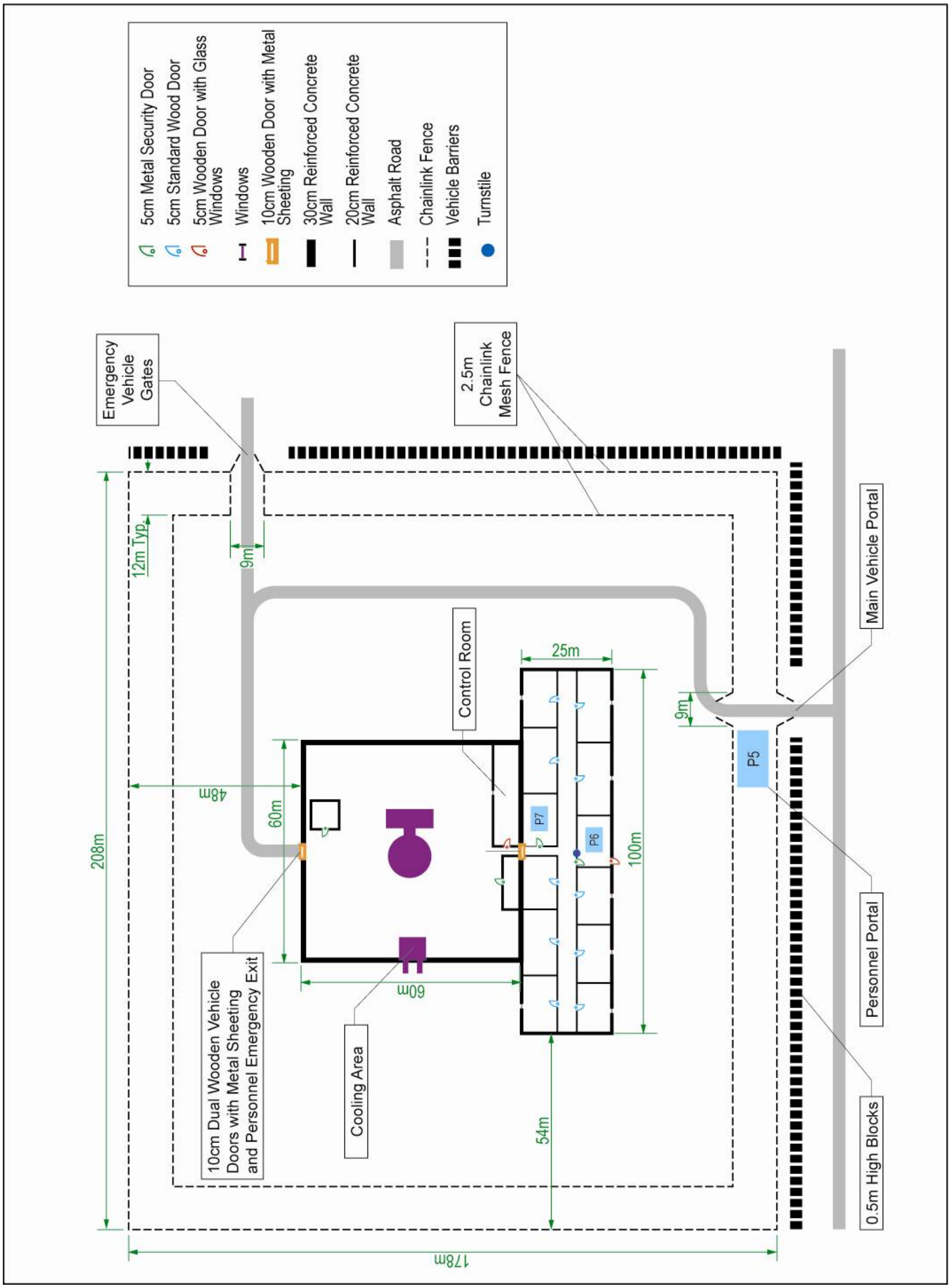
Load and run the computerized EXCEL^{TM} version of VEASI.

Using the information in the attached data (Table 18S-1) and the Exercise Data Book (Sections 7, 10, 12, 13, 14, 15), analyze the following path, and compute the probability of interrupting this sabotage attempt under normal daytime operating conditions at the PTR reactor facility. Draw the path in the diagram below for an adversary who:

1) climbs the outer fence
2) crosses the isolation zone (perimeter)
3) climbs the inner fence
4) crosses the protected area
5) penetrates the vehicle access door into the reactor hall
6) locates the reactor core and sets explosive charges

Note: Be sure to use the same unit of time throughout the problem.

PTR Wall Thicknesses and Distances



Exercise 1 - VEASI Analysis of Fence Intrusion (continued)

Guard response time = ____________

Element Strategy	Probability of Detection	Location	Time Delay (seconds)
1. Climbs the outer fence			
2. Crosses the isolation zone			
3. Climbs the inner fence			
4 Crosses the protected area			
5. Penetrates the vehicle access doors			
6. Locates the reactor core and sets explosive charges			

1) What is the probability of interruption given by VEASI for a response time of 180 seconds?

P_I = _____________

2) What is the probability of interruption if the guard response time drops from 180 seconds to 90 seconds?

P_I = _____________

3) What is the probability of interruption for the response time in question 1 if two minutes of access delay are added at the reactor core?

P_I = _____________

4) What is the probability of interruption if a fence vibration sensor is added at to the inner fence?

P_I = _____________

Exercise 2 - VEASI Analysis of Portal Entry

Using VEASI with Exercise Data Book (Sections 10, 12, 13, 14, 15), for the PTR, Building Floor Plan, Wall Thicknesses and Distances, Exterior Physical Protection Elements, Interior Physical Protection Elements, Access Control Plan), analyze the following path to determine the probability of interruption. Be careful when you consider the detection sequence in the personnel portals.

To compute the probability of detection of a series of sensors, multiply the probabilities of nondetection, and then subtract from 1.0 to get the combined probability of detection.

The adversary will probably use force after detection. Analyze the path for an adversary who:

1) Enters perimeter personnel portal using stolen badge

2) Stops for visual ID check, passes the guard (overcoming the guard, if necessary) and exits portal

3) Crosses protected area and enters uncontrolled door D61/1

4) Exchanges badges with guard, passes the guard (overcoming the guard, if necessary), passes metal detector, uses PIN badge to enter turnstile

5) Moves into the reactor hall R060 through the unlocked door D60/1

6) Penetrates door D90 into fresh fuel vault

7) Steals fresh fuel by using tools or explosives

8) Exits through emergency exit in shipping door D60/2 (which allows free exit)

9) Crosses protected area

10) Climbs inner fence

11) Crosses isolation zone

12) Climbs outer fence

Exercise 2 - VEASI Analysis of Portal Entry (continued)

Guard response time = ____________

Element Strategy	Probability of Detection	Location	Time Delay (seconds)
1. Enters personnel portal door with stolen badge			
2. Stops for visual ID check, pass guard and exit door			
3. Crosses protected area and enter door D61/1			
4. Exchanges badge with guard, pass ID and ME checks, enter turnstile with PIN			
5. Passes into reactor hall through door D60/1			
6. Penetrates door D90 into fresh fuel vault			
7. Steals fresh fuel			
8. Exits emergency exit in vehicle doors D60/2			
9. Crosses protected area			
10. Climbs inner fence			
11. Crosses isolation zone			
12. Climbs outer fence			

1. Using VEASI, what is the probability of interruption?

P_I = ______________

2. How would probability of interruption change if:

a. Response time increased by 30 seconds: P_I = ______________

b. Response time increased by 60 seconds: P_I = ______________

3. If you upgrade the physical protection system by mag-locking the emergency exit door with control from the SAS so as not to allow easy exit, how does this change P_I?

At the guard response time: P_I = ______________

If the guard response time increases by 60 seconds: P_I = ______________

Table 18S–1. Data for Physical Protection System Components

Threat:	Outsiders traveling on foot carrying high explosives (HE) and metal (ME)
Travel Times:	Running, approximately 4 meters/second
Doors in personnel portal:	12 second delay per door
30-cm wall, reinforced concrete:	2 minute delay
Climb fence:	10 second delay (climbing)
Tilt/vibration fence sensor	.75 probability of detection
5cm metal security door	45 seconds delay
10cm wooden shipping door with metal sheeting	30 seconds delay
Visual ID Check (ID):	0.5 probability of detection
Metal detector (ME):	0.9 probability of detection
Explosives detector (EX):	0.1 probability of detection
ID, ME, and EX time:	5 seconds delay for each
SNM detector (personnel):	0.9 probability of detection
SNM detector (vehicles):	0.5 probability of detection
Guard at post:	0.5 probability of detection
Guard at post:	30 second delay
Microwave exterior detection system:	0.7 probability of detection
Microwave interior detection system:	0.5 probability of detection
Detectors on building doors:	0.99 probability of detection
Interior detector:	0.9 probability of detection *when on* (off during normal daytime operations)
Time to steal material:	2 minutes
Time to sabotage facility (locate reactor core and set explosive charges)	45 seconds
Average guard response time:	3 minutes (NOTE: we are using this value for this exercise only to get results that are more than P_I=0.)
Standard deviation on all times:	30% of mean
Probability of guard force communication:	0.97

Application Considerations

1. Which adversary strategies can be analyzed using VEASI?
   a) theft only
   b) sabotage only
   c) both theft and sabotage
   d) neither theft nor sabotage

2. How many paths can be analyzed at one time using the VEASI model?
   a) only a single path at a time
   b) multiple paths at a time
   c) both a and b
   d) neither a nor b

3. The VEASI model incorporates which of the following for delay times:
   a) normal distribution
   b) Gaussian distribution
   c) discrete times only
   d) none of the above

4. The VEASI model incorporates which of the following for detection probabilities:
   a) normal distribution
   b) Gaussian distribution
   c) discrete probabilities only
   d) none of the above

5. The main purpose in using VEASI is to compute:
   a) probability of interruption
   b) probability of adversary success
   c) probability of communication
   d) probability of neutralization

6. The output of VEASI is:
   a) single path step probability
   b) cumulative probabilities over the path
   c) response force times
   d) path access delays

7. The output from EASI:
   a) always includes the most vulnerable path
   b) only includes the most vulnerable path
   c) may include the most vulnerable path
   d) never includes the most vulnerable path

8. In the VEASI model:
   a) detection always follows delay
   b) detection and delay are simultaneous
   c) delay always follows detection
   d) detection and delay are path dependent

9. What is the relationship between the probability of neutralization P_N and VEASI?
   a) P_N is independent of VEASI
   b) P_N X P_I = system effectiveness
   c) it is cumulative along the path
   d) both a and b

19. Multipath Tool:
Outsider Analysis with the Path Analysis (PANL) Model

Abstract. *The PANL computer code is used to evaluate PPS effectiveness against an outsider. PANL determines the most vulnerable path of an adversary sequence diagram as a measure of effectiveness. An analysis using PANL begins with identifying a target and constructing a site-specific adversary sequence diagram for that target. Next, delay and detection values must be defined for each path element on the adversary sequence diagram. The characteristics of the threat must be specified, as well as the adversary intrusion methods. Finally, the response force strategy and deployment time must be defined. All of this information is used as input to the PANL code. The code calculates the probability of interruption for paths on the adversary sequence diagram. It lists the most vulnerable paths in the VEASI format. The interpretation of these results can suggest the need for sensitivity analysis of data that has been input to the code, as well as possible physical protection system upgrades to the most vulnerable paths.*

19.1 Introduction

PANL Analyzes PPS Effectiveness Against Outsiders

The computer code called the Path Analysis (PANL) model has been developed to demonstrate how comprehensive path analyses of PPS effectiveness against outsiders can be performed using adversary sequence diagrams (ASD). PANL has been based on functional capabilities found in software used by U.S. DOE facilities to demonstrate that they meet DOE requirements for graded safeguards to protect their SNM. Graded safeguards require that all SNM will be subject to varying degrees of physical protection with increasing levels of effectiveness corresponding to the increasing strategic potential of the material in enrichment, quantity, and form.

An overview and demonstration of the methodology will be completed in this session and applications and practice with the code will be done in the subgroup session.

19.2 Measures of Effectiveness

Probability of Interruption,or P_I

The evaluation measure used by PANL to assess PPS effectiveness is the probability of interruption, P_I. Please note that earlier in the ITC, we designated Probability of Interruption as P_I. The PANL model shows that statistic as P(I). P_I is defined as the probability that the response force will interrupt the adversaries before they can complete their task. Thus, PANL provides only a partial measure of effectiveness. The other factor required to properly evaluate the effectiveness of the PPS is the probability of neutralization, or the ability of the response force to prevent the adversaries from completing their task.

19.3 Calculation Algorithm

Assumptions

The PANL algorithm for calculating P_I makes two conservative assumptions:

1. Adversaries have knowledge of the protection system characteristics.

2. Adversaries use an optimal penetration strategy.

Elements Required for Interruption

For interruption to occur, two conditions must be met:

1. the adversaries must be detected, and

2. they must be detected early enough on the path that the time remaining (TR) provided by the delay elements exceeds the response force time (RFT) to arrive.

Best Strategy for Adversary

Therefore, the optimal penetration strategy for the adversary is to avoid detection until a point is reached on the path where there is no longer enough delay to allow interruption, and then minimize delay along the remainder of the path. This strategy can be demonstrated by considering the relationship of detection, delay, and response along a path.

Events on the Path to the Target

On the ASD, a path consists of an ordered sequence of path elements through the facility to the target. However, a path can also be represented by an event line (a) as shown in Figure 19-1. This line represents the events on the path that the adversary takes from off site to the target location. The events shown on the line are:

- the location of the detection components p_1, p_2…
- the delay times (t_1, t_2…) provided by barrier and delay components, task times, and transit times
- the point where the path TR is equal to the RFT; namely TR.*

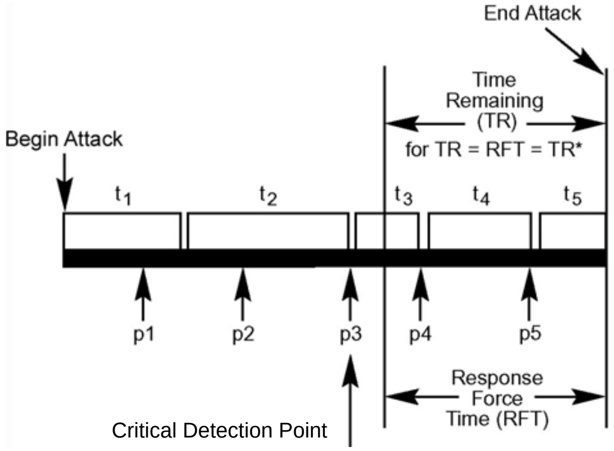


Figure 19-1. Event Time Line

Critical Detection Point

The first detection point encountered on the line prior to TR* (in this case p_3) is called the ***critical detection point***, CDP, because detection must occur either before this point or at this point to have interruption. For interruption to occur on a given path, there must be a CDP on the path.

A Path With No CDP

There are two ways that a path can fail to have a CDP:

- the total path time (in this case $t_1 + t_2 + t_3 + t_4 + t_5$) is greater than the RFT and there is no detector on the path prior to the TR* point, as shown on Figure 19-2.
- the total path time is less than the RFT, as shown on the event line in Figure 19-3.

Detectors After CDP are Ineffective

It should be noted on Figure 19-1 that detectors located beyond the CDP (in this case p4 and p5) are ineffective for interruption. This is because even if detection occurs after the CDP, the remaining delay time is not enough to allow the timely arrival of the response force.

Adversary Strategy: Minimize Delay and Avoid Detection

The optimal penetration strategy would be used by an adversary who knows the delay and detection values of all the components and the RFT and who could make the same calculations as PANL. This strategy is to proceed along a path by minimizing detection until the remaining path delay time is less than the RFT, and then to minimize delay without regard to further detection. This strategy decouples the detection and delay functions, because the adversary is attacking an element either by minimizing delay or by minimizing detection, depending on whether he has passed the CDP.

Determining the Critical Detection Point

Because delay is decoupled from detection at each element, the calculation algorithm is simplified. The CDP for each path is obtained by adding the minimum element delays, starting from the last element on the path until they add up to the RFT. Then the CDP is the first detection point prior to TR = TR* = RFT. If there is a CDP on the path, then detection probabilities are considered from off site to the CDP to give the P_I value for that path. If there is no CDP on the path, then the value of P_I is zero.

19.4 Evaluation Steps

Overview of Steps

The basic steps of the PANL method include:

1. Identify targets.
2. Construct an ASD for each target.
3. Define adversary characteristics—transportation and equipment.
4. List element strategies for each element.
5. Define PPS components and assign component performance
    - Define components at each protection layer in the ASD and assign performance.
    - Assign delay and detection values to each element using worksheets.
6. Define performance for each strategy: P_D, Total Delay, and Location of Detection.

7. Define response force characteristics—response strategy and RFT range.
8. Analyze and review results in VEASI.
9. Perform sensitivity analysis.
10. Perform upgrade analysis.

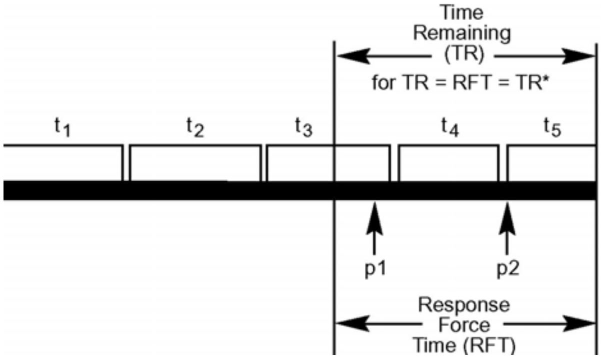


Figure 19-2. No Early Detection

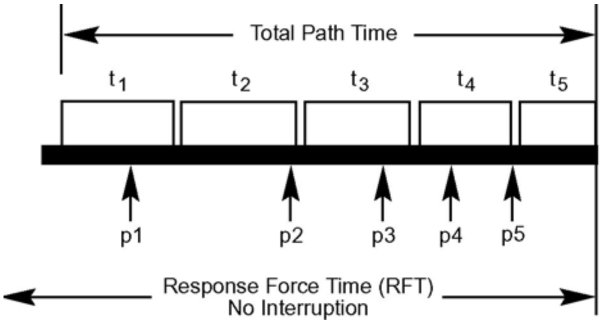


Figure 19-3. Response Time Too Long

19.4.1 Steps 1 and 2—Identify Targets

List Potential Targets and Rank Them

The locations and descriptions of all the potential targets in the facility should be listed. A priority ranking of the targets based on consequence or attractiveness will help the analyst select the target or targets for analysis.

Construct a Site-Specific ASD

A site-specific ASD is constructed for each target, or set of targets having a common location, by using facility and PPS information. The objective is to correctly model the PPS that exists at a site around each target. This site-specific ASD is created by first adding the security areas that exist at the facility and then specifying the path elements (PE) that represent ways to proceed from one area to the next. A list of the PEs is provided in Figure 19-4.

Path Elements:

DUC	-	Duct
EMX	-	Emergency Exit
FEN	-	Fenceline
GAT	-	Gateway
HEL	-	Helicopter Flight Path
ISO	-	Isolation Zone
PST	-	Material Passthrough
MAT	-	Material Portal
OVP	-	Overpass
DOR	-	Personnel Doorway
PER	-	Personnel Portal
SHD	-	Shipping/Receiving Doorway
SHP	-	Shipping/Receiving Portal

Path Elements, continued

SUR	-	Surface
TUN	-	Tunnel
VHD	-	Vehicle Doorway
VEH	-	Vehicle Portal
WND	-	Window

Target Locations:

BPL	-	Bulk Process Line
CGE	-	Cage
FLV	-	Floor Vault
GNL	-	Generic Location
GBX	-	Glovebox
IPL	-	Item Process Line
OPN	-	Open Location
TNK	-	Storage Tank

Figure 19-4. Path Elements and Target Locations

Example Facility and PPS Layout

Figure 19-5 shows a simplified example facility and PPS layout. Figure 19-6 shows the resulting site-specific ASD that represents this example facility. The labels “A,” “B,” “C,” and “D” in Figure 19-6 correspond to the appropriate physical areas on the ASD.

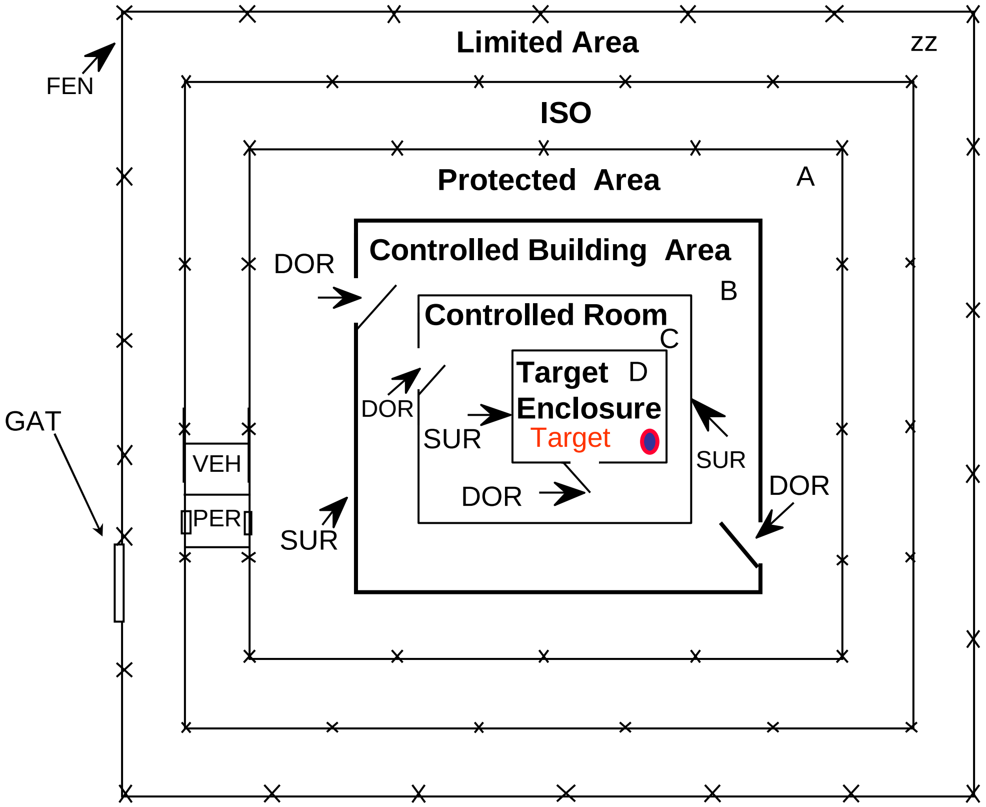


Figure 19-5. Example Facility and PPS Layout

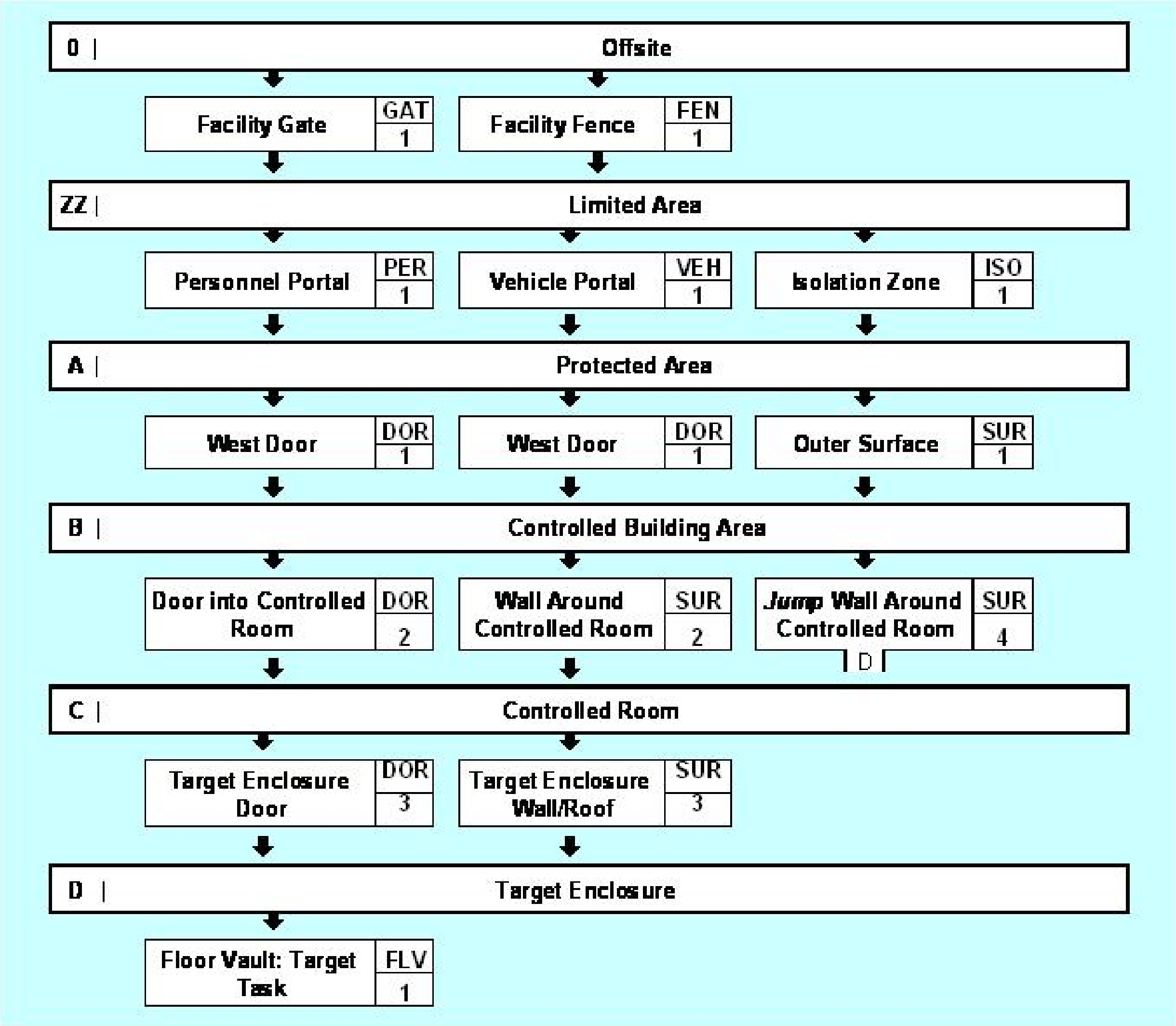


Figure 19-6. Example Facility ASD

19.4.2 Step 3—Specify Threat Characteristics

Define Equipment, Transportation, and Intrusion Methods Used by the Adversary

The site-specific threat must be defined in terms of:

- types of equipment carried by the adversary
- transportation used by the adversary
- adversary intrusion methods

Equipment Influences Values

Adversary equipment will influence the type of detection and delay values assigned at each element. The more contraband an adversary group tries to sneak past a portal, the higher the probability of detection. On the other hand, an adversary force with explosives will be able to defeat barriers more quickly than a force without explosives.

Categories of Equipment Used by Adversary

PANL uses seven categories of outsider adversary equipment:

- Land Vehicle—car, truck, or train
- Helicopte—a rotary aircraft
- Hand Tools—hammers, hand-boltcutters, ladders
- Power Tools—gas- or electric-powered equipment and thermal tools
- High Explosives
- Small Arms—weapons using 7.62 mm or smaller ammunition
- LAWs—Light Anti-Tank weapons used in this context to defeat security posts or towers

Combinations of Equipment

PANL has two threat types, varying in that they have different combinations of transportation as shown below in Figure 19-7 The "X's" indicate that a particular threat category listed by row has the capability listed at the top of the column. For example, the Terrorist on Foot does not use Land Vehicles to intrude on the site.

While there is not an explicit threat, per se, that does not have LAWs, the user can decide whether the adversary will use strategies employing LAWs or Small Arms against hardened guard posts or towers. Such decisions would be made on a case-by-case consideration of posts or towers rather than explicitly naming a threat that does not have LAWs.

Note: While earlier path analysis software used in the ITC offered more combinations of equipment than PANL, these two threats were all that were used in practice.

Adversary Intrusion Methods

PANL lets the user define a variety of adversary strategies for each element as any arbitary mix of force, stealth, and deceit.

Threat Name	Land Vehicles	Helicopters	Hand Tools	Power Tools	High Explosives	Small Arms	LAWs
Terrorist with Veh/Hel	X	X	X	X	X	X	X
Terrorist on Foot			X	X	X	X	X

Figure 19-7. Equipment Combinations Assigned to Each Threat Type

19.4.3 Step 4—List Element Defeat Strategies For Each Element

Element Defeat Strategies

An element defeat strategy is a description of how the adversary would defeat a specific element in the ASD, such as a door or surface or fence. One defeat strategy for a fence might be "quietly climb over the fence" while another one might be "drive large vehicle through the fence."

A good list of strategies is important for a good analysis

Recall that a good security effectiveness evaluation depends on having a complete ASD that includes the elements in the most vulnerable path because PANL cannot discover a path if one or more of the elements are left out of the ASD. In a similar fashion, a good security effectiveness evaluation depends on the user defining a comprehensive list of strategies for how the adversary will attack each element; PANL cannot discover a strategy that the user leaves out.

Entering strategies

The user defines defeat strategies for each element in the ASD (see Figure 19-8). If the adversary attack must consider exiting the facility then defeat strategies are needed for entry and exit. The following information is needed for each strategy:

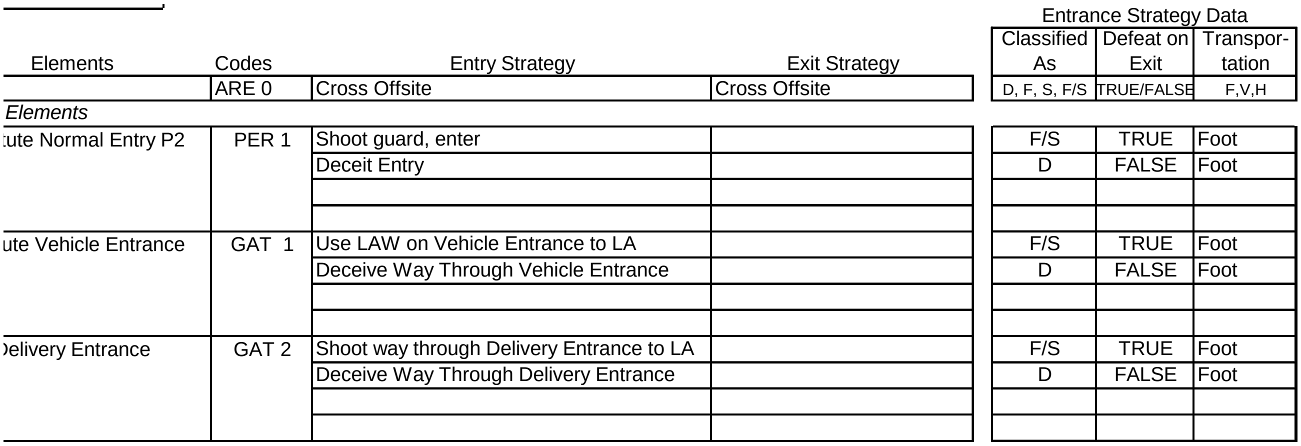
- Strategy name
- Direction—entry or exit
- Classification—Force (F), Stealth (S), Deceit (D), or (F/S)
- Exit Damage—Does the entry strategy disable the element detection and delay components for the exit path? The table below summarizes when exit damage is encountered for a path element strategy.

Adversary Tactic	Exit Damage ?
Force	True
Stealth	True or False
Deceit	False

- Transportation—on foot, in a land-vehicle, or by helicopter

Exit strategies and performance values

If the response strategy is containment (that is, the adversary is prevented from leaving the site with stolen material), then PANL needs to have strategies and performance data for elements for exit as well as entry. As a general rule, we suggest using primarily force or stealth strategies on exit to cut down on computational time; however, users can define deceit strategies if they prefer. (It is important to note that PANL will not allow deceit strategies to be used after the CDP.)



				Entrance Strategy Data		
Elements	Codes	Entry Strategy	Exit Strategy	Classified As	Defeat on Exit	Transpor-tation
	ARE 0	Cross Offsite	Cross Offsite	D, F, S, F/S	TRUE/FALSE	F,V,H
Elements						
;ute Normal Entry P2	PER 1	Shoot guard, enter		F/S	TRUE	Foot
		Deceit Entry		D	FALSE	Foot
ute Vehicle Entrance	GAT 1	Use LAW on Vehicle Entrance to LA		F/S	TRUE	Foot
		Deceive Way Through Vehicle Entrance		D	FALSE	Foot
)elivery Entrance	GAT 2	Shoot way through Delivery Entrance to LA		F/S	TRUE	Foot
		Deceive Way Through Delivery Entrance		D	FALSE	Foot

Figure 19-8. Assigning Strategies to Each Element

19.4.4 Step 5—Define Define PPS Security Components and Assign Component Performance

Specify P_D and Delay Values for Each Path Element

PANL uses the concept of timely detection in analyzing PPS vulnerabilities. This requires the user to specify, for each path element and strategy, the following:

- probability of detection and delay time values
- location of detection, specifying the relative positioning of detection occurring before, half-way through, or after delay.

This specification can be performed by the user in one of two ways—informal or systematic.

In the informal approach, the user would manually list what components are at each element and then identify the probabilities of detection and delay times. Next, the user would move directly to step 6 to enter element detection probabilities, delay times, and locations of detection directly into PANL, in a similar fashion as data was generated and entered into VEASI.

In the systematic approach, the process for using PANL is built around generating probabilities of detection and delay times for components from a "standard" database and entering these into a number of worksheets that structure the calculations of the composite, element probabilities, and delay times for the user. The final composite answers for each path element must still be entered into PANL by the user, but the intermediate calculations are also stored by PANL.

This section will focus on the systematic approach, since the informal approach was discussed in the VEASI section. The systematic approach will be covered in three topics:

- Background on the PANL "standard" database
- Assigning security components and their performance to each protection layer
- Assigning delay and detection to each protection element

Types of Components in the Standard Database

PANL includes a standard database of security components categorized in the following way:

- Detection components:
    - Access control—providing detection for deceit strategies
    - Contraband and SNM detection—providing detection for deceit strategies
    - Human surveillance (by security officers or employees)—providing detection for stealth and force strategies
    - Intrusion detection (typically by sensors)—providing detection for stealth and force strategies
- Delay components
    - Barriers
    - Locks (associated with gates and doors)

- Security officers
- Target tasks

PANL also accounts for transit time, but this is assigned separately from component performance.

Database Values Depend on Adversary Tools and Equipment

Each component has delay times and detection probabilities assigned for an appropriate subset of the following categories of adversary tools and equipment:

- no equipment
- metal contraband (type not specified)
- radioactive material
- hand tools
- power tools
- high explosives
- small arms (using up to 7.62 mm ammunition)
- LAWs
- land vehicle (such as a car or truck)

Representative Performance Values

Initially, the delay and detection values for a protection element are selected from reference values in the standard databases. The reference values for safeguard performance are based on laboratory and field experiments or on engineering judgments. Safeguard performance depends upon initial quality, design, installation and maintenance procedures, security procedures, and adversary capabilities. It is expected that, over time, countries will make a determination whether the reference values are indeed accurate for their use.

PANL Data Assumptions

PANL assumes that PPS data links and alarm assessment units are reliable and that security procedures and maintenance are consistently performed. If these conditions are not true or if there are single-point vulnerabilities or other common-mode failures in the alarm system or procedures, then the reference values should be degraded to reflect realistic performance. Whenever possible, safeguard performance values should be obtained by tests conducted at the facility being evaluated.

Analyst Can Assign Values

The analyst can assign his own estimates where the reference values are unrealistic or where a sufficiently similar reference safeguard is not present.

Assigning security components and performance by protection layer

PANL collects information about which components are used and their performance on a protection layer, rather than element-by-element basis. This is done for two reasons:

- it encourages users to think in terms of balanced protection across layers, and
- in many cases, identical protection components and performance values are used on a layer, so this should simplify data entry.

PANL includes pick lists, such as that shown in Figure 19-9. The pick list shows the choices associated with a given component and are listed as the percentage of probability of detection. PANL users record choices for each layer on these lists and transfer the data into spreadsheets recording component data for each layer (see Figure 19-10).

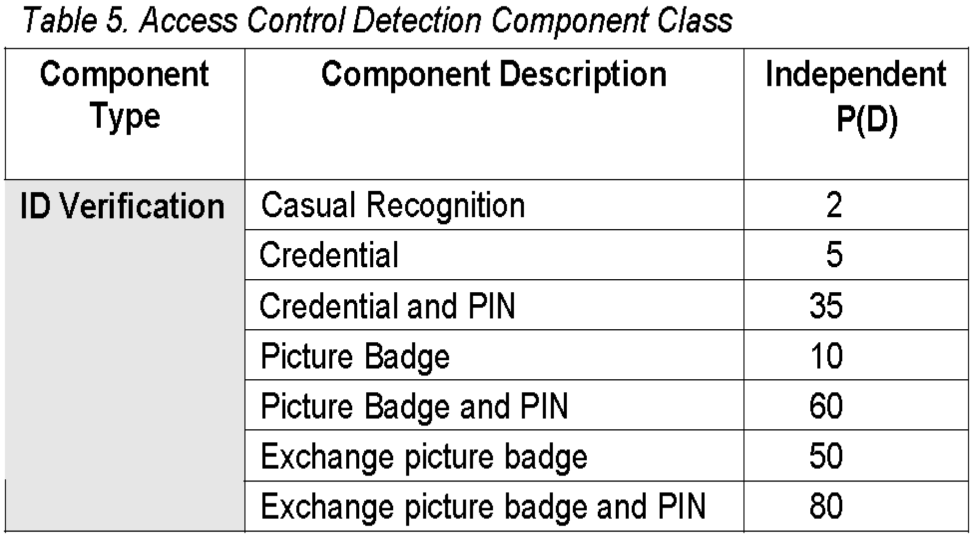


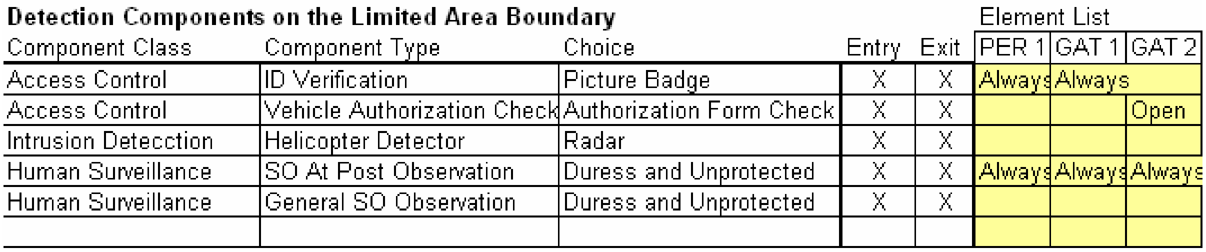
Table 5. Access Control Detection Component Class

Component Type	Component Description	Independent P(D)
ID Verification	Casual Recognition	2
	Credential	5
	Credential and PIN	35
	Picture Badge	10
	Picture Badge and PIN	60
	Exchange picture badge	50
	Exchange picture badge and PIN	80

Figure 19-9. Component Class Table for ID Verification Component and Associated Probability of Detection

Record component data on Protection Layer worksheets

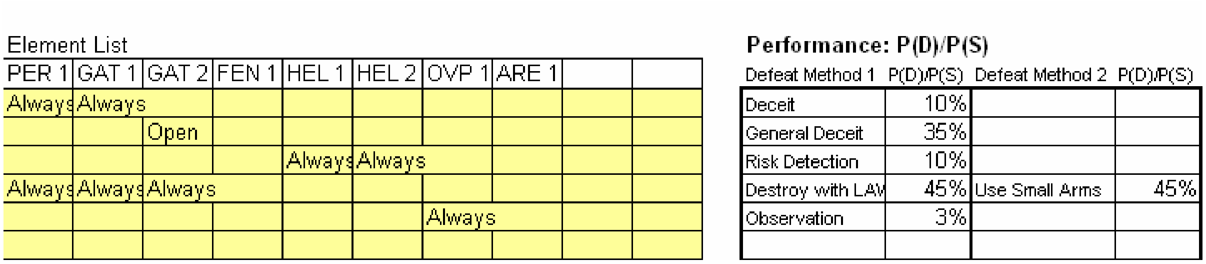
The protection layer sheets are completed by listing the security component (e.g., the picture badge in Figure 19-10) on the appropriate line and then assigning it to appropriate elements on that layer (in this case, the personnel portal, PER 1, and the two gates). The "Always" indicates the badge is always in use, whether the facility is open or closed; the "Open" under Gate GAT 2 indicates that the authorization form check is only used when the facility is open (that particular gate is non-operational during "Closed" conditions). Figure 19-11 shows ways that the components can be defeated along with the associated probabilities or delay times. In this figure, the picture badge has a probability of detection of 10% and the defeat method is given as "general" to indicate no further detail about the attack. (If the adversary had used explosives against a wall, then the appropriate defeat method would be "explosives.")



Detection Components on the Limited Area Boundary

					Element List		
Component Class	Component Type	Choice	Entry	Exit	PER 1	GAT 1	GAT 2
Access Control	ID Verification	Picture Badge	X	X	Always	Always	
Access Control	Vehicle Authorization Check	Authorization Form Check	X	X			Open
Intrusion Detecction	Helicopter Detector	Radar	X	X			
Human Surveillance	SO At Post Observation	Duress and Unprotected	X	X	Always	Always	Always
Human Surveillance	General SO Observation	Duress and Unprotected	X	X			

Figure 19-10. Component Choices Collected for a Protection Layer, Assigned to Elements, and with their Activity Noted



Element List

PER 1	GAT 1	GAT 2	FEN 1	HEL 1	HEL 2	OVP 1	ARE 1		
Always	Always								
		Open							
				Always	Always				
Always	Always	Always							
						Always			

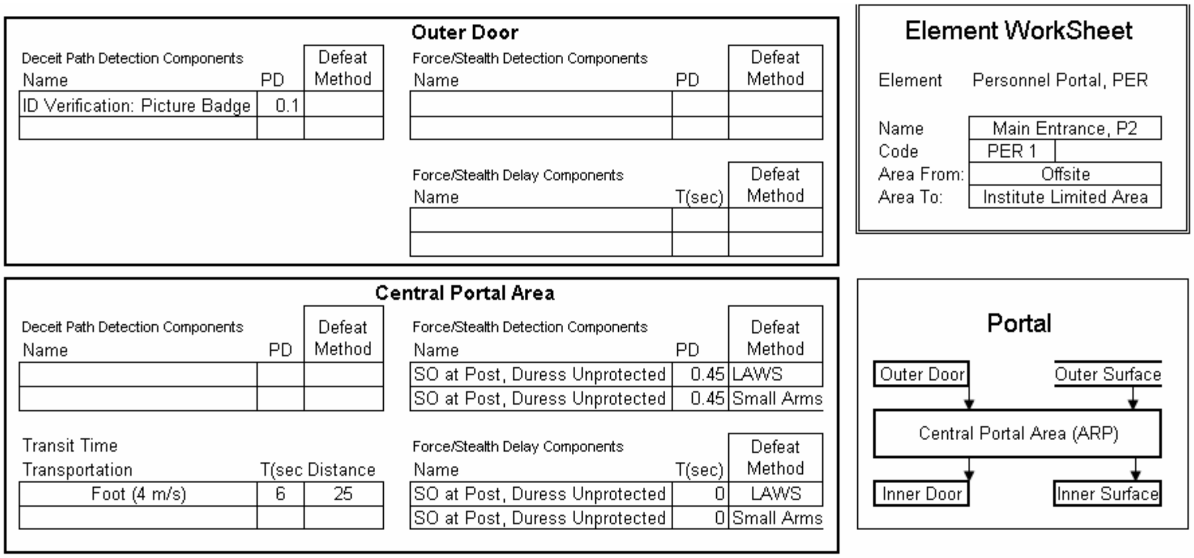
Performance: P(D)/P(S)

Defeat Method 1	P(D)/P(S)	Defeat Method 2	P(D)/P(S)
Deceit	10%		
General Deceit	35%		
Risk Detection	10%		
Destroy with LAW	45%	Use Small Arms	45%
Observation	3%		

Figure 19-11. Adversary Defeat Method and Performance Data Entered for Detection Components

Assign delay and detection to each protection element using element worksheets

The information about components at each element can then be displayed in one place to help calculate probability of detection, delay times, and location of detection at that element. Figure 19-12 shows a worksheet that serves as an aid in this process that represents a complex element called a Personnel Portal. Each portal has an outer door (and surface) as well as an inner door, an inner surface, and a central screening area. The worksheet organizes the component data for that element by which part of the portal it is associated with (the outer door and central portal area are displayed).



Outer Door

Deceit Path Detection Components

Name	PD	Defeat Method
ID Verification: Picture Badge	0.1	

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

Central Portal Area

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

Name	PD	Defeat Method
SO at Post, Duress Unprotected	0.45	LAWS
SO at Post, Duress Unprotected	0.45	Small Arms

Transit Time

Transportation	T(sec	Distance
Foot (4 m/s)	6	25

Force/Stealth Delay Components

Name	T(sec)	Defeat Method
SO at Post, Duress Unprotected	0	LAWS
SO at Post, Duress Unprotected	0	Small Arms

Element WorkSheet

Element	Personnel Portal, PER
Name	Main Entrance, P2
Code	PER 1
Area From:	Offsite
Area To:	Institute Limited Area

Figure 19-12. Part of the Portal Element Worksheet

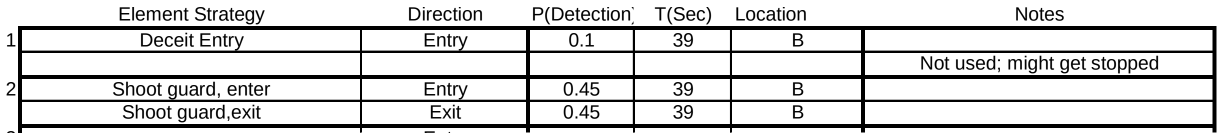
19.4.5 Step 6—Define VEASI Performance for each Strategy: P_D, Total Delay, and Location of Detection

Element Worksheets support these calculations

The information about each element is then combined to calculate probability of detection, delay times, and location of detection. Figure 19-13 displays part of the portal worksheet that shows the strategies created for the PER 1 portal. There is one deceit strategy listed, with no exit deceit strategy (we assume that the adversary no longer uses deceit on exit for this analysis) while the force/stealth strategy of shooting the guard has similar performance on both entry and exit.

Containment Response Strategy

When a containment response strategy is used, the analyst must be sure to include performance data for elements along the exit path from the target as well as the entry path. Exit performance values are not needed if the response strategy is denial.

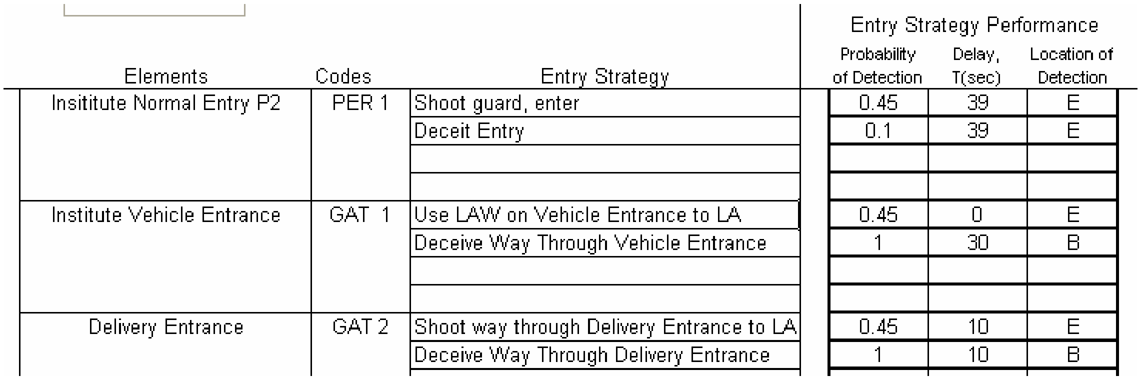


	Element Strategy	Direction	P(Detection)	T(Sec)	Location	Notes
1	Deceit Entry	Entry	0.1	39	B	
						Not used; might get stopped
2	Shoot guard, enter	Entry	0.45	39	B	
	Shoot guard,exit	Exit	0.45	39	B	

Figure 19-13. Strategy Section of the Portal Element Worksheet

Worksheet Data are Then Entered into PANL

However performance data is created—whether informally or systematically—it is then entered directly into PANL (see Figure 19-14). The figure shows entry performance; exit performance is entered in another section of the worksheet.



			Entry Strategy Performance		
Elements	Codes	Entry Strategy	Probability of Detection	Delay, T(sec)	Location of Detection
Insititute Normal Entry P2	PER 1	Shoot guard, enter	0.45	39	E
		Deceit Entry	0.1	39	E
Institute Vehicle Entrance	GAT 1	Use LAW on Vehicle Entrance to LA	0.45	0	E
		Deceive Way Through Vehicle Entrance	1	30	B
Delivery Entrance	GAT 2	Shoot way through Delivery Entrance to LA	0.45	10	E
		Deceive Way Through Delivery Entrance	1	10	B

Figure 19-14. Performance Data Entered by Element and Element Strategy

Exit effects of passing through an element on entry

A complication in analysis codes is that actions taken on the entry path may affect performance on the exit. If an element is passed through on entry then either detection, delay, or both at that element on exit will stay the same or decrease. An example would be a wall presenting a 60-second delay: if the adversary breaches through that wall on entry and also on exit, then the exit delay may be greatly reduced.

For delay components, exit delays are always set to zero if the element was used on entry. This rule prevents the possibility that the delay from the same component could be counted twice. This effect can be different, depending on whether the adversary strategy on entry was identified as forceful, stealthy, or deceitful.

- **Force**: If an adversary strategy is forceful, it is assumed that the exit damage variable will be set to true. In such a case, both detection and delay at the element will not occur on exit, leaving only the transit time across that element.

- **Stealth**: Stealth typically involves attempting to minimize detection, which can mean that the adversary will not attempt to degrade detection or delay at the element on entry. In such cases, the user might set the "exit damage" variable to false to indicate that detection and delay features can still be operating on exit. For example, notice in Figure 19-8 that exit damage is set to false for climbing over the outer walls and guard barracks because it is assumed that none of the detection and delay components are compromised by sneaking in. Be aware, though, that if the "exit damage" flag is set to false, that user should only assign a component's effectiveness on entry or exit so as not to double-count that detection or delay. Note that if the "exit damage" flag is set to true, then the element behaves as described above under the force description.
- **Deceit**: Deceit is similar to stealth in that the adversary is minimizing detection; in this case, however, the adversary is attempting to appear authorized in doing so. The "exit damage" variable is disabled (set to "NA" in the software), as PANL assumes that no exit damage exists after deceit on entry.

19.4.6 Step 7—Define Response Force Characteristics

Define Response Force

The response force must be defined in terms of response force strategy and RFT.

Response Force Strategies: Denial or Containment

The response force strategy refers to how the response attempts to defeat the adversary attack. The PANL model allows two types of response force strategies:

- ***Denial***: The response attempts to defeat the adversary force ***before it can cause sabotage or acquire material to steal at the target***. A denial response strategy is typically used to protect against sabotage by attacking forces. A denial analysis is also referred to as an "entry-only analysis" because it analyzes paths from off site to the target task, but ignores the exit part of the path.

- ***Containment***: The response attempts to defeat the adversary force ***before it can leave the site***, crossing to the Offsite Area after visiting the target. A containment response strategy is typically used to protect against theft when it is acceptable to allow the adversary force to acquire the material because they will be contained leaving the site. For containment, all paths from off site to the target and back off site again are analyzed.

Denial or containment can be used to protect against theft.
Warning: the current version of PANL takes much longer to analyze against a containment strategy than for a denial strategy. Be sure to analyze against a denial strategy – just to see if there are data entry problems – so that you know most of the data are correct before you run containment.

Planned Deployment Location Depends on Strategy

The RFT is the time in which the response force arrives at the planned deployment location after receiving the first alarm. The planned deployment location depends upon the response strategy:

- for ***denial,*** the deployment location is at the target;
- for ***containment***, the deployment location is around the perimeter.

Factors in the RFT Value

The RFT includes assessment, communication, and deployment time (the same definition used for VEASI). The specified value of RFT should be based on actual field trials or on estimated performance. The analyst should use RFT values that reflects the deployment time associated with a sufficient number of response persons to interrupt and neutralize the specified threat. Up to five RFTs can be entered for analysis.

19.4.7 Step 8—Analyze and Review the Results

PANL Outputs:

Once data entry is complete, PANL can be run to determine the value of P_I for the most vulnerable path through the ASD for each RFT (up to five are allowed). PANL shows three types of results:

- Sensitivity graph: How does worst-case P_I vary as a function of RFT?
- What is minimum P_I across all paths:
  - Through each element on entry
  - Around each element (as if it was not in the ASD)
- What does the most vulnerable path look like and what is its P_I?
- Results shown in VEASI

PANL Outputs: Path performance metrics are displayed and how they are ranked

The PANL code determines the value of P_I for most vulnerable paths through the ASD. The value of P_I is shown along with the location of the CDP and the secondary vulnerability measures Detection Potential and Time Remaining after Interruption. Though the P_I is the most important measure of vulnerability, it is also necessary to consider how deeply the CDP falls within the ASD and the size of the Time Remaining after Interruption, which represents the time remaining on a path after interruption occurs. The depth of the CDP is measured with Detection Potential, which is the number of points on the path prior to and including the CDP where detectors could be installed (recognize that not all are in place). A path with a low detection potential is more vulnerable than a path with a high Detection Potential, given equal P_Is. If two paths have the same P_I and Detection Potential, then they are ranked by Time Remaining after Interruption. The path with the smaller Time Remaining after Interruption is the more vulnerable.

P_I Sensitivity Graph

Figure 19-15 shows the Sensitivity Graph of how the P_I for the most vulnerable path varies as RFT changes from 60 up to 168 seconds. Be aware that the most vulnerable path for one RFT (such as 60 seconds) does not have to be the same as the most vulnerable path for another RFT (such as 124 seconds).

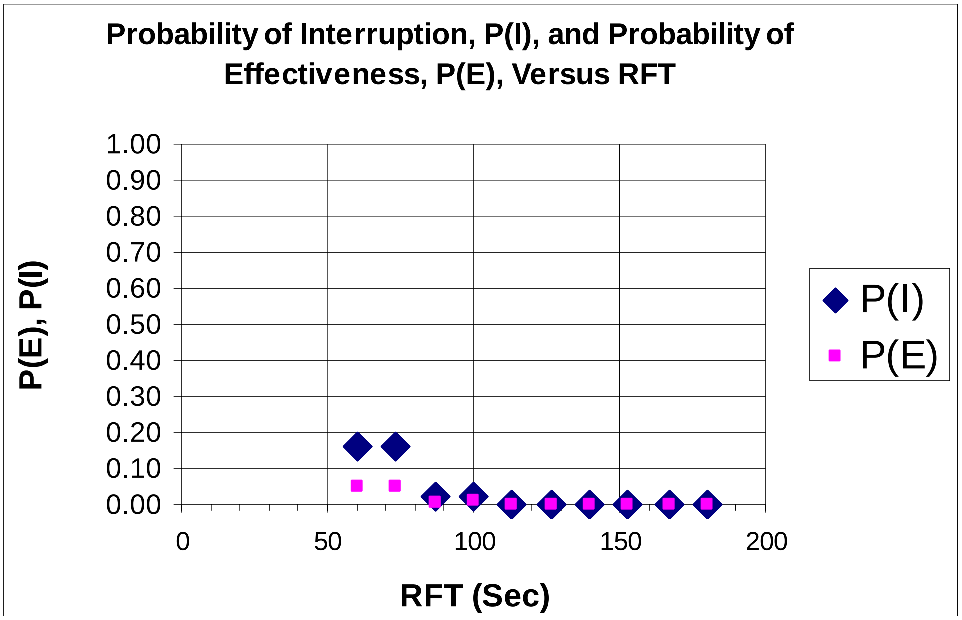


Figure 19-15. Sensitivity Graph of RFT Versus P_I

Estimates of the Probabilities of Interruption

The PANL P_I values represent the best point estimates of the P_I, assuming that the component values are realistic. Although conservative estimates of component values are used, some analysts will be concerned that the resulting P_I values do not accurately reflect actual PPS vulnerabilities. In this case, they can put lower estimates on the component values. It is important to realize that the P_I measure provides a relative ranking among paths and should be used as a measure of PPS effectiveness only after confirming these results with field tests and including an estimate of probability of neutralization.

Minimum PI Through and Around Each Element are Listed

Because PANL examines PI on every path in trying to find the best one, it also records the minimum value of P_I:

- through each element on entry, P_{IT}
- around each element (as if it was not in the ASD)

These can be of value in determining upgrades for elements. If there is an element where the minimum P_I through it is below the desired design P_I, $P_{I(desired)}$, then upgrades are needed on that element or on elements on previous or succeeding layers. In this case, the particular element might be usefully upgraded. On the other hand, if minimum P_I around that element is below $P_{I(desired)}$ then upgrades at that element alone will not be sufficient; thus, other elements will have to be upgraded also. Some elements, such as target elements, may be common to all paths.

In such cases, the minimum P_I around the element is set equal to 1.

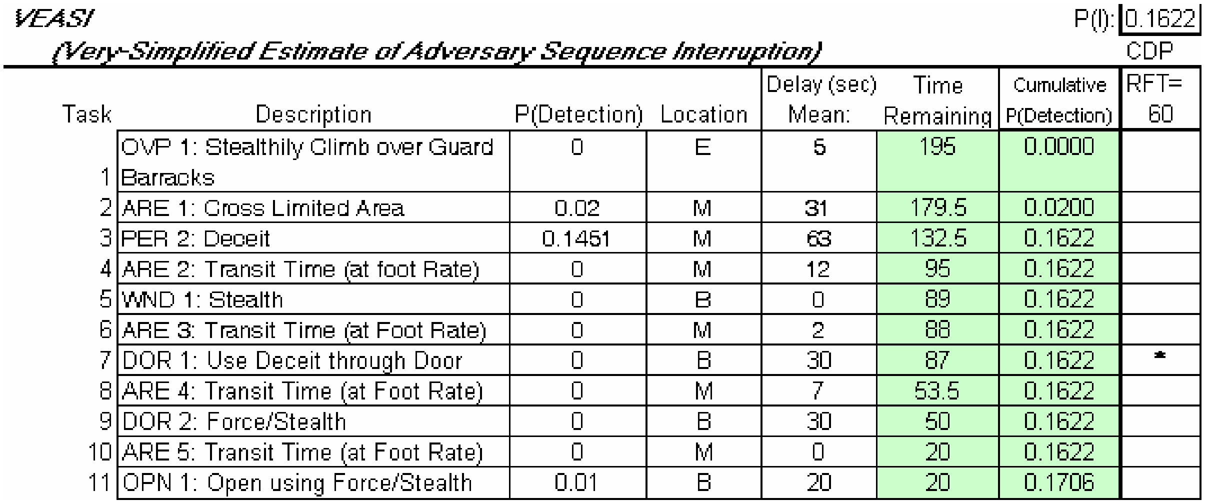
PANL Provides Detailed Description

A detailed description of the selected path is also given in the VEASI format (see Figure 19-16).

If the response strategy is…

- ***denial***, then the path is entry-only, leading from offsite to the target, and the path is represented by a single heading, "ENTRY".
- ***containment***, then the path leads from offsite into the target and back out; the path is divided into both "ENTRY" and "EXIT" headings.
-

The CDP, if one exists, is identified with a "*" pointing to the task where the critical detection does occur. PANL also shows the cumulative Probability of Detection, without consideration of timeliness. The cumulative delay along the path is also shown.



VEASI

(Very-Simplified Estimate of Adversary Sequence Interruption)

P(I): 0.1622

CDP

Task	Description	P(Detection)	Location	Delay (sec) Mean:	Time Remaining	Cumulative P(Detection)	RFT= 60
1	OVP 1: Stealthily Climb over Guard Barracks	0	E	5	195	0.0000	
2	ARE 1: Cross Limited Area	0.02	M	31	179.5	0.0200	
3	PER 2: Deceit	0.1451	M	63	132.5	0.1622	
4	ARE 2: Transit Time (at foot Rate)	0	M	12	95	0.1622	
5	WND 1: Stealth	0	B	0	89	0.1622	
6	ARE 3: Transit Time (at Foot Rate)	0	M	2	88	0.1622	
7	DOR 1: Use Deceit through Door	0	B	30	87	0.1622	*
8	ARE 4: Transit Time (at Foot Rate)	0	M	7	53.5	0.1622	
9	DOR 2: Force/Stealth	0	B	30	50	0.1622	
10	ARE 5: Transit Time (at Foot Rate)	0	M	0	20	0.1622	
11	OPN 1: Open using Force/Stealth	0.01	B	20	20	0.1706	

Figure 19-16. Path Display

19.4.8 Step 9—Perform Sensitivity Analyses

Determine Effects of Changes

Sensitivity analyses are performed on a PPS design to determine the effect of changes in the elements and safeguards and in the response capabilities. This is an important step that investigates the sensitivity of results to suspected uncertainties in safeguard performance. ***An intelligent analysis can reveal places where relatively small changes can produce significant improvements in PPS effectiveness.*** It can also reveal whether small changes in RFT can result in large changes in P_I. Because RFT affects all paths, PANL allows the analyst to vary the RFT over a specified range and then calculates the P_I of the most vulnerable paths for each RFT. The Sensitivity Graph depicts the variation in the worst-case P_I as RFT changes.

Detailed Analysis of a Single Path

Detailed analysis of a single path is usually done after PANL has calculated the P_Is for a PPS that has been configured by a specific ASD. Any of the vulnerable paths listed by PANL can be analyzed in VEASI to determine the effect of changing elements on the path, components in an element, area or element transit times, and RFT. The cost and effectiveness of alternatives are compared, and any significant ways to improve the system are recorded.

Analyses to determine the sensitivity of the PPS to changes in the RFT are extremely useful. The uncertainty in the response time can be large. Thus, paths that do not have considerable surplus time after interruption, using the best point estimate of RFT, are candidates for upgrade.

19.4.9 Step 10—Perform Upgrade Analyses

Consider Possible Upgrades

PANL does not determine whether the P_I values are acceptable; the analyst must make that determination. PANL does provide assistance for the analyst in considering possible upgrades to the most vulnerable paths. PANL provides:

- the summary of element performance for each layer, allowing the analyst to examine the detection and delay values across each layer to determine if there are weaknesses in detection at layers before the CDP or weaknesses in delay at layers after the CDP.
- a graph showing the $\boldsymbol{P_I}$ for the most vulnerable path and
- a description of the vulnerable path with a "*" that indicates the CDP and whether it is on the entry or exit part of the path.

The path can be upgraded by adding detectors to path segments prior to and including the CDP. Adding them at the beginning of the path is generally preferred if costs of alternatives are about the same. A path can also be upgraded by adding delay to path segments past the CDP. Adding delays close to the target or at the surfaces and entryways of buildings and rooms is generally preferred.

Determining upgrades

The analyst determines whether the:

- P_I values are too low for some paths.
- vulnerability is caused by inadequate detection, not enough delay, or both.

Furthermore, even though P_I is adequate, the analyst may decide that Time Remaining after Interruption is marginal and that more delay is needed to ensure response arrival. PANL also displays the path time remaining after the CDP as well as the interruption time surplus or deficiency to assist the user in making this determination.

Test Several Ways to Improve

Typically, there will be several ways to improve performance. These

Performance

alternatives can be tested for effectiveness in PANL by modifying the detection and delay values at the elements involved and then re-analyzing. Once it is clear that the upgrades do provide the required performance, the analyst can then go back to the element worksheets and make those changes incorporating the appropriate components.

Protection May Not Be Balanced

The analyst may determine that protection is not balanced, with some paths having too little or too much delay or detection relative to other paths. Some paths may not have protection in depth and instead concentrate protection in a single element. It is good design practice to obtain the required P_I by using more than one layer of protection.

Consider Upgrade Alternatives

A number of upgrade alternatives should be considered before a final upgrade design is selected. Both hardware and response force upgrades should be considered, and the compromises between detection, delay, and response studied. For example, it may be more cost effective to reduce the response deployment time by stationing forces at different locations than by adding concrete walls.

Seek Common Elements

In reviewing the vulnerable paths, an element that is common to many paths should be sought. The addition of an element that is not in the current ASD should be considered especially if it can reduce vulnerabilities that are common to many paths. There may be upgrades that produce large changes in PPS effectiveness for small costs.

Reconsider Values to Ensure They Are Justified

A survey of all of the most vulnerable paths should be made before any upgrade decisions are made. If all of the paths have very high P_Is, then it is likely that unrealistic values of component detection and delay were selected. The analyst should reconsider these values to be sure that they are justified.

Determining How Much Protection Is Enough

Typically a National Authority sets performance levels P_{EL} and P_{EC}, where where $P_{EL} > P_{EC}$. Licenses would be approved if the facility performance is above P_{EL} (as achieving low risk) while facilities with P_E falling between P_{EC} and P_{EL} would have moderate risk and be given a conditional license, where there might be a need to take temporary measures while a risk reduction plan was being implemented.

Desired P_I and Required P_I Levels

Within the low-risk category, it may be useful to further define a desired Performance Level, $P_{E(Desired)}$ and a Required Performance Level, $P_{E(Required)}$. In terms of PANL, such an approach can be used to determine desired and required levels of P_I for a target based on a known P_N:

Desired Facility P_I Level $=P_{E(Desired)}/P_N$
Required Facility P_I Level $=P_{E(Required)}/P_N$
A smaller value of P_N requires higher Desired and Required P_I Levels.

19.5 Summary

Uses of PANL

The PANL code uses the ASD to evaluate the effectiveness of the PPS at a facility. It identifies the paths that adversaries can follow to accomplish sabotage or theft. For a specific PPS and threat, the most vulnerable path can be determined. The path P_I establishes the effectiveness of the total PPS.

Review of PANL Functions

The use of PANL to analyze the P_I against an outsider threat can be illustrated by the following PANL Functional Diagram (Figure 19-17). This diagram incorporates most of the PANL instructions that were given in this course, and will serve as a good review.

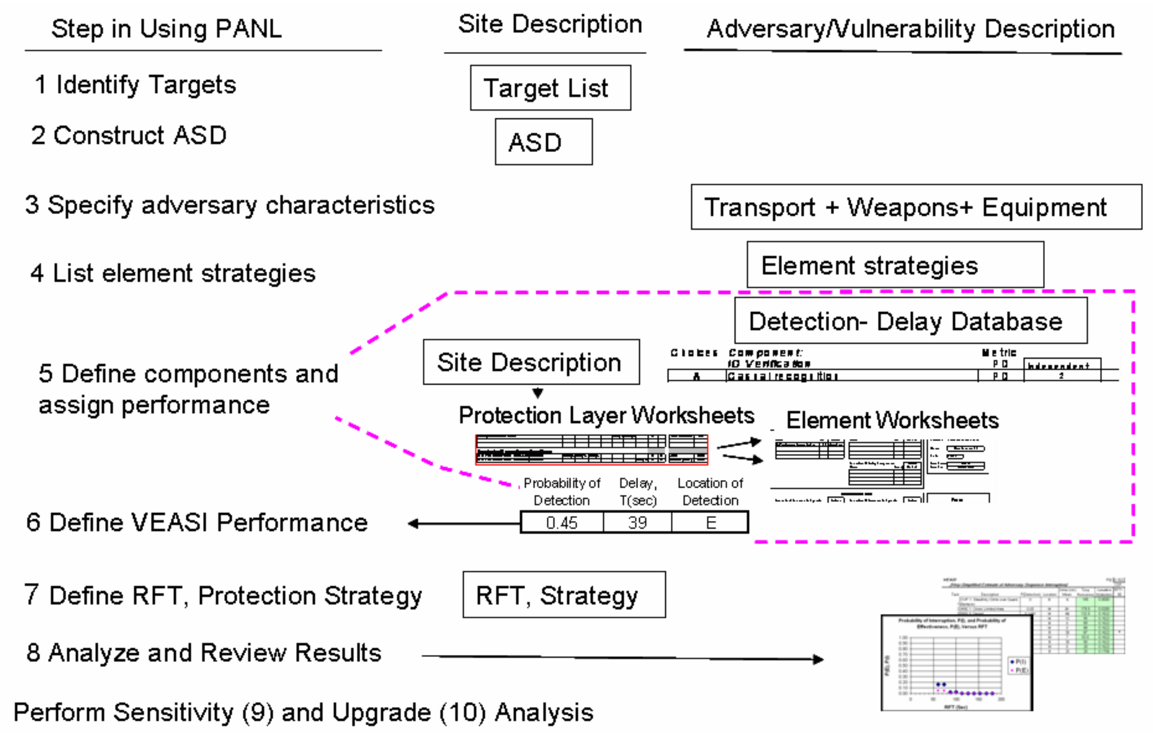
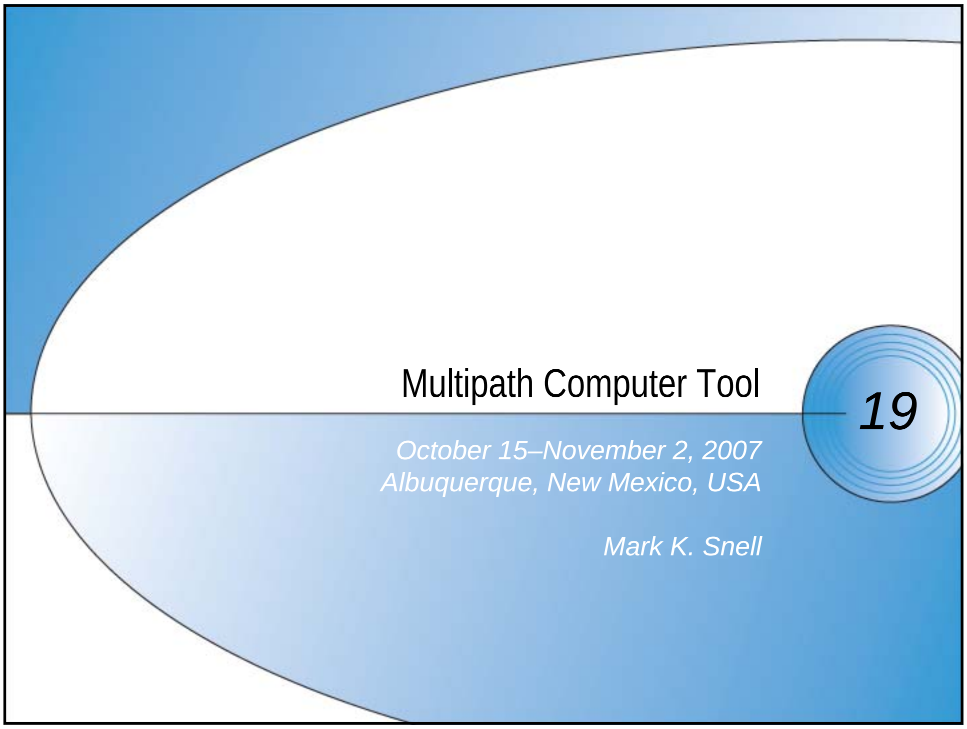

Step in Using PANL
Site Description
Adversary/Vulnerability Description
1 Identify Targets
Target List
2 Construct ASD
ASD
3 Specify adversary characteristics
Transport + Weapons+ Equipment
4 List element strategies
Element strategies
Detection- Delay Database
5 Define components and assign performance
Site Description
Protection Layer Worksheets
Element Worksheets
Probability of Detection
Delay, T(sec)
Location of Detection
6 Define VEASI Performance
0.45
39
E
7 Define RFT, Protection Strategy
RFT, Strategy
8 Analyze and Review Results
Perform Sensitivity (9) and Upgrade (10) Analysis

Figure 19-17. PANL-4 Functional Diagram

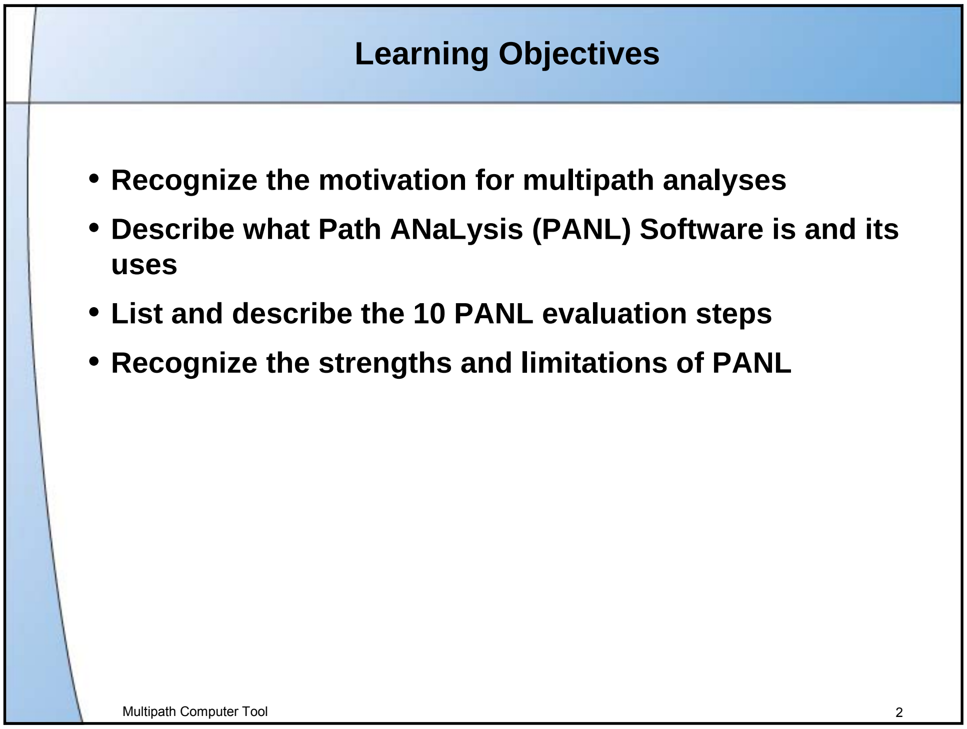


Multipath Computer Tool

19

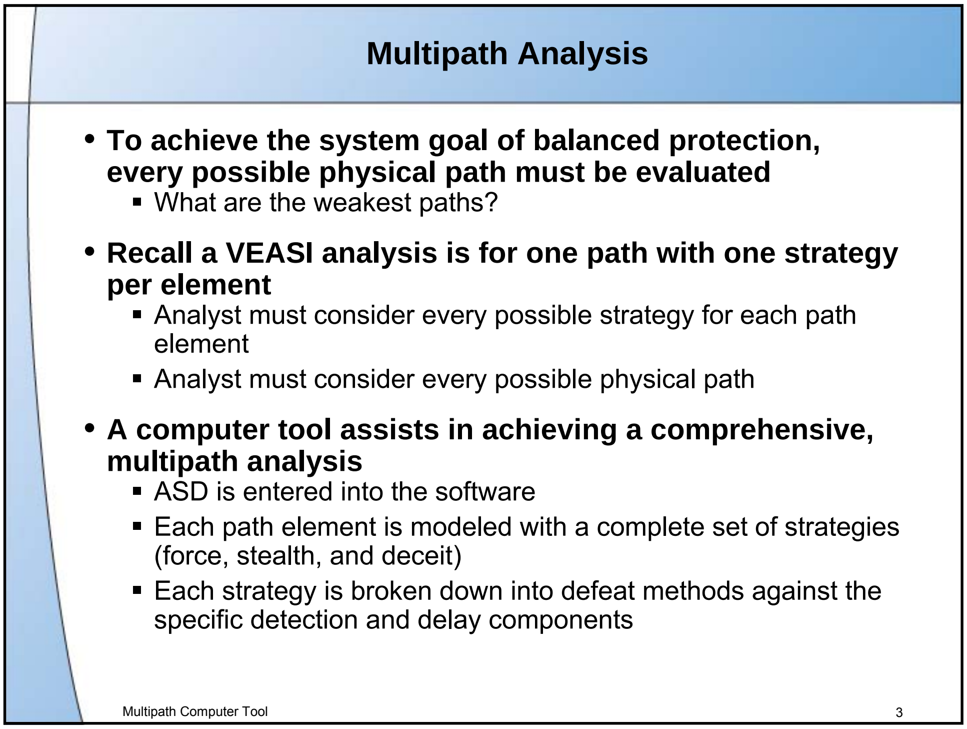
October 15–November 2, 2007
Albuquerque, New Mexico, USA

Mark K. Snell



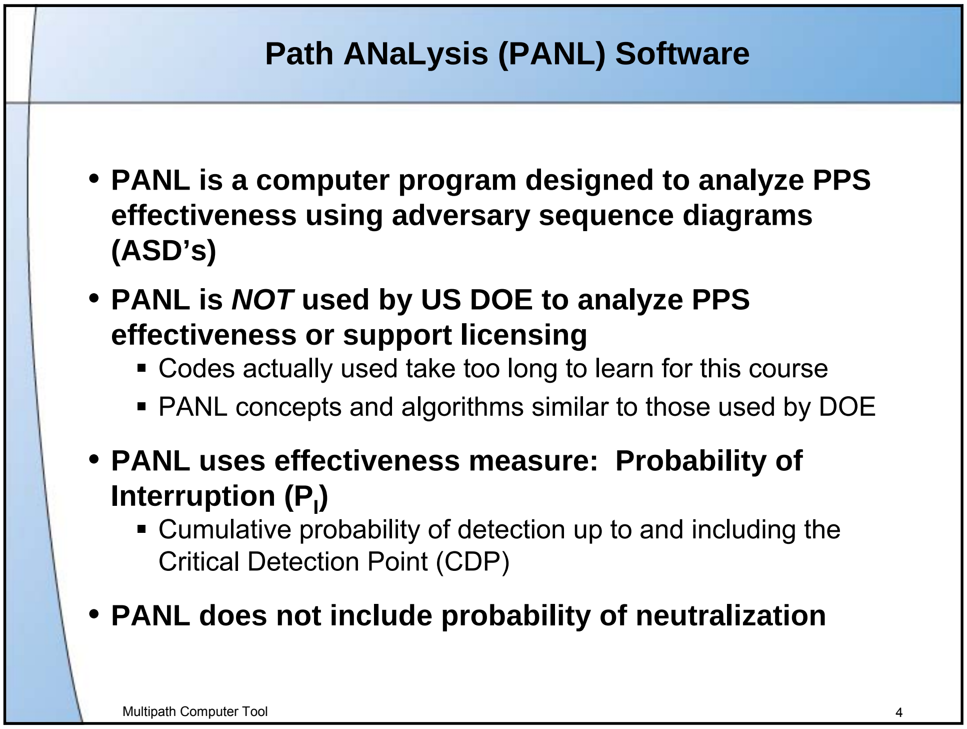
Learning Objectives

- Recognize the motivation for multipath analyses
- Describe what Path ANaLysis (PANL) Software is and its uses
- List and describe the 10 PANL evaluation steps
- Recognize the strengths and limitations of PANL



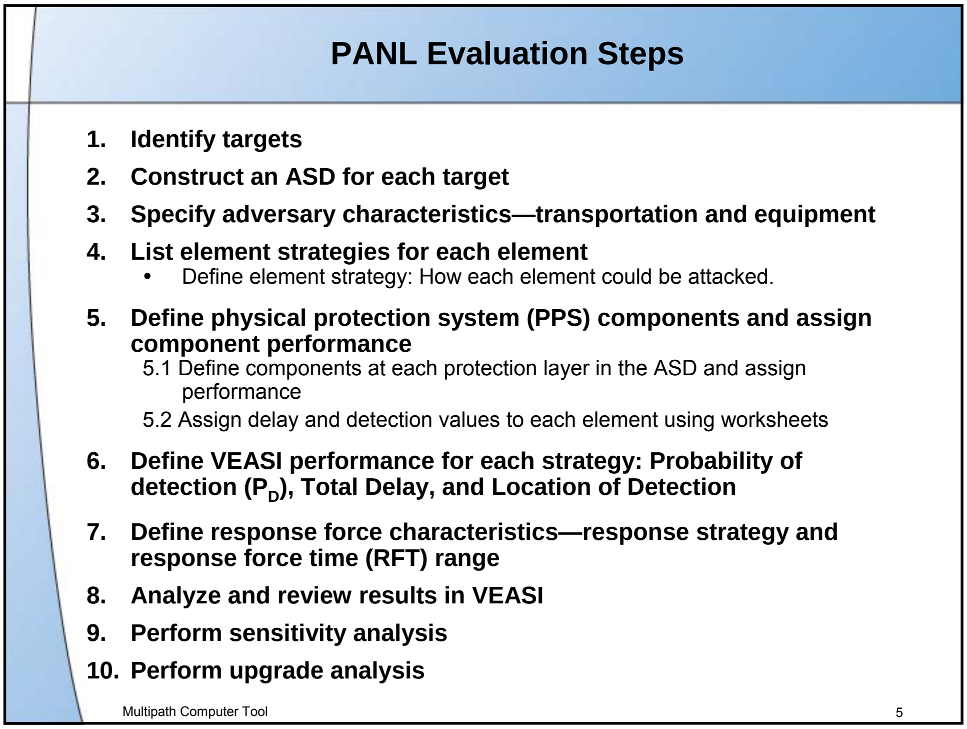
Multipath Analysis

- **To achieve the system goal of balanced protection, every possible physical path must be evaluated**
  - What are the weakest paths?
- **Recall a VEASI analysis is for one path with one strategy per element**
  - Analyst must consider every possible strategy for each path element
  - Analyst must consider every possible physical path
- **A computer tool assists in achieving a comprehensive, multipath analysis**
  - ASD is entered into the software
  - Each path element is modeled with a complete set of strategies (force, stealth, and deceit)
  - Each strategy is broken down into defeat methods against the specific detection and delay components



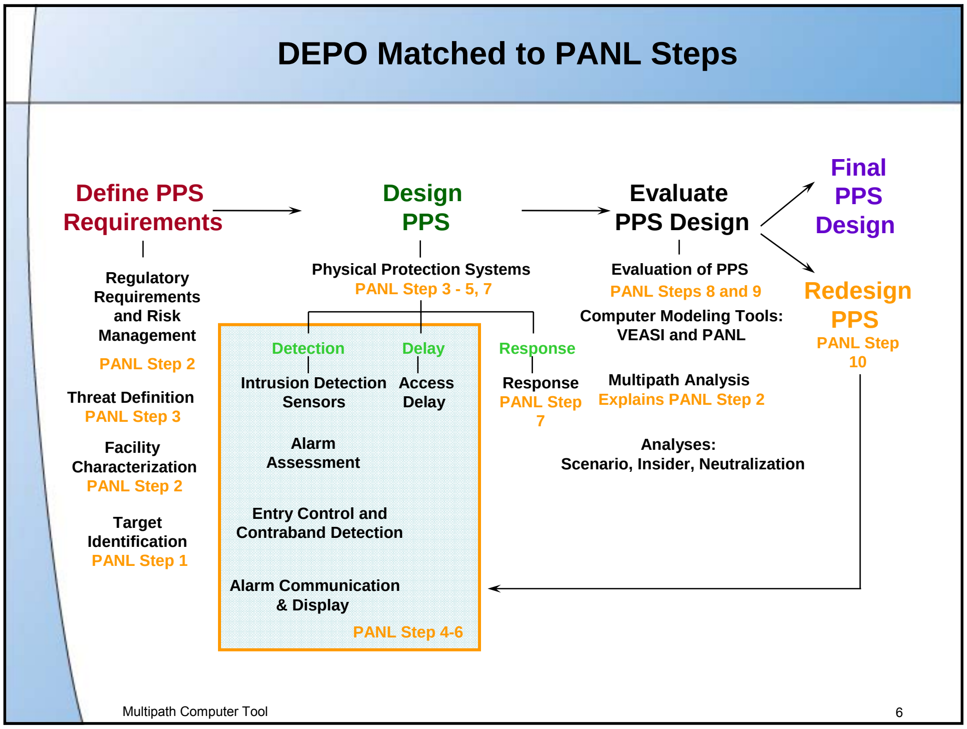
Path ANaLysis (PANL) Software

- **PANL is a computer program designed to analyze PPS effectiveness using adversary sequence diagrams (ASD's)**
- **PANL is *NOT* used by US DOE to analyze PPS effectiveness or support licensing**
  - Codes actually used take too long to learn for this course
  - PANL concepts and algorithms similar to those used by DOE
- **PANL uses effectiveness measure: Probability of Interruption (P_I)**
  - Cumulative probability of detection up to and including the Critical Detection Point (CDP)
- **PANL does not include probability of neutralization**



PANL Evaluation Steps

1. **Identify targets**
2. **Construct an ASD for each target**
3. **Specify adversary characteristics—transportation and equipment**
4. **List element strategies for each element**
   - Define element strategy: How each element could be attacked.
5. **Define physical protection system (PPS) components and assign component performance**
   - 5.1 Define components at each protection layer in the ASD and assign performance
   - 5.2 Assign delay and detection values to each element using worksheets
6. **Define VEASI performance for each strategy: Probability of detection (P_D), Total Delay, and Location of Detection**
7. **Define response force characteristics—response strategy and response force time (RFT) range**
8. **Analyze and review results in VEASI**
9. **Perform sensitivity analysis**
10. **Perform upgrade analysis**



DEPO Matched to PANL Steps

Define PPS Requirements

Regulatory Requirements and Risk Management
PANL Step 2

Threat Definition
PANL Step 3

Facility Characterization
PANL Step 2

Target Identification
PANL Step 1

Design PPS

Physical Protection Systems
PANL Step 3 - 5, 7

Detection
Intrusion Detection Sensors
Alarm Assessment
Entry Control and Contraband Detection
Alarm Communication & Display

Delay
Access Delay

PANL Step 4-6

Response
Response
PANL Step 7

Evaluate PPS Design

Evaluation of PPS
PANL Steps 8 and 9

Computer Modeling Tools: VEASI and PANL

Multipath Analysis
Explains PANL Step 2

Analyses:
Scenario, Insider, Neutralization

Final PPS Design

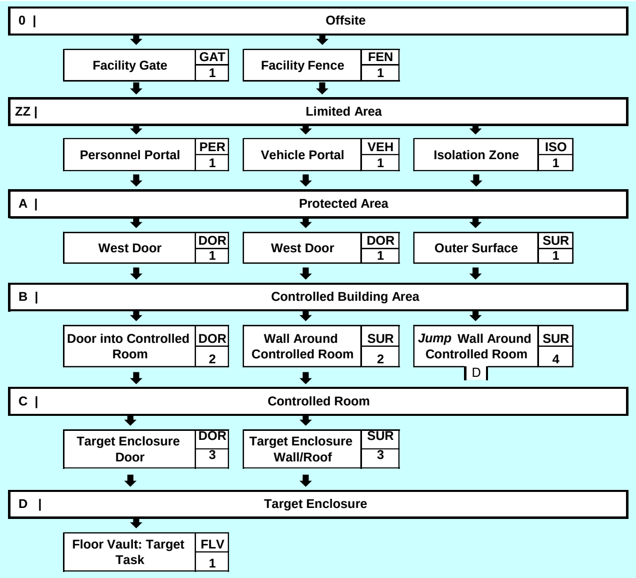
Redesign PPS
PANL Step 10

1. Identify Targets

- Sabotage targets
- Theft targets

2. Construct Target-Specific ASD (for each target and objective)

- Identify physical areas and protection layers
- Add these physical areas to ASD
- Add Path Elements (PE) present between physical area layers
- Modify layers and areas, if necessary, using jumps



0 | Offsite

Facility Gate GAT 1
Facility Fence FEN 1

ZZ | Limited Area

Personnel Portal PER 1
Vehicle Portal VEH 1
Isolation Zone ISO 1

A | Protected Area

West Door DOR 1
West Door DOR 1
Outer Surface SUR 1

B | Controlled Building Area

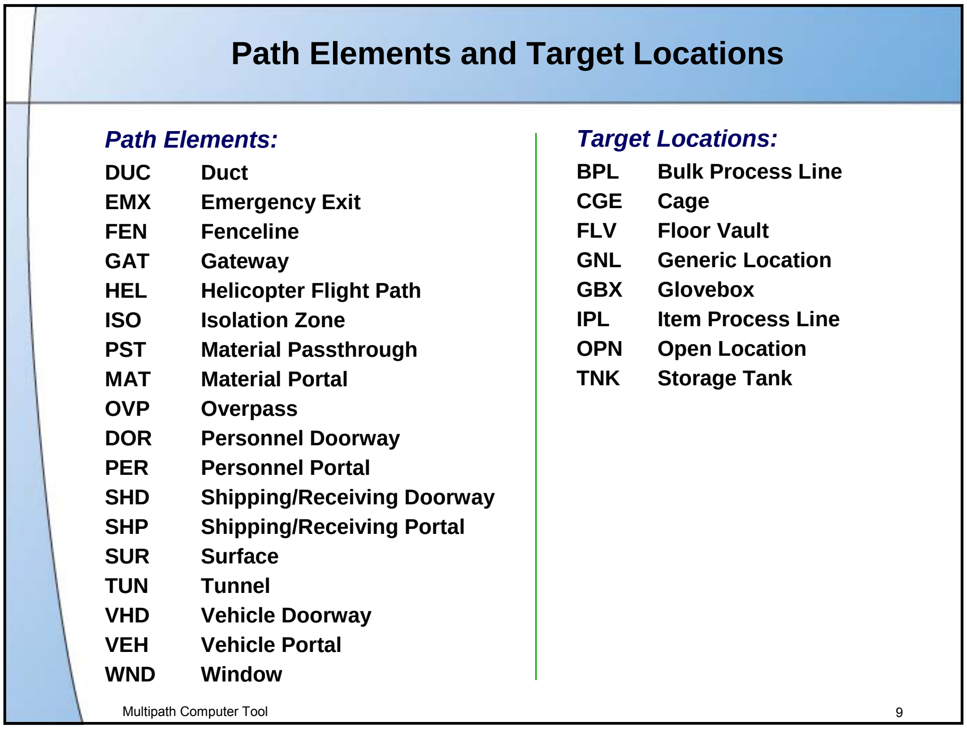
Door into Controlled Room DOR 2
Wall Around Controlled Room SUR 2
Jump Wall Around Controlled Room SUR 4
D

C | Controlled Room

Target Enclosure Door DOR 3
Target Enclosure Wall/Roof SUR 3

D | Target Enclosure

Floor Vault: Target Task FLV 1



Path Elements and Target Locations

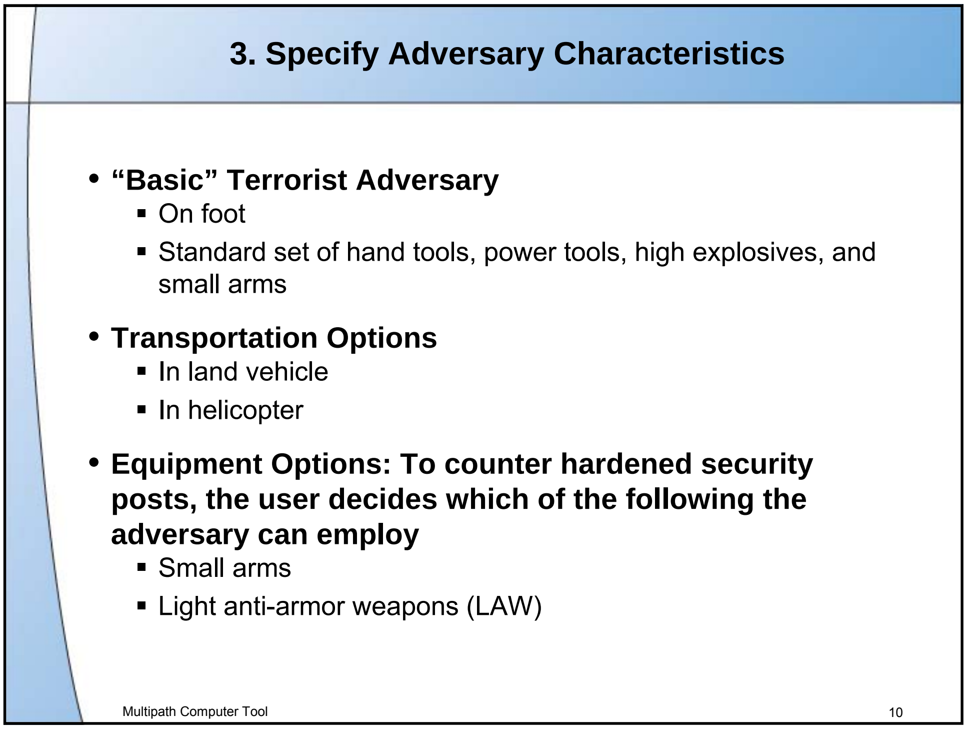
Path Elements:

DUC	Duct
EMX	Emergency Exit
FEN	Fenceline
GAT	Gateway
HEL	Helicopter Flight Path
ISO	Isolation Zone
PST	Material Passthrough
MAT	Material Portal
OVP	Overpass
DOR	Personnel Doorway
PER	Personnel Portal
SHD	Shipping/Receiving Doorway
SHP	Shipping/Receiving Portal
SUR	Surface
TUN	Tunnel
VHD	Vehicle Doorway
VEH	Vehicle Portal
WND	Window

Target Locations:

BPL	Bulk Process Line
CGE	Cage
FLV	Floor Vault
GNL	Generic Location
GBX	Glovebox
IPL	Item Process Line
OPN	Open Location
TNK	Storage Tank

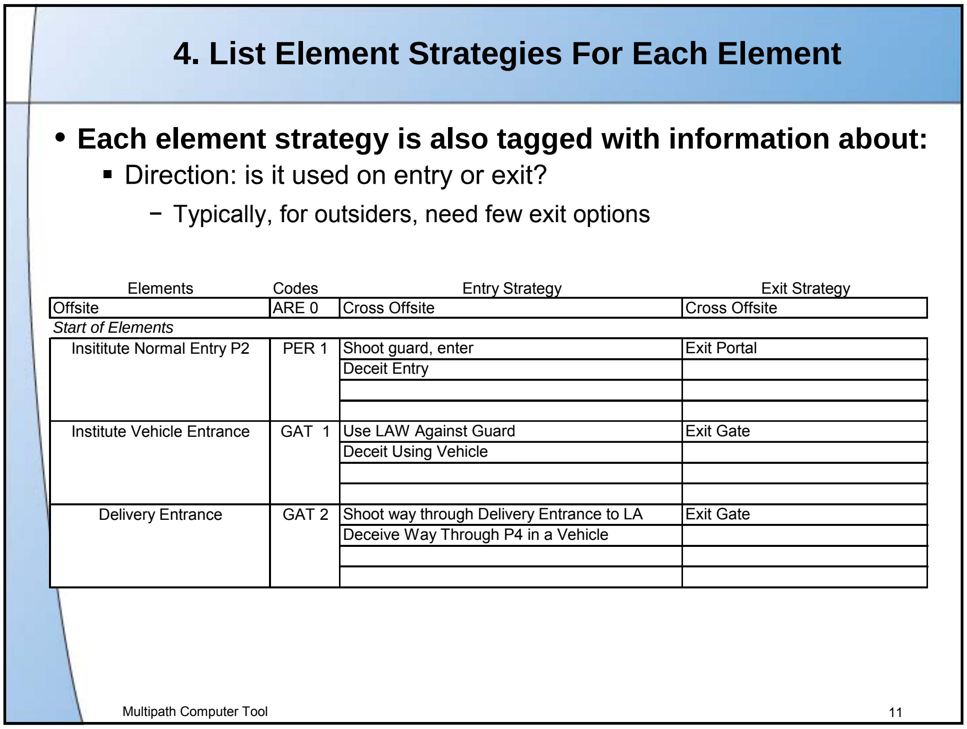
Multipath Computer Tool 9



3. Specify Adversary Characteristics

- **"Basic" Terrorist Adversary**
  - On foot
  - Standard set of hand tools, power tools, high explosives, and small arms
- **Transportation Options**
  - In land vehicle
  - In helicopter
- **Equipment Options: To counter hardened security posts, the user decides which of the following the adversary can employ**
  - Small arms
  - Light anti-armor weapons (LAW)

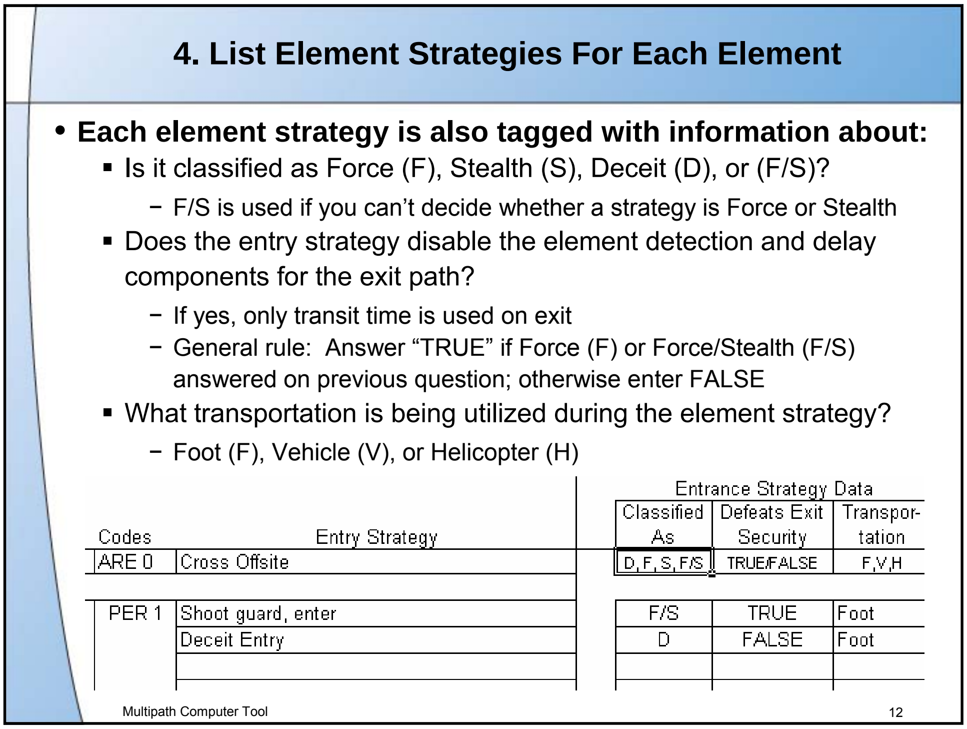
Multipath Computer Tool 10



4. List Element Strategies For Each Element

- **Each element strategy is also tagged with information about:**
  - Direction: is it used on entry or exit?
    - Typically, for outsiders, need few exit options

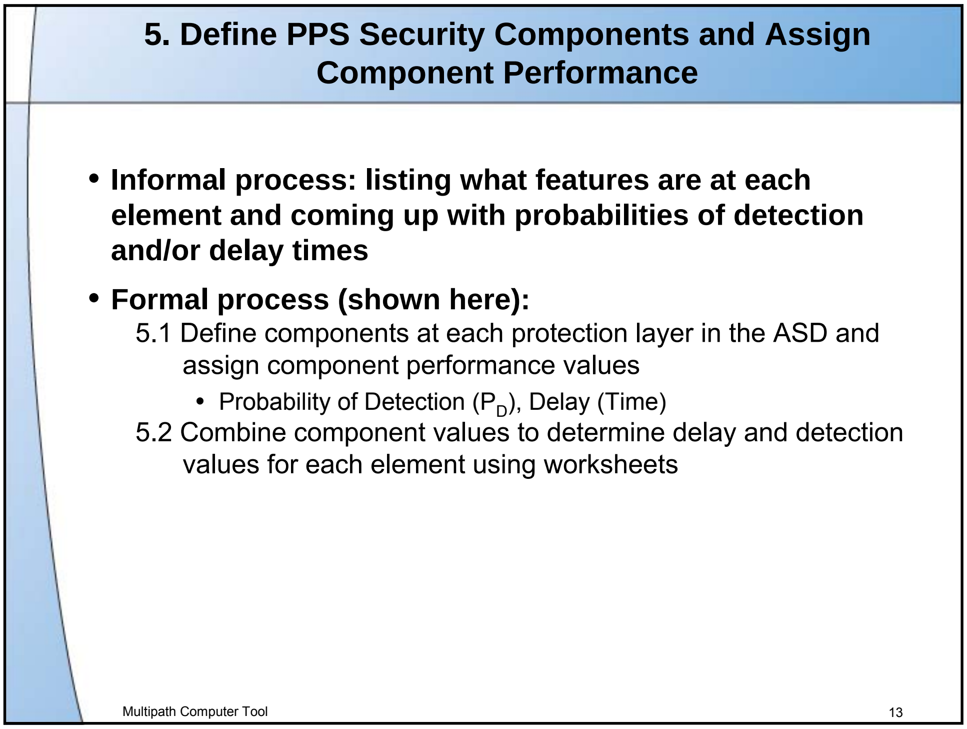
Elements	Codes	Entry Strategy	Exit Strategy
Offsite	ARE 0	Cross Offsite	Cross Offsite
Start of Elements			
Insititute Normal Entry P2	PER 1	Shoot guard, enter	Exit Portal
		Deceit Entry	
Institute Vehicle Entrance	GAT 1	Use LAW Against Guard	Exit Gate
		Deceit Using Vehicle	
Delivery Entrance	GAT 2	Shoot way through Delivery Entrance to LA	Exit Gate
		Deceive Way Through P4 in a Vehicle	



4. List Element Strategies For Each Element

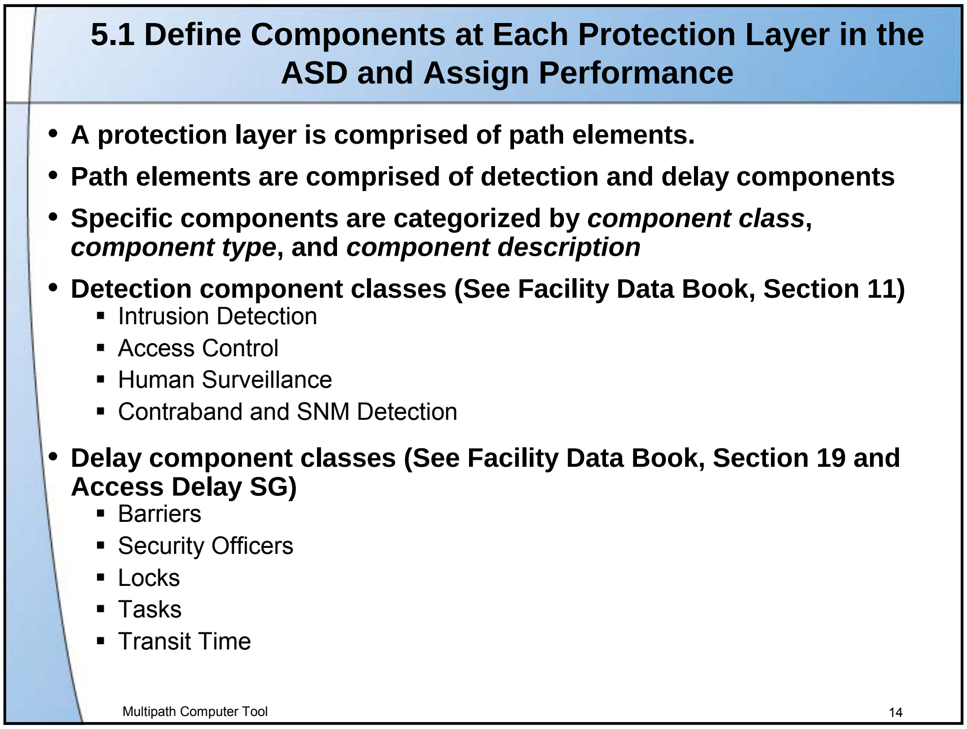
- **Each element strategy is also tagged with information about:**
  - Is it classified as Force (F), Stealth (S), Deceit (D), or (F/S)?
    - F/S is used if you can't decide whether a strategy is Force or Stealth
  - Does the entry strategy disable the element detection and delay components for the exit path?
    - If yes, only transit time is used on exit
    - General rule: Answer "TRUE" if Force (F) or Force/Stealth (F/S) answered on previous question; otherwise enter FALSE
  - What transportation is being utilized during the element strategy?
    - Foot (F), Vehicle (V), or Helicopter (H)

		Entrance Strategy Data		
Codes	Entry Strategy	Classified As	Defeats Exit Security	Transportation
ARE 0	Cross Offsite	D, F, S, F/S	TRUE/FALSE	F,V,H
PER 1	Shoot guard, enter	F/S	TRUE	Foot
	Deceit Entry	D	FALSE	Foot



5. Define PPS Security Components and Assign Component Performance

- **Informal process: listing what features are at each element and coming up with probabilities of detection and/or delay times**
- **Formal process (shown here):**
  - 5.1 Define components at each protection layer in the ASD and assign component performance values
    - Probability of Detection (P_D), Delay (Time)
  - 5.2 Combine component values to determine delay and detection values for each element using worksheets



5.1 Define Components at Each Protection Layer in the ASD and Assign Performance

- **A protection layer is comprised of path elements.**
- **Path elements are comprised of detection and delay components**
- **Specific components are categorized by *component class*, *component type*, and *component description***
- **Detection component classes (See Facility Data Book, Section 11)**
  - Intrusion Detection
  - Access Control
  - Human Surveillance
  - Contraband and SNM Detection
- **Delay component classes (See Facility Data Book, Section 19 and Access Delay SG)**
  - Barriers
  - Security Officers
  - Locks
  - Tasks
  - Transit Time

5.1 Define PPS Security Components and Assign Component Performance (continued)

- **Detection/delay values for different adversary tools and weapons**
  - If using a force or force/stealth tactic, the probability of detection and delay times depend on the tools and weapons used
  - If using a deceit tactic, tools and weapons may be detected as contraband
- **Option exists for user to define values**

5.1 Define Components at Each Protection Layer in the ASD and Assign Performance

- **Extracts from Component Class Tables in Section 11 and 19 of Data Book**

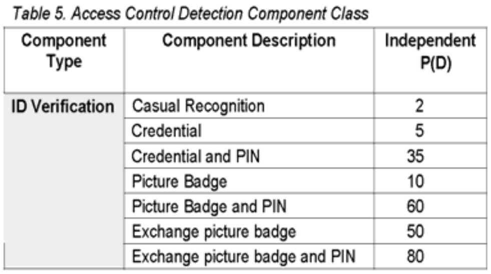


Table 5. Access Control Detection Component Class

Component Type	Component Description	Independent P(D)
ID Verification	Casual Recognition	2
	Credential	5
	Credential and PIN	35
	Picture Badge	10
	Picture Badge and PIN	60
	Exchange picture badge	50
	Exchange picture badge and PIN	80

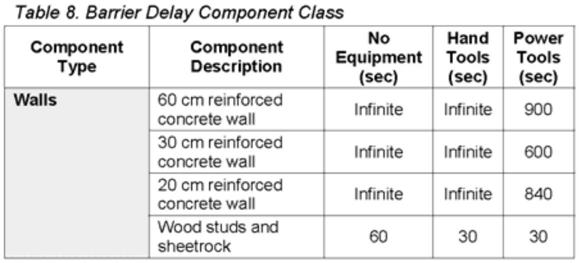
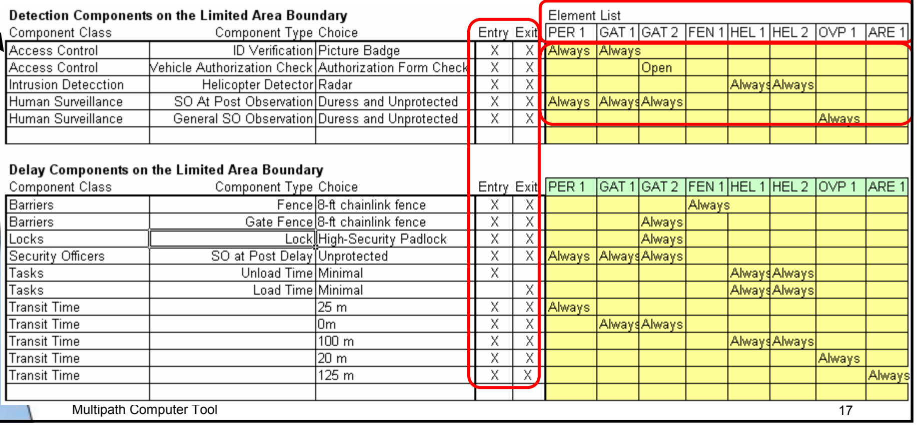


Table 8. Barrier Delay Component Class

Component Type	Component Description	No Equipment (sec)	Hand Tools (sec)	Power Tools (sec)
Walls	60 cm reinforced concrete wall	Infinite	Infinite	900
	30 cm reinforced concrete wall	Infinite	Infinite	600
	20 cm reinforced concrete wall	Infinite	Infinite	840
	Wood studs and sheetrock	60	30	30

5.1 Define Components at Each Protection Layer in the ASD and Assign Performance (Continued)

- **Enter into Protection Layer Sheet**
  - Description/Choice
  - Element Information
    - At what elements/areas the security component occurs
    - When it is implemented: Always or only during one condition (Open or Closed)
    - Direction implemented: Entry and/or Exit



Detection Components on the Limited Area Boundary

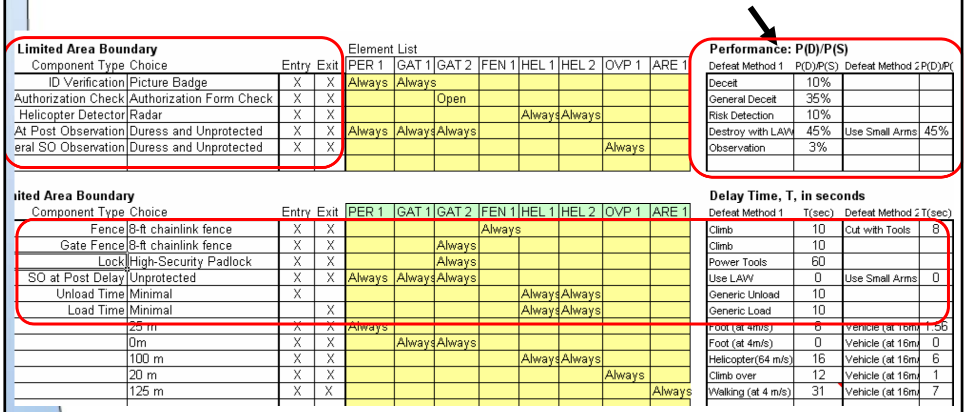
Component Class	Component Type	Choice	Entry	Exit	PER 1	GAT 1	GAT 2	FEN 1	HEL 1	HEL 2	OVP 1	ARE 1
Access Control	ID Verification	Picture Badge	X	X	Always	Always						
Access Control	Vehicle Authorization Check	Authorization Form Check	X	X			Open					
Intrusion Detecction	Helicopter Detector	Radar	X	X					Always	Always		
Human Surveillance	SO At Post Observation	Duress and Unprotected	X	X	Always	Always	Always					
Human Surveillance	General SO Observation	Duress and Unprotected	X	X							Always	

Delay Components on the Limited Area Boundary

Component Class	Component Type	Choice	Entry	Exit	PER 1	GAT 1	GAT 2	FEN 1	HEL 1	HEL 2	OVP 1	ARE 1
Barriers	Fence	8-ft chainlink fence	X	X				Always				
Barriers	Gate Fence	8-ft chainlink fence	X	X			Always					
Locks	Lock	High-Security Padlock	X	X			Always					
Security Officers	SO at Post Delay	Unprotected	X	X	Always	Always	Always					
Tasks	Unload Time	Minimal	X						Always	Always		
Tasks	Load Time	Minimal		X					Always	Always		
Transit Time		25 m	X	X	Always							
Transit Time		0m	X	X		Always	Always					
Transit Time		100 m	X	X					Always	Always		
Transit Time		20 m	X	X							Always	
Transit Time		125 m	X	X								Always

5.1 Define Components at Each Protection Layer in the ASD and Assign Performance (Continued)

- **Enter into Protection Layer Sheets (Continued)**
  - Performance Data



Limited Area Boundary — **Performance: P(D)/P(S)**

Component Type	Choice	Entry	Exit	PER 1	GAT 1	GAT 2	FEN 1	HEL 1	HEL 2	OVP 1	ARE 1	Defeat Method 1	P(D)/P(S)	Defeat Method 2	P(D)/P(
ID Verification	Picture Badge	X	X	Always	Always							Deceit	10%		
Authorization Check	Authorization Form Check	X	X			Open						General Deceit	35%		
Helicopter Detector	Radar	X	X					Always	Always			Risk Detection	10%		
At Post Observation	Duress and Unprotected	X	X	Always	Always	Always						Destroy with LAW	45%	Use Small Arms	45%
eral SO Observation	Duress and Unprotected	X	X							Always		Observation	3%		

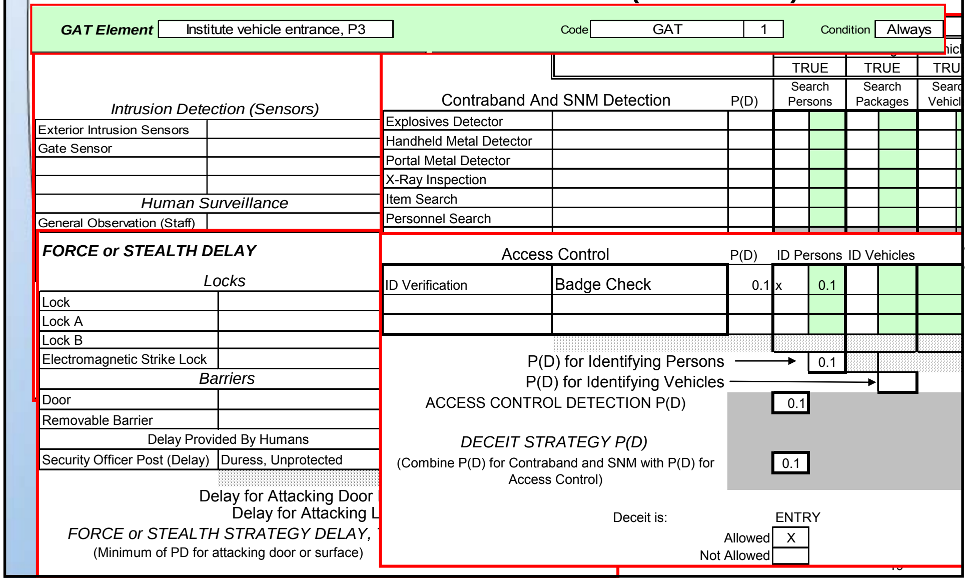
ited Area Boundary — **Delay Time, T, in seconds**

Component Type	Choice	Entry	Exit	PER 1	GAT 1	GAT 2	FEN 1	HEL 1	HEL 2	OVP 1	ARE 1	Defeat Method 1	T(sec)	Defeat Method 2	T(sec)
Fence	8-ft chainlink fence	X	X				Always					Climb	10	Cut with Tools	8
Gate Fence	8-ft chainlink fence	X	X			Always						Climb	10		
Lock	High-Security Padlock	X	X			Always						Power Tools	60		
SO at Post Delay	Unprotected	X	X	Always	Always	Always						Use LAW	0	Use Small Arms	0
Unload Time	Minimal	X						Always	Always			Generic Unload	10		
Load Time	Minimal		X					Always	Always			Generic Load	10		
	25 m	X	X	Always								Foot (at 4m/s)	6	Vehicle (at 16m/	1.56
	0m	X	X		Always	Always						Foot (at 4m/s)	0	Vehicle (at 16m/	0
	100 m	X	X					Always	Always			Helicopter(64 m/s)	16	Vehicle (at 16m/	6
	20 m	X	X							Always		Climb over	12	Vehicle (at 16m/	1
	125 m	X	X								Always	Walking (at 4 m/s)	31	Vehicle (at 16m/	7

- **This sheet allows us to inspect for effectiveness and balance on a protection layer**

5.2 Assign Delay and Detection Values to Each Element Using Worksheets

- **5.2.1 Enter element information on sheet (Gate shown)**



GAT Element Institute vehicle entrance, P3 Code GAT 1 Condition Always

Intrusion Detection (Sensors)	
Exterior Intrusion Sensors	
Gate Sensor	
Human Surveillance	
General Observation (Staff)	

Contraband And SNM Detection		P(D)	TRUE Search Persons		TRUE Search Packages		TRU Searc Vehicl
Explosives Detector							
Handheld Metal Detector							
Portal Metal Detector							
X-Ray Inspection							
Item Search							
Personnel Search							

FORCE or STEALTH DELAY

Locks	
Lock	
Lock A	
Lock B	
Electromagnetic Strike Lock	
Barriers	
Door	
Removable Barrier	
Delay Provided By Humans	
Security Officer Post (Delay)	Duress, Unprotected

Delay for Attacking Door
Delay for Attacking L
FORCE or STEALTH STRATEGY DELAY,
(Minimum of PD for attacking door or surface)

Access Control		P(D)	ID Persons		ID Vehicles	
ID Verification	Badge Check	0.1	x	0.1		

P(D) for Identifying Persons → 0.1
P(D) for Identifying Vehicles →
ACCESS CONTROL DETECTION P(D) 0.1

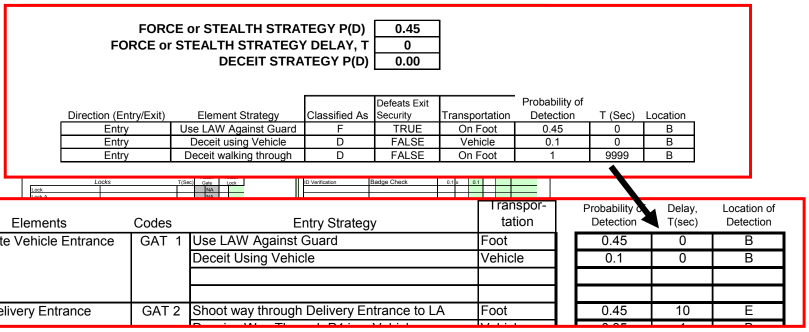
DECEIT STRATEGY P(D)
(Combine P(D) for Contraband and SNM with P(D) for Access Control) 0.1

Deceit is: ENTRY
Allowed X
Not Allowed

6. Define VEASI Performance for Each Strategy: P_D, Total Delay, and Location of Detection

- **6.1 For each element, combine**
  - Element strategies that you identified as credible in step 4 with
  - Relevant force, stealth, or deceit performance data in step 5

Result: a list of element strategies and their associated performance values (P_D, Total Delay, and location of detection) for a new table shown here for this element

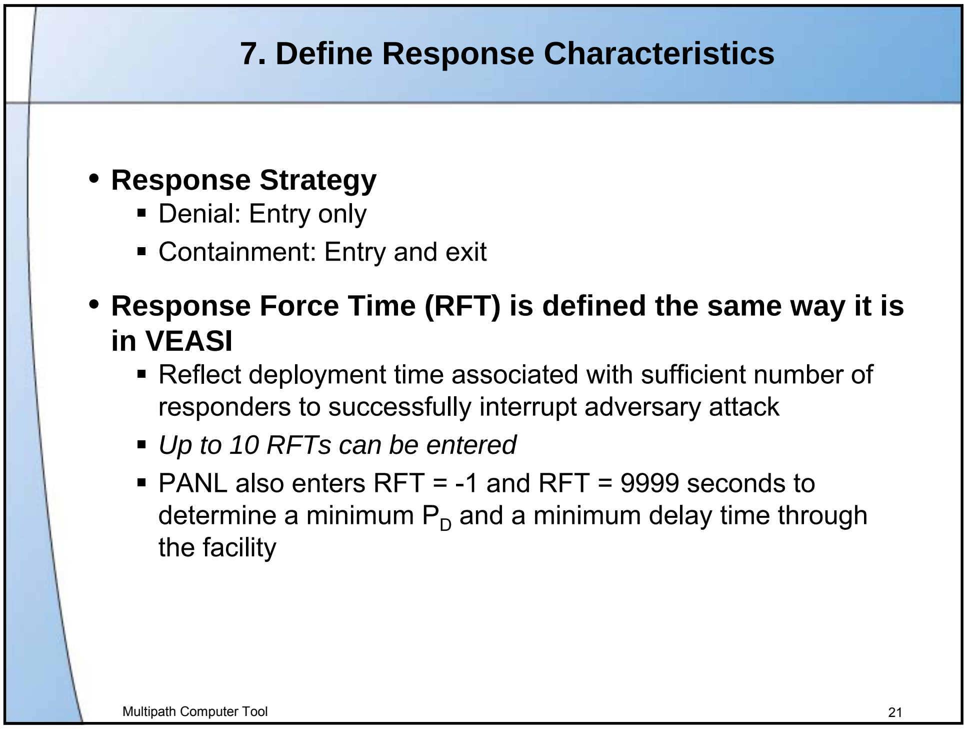


FORCE or STEALTH STRATEGY P(D) 0.45
FORCE or STEALTH STRATEGY DELAY, T 0
DECEIT STRATEGY P(D) 0.00

Direction (Entry/Exit)	Element Strategy	Classified As	Defeats Exit Security	Transportation	Probability of Detection	T (Sec)	Location
Entry	Use LAW Against Guard	F	TRUE	On Foot	0.45	0	B
Entry	Deceit using Vehicle	D	FALSE	Vehicle	0.1	0	B
Entry	Deceit walking through	D	FALSE	On Foot	1	9999	B

Elements	Codes	Entry Strategy	Transpor-tation	Probability of Detection	Delay, T(sec)	Location of Detection
Institute Vehicle Entrance	GAT 1	Use LAW Against Guard	Foot	0.45	0	B
		Deceit Using Vehicle	Vehicle	0.1	0	B
Delivery Entrance	GAT 2	Shoot way through Delivery Entrance to LA	Foot	0.45	10	E

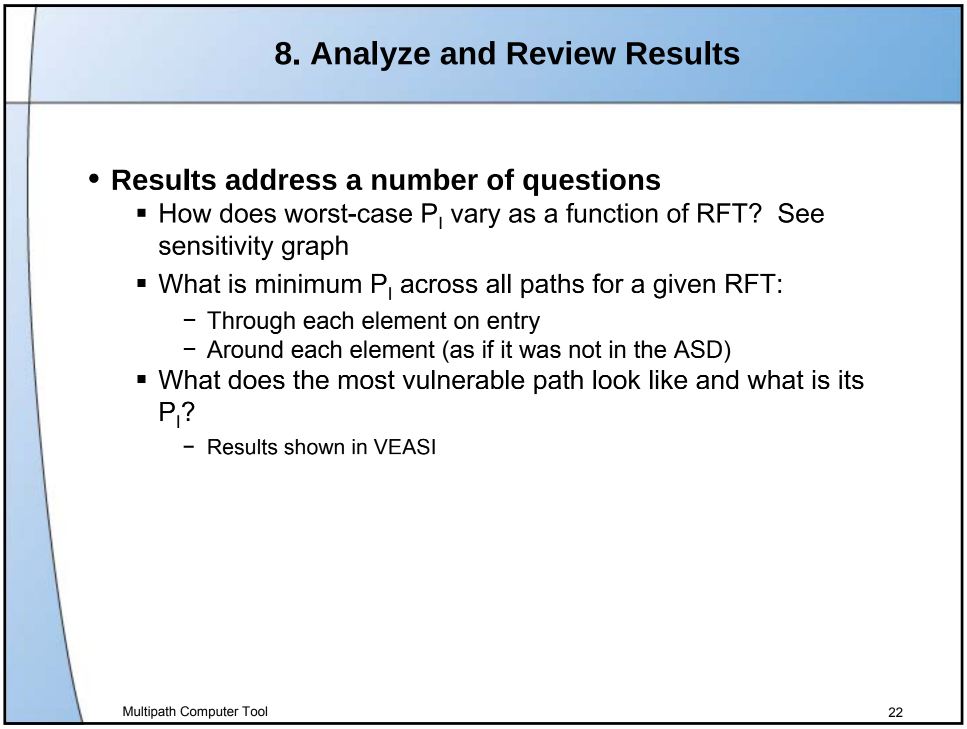
Multipath Computer Tool 20



7. Define Response Characteristics

- **Response Strategy**
  - Denial: Entry only
  - Containment: Entry and exit
- **Response Force Time (RFT) is defined the same way it is in VEASI**
  - Reflect deployment time associated with sufficient number of responders to successfully interrupt adversary attack
  - *Up to 10 RFTs can be entered*
  - PANL also enters RFT = -1 and RFT = 9999 seconds to determine a minimum P_D and a minimum delay time through the facility

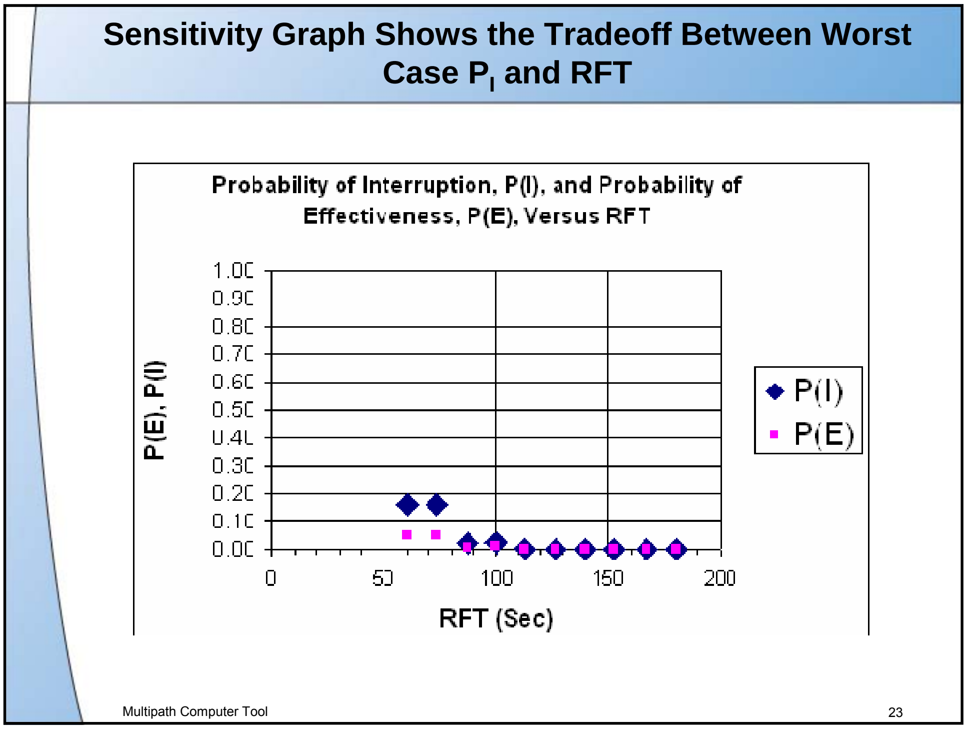
Multipath Computer Tool 21



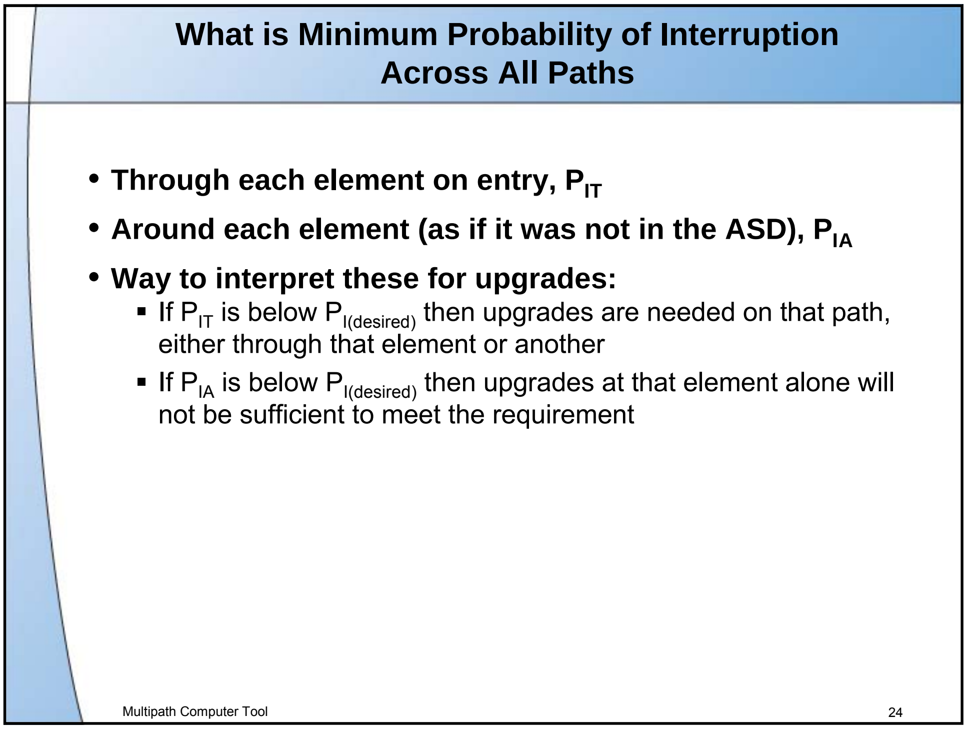
8. Analyze and Review Results

- **Results address a number of questions**
  - How does worst-case P_I vary as a function of RFT? See sensitivity graph
  - What is minimum P_I across all paths for a given RFT:
    - Through each element on entry
    - Around each element (as if it was not in the ASD)
  - What does the most vulnerable path look like and what is its P_I?
    - Results shown in VEASI

Multipath Computer Tool 22



Sensitivity Graph Shows the Tradeoff Between Worst Case P_I and RFT



What is Minimum Probability of Interruption Across All Paths

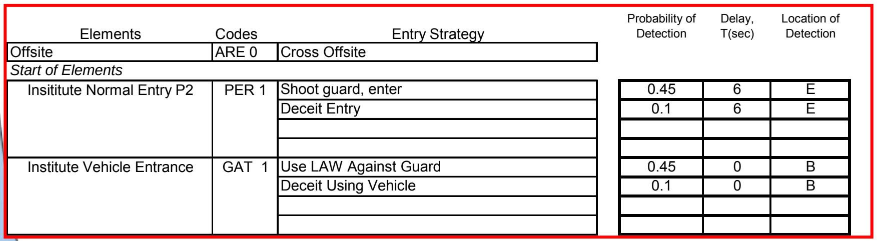
- **Through each element on entry, P_{IT}**
- **Around each element (as if it was not in the ASD), P_{IA}**
- **Way to interpret these for upgrades:**
  - If P_{IT} is below $P_{I(desired)}$ then upgrades are needed on that path, either through that element or another
  - If P_{IA} is below $P_{I(desired)}$ then upgrades at that element alone will not be sufficient to meet the requirement

VEASI Displays Important Path Information

- **Path Statistics**
  - P_I and TRI (Time Remaining after Interruption)
  - CDP location
  - Cumulative delay after CDP
- **Description of the path**
  - Which elements the adversary is defeating
  - Strategy about how these elements are being defeated

9. Perform Sensitivity Analysis

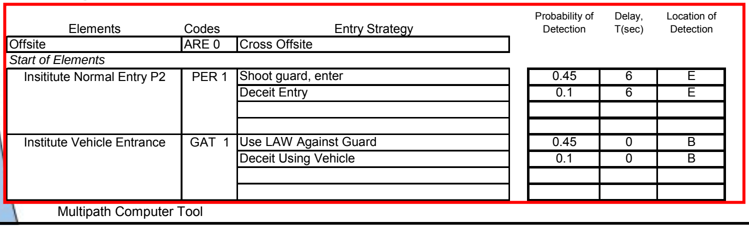
- **Investigate sensitivity of results to changes in detection, delay, and response values**
- **Make temporary changes in PANL**
- **Compensate for uncertainties in component and response data**
- **Investigate paths with very high P_I**
- **Confirm with field tests and exercises**



Elements	Codes	Entry Strategy	Probability of Detection	Delay, T(sec)	Location of Detection
Offsite	ARE 0	Cross Offsite			
Start of Elements					
Insititute Normal Entry P2	PER 1	Shoot guard, enter	0.45	6	E
		Deceit Entry	0.1	6	E
Institute Vehicle Entrance	GAT 1	Use LAW Against Guard	0.45	0	B
		Deceit Using Vehicle	0.1	0	B

10. Perform Upgrade Analysis

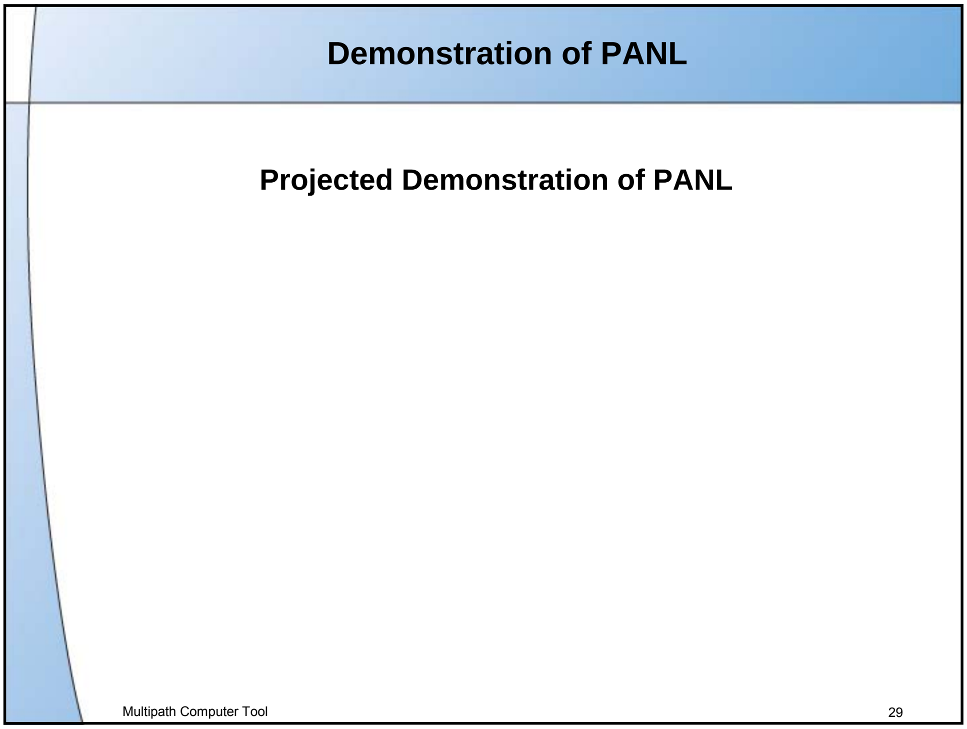
- **Determine whether P_I for your proposed system is greater than or equal to the required P_I ($P_{I\ required}$) from your regulator**
- **Study PPS upgrade effectiveness prior to implementation**
- **Strive for:**
  - Balanced system
  - Protection-in-depth
- **Look for weak PEs across each layer and with low minimum P_I through them**
- **Change RFT to affect all paths**



Elements	Codes	Entry Strategy	Probability of Detection	Delay, T(sec)	Location of Detection
Offsite	ARE 0	Cross Offsite			
Start of Elements					
Insititute Normal Entry P2	PER 1	Shoot guard, enter	0.45	6	E
		Deceit Entry	0.1	6	E
Institute Vehicle Entrance	GAT 1	Use LAW Against Guard	0.45	0	B
		Deceit Using Vehicle	0.1	0	B

After Testing Upgrades Parametrically, Redefine Your Element Worksheets

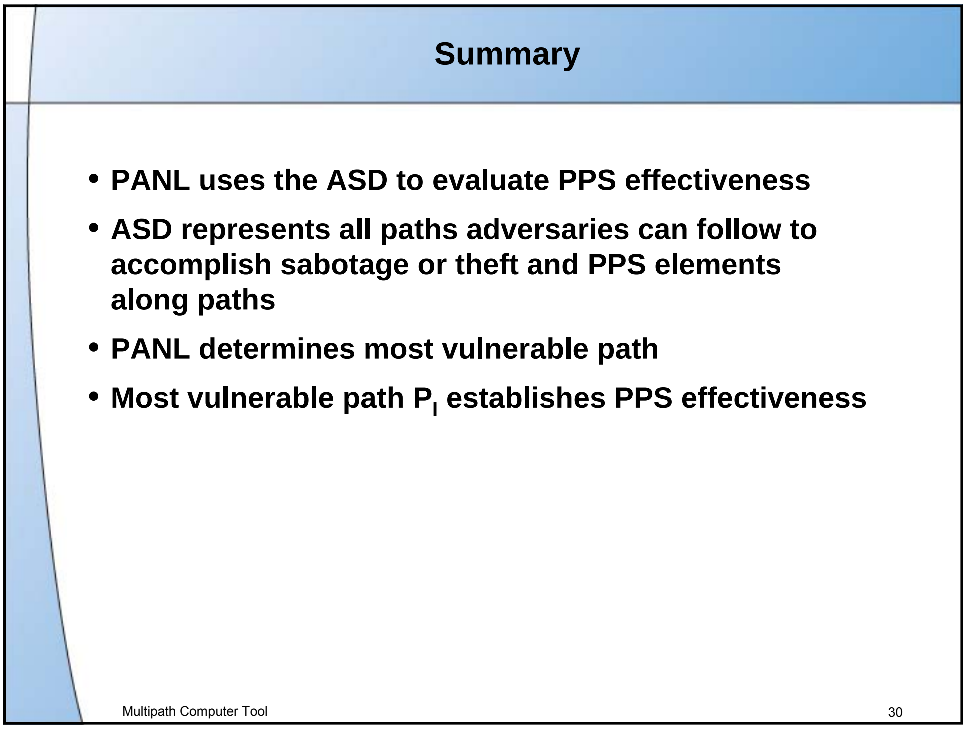
- **Remove the performance value parameter changes tested in PANL**
- **Return to worksheets and install the specific components in an upgrade version of the worksheets**
- **Return to PANL with the new performance data to demonstrate the value of the upgraded facility**



Demonstration of PANL

Projected Demonstration of PANL

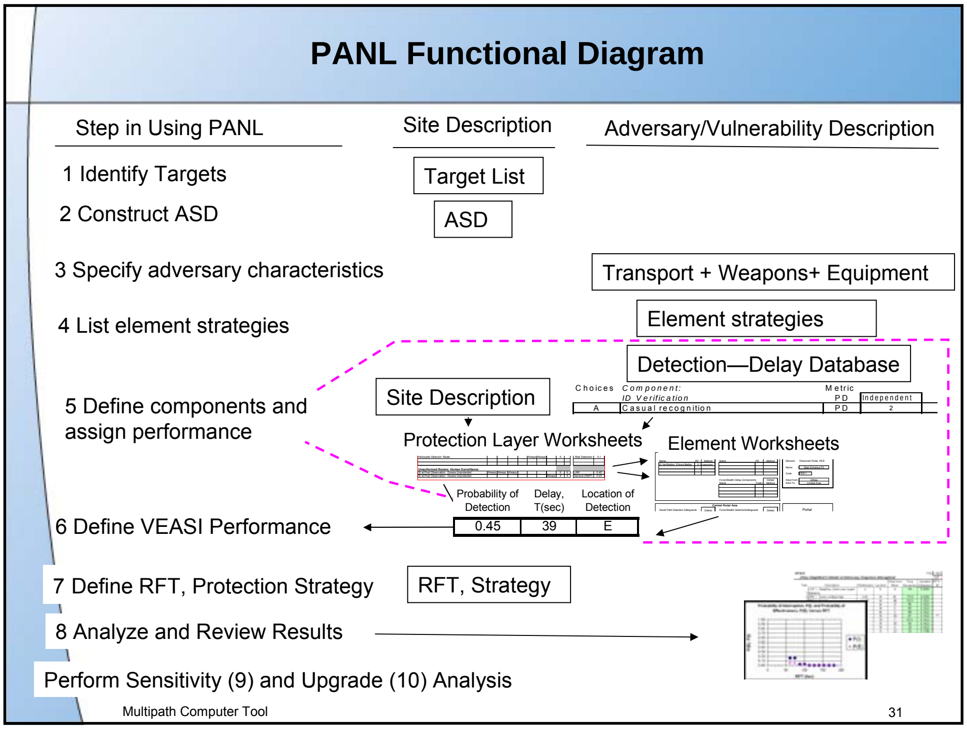
Multipath Computer Tool 29



Summary

- **PANL uses the ASD to evaluate PPS effectiveness**
- **ASD represents all paths adversaries can follow to accomplish sabotage or theft and PPS elements along paths**
- **PANL determines most vulnerable path**
- **Most vulnerable path P_I establishes PPS effectiveness**

Multipath Computer Tool 30



PANL Functional Diagram

Step in Using PANL	Site Description	Adversary/Vulnerability Description
1 Identify Targets	Target List	
2 Construct ASD	ASD	
3 Specify adversary characteristics		Transport + Weapons+ Equipment
4 List element strategies		Element strategies

5 Define components and assign performance

Detection—Delay Database

Choices	*Component:* *ID Verification*	Metric PD	Independent
A	Casual recognition	PD	2

Site Description

Protection Layer Worksheets

Element Worksheets

Probability of Detection	Delay, T(sec)	Location of Detection
0.45	39	E

6 Define VEASI Performance

7 Define RFT, Protection Strategy — RFT, Strategy

8 Analyze and Review Results

Perform Sensitivity (9) and Upgrade (10) Analysis

Multipath Computer Tool 31

Subgroup 19
Multipath Computer Tool

Session Objectives

After the session, the participants will be able to do the following:

1. Enter the ASD into PANL for the PTR
2. Determine the input data to the PANL software for a given threat, facility condition, and target
3. Analyze the effectiveness of a PPS using the PANL software
4. Understand how to perform system upgrade analysis
5. Complete a sensitivity analysis for input data to the PANL software.

PANL User's Manual and PANL Reference Manual

Review the PANL User's and Reference Manuals.

Exercises

1. Enter the PTR adversary sequence diagram into PANL
2. PANL Facility Module: Physical Areas
3. PANL Facility Module: Protection Element data
4. PANL Outsider Module: 4.1) setup, 4.2) minimum total system delay, 4.3) minimum total system assessed detection probability
5. PANL Outsider Module: Most Vulnerable Path, System Balance, and Protection-in-Depth
6. Upgrade and Sensitivity Analysis

Note: To complete the exercises quickly, perform the steps in the boxes. For explanatory information, read the additional text.

Exercise 1: Enter the ASD for the PTR

In this exercise you will enter into PANL the ASD you created in Subgroup 17S.

	What You Do	Comments/Prompts
1	Double click on the folder entitled “PANL”.	
2	Double click on the application file “PANL_EX1.XLS”. This is an **EXCEL™** file.	
3	Click on the “Enter ASD” button on the Master PANL worksheet.	This adds a new ASD sheet. To go to the ASD Definition sheet, click on the ASD Definition tab.
4	Fill in the area names on the left (under “Name”) and name the protection layers on the right (under “Inside Protection Layer”).	Enter as many areas and protection layers as you need for the PTR ASD.
5	Click on the “Add Areas to Diagram” button	A series of “Area settings for Area” dialogs will be shown to you.
6	For the areas outside the building, such as the Protected Area and Limited Area, Select “Traversable by Vehicle and Foot;” for the other areas select “Traversable by Foot Only.” Also there is a “Jump to Area” Code consisting of one or more letters; leave this the way it is and click on the Okay button.	
7	Scroll up in the top window until you see the Offsite area (in white).	This is line 102.
8	To enter elements, select a cell one row below the Offsite area in columns D, I, N, S, X, AC, AH, AM, AR ….etc. and enter the Cntrl-e key combination. (This requests PANL to add an element at this point.)	An element settings dialog will be displayed. Note: Always select a cell one row below the area and in the right columns or else PANL will show an error message.
9	On the left-hand side of the dialog, select the type of element: a non-jump versus a jump element versus a target location. Also, enter a name (such as “perimeter entry portal” and not a cryptic “SUR 3” if you can help it) for the element. Click on the okay button.	This should be a plain-text name that is a good identifier for the element.
10	If you select a jump element in the dialog, the drawing process finishes with a white box selected. Enter the “Jump to Area” Code for the area the element jumps to (for example, jumping to the Protected Area from Offsite would be accomplished by entering an A).	Note: It is up to you to make sure that the “Jump to Area” Code is correct.
11	Enter the type of element (SUR or PER) in the top right-hand box. (See Path Elements and Target Location Card)and enter an index below that.	Note: to remove an element, select the cells that it covers and enter Control-D.
12	Enter an index number below the element.	Note: The number corresponds with the order of entry.
13	Repeat steps 8-11 until all path elements are entered	

14	Save the ASD by clicking on “File”, Select “Save As….” on the drop down menu.	
15	Enter the name “PANL_EX1ASD.XLS”. Exit **EXCEL™**.	

Preparation for PANL Facility Module Exercise 2

The preparation phase assumes that PANL_EX1ASD.XLS has been loaded onto your laptop and that the PANL folder is on the computer desktop.

Exercise 2. Entering Adversary Characteristics and Element Strategies into PANL.

This exercise will give participants practice entering information about the threat and element strategies for defeating each element and area. The computer screen shows the ASD for this exercise. Some of the PANL data has already been entered.

2.1 Select threat transportation and equipment options

	What You Do	Comments/Prompts
1	Click on the button just to the left over the ASD that says "Element Strategies"	This is still on the ASD Definition worksheet you entered the ASD onto. PANL should go to the "Element Strategies" worksheet
2	Select the Import ASD button on the top, left-hand side of the Element Strategies worksheet.	PANL should now list the areas and elements in order down to the target.
3	In the area that is labeled Transportation, click on "Foot Travel" and leave the vehicle and helicopter checkboxes unchecked. Click on the checkboxes for Uses Small Arms and for Uses LAWs.	Since strategies are entered by users and not checked by PANL, it is up to the user to be consistent in using transportation or not. The checkboxes are in PANL for information purposes only.

2.2 Enter strategies for areas and elements.

For the Limited Area 1 and the Protected Area enter the appropriate strategies for each element and area in the middle columns of the spreadsheet, first on entry and then on exit. Merely add rows to enter additional strategies if you come up with more than 4. Table 19-1 below lists examples of strategies for different elements. You will also need to enter the following information about each strategy:

- Is it classified as Force (F), Stealth (S), Deceit (D) or (F/S)?
- Does the strategy defeat the element detection and delay on exit if passed through on entry previously? (The assumption for force strategies is to set this variable to True, so that a fence or wall, for example, is not there to be attacked again on exit.) Some stealth attacks, such as climbing walls, do require the adversary to attack the wall twice; in such cases this should be set to False.
- What transportation is the strategy assuming? PANL will let you enter a strategy for a type of transportation you left out in the check boxes. On the other hand, that strategy will be ignored if you analyze your dataset.

Element Type	Example Strategies
Doors/portals/gates with access allowed	Enter/exit using deceit and hiding contraband; Enter/exit using force or stealth
Fences/isolation zones/overpasses	Climb over; Penetrate using force or stealth
Surfaces	Penetrate using force; Penetrate stealthily
Helicopter Flight Path	Covert landing of helicopter; Parachute
Target Locations (Entry)	Stealth; deceit; force to acquire target/perform sabotage
Target Locations (Exit)	Stealth; deceit; force to remove target.

Figure 19.1. Example Strategies for Different Elements

	What You Do	**Comments/Prompts**
1	Enter entry and exit strategies	These are found in the columns F and G
2	Classify strategy as Force (F), Stealth (S), Deceit (D) or (F/S)	Enter text as F, S, D, or F/S (use this if you can't decide whether something is F or S) in column I for entry strategies and L for exit strategies.
3	Indicate whether the strategy defeats all of the element detection and delay on exit if passed through on entry previously.	Enter TRUE or FALSE in column J for entry strategies and M for exit strategies.
4	Record the type of transportation that the strategy assumes.	Enter "Foot" or "Vehicle" or "Helicopter" in column K for entry strategies and N for exit strategies.

Exercise 3. Define PPS Security Components and Assign Component Performance

This exercise will give participants practice collecting information about the security components on a protection layer and then assigning them and their performance to particular elements on that layer. Enter each component and its performance data under the appropriate section (lists of choices and performance data are found in tables associated with each category of component):

- Detection components:
  - Access control - providing detection for deceit strategies – *See table 3 in the attached section*
  - Contraband and SNM detection - providing detection for deceit strategies – *see Table 5 in the attached section*.
  - Intrusion detection (typically by sensors) - providing detection for stealth and force strategies – *see Table 1 in the attached section*.

  - Human surveillance (by security officers or employees) – providing detection for stealth and force strategies -- *See Table 4 in the attached section.*
- Delay components
  - Barriers -- *See Table 2 in the attached section*.
  - Locks -- *See Table 2 in the attached section*.
  - Target Tasks -- *Typically, user defined*
  - Security Officers – *See Table 4 in the attached section.*
  - Transit times -- *Typically, user defined*.

3.1 Enter protection layer data

Use the protection layer worksheet included here, along with the description of the site, to describe all of the detection and delay components that make up the elements comprising the PTR PA Boundary protection layer.

Start by filling in the name of the layer at the top and list the elements (e.g,. PER 2, ISO 1) making up this layer in the boxes under "Select Elements" heading.

Next, for each component, enter the following data in a row in the detection or delay section (depending upon whether it affords detection or delay):

- list the component class (e.g., Intrusion detection), component type (e.g., helicopter detector) and Choice (e.g. radar) in the three left-most columns
- indicate whether the component is active against the adversary or not on entry by making an "X" under the entry column; do the same for exit
- indicate whether the component is always active at each of the five elements by entering "always" in the box in the appropriate column. Enter "open" if the component is active only when the element is opened or operational (e.g., a badge check when a portal is open to let people through) and enter "closed" if the component is active only when the element is closed or non-operational (e.g., a sensor in an entry portal). If a component is not found at an element, leave the box blank.
- On the right hand-side of the form enter a defeat method for the component (e.g., "use hand tools" or "use explosives" or "use deceit") along with the performance value from the tables in Section 11.

Assume "open" corresponds to normal shift workday conditions and assume that the adversary is either on foot or in a truck. . Review Sections 6, 7, and 12 through 15 from the Exercise Data Book to determine the physical protection element features.

After completing the table, enter the data into PANL by following these instructions.

	What You Do	**Comments/Prompts**
1	Click on the button at the top of the Element Strategies worksheet that says "Enter Protection Layer Components"	PANL should go to the "Protection Layer" worksheet and list the areas and protection layers in a list box at the top of the sheet.

2	Select the area “Institute Limited Area” in the list box.	PANL will then move to a row that lists the elements in the protection layer just inside the area selected in the list box. Elements are listed as codes and numbers (e.g., SUR 3) across the top of the rows G to P.
3	Using your paper worksheet as a reference, enter the component data for the PA Boundary protection layer in the Protection Layer worksheet in PANL.	
4	For each component open the pull-down menu underneath each element to select whether that component is active Always, when the element is in an “open” state, when it is “closed”, or leave the choice as blank if the component is not found at that element	If there is one procedure applied when an element is open and another when it is closed, record these as two different components on two separate lines even if the performance numbers are identical.
5	Record whether the component is active on entry and/or on exit by putting x’s in the appropriate Entry/Exit column	If the same procedure has different activities at two different elements, record them as separate components.
6	Copy the performance data from the appropriate table of Tables 1-5 in to the boxes at the right of the diagram along with an appropriate description of how the component was defeated as the “defeat method.”	Enter into columns AB and following. Note: For components where explosive attacks result in Stage 1 and State 2 delays, then enter these times in two sets of neighboring columns. The 4 columns should look like: Defeat Method 1: “Explosives stage 1” T(sec): *{Enter Stage 1 delay here}* Defeat Method 2: “ Explosives stage 2” T(sec): *{Enter Stage 2 delay here}*

3.2 Enter protection layer data onto Element Worksheets

This exercise will give participants practice in preparing the input data for the PANL protection path elements. Path elements are represented by rectangles that are connected to the areas they join.

Use the worksheets below to record component data from the Protection Layer Worksheet for certain elements suggested by your subgroup instructor for the Protected Area (only enter components for the normal shift workday conditions). Then, after reviewing this data, record performance data (P(D), T, Location of Detection) for the element strategies you defined for these elements. If necessary, combine probabilities or delays as discussed in subgroup 18S. Note: To combine probabilities of detection, multiply non-detection probabilities:

$P(\text{Detection}) = 1- (1-PD_1)*(1-PD_2)* \ldots(1-PD_n)$

where PD_j is the probability of detection for component j, j = 1,…, n.

Note: Common elements to use for this exercise are shown in Figure 19.1 below.

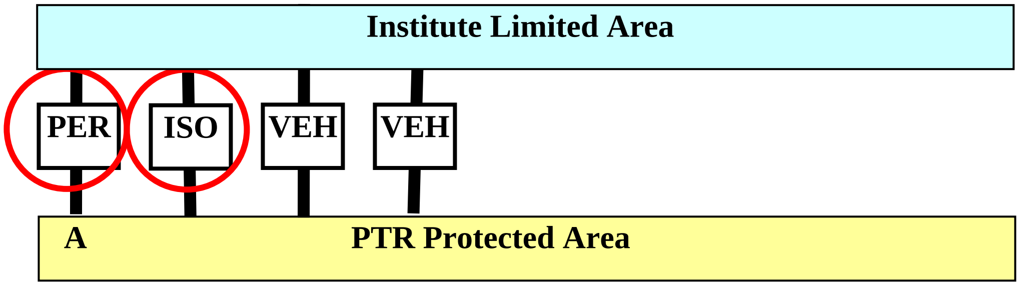
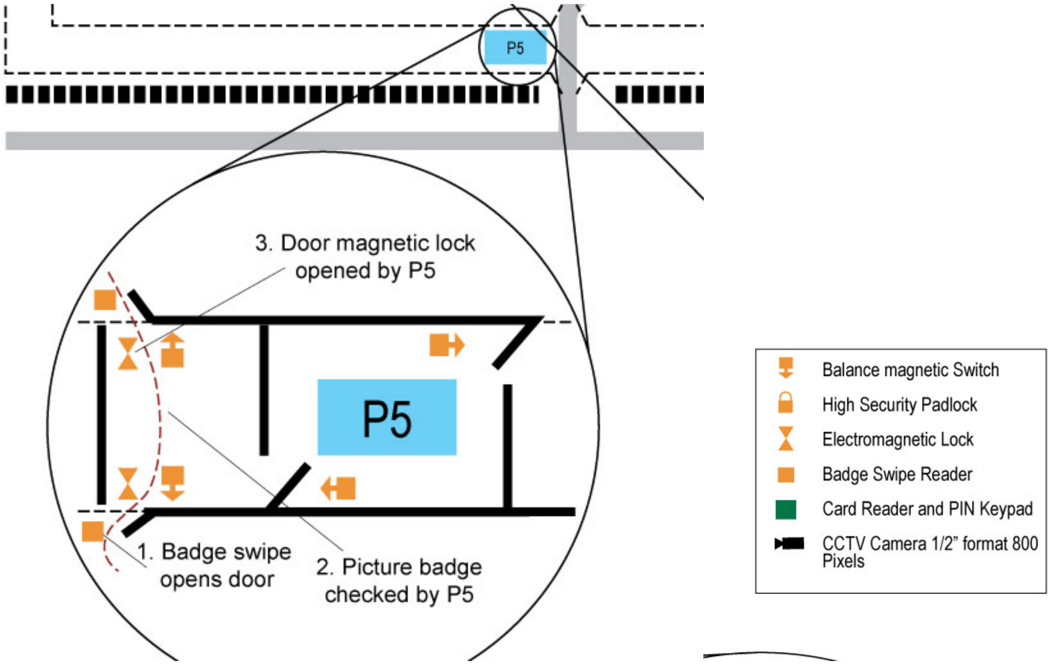


Figure 19.1. ASD and Path Elements for PTR Research Reactor Facility


P5
3. Door magnetic lock opened by P5
P5
1. Badge swipe opens door
2. Picture badge checked by P5
Balance magnetic Switch
High Security Padlock
Electromagnetic Lock
Badge Swipe Reader
Card Reader and PIN Keypad
CCTV Camera 1/2" format 800 Pixels

In defining P5, the Personnel Portal (PER) into the PTR Protected Area, note that an Electromagnetic Strike Lock that is released when the person passes the associated identity check. Change the Hand Tool and High Explosive delays assigned to this Electromagnetic Strike Lock from both 20 seconds (in the database) to 60 seconds (assume that the P5 locks are better).

Protection Layer Worksheet For Layer ________________

Detection Component List					Element List					Performance: P(D)							
Component Class	Component Type	Choice	Entry	Exit						Defeat Method 1	P(D)	Defeat Method 2	P(D)	Defeat Method 3	P(D)	Defeat Method 4	P(D)

Delay Component List										Delay Time, T, in seconds							
Component Class	Component Type	Choice	Entry	Exit						Defeat Method 1	T(sec)	Defeat Method 2	T(sec)	Defeat Method 3	T(sec)	Defeat Method 4	T(sec)

Outer Door

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

Element WorkSheet

Element	Personnel Portal, PER
Name	
Area From:	
Area To:	

Outer Surface

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

Central Portal Area

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

Name	PD	Defeat Method

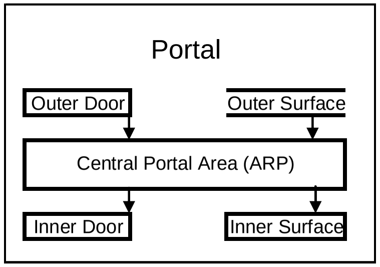
Transit Time

Transportation	T(sec	Distance
Foot (3 m/s)		

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

Portal



Inner Door

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

	Assessment	P(A)
1		
2		

Inner Door

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

	Element Strategy	Direction (Entry/Exit)	P(Detection	T(Sec)	Location	Notes	Use
1							
2							
3							
4							

Element WorkSheet

Element Vehicle Portal, VEH

Name	
Area From:	
Area To:	

Outer Door

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

Outer Surface

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

Central Portal Area

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

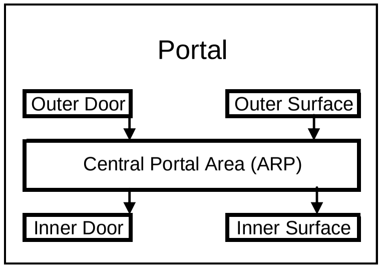
Name	PD	Defeat Method

Transit Time

Transportation	T(se	Distance
Foot (3 m/s)		

Force/Stealth Delay Components

Name	T(sec)	Defeat Method



Inner Door

Deceit Path Detection Components

Name	PD	Defeat Method

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

	Assessment	P(A)
1		
2		

Inner Door

Force/Stealth Detection Components

Name	PD	Defeat Method

Force/Stealth Delay Components

Name	T(sec)	Defeat Method

	Element Strategy	Direction (Entry/Exit)	P(Detection)	T(Sec)	Location	Notes	Use
1							
2							
3							
4							

Element WorkSheet

Element Isolation Zone, ISO *or Overpass, OVP*

Name	
Code	
Area From:	
Area To:	

Outer Fence

Force/Stealth DetectionSafeguards Name	PD	Defeat Method

Force/Stealth Delay Components Name	T(sec	Defeat Method

Central Zone Area

Force/Stealth Detection Components Name	PD	Defeat Method

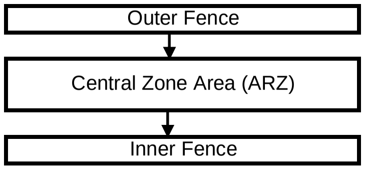
Force/Stealth Delay Components Name	T(sec	Defeat Method

Inner Fence

Force/Stealth DetectionSafeguards Name	PD	Defeat Method

Force/Stealth Delay Components Name	T(sec	Defeat Method

Isolation Zone/Overpass



	Assessment	P(A)
1		
2		

	Element Strategy	Direction (Entry/Exit)	P(Detection)	T(Sec)	Location	Notes	Use
1							
2							
3							
4							

3.3 Determine performance values for Areas

Determine the performance values – P(D), delay, and location of detection – for the two areas indicated in the diagram below on the worksheets on the next page. Use Sections 6 and 12 from the Exercise Data Book. Assume normal shift workday conditions for the analysis and that the adversary is either on foot or in a truck. Assume a random patrol by a security officer is conducted 24 hours/day in the Limited Area.

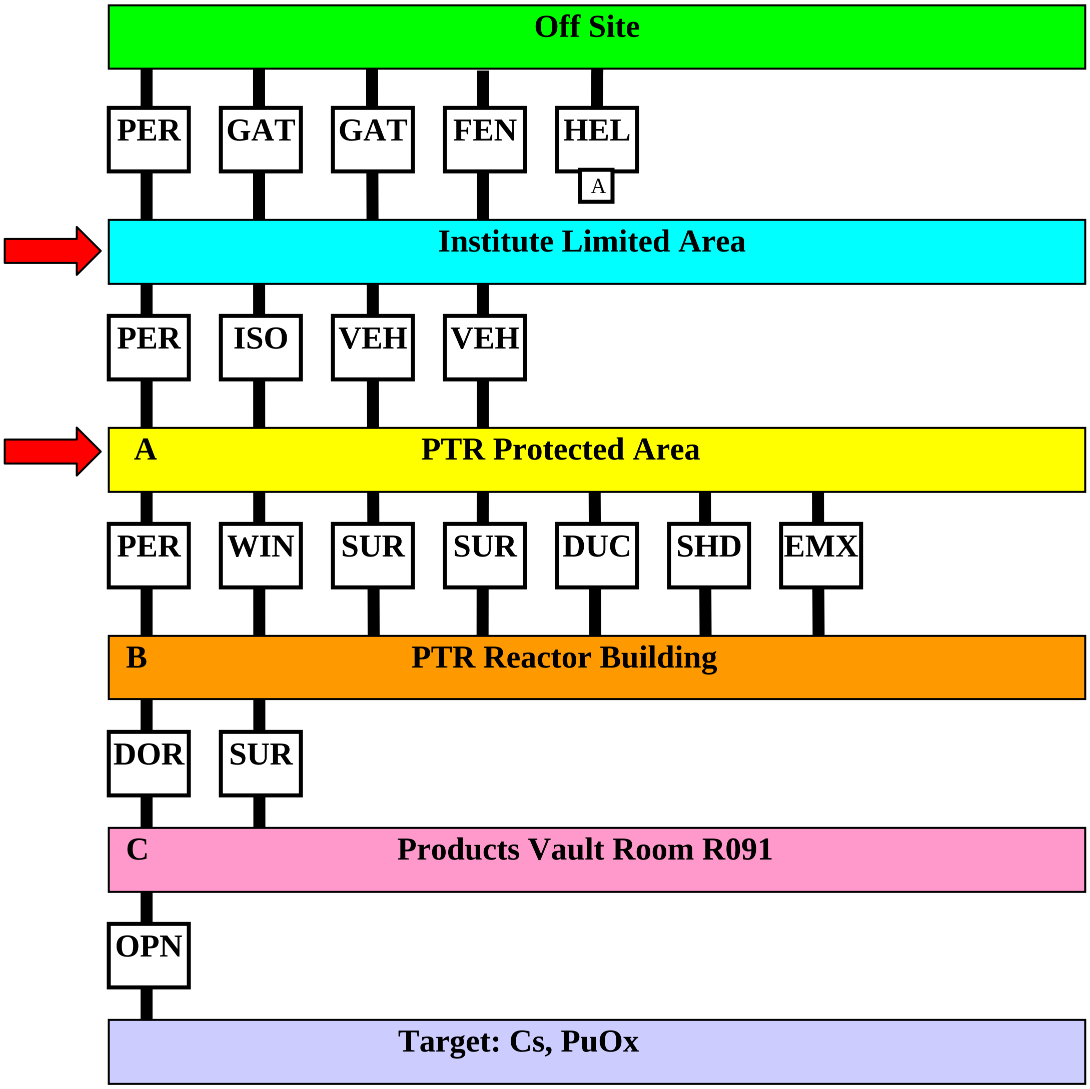


Figure 19.2. ASD for the PTR Research Reactor

Area: Limited Area Strategy: Cross on Foot P_D: ________________ T(sec): ______________ Location: B M E	Area: Limited Area Strategy: Cross with Vehicle P_D: ________________ T(sec): ______________ Location: B M E
Area: Protected Area Strategy: Cross on Foot P_D: ________________ T(sec): ______________ Location: B M E	Area: Protected Area Strategy: Cross with Vehicle P_D: ________________ T(sec): ______________ Location: B M E

3.4 Determine Probability of Detection for Screening for Contraband and SNM

The forms below are developed to determine the probability of detection provided by a set of contraband detection procedures and technology found at a single element.

There are two forms, one for entry and the other for exit that need to be filled out.

	What You Do	Comments/Prompts
1	To begin filling out either form, indicate the element being modeled, the element code (e.g. “PER 3”) and the contraband model number (a unique index assigned to this combination of components).	
2	Along the top of the form write indicate with “true” or “false” what types of people or items are allowed across this element: personnel, packages, vehicles or cargo, authorized (and unchecked) items, such as, perhaps, tools and equipment, or other means (such as mailing items in or throwing them over a	

	perimeter boundary).	
3	You may cross out any column with a “false” because if something is not allowed, there is no need to look for contraband along that means of entry/exit.	
4	Next, use the forms below to record (1) what contraband detection components (and their appropriate probabilities of detection) are used for detecting contraband when entering through the portal into the reactor building, P3, and (2) what SNM detection components are used on exit.	
5A	For the entry worksheet, find the column with the lowest probability of detection and choose it as the defeat method (that is, “hide on person” or “hide in vehicle”) for getting contraband past this element. ***OR***	This is the version done by hand
5B	Transfer the data to PANL’s Entry Contraband Modeling worksheet and have PANL calculate the combined probabilities.	This uses a PANL spreadsheet.
6A	Perform similar steps to steps 2 through 5B for the exit of SNM.	See discussion below for how to do this.

For exit, the Contraband Modeling worksheet considers primarily detection of getting SNM out (we assume that adversaries have not been detected so far will abandon all but the SNM and small weapons if they try to exit by deceit). It has two options: either take the material straight through the SNM detector (and risk detection against the probability of detection in the database) OR attempt to shield the material and take it out. Setting the latter probability of detection is beyond the scope of what PANL can determine and is therefore left to the user to specify. Note that a common way of defining this probability is to consider using a metal detector, search, or X-ray to search for shielding and take the associated probability of detection from the entry Contraband Detection Worksheet.

? What is the lowest Probability of Detection of contraband on entry?

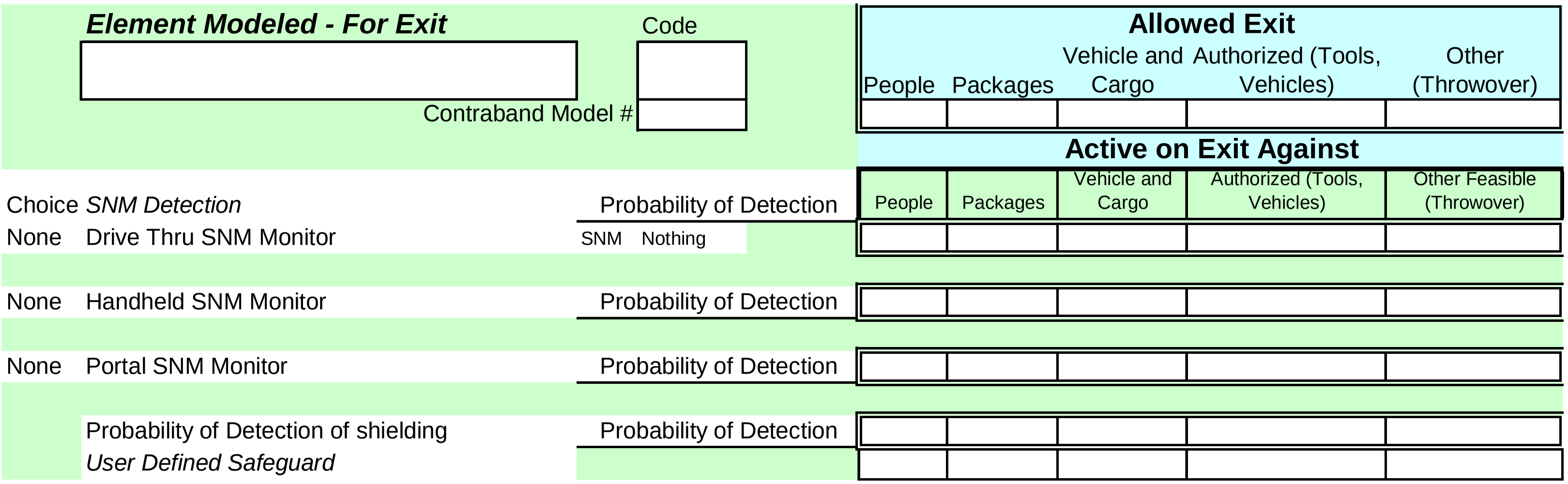
? What is the lowest Probability of Detection of contraband on exit?

sssss

Element Modeled - For Entry	Code	**Allowed Entry** People	Packages	Vehicle and Cargo	Authorized (Tools, Vehicles)	Other Feasible (Throwover)
Contraband Model #							

Choice	*Metal Detection*	Probability of Detection Tools	Explosives	Small Arms	**Active on Entry Against** People	Packages	Vehicle and Cargo	Authorized (Tools, Vehicles)	Other Feasible (Throwover)
	- Handheld								
	A. Ferrous and solid lead materials	75	25	50					
	B. Ferrous materials and all forms of lead	75	25	50					
	C. Ferrous materials only	75	25	50					
	- Portal								
	A. Ferrous and solid lead materials	90	80	60					
	B. Ferrous materials and all forms of lead	90	80	60					
	C. Ferrous materials only	90	80	60					
	Xray								
	Standard	90		60					
	Search				▨	▨	▨	▨	▨
	- Personnel					▨	▨		
	A.Patdown	90	30	90		▨	▨		
	B. Strip inspection	90	90	90		▨	▨		
	- Item				▨		▨		
	A. Cursory	10	10	10	▨		▨		
	B. Rigorous	75	45	75	▨		▨		
	- Vehicle				▨	▨			
	A. Cursory	10	10	10	▨	▨			
	B. Rigorous including cargo	50	25	50	▨	▨			
	Explosive Detector								
	A. Animal olfaction		10						
	B. Handheld vapor collection		45						
	C. Thermal neutron		25						
	D. Vapor collection		35						

Figure 19.3. Contraband Modeling Worksheet (Entry)



Element Modeled - For Exit Code

Contraband Model #

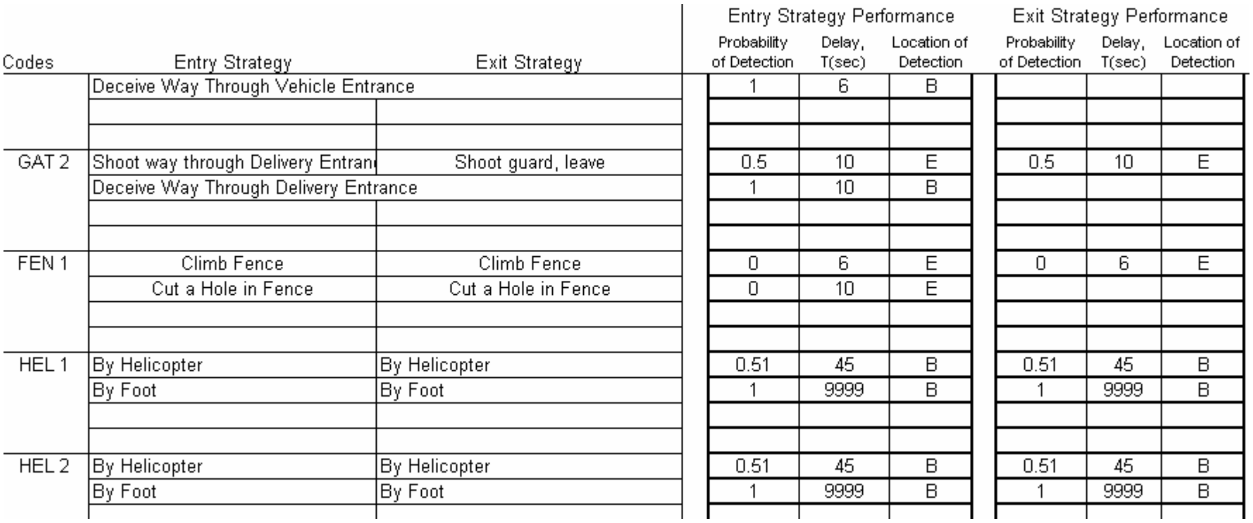
			Allowed Exit				
			People	Packages	Vehicle and Cargo	Authorized (Tools, Vehicles)	Other (Throwover)
			Active on Exit Against				
Choice	*SNM Detection*	Probability of Detection	People	Packages	Vehicle and Cargo	Authorized (Tools, Vehicles)	Other Feasible (Throwover)
None	Drive Thru SNM Monitor	SNM Nothing					
None	Handheld SNM Monitor	Probability of Detection					
None	Portal SNM Monitor	Probability of Detection					
	Probability of Detection of shielding	Probability of Detection					
	User Defined Safeguard						

Figure 19.4. Contraband Modeling Worksheet (Exit)

3.5 Save Enter the performance data into PANL_EX1ASD.XLS and save it as PANL_EX3.xls

To enter data into PANL, select the “Input Performance Data” Tab and input the data in the appropriate columns (see Figure 19.5) for the elements and areas and element strategies you worked on in 3.1 to 3.5. When you have completed entering data, save your file.

	What You Do	Comments/Prompts
1	To enter data, return to the “Element Strategies” worksheets and select “Input Performance Data.”	
2	Input the performance data – (PD, delay time, and location of detection) for the element and element strategies you worked on.	See Figure 19.5 below for the appropriate columns.
2	Select “Save As….” on the drop down menu.	
3	Enter the filename “PANL_EX3.xls” and then click on the “Save” button.	Don’t forget to save your work.



			Entry Strategy Performance			Exit Strategy Performance		
Codes	Entry Strategy	Exit Strategy	Probability of Detection	Delay, T(sec)	Location of Detection	Probability of Detection	Delay, T(sec)	Location of Detection
	Deceive Way Through Vehicle Entrance		1	6	B			
GAT 2	Shoot way through Delivery Entran	Shoot guard, leave	0.5	10	E	0.5	10	E
	Deceive Way Through Delivery Entrance		1	10	B			
FEN 1	Climb Fence	Climb Fence	0	6	E	0	6	E
	Cut a Hole in Fence	Cut a Hole in Fence	0	10	E			
HEL 1	By Helicopter	By Helicopter	0.51	45	B	0.51	45	B
	By Foot	By Foot	1	9999	B	1	9999	B
HEL 2	By Helicopter	By Helicopter	0.51	45	B	0.51	45	B
	By Foot	By Foot	1	9999	B	1	9999	B

Figure 19.5. Depiction of Element Strategies Worksheet

Exercise 4. PANL Path Analysis

PANL uses the information performance data and the ASD connectivity and supplements it with information about the facility response to that adversary

This exercise will show the participants how to enter the settings for an analysis in PANL, to find the most-vulnerable path and then review the path results. We will continue with the example of the PTR physical protection system.

For this analysis **assume the following information:**

- The response strategy is to prevent an adversary theft of fresh fuel for vault R090.
- The expected response force time range is 60 to 600 seconds (i.e., 1 to 10 minutes).
- The threat will be a terrorist traveling on foot.
- The adversary will use the following intrusion methods: force, stealth, and deceit (so use all of the strategies listed).
- The facility state will be normal shift workday conditions.

4.1 PANL Analysis Setup

	What You Do	**Comments/Prompts**
1	On the Element Strategies worksheet, review each element's strategy and performance value list (the entry values are shown first and then the exit values). Deactivate strategies that are associated with vehicle or helicopter transportation	Enter TRUE to Activate and FALSE to Deactivate Strategies in columns AB and AC. Note: This causes the threat to travel on foot at all times.
2	Also deactivate all off shift strategies.	Note: This causes the state to be normal workday conditions.
3	At the top of the Element Strategies worksheet, select "Create and Run Path Analysis."	This moves to the Analysis 1 worksheet.
4	Then, fill in the response information: For RFT's enter 10 as the number of RFT's and then enter 60, 120, 180, 240, 300, 360, 420, 480, 540, and 600 as values.	Enter number of RFTs in cell B5 and the RFT numbers in cells B7 to B16. (The cells B17 and B18 are filled in by PANL.)
5	Then click on the "Containment" response strategy checkbox under Response Strategy.	Enter P(N)'s if you like in column I. Determining P(N) for several RFT's is covered in more detail in the Neutralization Subgroup.

4.2 Execute The Analyze Command And Save Your File

After entering the data for the outsider analysis setup data, execute the analysis.

	What You Do	Comments/Prompts
1	Select “Run Path Analysis” button at the top of the Element Strategies worksheet.	
2	Review and discuss your results.	
3	Select “File” on the top menu bar.	
4	Select “Save as…” on the drop down menu.	
5	Select “Save as…” on the drop down menu. Save your file as “PANL_EX4.xls” and then click on the “Save” button”.	
6	Save your file as “PANL_EX4.xls”.	

4.3 Determining Minimum Delay and Minimum Probability of Assessed Detection

It is useful to determine the minimum delay through the entire physical protection system. If this time is less than the Response Force Time, delay needs to be increased before any detection contributes to Probability of Interruption.

4.3.1 Minimum Delay Through The Physical Protection System (PPS)

This part of the exercise will help the participants understand how to determine minimum delay through the PPS. This exercise requires working in the Outsider Module.

	What You Do	Comments/Prompts
1	Examine cell H18.	
2	Answer the questions below.	

? What is the Total System Minimum Delay (shown as Cumulative Path Delay in the PANL Report) for a theft attack? ________________

☛ Review the critical path**.**

It may also be useful to determine the minimum Probability of Assessed Detection through the entire (without concern for whether it is timely or not) physical protection system because if this probability is low, Probability of Interruption will be low.

4.3.2 Minimum Probability of Detection Through The Physical Protection System

This part of the exercise will help the participants understand how to determine minimum Probability of Detection (P_D) through the system.

	What You Do	Comments/Prompts
1	Examine cell H17	
2	Answer the questions below.	

? What is the Total System Minimum Probability of Assessed Detection (P_{AD}) as measured by Probability of Interruption for the Most Vulnerable Path?

____

☛ Review the critical path.

? Are the critical pathways for minimum delay and minimum Probability of Assessed Detection the same? Yes No

? Why or why not?

____

? What is the significance of the results for Section 4.3?

____

____

Preparation for PANL Exercise 5

This exercise assumes that you are starting in the PANL application, with the file "PANL_EX4.xls" already loaded but the analysis not set up yet. ***If you have completed exercise 4, go directly to the body of Exercise 5***.

	What You Do	Comments/Prompts
1	On the Element Strategies worksheet, review each element's strategy and performance value list (the entry values are shown first and then the exit values). Deactivate strategies that are associated with vehicle or helicopter transportation	Enter TRUE to Activate and FALSE to Deactivate Strategies in columns AB and AC. Note: This causes the threat to travel on foot at all times.
2	Also deactivate all off shift strategies.	Note: This causes the state to be normal workday conditions.
3	At the top of the Element Strategies worksheet, select "Create and Run Path Analysis."	This moves to the Analysis 1 worksheet.
4	Then, fill in the response information: For RFT's enter 10 as the number of RFT's and then enter 60, 120, 180, 240, 300, 360, 420, 480, 540, and 600 as values.	Enter number of RFTs in cell B5 and the RFT numbers in cells B7 to B16. (The cells B17 and B18 are filled in by PANL.)
5	Then click on the "Containment" response strategy checkbox under Response Strategy.	Enter P(N)'s if you like in column I. Determining P(N) for several RFT's is covered in more detail in the Neutralization Subgroup.

<u>Execute the Analyze Command</u>

After entering the analysis data for PANL, you will want to execute the analysis.

	What You Do	Comments/Prompts
1	Select "Run Path Analysis" button at the top of the Analysis worksheet.	
2	Review and discuss your results.	
3	Select "File" on the top menu bar.	
4	Select "Save as…" on the drop down menu.	
5	Select "Save as…" on the drop down menu. Save your file as "PANL_EX4.xls" and then click on the "Save" button".	
6	Save your file as "PANL_EX5.xls".	

Exercise 5 – Most Vulnerable Path, System Balance, Protection-in-Depth

5.1 RFT sensitivity analysis and path analysis

You are now going to review a sensitivity analysis.

	What You do	Comments/Prompts
1	At the top of the Performance Data worksheet, select “Sensitivity Graph.”	
2	Use the graph to answer the questions following the figure.	The figure below is just shown as an illustration.

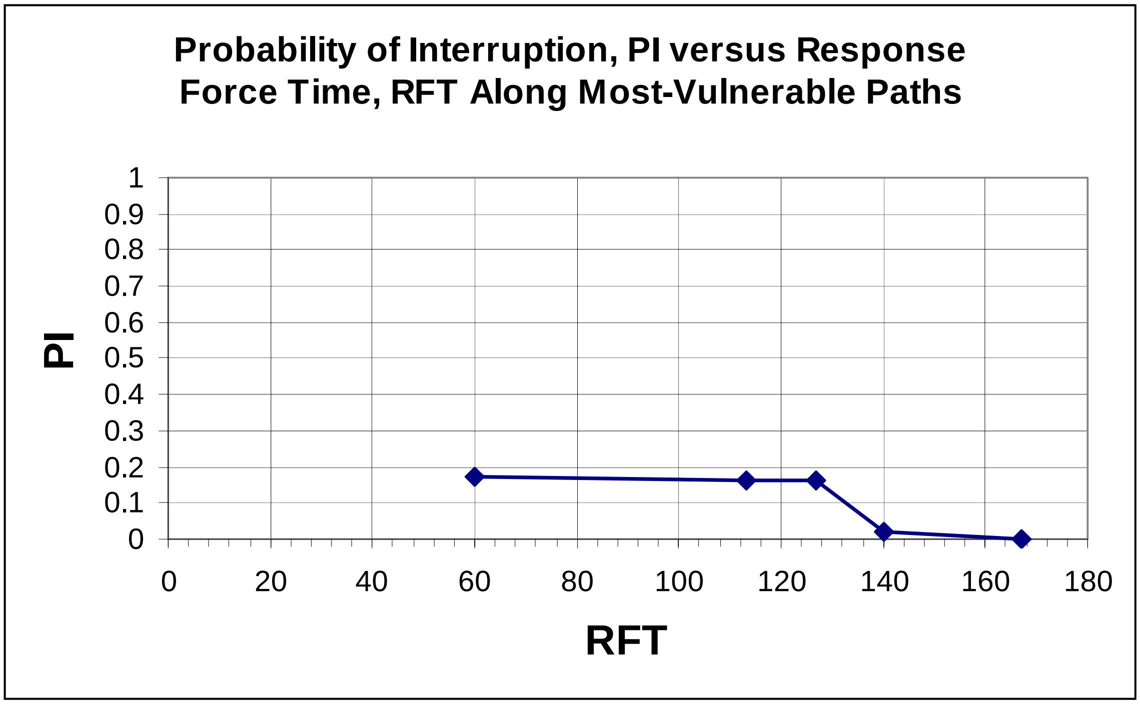


Figure 19.6. Sensitivity Graph (Most Vulnerable Path to RFT (from 60 to 180 seconds))

? What is the largest value of P_I for this range of RFTs?

____

? Is this an acceptable result? Yes No

> **Note:** When evaluating a facility, it is useful to distinguish between a desired level of performance – the level of security performance you would like to achieve – and a required level of performance – this is the minimal security performance required (or acceptable to regulatory decision-makers) to protect against the threat. For the present exercise, assume that the desired P_I level is 1.0 and the required P_I level is *.94*.

? What is the largest RTF where P_I is greater than 10%?

__________________seconds

	What You Do	Comments/Prompts
1	Examine cells D7 to D16 associated with RFT's in cells B7 to B16.	
2	Answer the following questions.	

? What is P_I at this RFT? __________________________

? Where is the critical detection point for this RFT?
____

? What is the cumulative path delay remaining after the Critical Detection Point? ________________seconds

? What is the time remaining after interruption? _______________seconds

? Describe the most vulnerable path for this RFT.

____

____

____

5.2 System Balance

This exercise looks at the system balance in terms of the Probability Detection (P(D)) and Delay at different protection layers.

5.2.1 Protected Area Boundary

Using the information from the Element Strategies worksheet and the Analysis worksheet, complete the table below for the protection layer between the Institute Limited Area and the PTR Protected Area, by filling in the:

- From Element Strategies worksheet:
  - o Minimum probability of detection for each element against forceful or stealthy tactics (e.g., leave out Deceit strategies) on entry;
  - o Minimum delay time across each element across all forceful or stealthy strategies on entry;
- From Analysis worksheet:
  - o Minimum Probability of Interruption through this element (see Minimum P_I Through Element listing at the top right in columns AA to AL of the worksheet); and
  - o Minimum Probability of Interruption through this element (see Minimum P_I Around Element listing at the top of columns AN to AY of the worksheet).

Probability of Assessed Detection and Delay Protection Path Elements for the Layer Between the Limited Area and the Protected Area

	Protection Path Elements			
	PER	ISO	VEH	VEH
Force/Stealth P(D)				
Delay (seconds)				
Min P_I Through this Element				
Min P_I Around this Element				

Balanced Detection

? Does this PPS layer have balanced detection? Yes No

? Which elements need detection upgrades?

____

? What P_D on these elements would give a balanced detection layer?

____

Balanced Delay

? Does this PPS layer have balanced delay? Yes No

? Which elements need delay upgrades?

____

? What delay on these elements would give a balanced delay layer?

____

5.2.1 Protection Layer between the Protected Area and the Reactor Building

Using the information from the Performance Data worksheet, now complete the table below for the protection layer between the PTR Protected Area and the PTR Reactor Building by filling in the:

- From Element Strategies worksheet:
  - Minimum probability of detection for each element against forceful or stealthy tactics (e.g., leave out Deceit strategies) on entry; and
  - Minimum delay time across each element across all forceful or stealthy strategies on entry.
- From Analysis worksheet:
  - Minimum Probability of Interruption through this element (see Minimum P_I Through Element listing at the top right in columns AA to AL of the worksheet); and
  - Minimum Probability of Interruption through this element (see Minimum P_I Around Element listing at the top of columns AN to AY of the worksheet).

	Protection Path Elements						
	PER	**WND**	**SUR**	**SUR**	**DUC**	**SHD**	**EMX**
Force/Stealth P(D)	0.45		0.0			0.20	
Delay (seconds)	2		120			12	
Min P_I Through this Element							
Min P_I Around							

this Element							

Balanced Detection

? Does this PPS layer have balanced detection? Yes No

? Which elements need detection upgrades?

____

? What P_{AD} on these elements would give a balanced detection layer?________________________

Balanced Delay

? Does this PPS layer have balanced delay? Yes No

? Which elements need delay upgrades?

____

? What delay on these elements would give a balanced delay layer?

____

5.2.2 Protection in Depth

Consider only the **minimum** values of detection and delay for only the two layers discussed above.

? Does this part of the system have detection protection-in-depth?
Yes No

? Why or why not?

____

? If not, what would be a recommended upgrade?

____

? Does this part of the system have delay protection-in-depth? Yes No

? Why or why not?

____

____

? If not, what would be a recommended upgrade?

____

Preparation for PANL Exercise 6

Exercise 6 assumes that you are starting in the PANL application, with the file “PANL_EX5.xls” already loaded.

.

Exercise 6 – Upgrade and Sensitivity Analysis

The PANL software provides a sensitivity analysis for response force time values because response force time affects all paths. The results of this analysis are presented by the graph given as a part of the PANL Outsider results (see Figure 19.6 for an example of this graph).

A sensitivity analysis can also be done for any of the element input values but requires one analysis per parameter. This exercise looks at varying the target task delay time. Consider a worst-case value (3 minutes) and a best-case value (6 minutes) and two values (4 minutes and 5 minutes) between these.

6.1 Sensitivity Analysis - Preparation

Consider the target task time for R091, currently set to 15 seconds (time to collect a goal quantity).

	What You Do	Comments/Prompts
1	On the Element Strategy worksheet scroll down until you see the OPN location (around line 130) and in the lower-right hand pane scroll to column Q.	
2	Enter 180 seconds as the OPN location delay time.	
3	Select the “Create and Run Path Analysis” button	This should take you to the analysis page. Record P_I for RFT = 15 sec. in the following table.
4	Select “Run Path Analysis” to execute the analysis.	This uses the same analysis settings found in PANL_EX5.xls.
5	Save as PANL_EX6_180.xls	Record P_I for RFT = 180 seconds.
6	Perform steps 2-4, but this time with 240 seconds as the OPN location delay time on the Element Strategy worksheet. Save as PANL_EX6_240.xls	Record P_I for RFT = 240 seconds.
7	Similar to 6, but use 300 sec. at the OPN location. Save as PANL_EX6_300.xls.	Record P_I for RfT = 300 seconds.
8	Repeat 7, but with 360 sec.	Record P_I for RFT = 360 seconds.
8	Answer the following questions.	Based on data in the table.

	Target Task Time	**P_I**	**Time Remaining after Interruption (TRI)**
Best case value:	6 min.(360 sec.)		
Intermediate value 1:	5 min.(300 sec.)		
Intermediate value 2:	4 min.(240 sec.)		
Worst case value:	3 min.(180 sec.)		

? Are any of these delay values acceptable if the desired P_I level is 1.0 and the required P_I level is *.94*? Yes No

Note: When evaluating a facility, it is useful to distinguish between a desired level of performance (the level of security performance you would like to achieve) and a required level of performance (the minimal security performance required [or acceptable to regulatory decision-makers] to protect against the threat).

6.2 Physical Protection System Upgrades

	What You Do	**Comments/Prompts**
1	Study the PANL results in Exercise 5 especially the balance results.	
2	Propose and enter two PPS upgrades for the research reactor.	Consider improving detection before the critical detection point and delay after the critical detection point.
3	At the top of the Performance Data worksheet with no results, select “New.”	This creates a new worksheet with your performance values that will not be affected by this set of analyses.
3	Enter upgrades in PANL_EX6.xls	
4	Analyze with the PANL and note the results.	For your analysis, analyze for an adversary on foot.

? Summarize each of the following:

Detection Upgrade(s)

____

____

____

Delay Upgrade(s)

____

____

____

? What is the probability of interruption and the time remaining after interruption (TRI) for the most vulnerable path for the upgrades entered above for a response force time of 320 seconds?

P_I __________ **TRI** __________

When upgrading a facility, it is useful to distinguish between a desired level of performance (the level of security performance you would like to achieve) and a required level of performance (the minimal security performance required [or acceptable to regulatory decision-makers] to protect against the threat). These levels can be determined using the concept of risk, covered later in this course. For the present exercise, assume that the desired P_I level is 1.0 and the required P_I level is 0.*94*.

? Will your upgrades allow you to achieve the acceptable P_I? Yes No

? Will your upgrades allow you to achieve the desired P_I? Yes No

Application Considerations

1. A measure of PPS effectiveness provided by PANL is the probability of interruption. How does this measure relate to the probability of neutralization?

2. Can the PANL software be used to analyze a specific single path?

3. Why would you want to do a sensitivity analysis for your input data for the PANL software?

4. What input data to the PANL software do you feel most uncomfortable about? Why?

5. How could you use PANL to analyze an insider threat scenario?

20. Neutralization Analysis

Abstract. *Response, along with detection and delay, is one of the three major physical protection functions in the DEPO. Probability of neutralization (P_N) is one of the measures of effectiveness of the response function, along with the comparison of delay times and response times. This probability determination first requires making the choice of a determination methodology, and then requires information about the response forces, the threat, and the physical protection system (PPS). Information required includes not only specific characteristics such as weapons and training, but also the Rules of Engagement at the facility and the Order of Battle at each target set. There are five general categories of methodologies: expert opinion, simple numerical methods, complex computer simulations, physical engagement simulations, and actual engagements.*

20.1 Introduction

Probability of Neutralization (P_N) Is the Measure of Effectiveness of Response

The PPS at a nuclear facility consists of detection, delay, and response functions. The purpose of the response function is to render the adversary incapable of completing his goal. The response function at a facility can be characterized by collecting the appropriate data. However, the analyst must still develop some measure of effectiveness of the response.

For ***sensors***, the measure of effectiveness is the ***probability of detection***.
For ***barriers***, the measure of effectiveness is the ***delay time***.
For ***response***, the measure is ***probability of neutralization***.

The determination of this probability will require information about the response forces, the threat, and the PPS, as well as the choice of a methodology. The purpose of this lecture is to provide the necessary information and a suggested approach to allow the determination of probability of neutralization.

20.2 Terminology and Definitions

Engagements and Wins

Before attempting to determine the effectiveness of a response force in neutralizing an adversary force, some terms must be defined. An engagement is defined as an event where two opposing forces, such as the response force and an adversary force, use weapons and tactics in an attempt to achieve their respective goals. Obviously, since many random variables are involved in the engagement, there are many possible outcomes. A win is defined as one of the following outcomes of the engagement: the adversary force is killed, captured, or abandons the attack and flees.

Probability

Probability is the chance that a given event will have a certain outcome. More precisely, if there exists a number n of equally likely possible outcomes to an event, of which a number s of these outcomes are regarded as favorable, then the probability of a favorable outcome is given by the ratio s/n (Reference 1). If the event under consideration is an engagement, then the favorable outcome is a win.

Probability of Neutralization defined

In light of the above, probability of neutralization is now easily defined by the following equation:

$$PN = N(\text{wins}) / N(\text{engagements})$$

The number of engagements in the denominator is a statistically significant number in accordance with the Law of Large Numbers. This law states that as the number of times in which an event is repeated becomes larger and larger, the proportion of successful outcomes will tend to come closer and closer to the actual probability of success. In using the defining equation in an analysis process, it should be kept in mind that all engagements must have the same initial conditions, and there are only two possible outcomes per engagement: win or loss.

Processes

There are two types of processes that can determine the outcome of an event: *deterministic* processes and *stochastic* processes. A deterministic process is one in which results or outcomes are causally determined either by preceding events or by natural laws. When an event is governed by deterministic processes, the outcome only needs to be calculated once, because given the same initial conditions, the event will always have the same outcome.

Unfortunately, engagements are *stochastic* processes. A stochastic process is one in which various random outcomes are possible due to the fact that the process involves random variables. The probability of casualty attributed to a weapon is an example of a random variable in an engagement. Figure 22-1 illustrates the probability of casualty versus range for a generic handgun (HG) and a generic semi-automatic rifle (SAR).

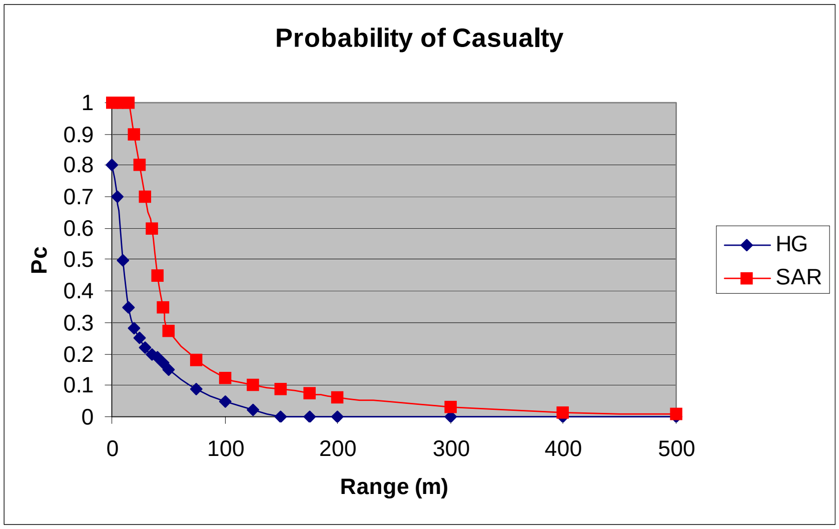


Figure 20-1. Probability of casualty vs. range.

20.3 Threat Data

Threat Posture

Neutralization analysis requires data on the threat, the response, and the PPS. Threat data includes threat type and numbers, targets, goals, and the information gathered during the Threat Definition process. Information about the threat necessary for P_N analysis is summarized in Table 20-1.

Table 20-1. Threat Posture Data

• Target	• Special tactics – Ambush – Diversion – Vehicle bomb
• Strategy	
• Type	
• Number	
• Weapons	• Body armor
• Transport	• Communications
• Training	• Path delay in
• Equipment	• Target task time
	• Path delay out

20.4 Response Force Data

Response Force Posture

Similar, but more detailed, information is required about the response forces to determine P_N. In addition to response force posture data, listed in Table 20-2, the Rules of Engagement and Order of Battle for each target must be known. The response force posture data contains the usual information about weapons, strategies, numbers of guards, transport, response times, etc., for each target.

Table 20-2. Response Force Posture Data

• Strategy	• Body armor
• Guard types	• Communications
• Numbers	• Response times: – alarm communication – assessment – deployment order – preparation – travel – deployment
• Weapons	
• Locations	
• Transport	
• Tactics	
• Training	
• Equipment	

Rules of Engagement

Rules of Engagement include the conditions and procedures under which various elements of the response force must operate, including when the use of deadly force might be authorized. For the purposes of P_N analysis, it is sound practice to collect sufficient information to construct a table for each target similar to that shown in Table 20-3. As shown in the table, the rules of engagement for each response group or type of responder should include a strategy and an objective, as well as tactics and techniques.

Strategies

Strategies for Table 20-3 could include, but may not be limited to:

- Deterrence,
- Denial,
- Containment,
- Pursuit, and
- Recapture/recovery.

Objectives of the Strategy

Each strategy should have an objective, which may include:

- Observation,
- Delay,
- Interruption,
- Neutralization,
- Arrest, and
- Backup

Tactics

A strategy is implemented through the use of tactics. Tactics are very dependent on the facility, competent authority regulations, and the organization that trains and controls the response. Tactics can include:

- Engage at will,
- Engage on command,
- Engage on necessity, and
- Coordinated engagement.

Techniques for Executing Tactics

Finally, there are the techniques that the response uses with each tactic-strategy combination. Techniques may include, in increasing order of force:

- Verbal command,
- Non-lethal force,
- Deadly force, and
- Other.

Table 20-3. Rules of Engagement

Response	Strategy	Objective	Tactic	Technique
Target posts				
Other posts				
Patrols				
Tactical teams				
Local Law Enforcement Agencies (LLEAs)				
Other				

Order of Battle

The Order of Battle ***as defined for this discussion*** is the temporal order in which individual guards or groups of responders are encountered by the adversary. The encounters may occur either as the adversary traverses the path to and from the target, or as successive responders arrive at a specific battle site and engage the adversary. The Order of Battle is target-specific, so it is recommended that a table such as Table 20-4 be completed for each target along the most vulnerable path of each target.

Table 20-4. Example Order of Battle

Target: R091 vault		**Condition:** offshift	
Response	**Type**	**numbers**	**time**
1st	Portal guards	2	0 sec
2nd	Interior post	1	30 sec
3rd	Ft. patrol	1	60 sec
4th	Special Response Team (SRT)	5	180 sec
5th	LLEA	4	30 min

20.5 Neutralization Analysis Methods

Methods for Determining P_N

Methods for determining probability of neutralization (P_N) include:

- expert judgment (opinion),
- simple numerical calculations,
- complex numerical simulations (computerized war games),
- physical engagement exercises (force-on-force), and
- actual engagements.

Each category has its advantages and disadvantages, primarily in terms of time, cost, and accuracy.

Expert Judgment

Expert judgment is the opinion of one or more subject matter experts about the effectiveness of the response forces. This opinion must be tempered by the background and experience of the expert, knowledge of the response forces at the facility, and knowledge of the threat. Expert judgment is difficult to verify, and, unless the same expert is involved in all of the estimations, results can vary from site to site and even target to target. Further, if two or more experts disagree, there is no way to tell if the P_N is valid.

Tabletop Analysis

Tabletop (or sand table or military map) analysis involves using a map or site schematic with either icons or figurines to represent combat elements. This method has been used in warfare at least since Roman Legion times, and probably earlier. Commanders can place the icons in various positions on the map and debate the outcome of possible engagements. A crucial element for tabletop analysis is the method used to determine the outcome of engagements. Expert judgment, data tables, or a set of rules with simple numerical calculations are the most common methods.

Simple Numerical Calculations

Simple numerical calculations are often used in place of or to augment expert judgment determinations. Simple numerical calculations include data tables, curve-fitted equations, continuous time Markov chain (CTMC) methods, and Monte Carlo methods. Figure 20-2 is an example of a data table. The figure presents a comparison of a curve-fit equation with the results of a more complex CTMC solution.

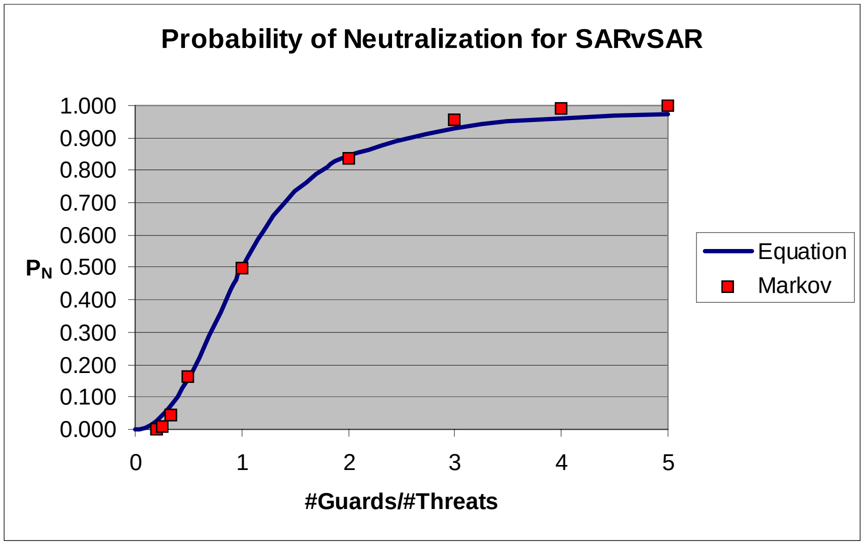


Figure 20-2. Curve-fit equation and Markov chain solution.

Markov Chains

Since engagements are stochastic processes, the analysis of an engagement must involve a solution technique that incorporates probabilities. Two preferred methods are the Markov Chain method and Monte Carlo simulations.

The Markov Chain method is a path-independent stochastic process in which probabilities of occurrence of future states depend only on the present state or the immediately preceding state. Reference 2 uses this process to develop a state transition diagram and solve the resulting time-dependent transitions from initial state to all probable outcomes of interest. Reference 3 discusses the general development and solution of CTMC. Figure 20-3 illustrates the state transition diagram, where the transition rates are listed as Greek variables between the various states.

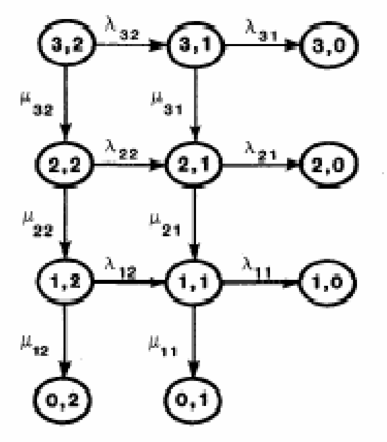


Figure 20-3. Markov chain state transition diagram.

The ASSESS Neutralization Module (Reference 4) is an example of a numerical method based on Markov chains. This computer methodology uses probability of kill (P_K) data for various weapons and analysts' descriptions of firing posture, exposure, and other factors to simulate engagements in a manner similar to battles fought in the 1700s. That is, all the combatants stand in a line and fire at each other. A Markov chain is constructed to determine P_N as a function of successive volleys fired by both sides. The main advantages of such simple numerical calculations are (1) low cost and (2) reproducible results, as long as the same input data are used.

Monte Carlo Simulations

Monte Carlo methods involve the use of random sampling techniques. Monte Carlo computer simulations are used to obtain approximate solutions to mathematical or physical problems involving a range of variables, each of which has a calculated probability of being the solution.

Table 20-5 presents an example of a Monte Carlo process for determining the outcome of individual engagements. Two coins are flipped to determine the results of a guard and a threat each firing one shot at the other. A "head' means that the shooter missed his target, and a "tail" means that the target was killed. Thus the implied probability of casualty of each weapon is 50%. One possible outcome, number 1, is that both shooters miss. In this case, the coins are flipped again, representing a second shot. The process is repeated until the engagement outcome obtained is either possibility 2, 3, or 4. If a statistically significant number of engagements are evaluated in this manner, and all wins and losses are recorded, the probability of neutralization for this specific type of engagement can be calculated using the defined formula presented above. It is interesting to note that even though the implied weapon probability of casualty is 50%, the probability of neutralization for this engagement is 66.7%.

Table 20-5. Monte Carlo Simulation of 1 vs. 1 Engagement

Outcome:	1		2		3		4	
Combatant:	guard	threat	guard	threat	guard	threat	guard	threat
Toss result:	H	H	T	H	H	T	T	T
Represents:	misses	misses	hits	misses	misses	hits	hits	hits
Shot result:	alive	alive	alive	dead	dead	alive	dead	dead
Net result:	Shoot again		win		loss		win	

Computerized Engagement Simulations

Computerized engagement simulations are a third category. The Joint Tactical Simulation (JTS) will be used as an example in this discussion. The JTS is a multi-user computer simulation developed for analysis of large-scale force-on-force engagements. JTS was adapted from a U.S. Army application by one of the U.S. Department of Energy (DOE) national laboratories for use in doctrinal planning. JTS evolved from the original military map and tabletop exercises, but is more sophisticated. JTS requires a minimum of two highly trained users and significant setup time. The simulation also requires at least three networked computers, one each for threat and response, and one for administrative control.

The simulation contains large databases for weapons, equipment, and individual combatant performance, including operations on varied terrain and day/night conditions. JTS also requires at least two real-time war-gamers to operate the system and simulate the engagement, and one specialist to design the battlefield and activate the appropriate numerical combatants. The results have been shown to be “operator- and player-dependent”; i.e., a skilled computer game player can sometimes defeat more able military tacticians and thus skew the results.

Simulated Physical Engagements

Simulated physical engagements are also known as force-on-force (FOF) exercises. FOF exercises are not actually evaluation methodologies but should be considered training exercises or validation exercises. At a real facility, FOF requires four groups: mock adversaries, mock responders, referees, and the on-duty response force personnel. These exercises are expensive in terms of both personnel and planning, are usually run only a few times at a facility, and can also produce skewed results. Statistically, there are usually not enough engagements to produce a probability of system win with a high confidence level. For example, if only one exercise is completed and the response forces lose, does this mean that the response force probability of neutralization is zero? Probably not!

Actual Engagements

Actual engagements have one big advantage: the outcome is a known fact. Obviously, comparison of actual engagements results with either live fire or simulation exercises can be complex and costly; however, such comparisons prove the validity of simulation techniques. A comparison of these five general methods in terms of cost and accuracy are shown qualitatively in Figures 20-4 and 20-5.

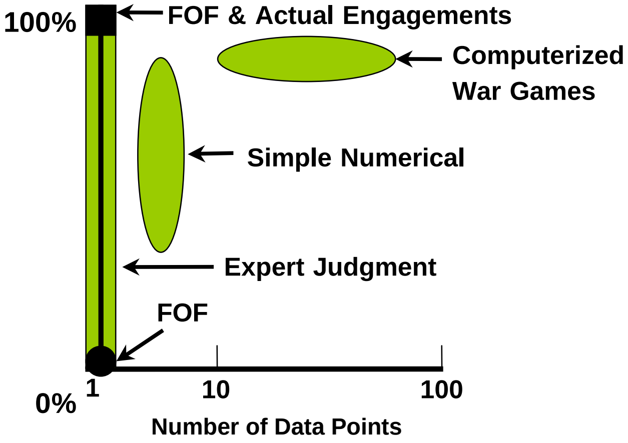


Figure 20-4. Relative accuracy of P_N methods.

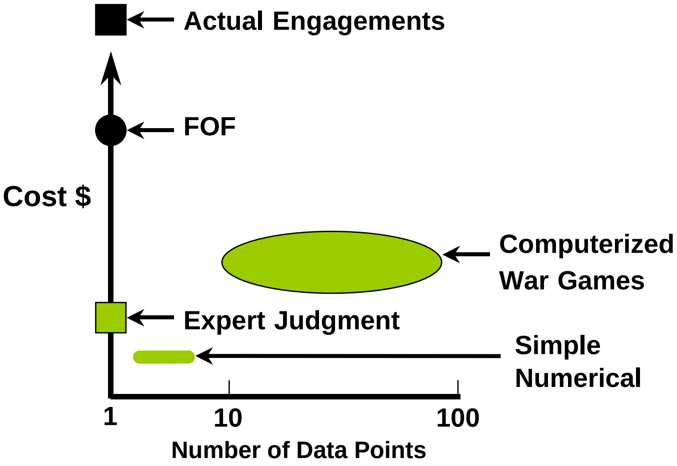


Figure 20-5. Relative cost of P_N methods.

Assessing P_N Accuracy

Figure 20-4 can be misleading as it suggests that computerized war games , F_OF, and actual battles have the highest precision; further, since dozens of data points can be collected from computerized war games this would seem to be the best approach of the three to take. Actually, each approach has relative strengths and weaknesses and computer games are no exception – see Figure 20-6. As seen in that figure, FoF exercises are good at replicating tactical behaviors by individuals, while computer-based war-games are good at producing all munitions effects and creating a comprehensive history of events. Table-tops can be performed in such a way that they explore group decision making by both the adversary leader and the security leader as this is either helped or hurt by security plans.

Force-on-Force	Computer-Based	Table-tops
Good at replicating individual behaviors ▪ Individual and team tactics	**Good at replicating events** • Munitions effects	**Good at replicating decision-making** • Security/adversary commanders • Completeness of plans
More required tasks actually executed • Murphy's law	**Comprehensive view and record of events** ▪ Engagements ▪ Movement	**Transparency to observers** ▪ Event handling ▪ Technical decisions
More fidelity in representing actual site: ▪ Terrain fidelity ▪ Actual responders	**Flexibility of application:** • Any attack location/ situation • Can run multiple iterations to develop statistical data • Less impact on operations	**When lead by an expert "ring-master" tabletops can:** ▪ Identify issues to be addressed by other simulations ▪ Bring in stakeholders as supporters that the simulation was done correctly

Figure 20-6. Relative Strengths of P_N methods.

20.6 Neutralization Analysis Process

Select a Methodology

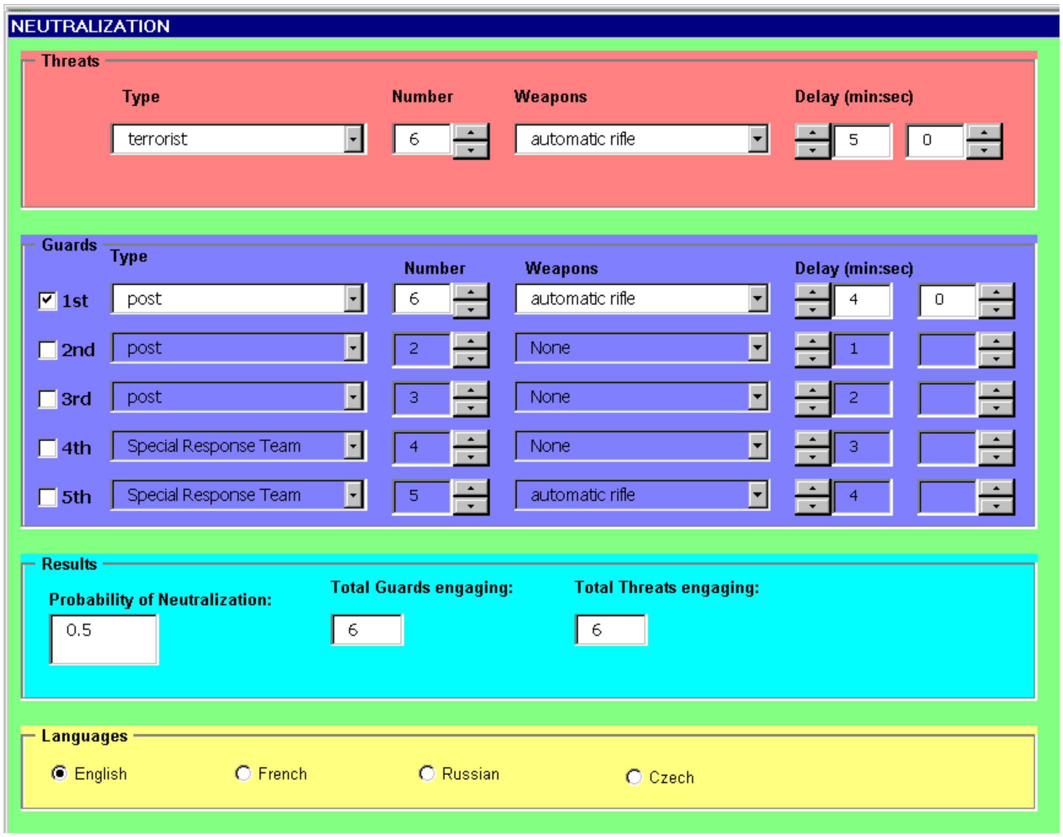
Once the appropriate data are collected, the neutralization analysis may begin. The first step is to select a methodology. In this course, a simple numerical method will be used to calculate P_N along paths. This method was developed specifically for use in this course, and the computer menu is shown in Figure 20-7.

Example Methodology with Simple Numerical Analysis

The method is based on the Markov chain concept, and uses data tables for varying numbers of guards engaging varying numbers of threats with all other engagement parameters except numbers, weapons, and arrival times being equal. Force-multiplication coefficients are used to account for differences in weapons. An exponential decay function is used to compute the effects on P_N caused when successive response groups in the Order of Battle have varying arrival times. The purpose of this basic technique is to emphasize the three most important factors for the response:

- numbers,
- weapons, and
- arrival times.

As with other data used in this course, the numbers used and derived are for teaching purposes only.



NEUTRALIZATION

Threats

Type	Number	Weapons	Delay (min:sec)	
terrorist	6	automatic rifle	5	0

Guards

	Type	Number	Weapons	Delay (min:sec)	
☑ 1st	post	6	automatic rifle	4	0
□ 2nd	post	2	None	1	
□ 3rd	post	3	None	2	
□ 4th	Special Response Team	4	None	3	
□ 5th	Special Response Team	5	automatic rifle	4	

Results

Probability of Neutralization: 0.5

Total Guards engaging: 6

Total Threats engaging: 6

Languages

● English ○ French ○ Russian ○ Czech

Figure 20-7. ITC neutralization analysis menu.

20.7 Summary

PPS effectiveness is the product of two probabilities: P_I and P_N. P_I, determined from “timely detection,” is a measure of the effectiveness of the system detection and delay along a path. P_I describes only the cumulative probability that the adversary may be interrupted. This metric alone does not answer the question of who wins—the response force or the adversary? P_N is the measure of effectiveness of the response against the adversary, independent of P_I. Together, the two define how effective the overall PPS is.

This session discussed five methods for determining the probability of neutralization (P_N). The example shows how a Markov Chain analysis technique has been put into a simple computer interface to allow the calculation of this important system parameter and then allow the analyst to compute overall system effectiveness. This computer model uses input data about the adversary and defender numbers, weapons, system delay, and response times. The output is an estimate of the probability that the defending force will be successful, or P_N.

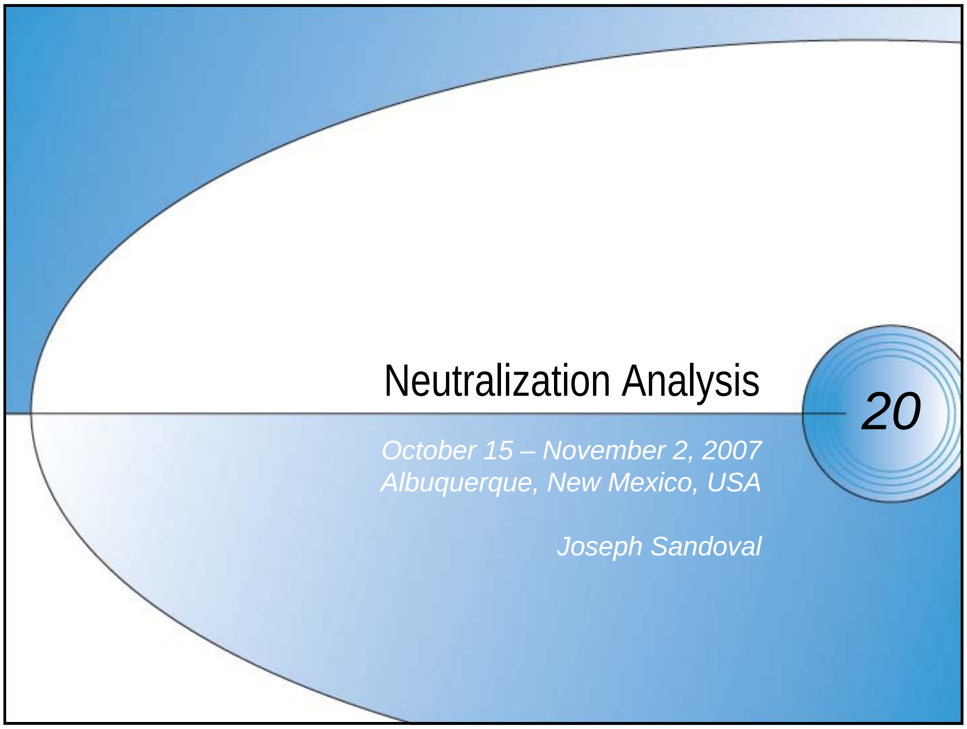
20.8 References

1. J.E. Freund, “Introduction to Probability,” Dover Publications, 1973.

2. D. Engi and C.P. Harlan, “Brief Adversary Threat Loss Estimator User’s Guide,” SAND80-0952, Sandia National Laboratories, NM, 1981.

3. D.M. Nicol and P. Heidelberger, “Parallel Algorithms for Simulating Continuous Time Markov Chains,” NASA CR-189729, 1992.

4. “Analytic System and Software for Evaluating Safeguards and Security – User’s Manual,” Sandia National Laboratories, Albuquerque, NM, 1992.

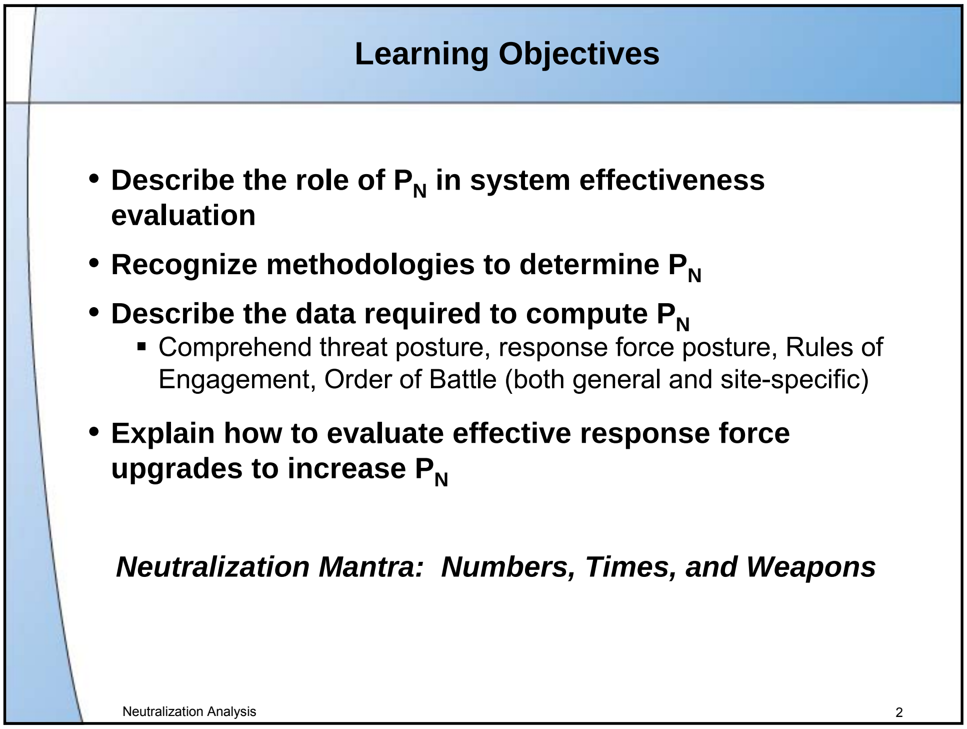


Neutralization Analysis

20

October 15 – November 2, 2007
Albuquerque, New Mexico, USA

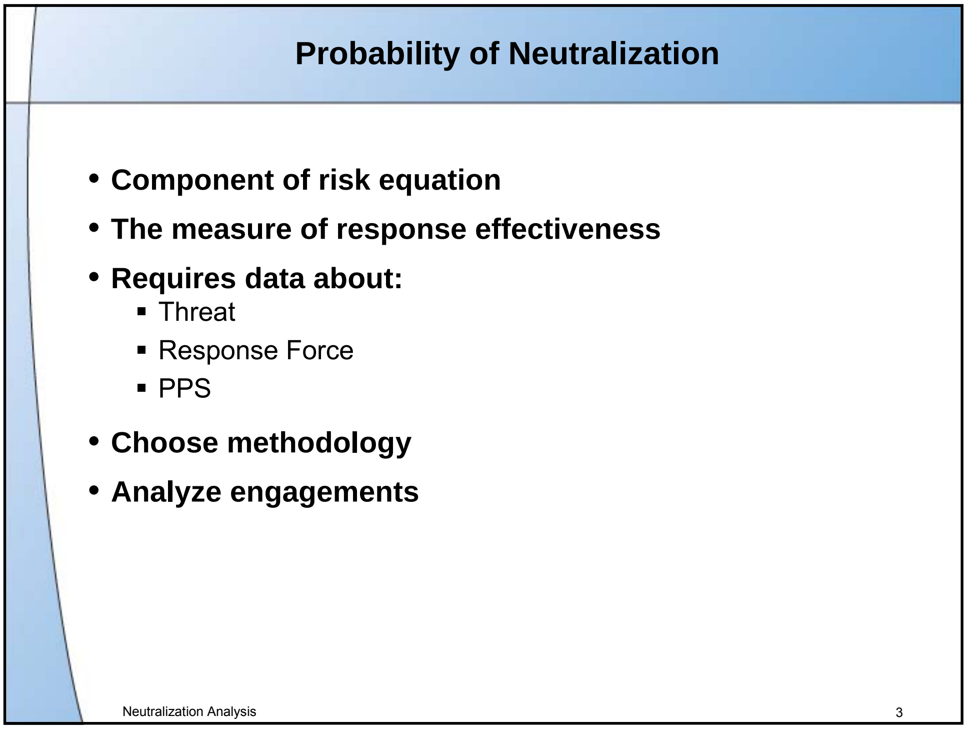
Joseph Sandoval



Learning Objectives

- **Describe the role of P_N in system effectiveness evaluation**
- **Recognize methodologies to determine P_N**
- **Describe the data required to compute P_N**
  - Comprehend threat posture, response force posture, Rules of Engagement, Order of Battle (both general and site-specific)
- **Explain how to evaluate effective response force upgrades to increase P_N**

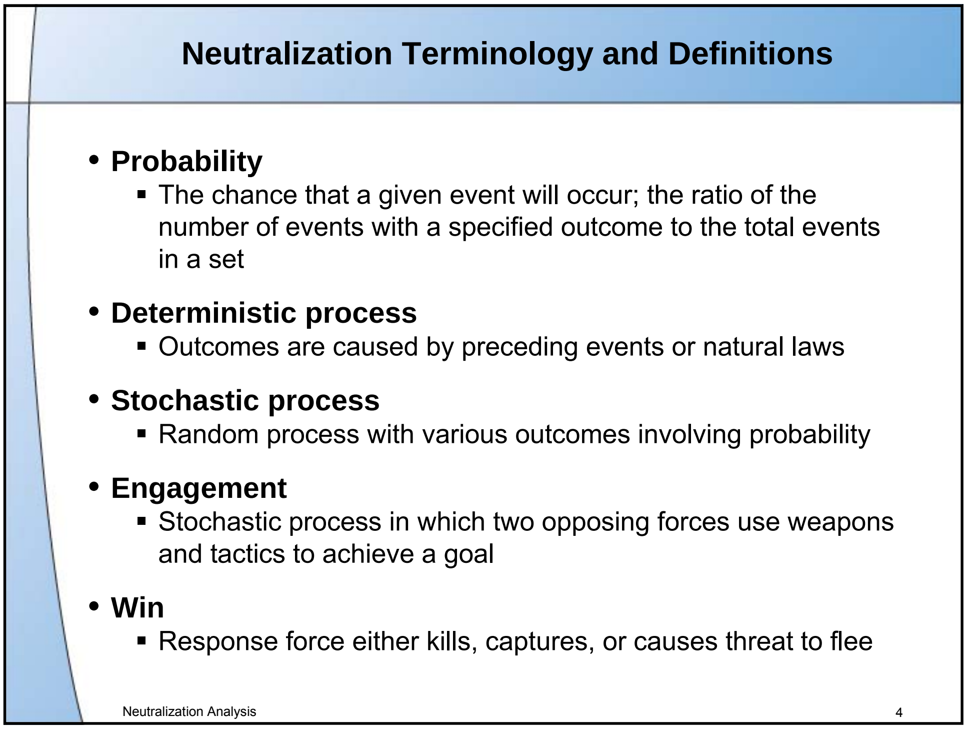
Neutralization Mantra: Numbers, Times, and Weapons



Probability of Neutralization

- **Component of risk equation**
- **The measure of response effectiveness**
- **Requires data about:**
  - Threat
  - Response Force
  - PPS
- **Choose methodology**
- **Analyze engagements**

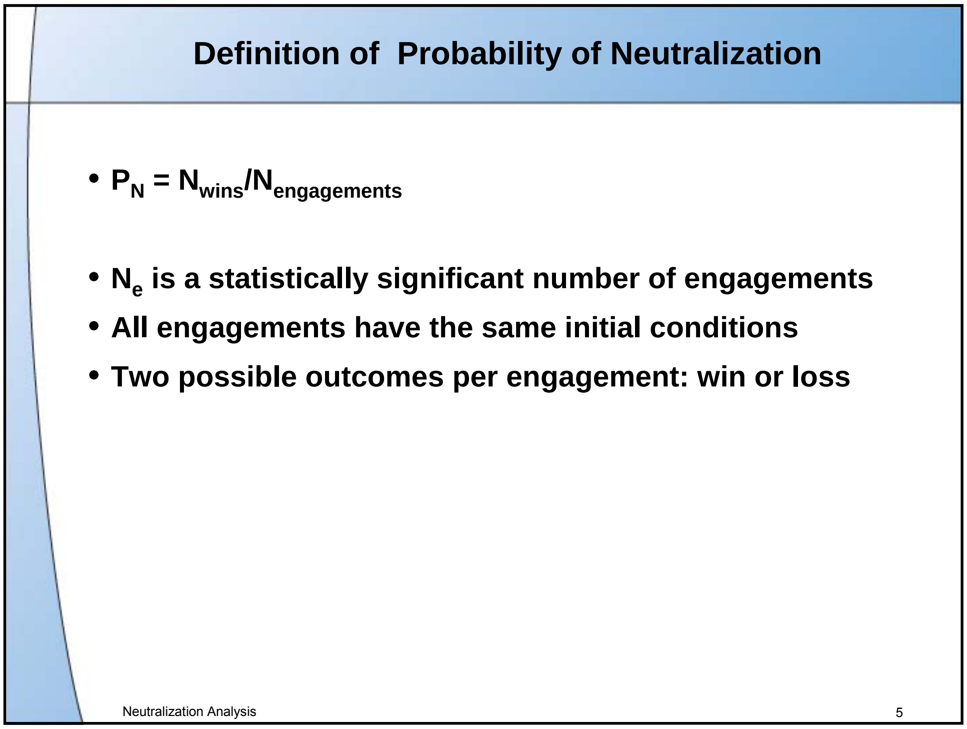
Neutralization Analysis 3



Neutralization Terminology and Definitions

- **Probability**
  - The chance that a given event will occur; the ratio of the number of events with a specified outcome to the total events in a set
- **Deterministic process**
  - Outcomes are caused by preceding events or natural laws
- **Stochastic process**
  - Random process with various outcomes involving probability
- **Engagement**
  - Stochastic process in which two opposing forces use weapons and tactics to achieve a goal
- **Win**
  - Response force either kills, captures, or causes threat to flee

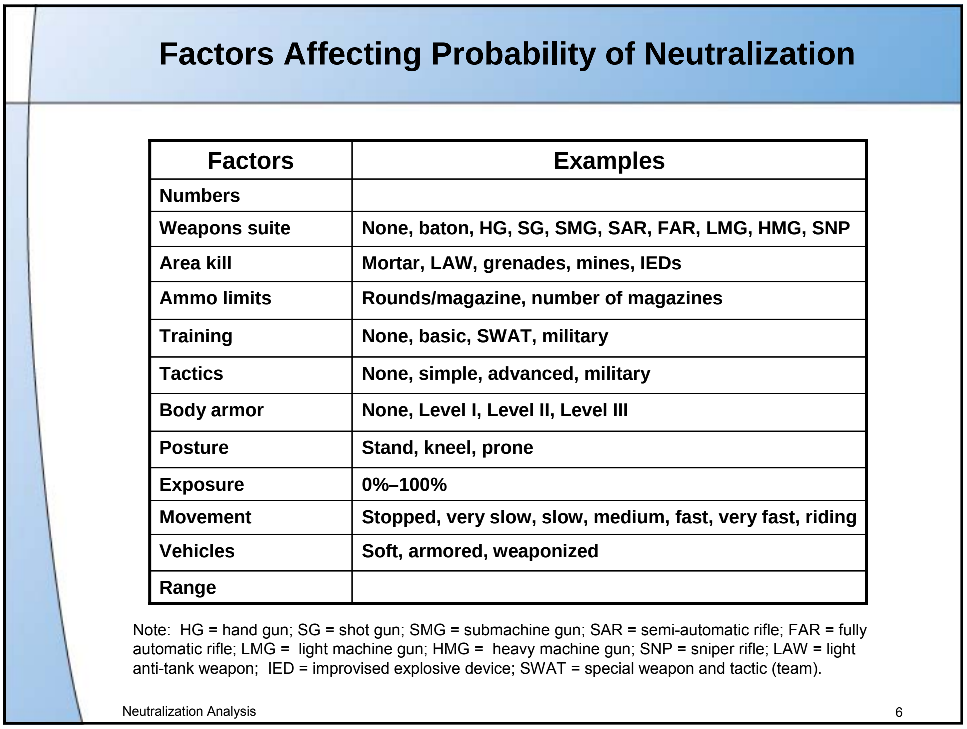
Neutralization Analysis 4



Definition of Probability of Neutralization

- $P_N = N_{wins}/N_{engagements}$

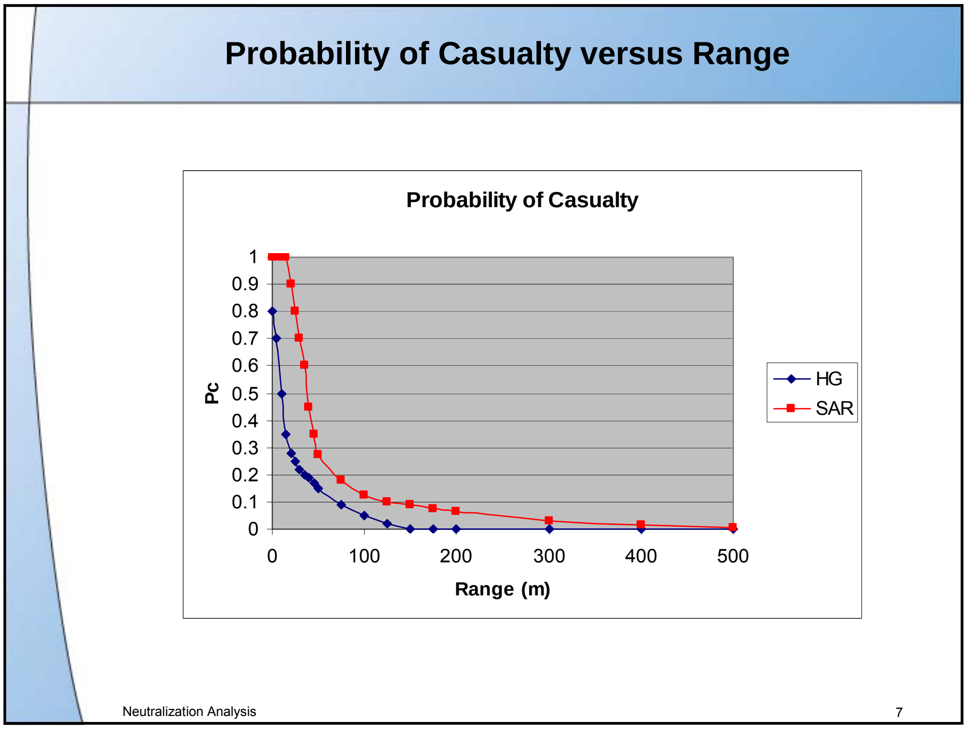
- N_e is a statistically significant number of engagements
- All engagements have the same initial conditions
- Two possible outcomes per engagement: win or loss



Factors Affecting Probability of Neutralization

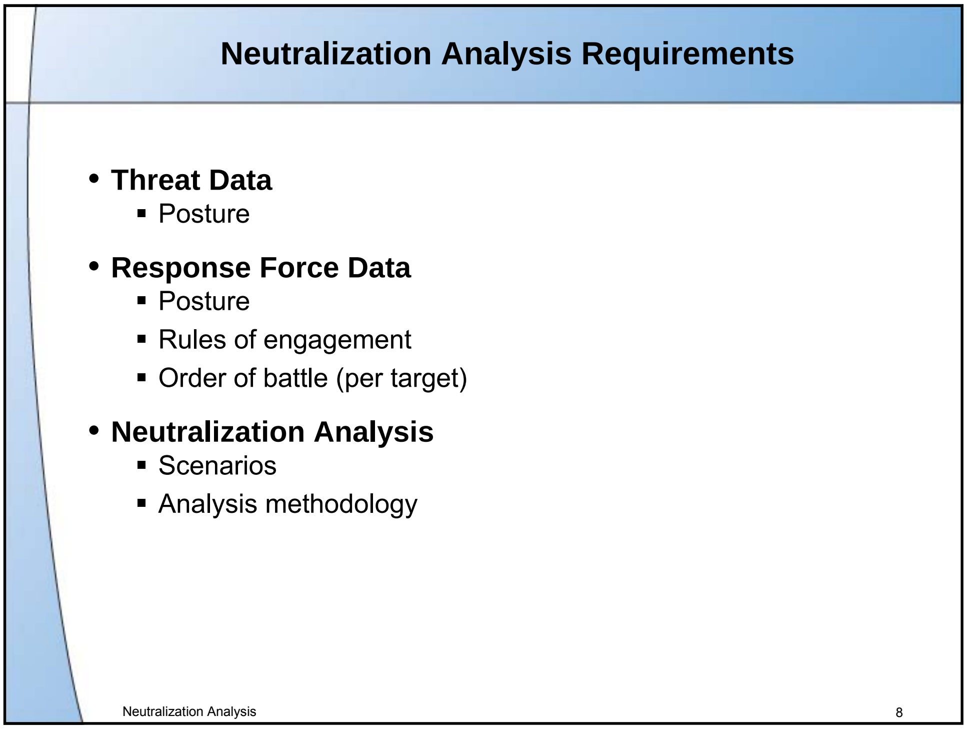
Factors	Examples
Numbers	
Weapons suite	None, baton, HG, SG, SMG, SAR, FAR, LMG, HMG, SNP
Area kill	Mortar, LAW, grenades, mines, IEDs
Ammo limits	Rounds/magazine, number of magazines
Training	None, basic, SWAT, military
Tactics	None, simple, advanced, military
Body armor	None, Level I, Level II, Level III
Posture	Stand, kneel, prone
Exposure	0%–100%
Movement	Stopped, very slow, slow, medium, fast, very fast, riding
Vehicles	Soft, armored, weaponized
Range	

Note: HG = hand gun; SG = shot gun; SMG = submachine gun; SAR = semi-automatic rifle; FAR = fully automatic rifle; LMG = light machine gun; HMG = heavy machine gun; SNP = sniper rifle; LAW = light anti-tank weapon; IED = improvised explosive device; SWAT = special weapon and tactic (team).



Probability of Casualty versus Range

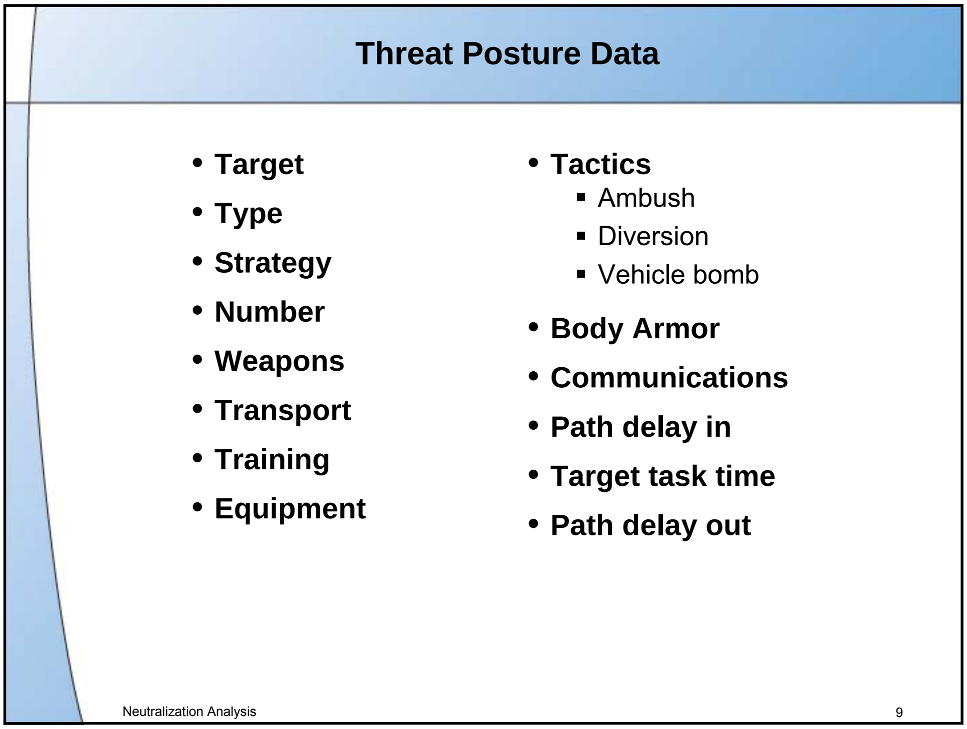
Neutralization Analysis 7



Neutralization Analysis Requirements

- **Threat Data**
  - Posture
- **Response Force Data**
  - Posture
  - Rules of engagement
  - Order of battle (per target)
- **Neutralization Analysis**
  - Scenarios
  - Analysis methodology

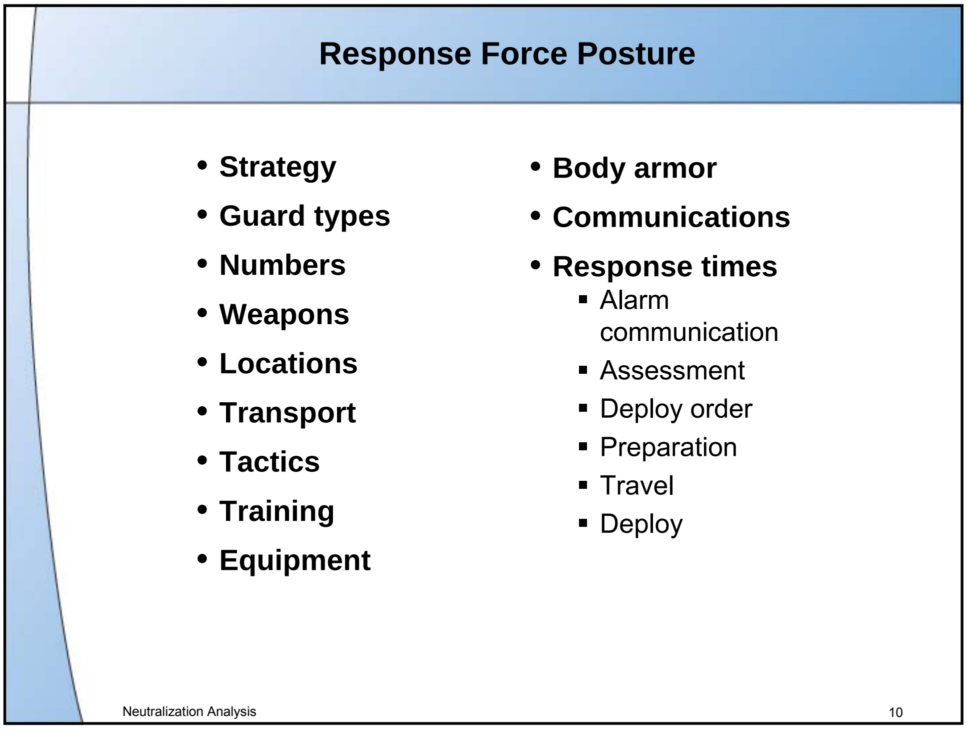
Neutralization Analysis 8



Threat Posture Data

- **Target**
- **Type**
- **Strategy**
- **Number**
- **Weapons**
- **Transport**
- **Training**
- **Equipment**
- **Tactics**
  - Ambush
  - Diversion
  - Vehicle bomb
- **Body Armor**
- **Communications**
- **Path delay in**
- **Target task time**
- **Path delay out**

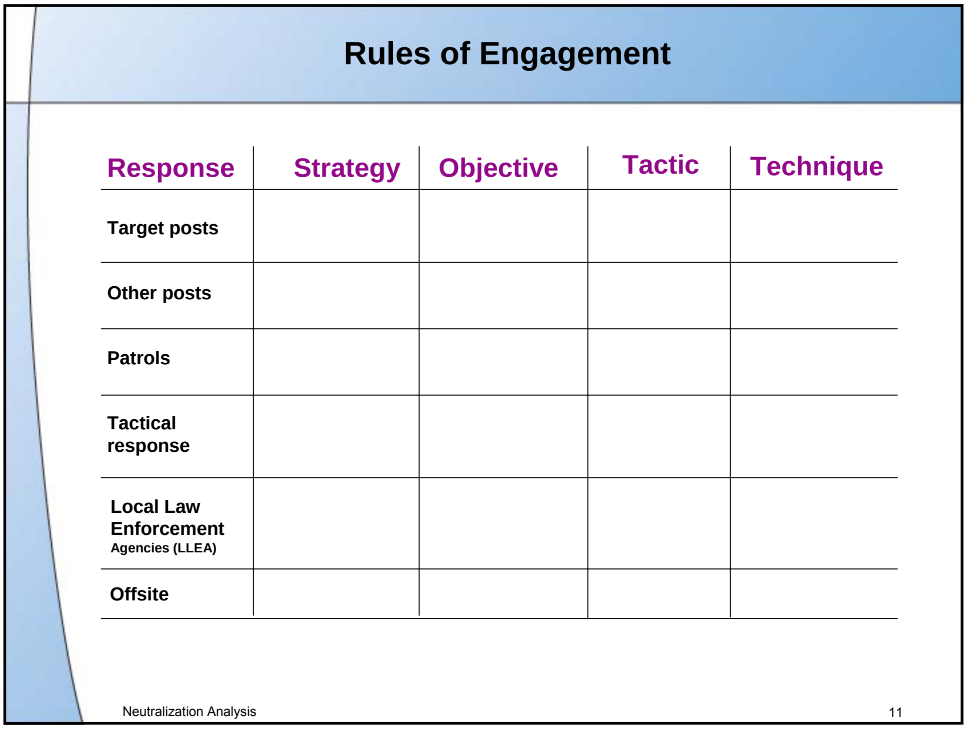
Neutralization Analysis 9



Response Force Posture

- **Strategy**
- **Guard types**
- **Numbers**
- **Weapons**
- **Locations**
- **Transport**
- **Tactics**
- **Training**
- **Equipment**
- **Body armor**
- **Communications**
- **Response times**
  - Alarm communication
  - Assessment
  - Deploy order
  - Preparation
  - Travel
  - Deploy

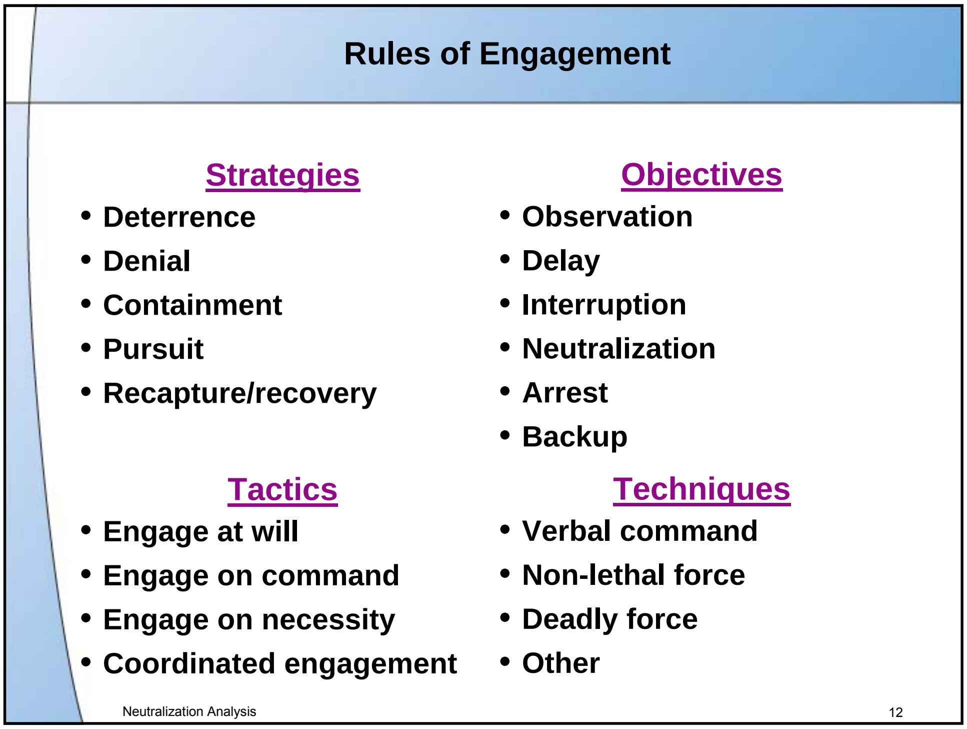
Neutralization Analysis 10



Rules of Engagement

Response	Strategy	Objective	Tactic	Technique
Target posts				
Other posts				
Patrols				
Tactical response				
Local Law Enforcement Agencies (LLEA)				
Offsite				

Neutralization Analysis 11



Rules of Engagement

Strategies

- Deterrence
- Denial
- Containment
- Pursuit
- Recapture/recovery

Objectives

- Observation
- Delay
- Interruption
- Neutralization
- Arrest
- Backup

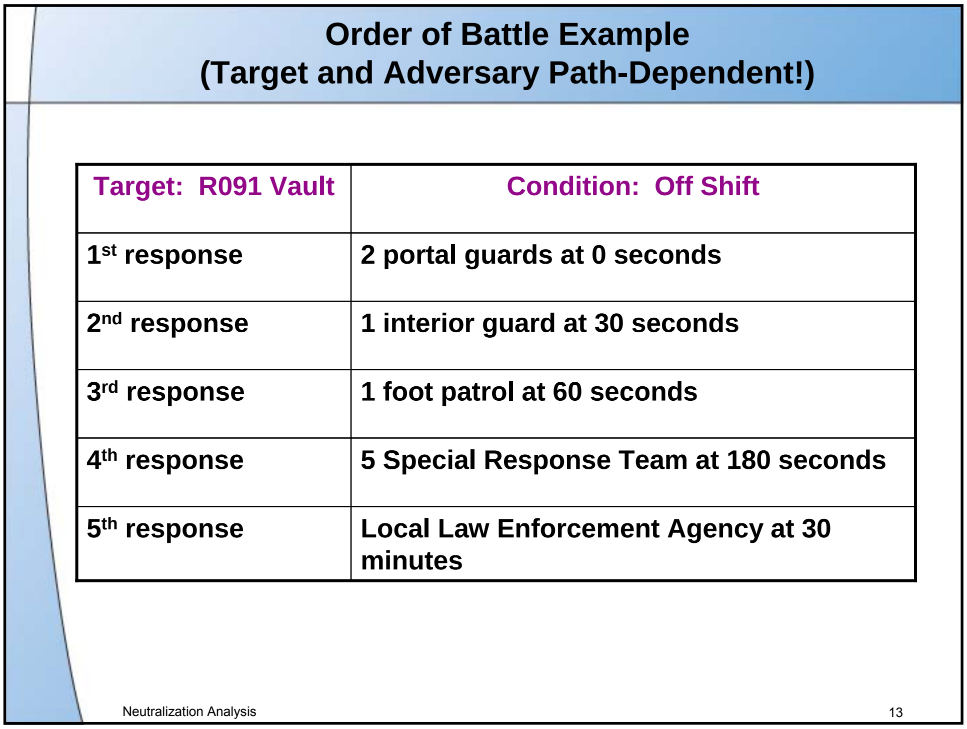
Tactics

- Engage at will
- Engage on command
- Engage on necessity
- Coordinated engagement

Techniques

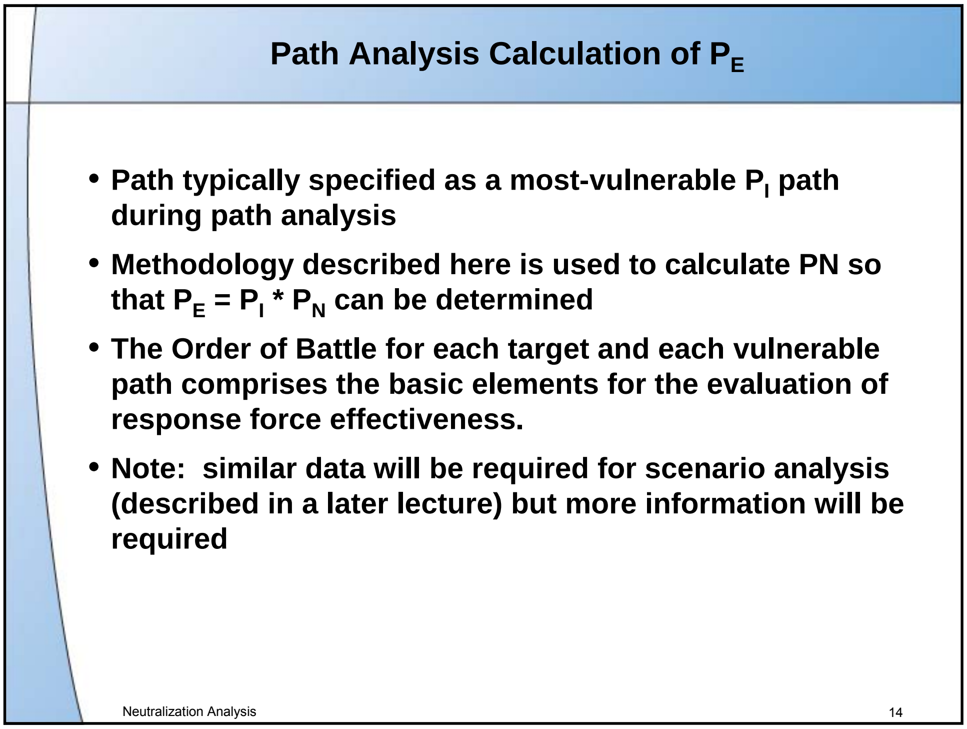
- Verbal command
- Non-lethal force
- Deadly force
- Other

Neutralization Analysis 12



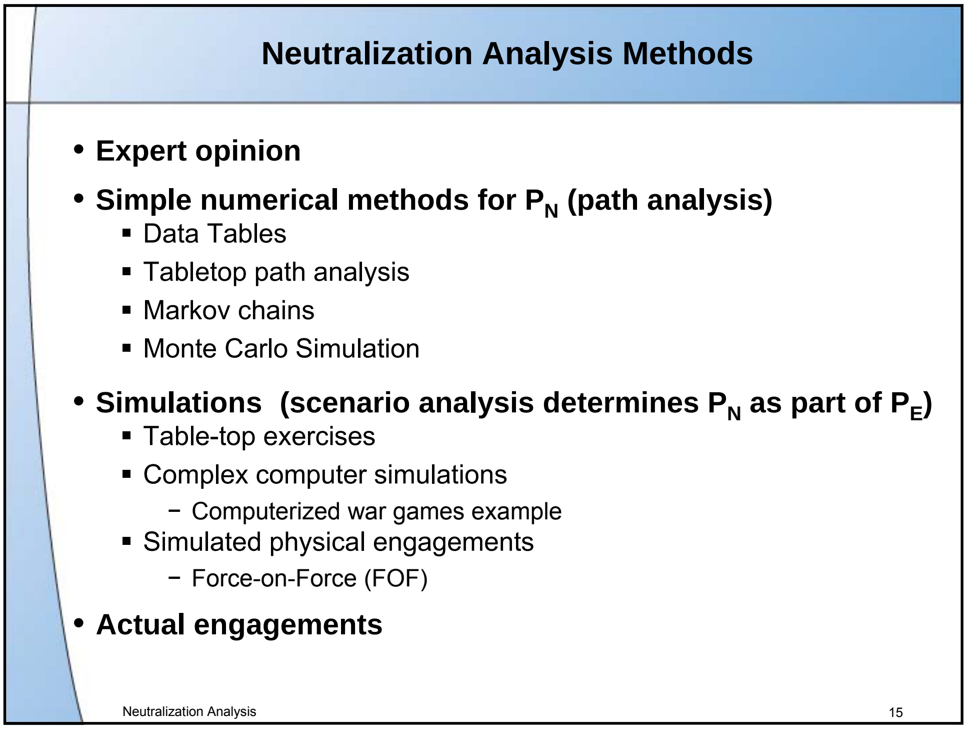
Order of Battle Example (Target and Adversary Path-Dependent!)

Target: R091 Vault	Condition: Off Shift
1st response	2 portal guards at 0 seconds
2nd response	1 interior guard at 30 seconds
3rd response	1 foot patrol at 60 seconds
4th response	5 Special Response Team at 180 seconds
5th response	Local Law Enforcement Agency at 30 minutes



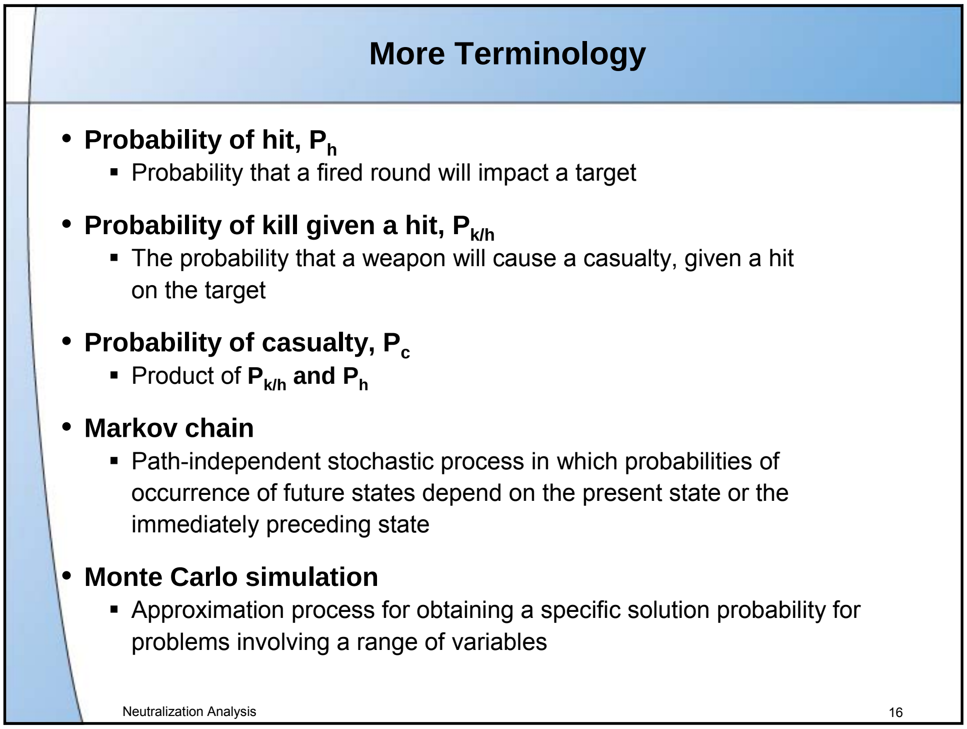
Path Analysis Calculation of P_E

- Path typically specified as a most-vulnerable P_I path during path analysis
- Methodology described here is used to calculate PN so that $P_E = P_I * P_N$ can be determined
- The Order of Battle for each target and each vulnerable path comprises the basic elements for the evaluation of response force effectiveness.
- Note: similar data will be required for scenario analysis (described in a later lecture) but more information will be required



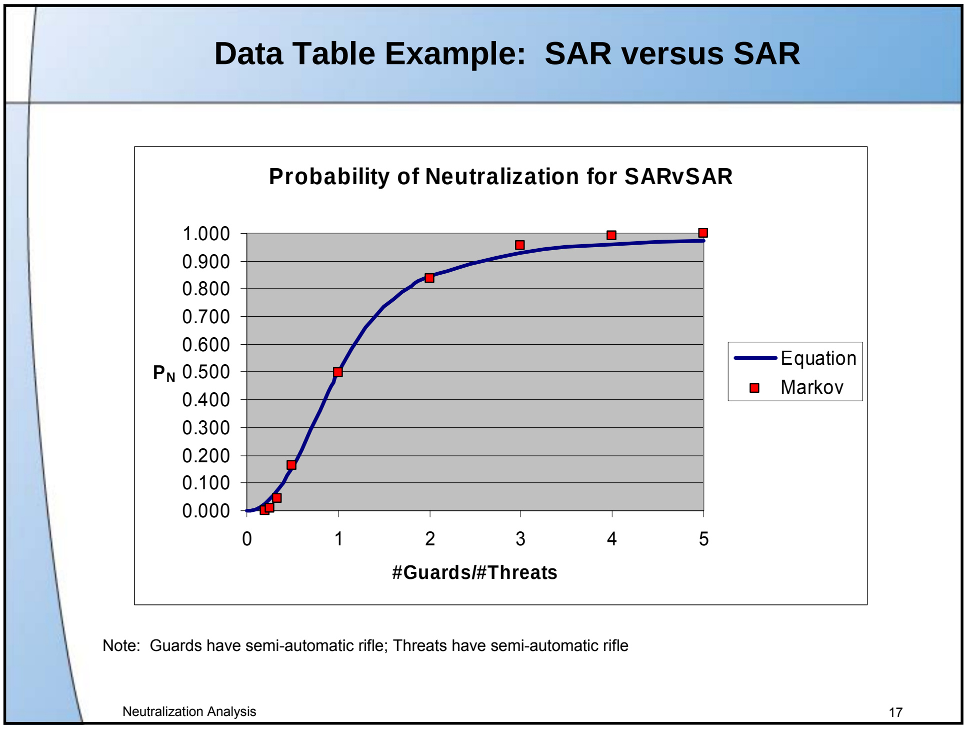
Neutralization Analysis Methods

- **Expert opinion**
- **Simple numerical methods for P_N (path analysis)**
  - Data Tables
  - Tabletop path analysis
  - Markov chains
  - Monte Carlo Simulation
- **Simulations (scenario analysis determines P_N as part of P_E)**
  - Table-top exercises
  - Complex computer simulations
    - Computerized war games example
  - Simulated physical engagements
    - Force-on-Force (FOF)
- **Actual engagements**



More Terminology

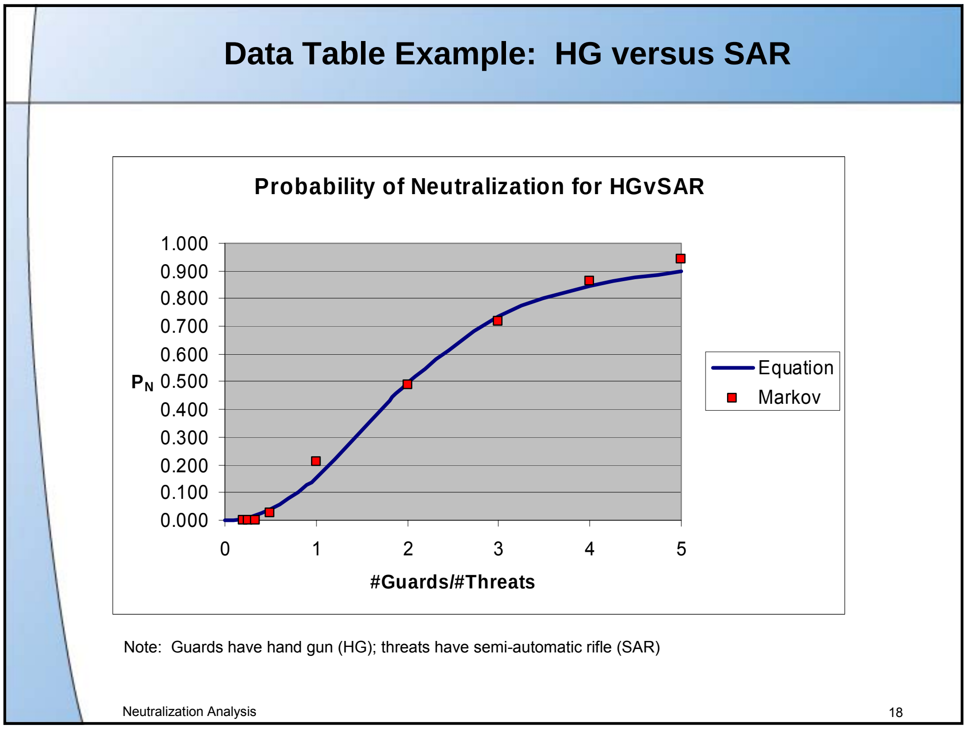
- **Probability of hit, P_h**
  - Probability that a fired round will impact a target
- **Probability of kill given a hit, $P_{k/h}$**
  - The probability that a weapon will cause a casualty, given a hit on the target
- **Probability of casualty, P_c**
  - Product of $P_{k/h}$ **and** P_h
- **Markov chain**
  - Path-independent stochastic process in which probabilities of occurrence of future states depend on the present state or the immediately preceding state
- **Monte Carlo simulation**
  - Approximation process for obtaining a specific solution probability for problems involving a range of variables



Data Table Example: SAR versus SAR

Note: Guards have semi-automatic rifle; Threats have semi-automatic rifle

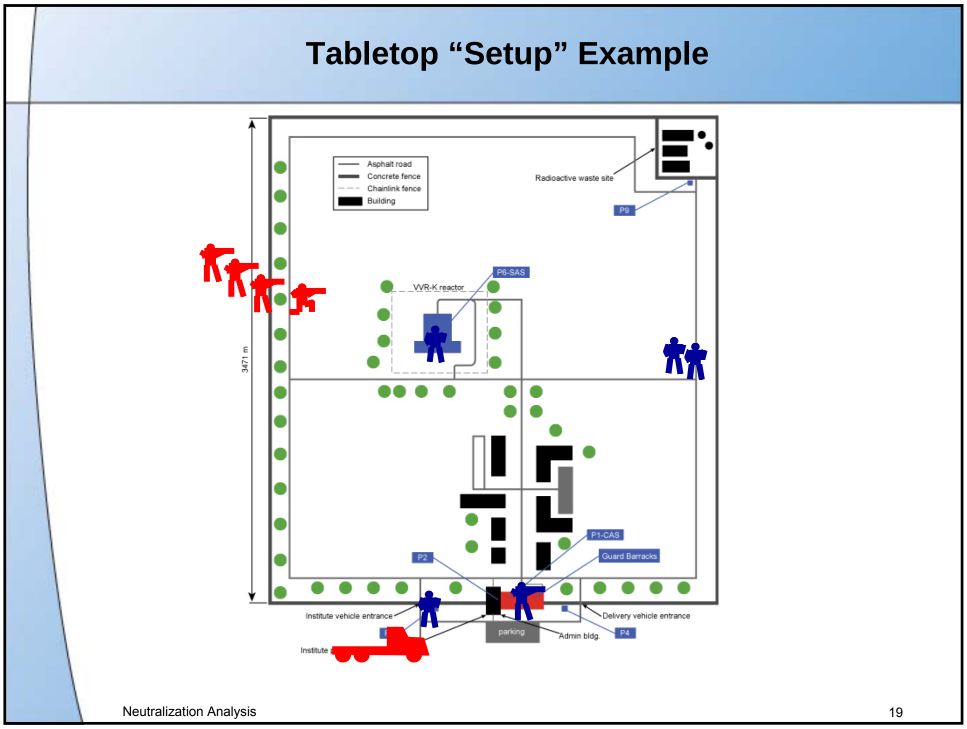
Neutralization Analysis 17



Data Table Example: HG versus SAR

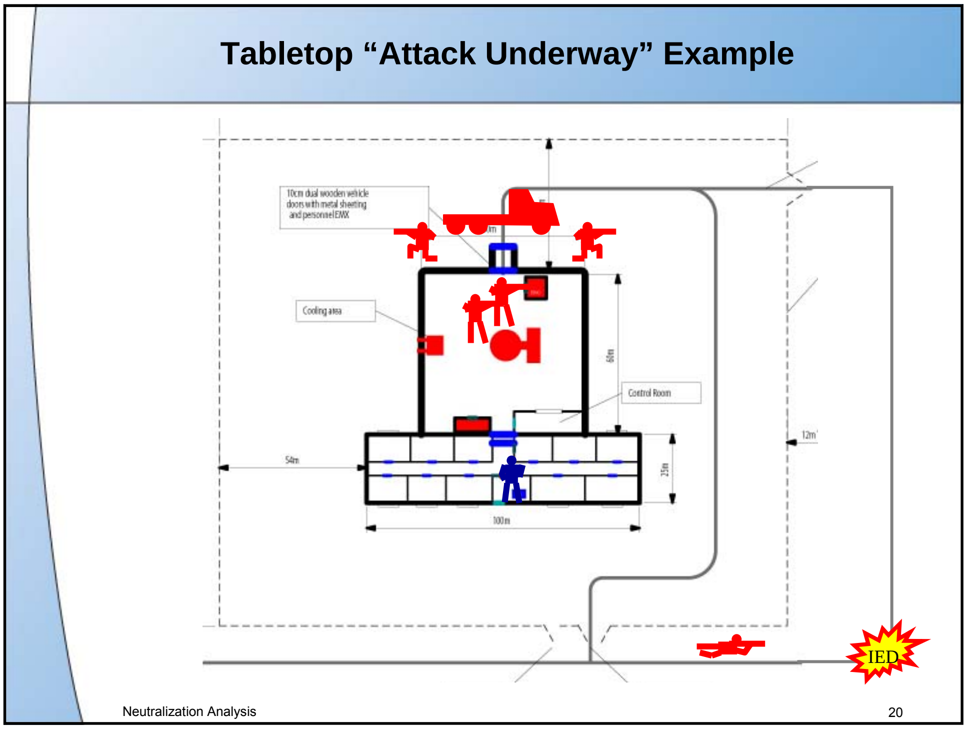
Note: Guards have hand gun (HG); threats have semi-automatic rifle (SAR)

Neutralization Analysis 18



Tabletop “Setup” Example

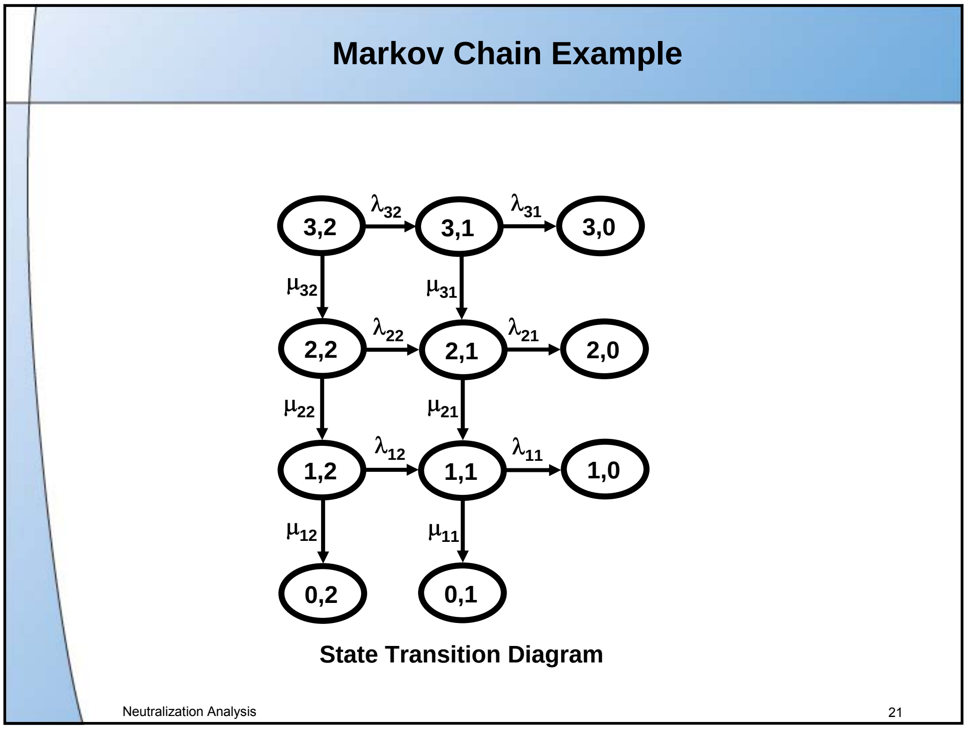
Neutralization Analysis 19



Tabletop “Attack Underway” Example

10cm dual wooden vehicle doors with metal sheeting and personnel EMX
Cooling area
Control Room
60m
54m
35m
100m
12m
IED

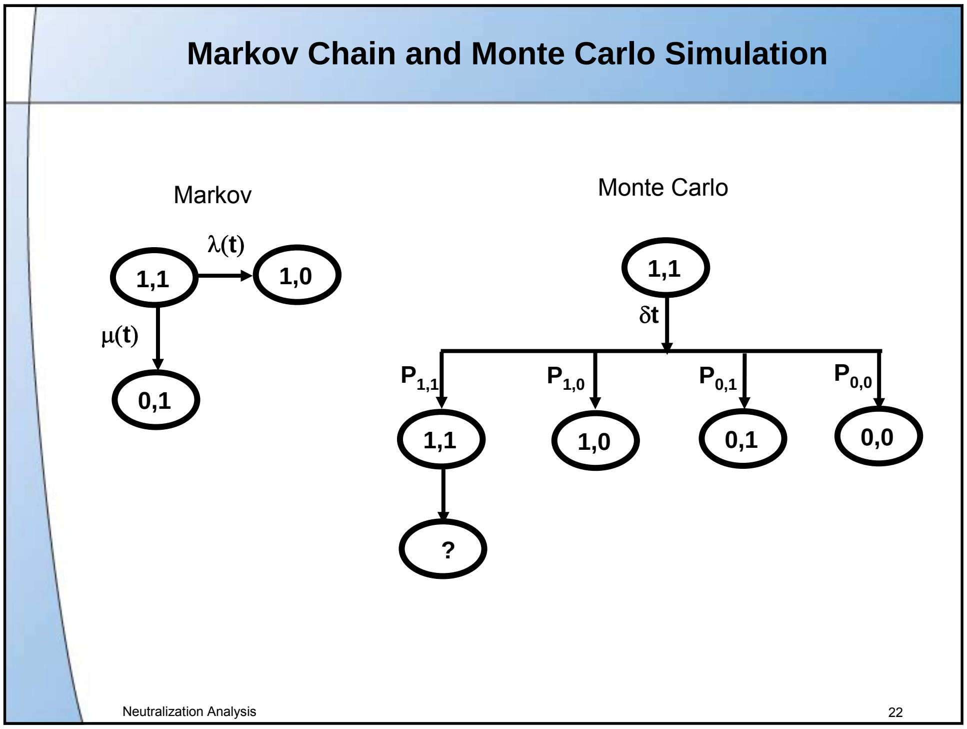
Neutralization Analysis 20



Markov Chain Example

State Transition Diagram

Neutralization Analysis 21



Markov Chain and Monte Carlo Simulation

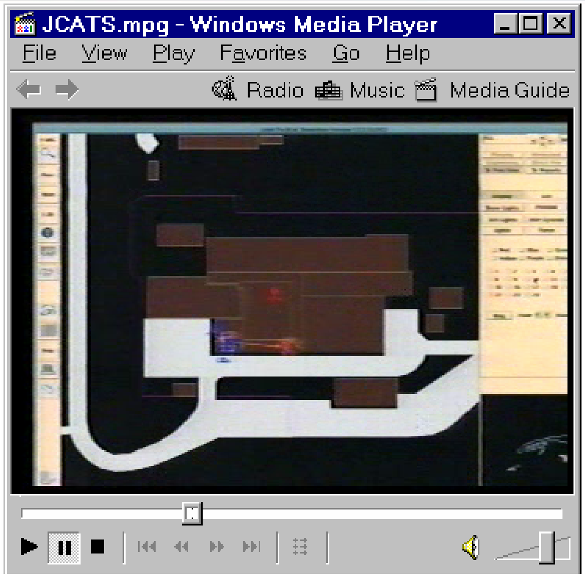
Neutralization Analysis 22

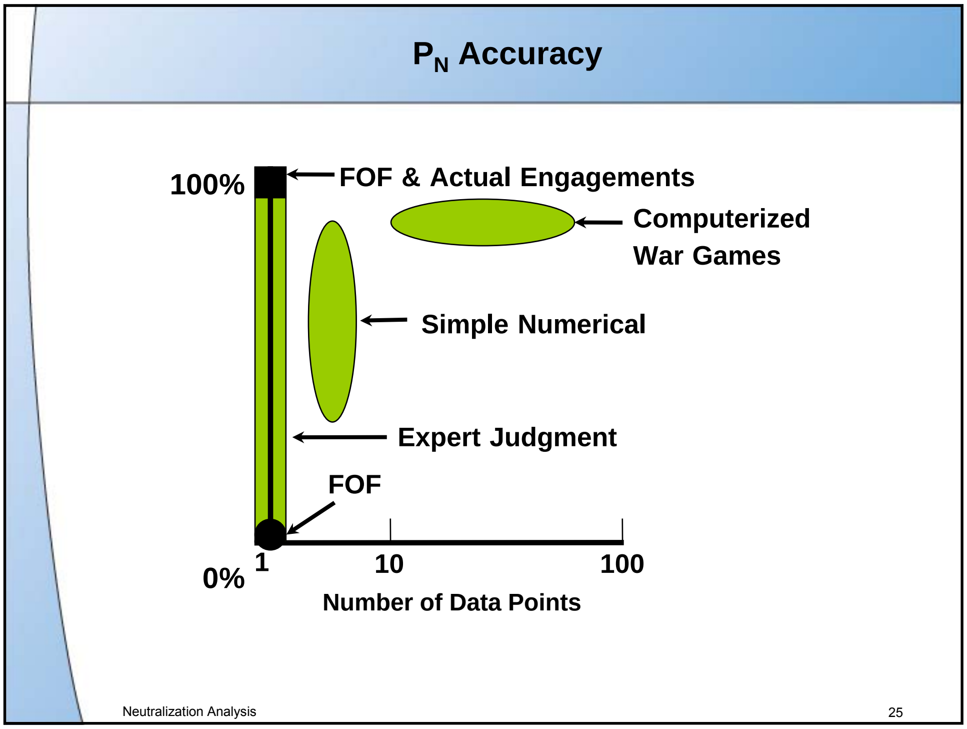
Monte Carlo Example: 1 versus 1 engagement

- All engagement parameters are equal
- Coin flip by guard and adversary simulates shot
- Head or tail determines hit or miss (P_h=0.5)
- Assume $P_{k/h}$ =1

Outcome:	1		2		3		4	
Combatant:	Guard	Threat	Guard	Threat	Guard	Threat	Guard	Threat
Toss result:	H	H	T	H	H	T	T	T
Represents:	Misses	Misses	Hits	Misses	Misses	Hits	Hits	Hits
Shot result:	Alive	Alive	Alive	Dead	Dead	Alive	Dead	Dead
Net result:	Shoot again		Win		Loss		Win	

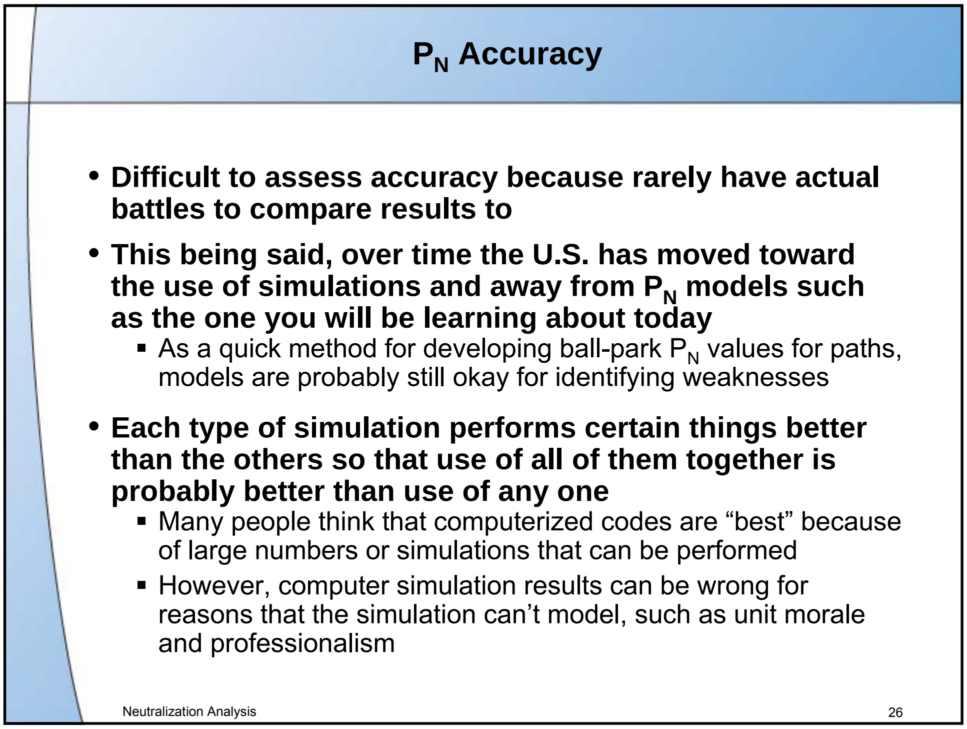
Computer Simulation Example





P_N Accuracy

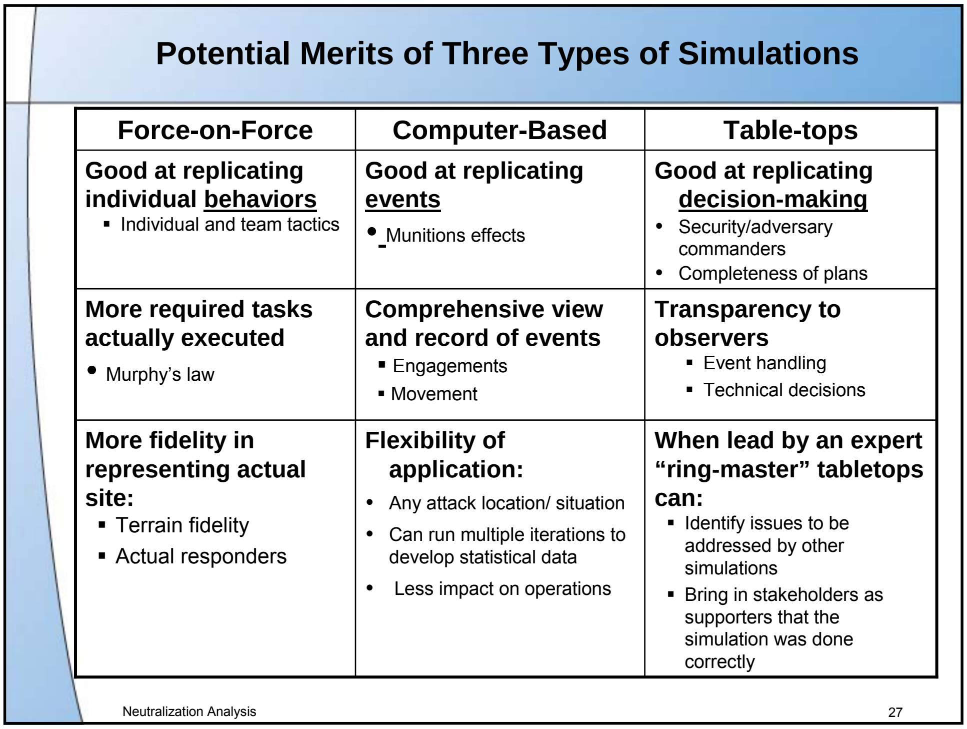
Neutralization Analysis 25



P_N Accuracy

- **Difficult to assess accuracy because rarely have actual battles to compare results to**
- **This being said, over time the U.S. has moved toward the use of simulations and away from P_N models such as the one you will be learning about today**
  - As a quick method for developing ball-park P_N values for paths, models are probably still okay for identifying weaknesses
- **Each type of simulation performs certain things better than the others so that use of all of them together is probably better than use of any one**
  - Many people think that computerized codes are “best” because of large numbers or simulations that can be performed
  - However, computer simulation results can be wrong for reasons that the simulation can’t model, such as unit morale and professionalism

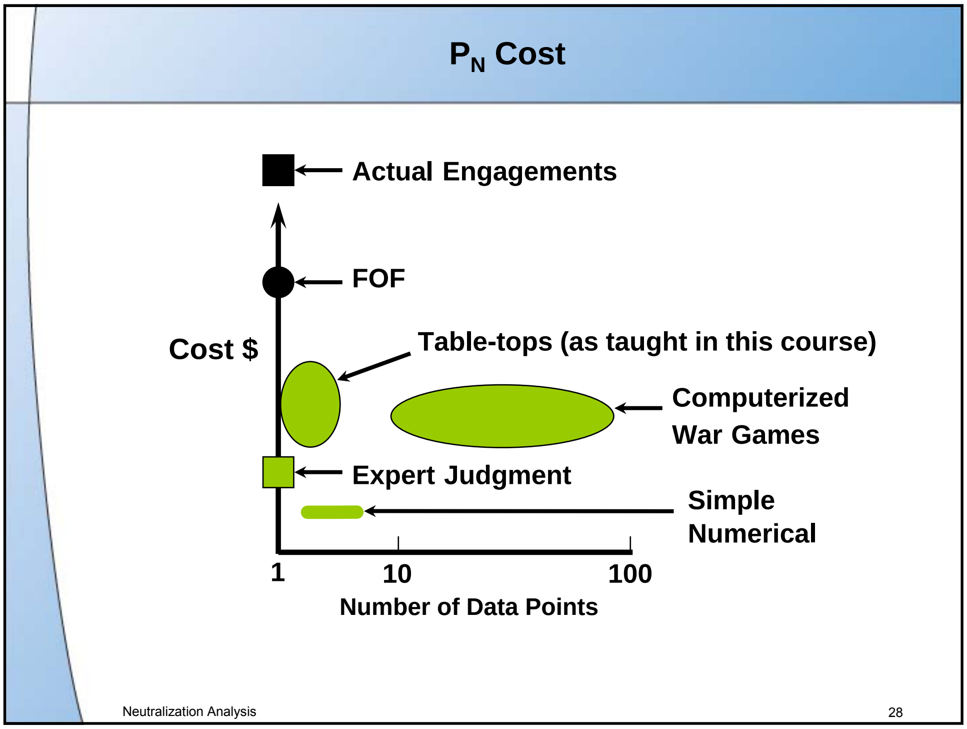
Neutralization Analysis 26



Potential Merits of Three Types of Simulations

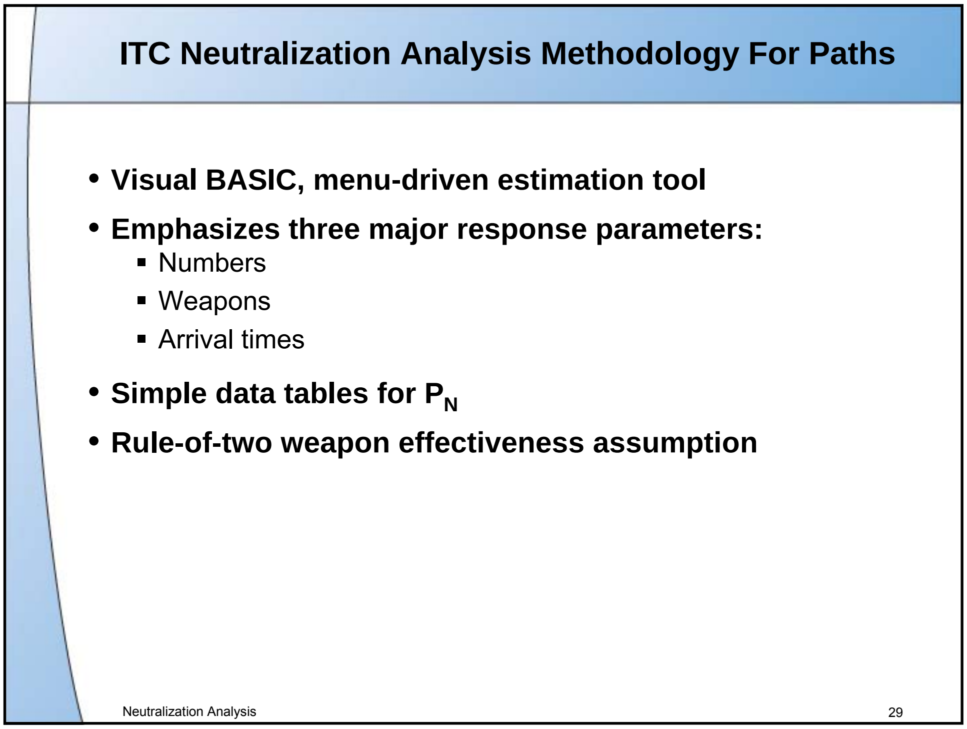
Force-on-Force	Computer-Based	Table-tops
Good at replicating individual <u>behaviors</u> ▪ Individual and team tactics	**Good at replicating <u>events</u>** • Munitions effects	**Good at replicating <u>decision-making</u>** • Security/adversary commanders • Completeness of plans
More required tasks actually executed • Murphy's law	**Comprehensive view and record of events** ▪ Engagements ▪ Movement	**Transparency to observers** ▪ Event handling ▪ Technical decisions
More fidelity in representing actual site: ▪ Terrain fidelity ▪ Actual responders	**Flexibility of application:** • Any attack location/ situation • Can run multiple iterations to develop statistical data • Less impact on operations	**When lead by an expert "ring-master" tabletops can:** ▪ Identify issues to be addressed by other simulations ▪ Bring in stakeholders as supporters that the simulation was done correctly

Neutralization Analysis 27



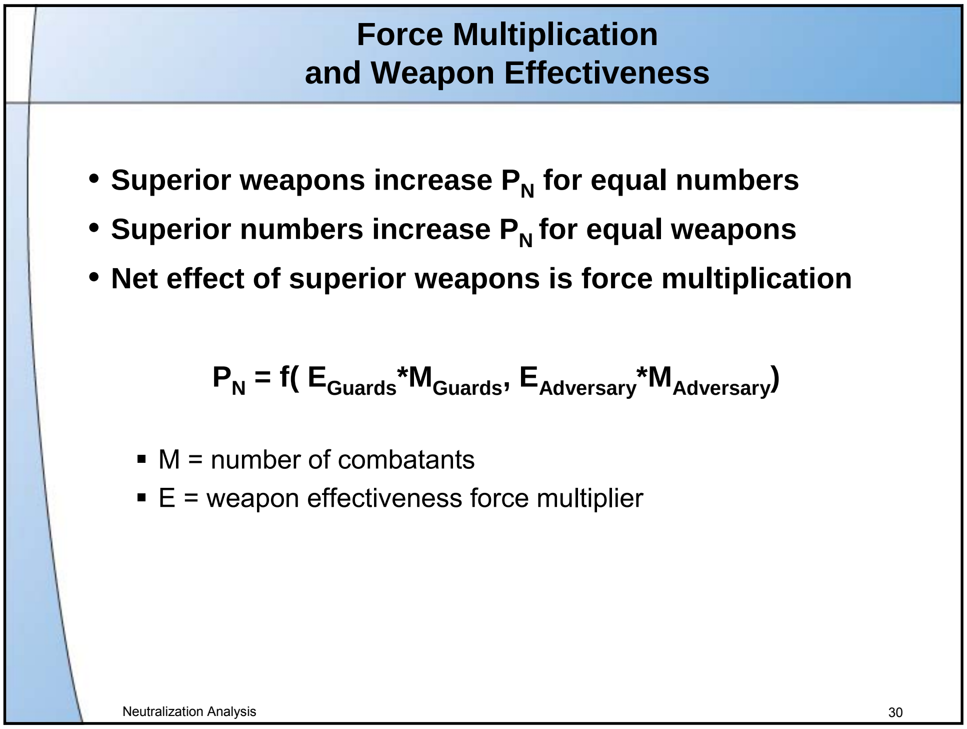
P_N Cost

Neutralization Analysis 28



ITC Neutralization Analysis Methodology For Paths

- **Visual BASIC, menu-driven estimation tool**
- **Emphasizes three major response parameters:**
  - Numbers
  - Weapons
  - Arrival times
- **Simple data tables for P_N**
- **Rule-of-two weapon effectiveness assumption**

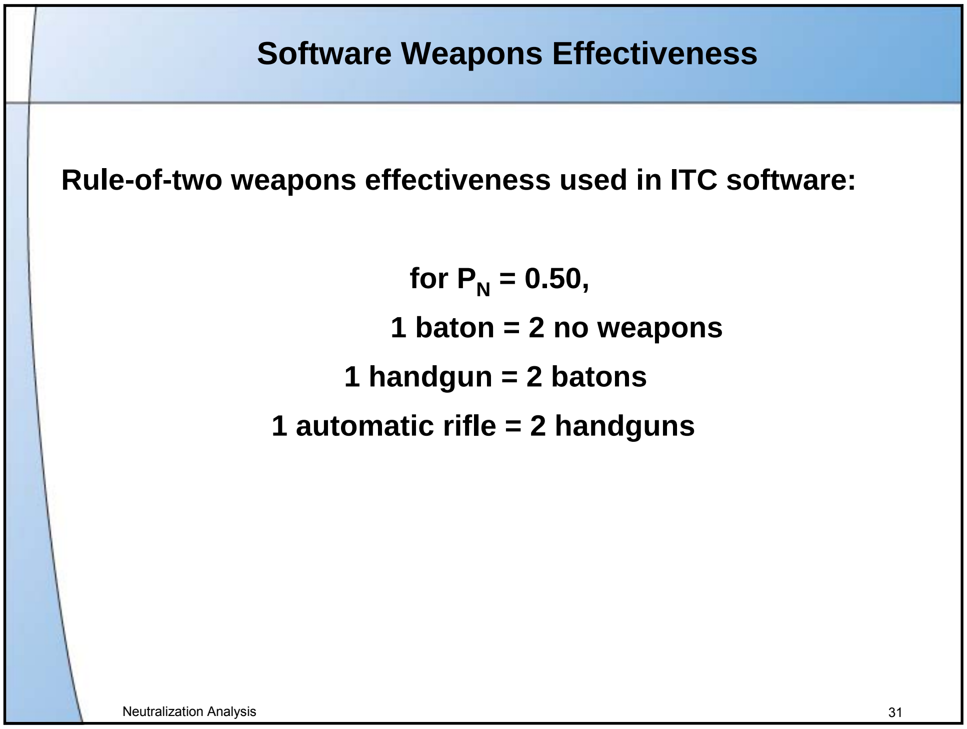


Force Multiplication and Weapon Effectiveness

- **Superior weapons increase P_N for equal numbers**
- **Superior numbers increase P_N for equal weapons**
- **Net effect of superior weapons is force multiplication**

$$P_N = f(E_{Guards}*M_{Guards}, E_{Adversary}*M_{Adversary})$$

- M = number of combatants
- E = weapon effectiveness force multiplier



Software Weapons Effectiveness

Rule-of-two weapons effectiveness used in ITC software:

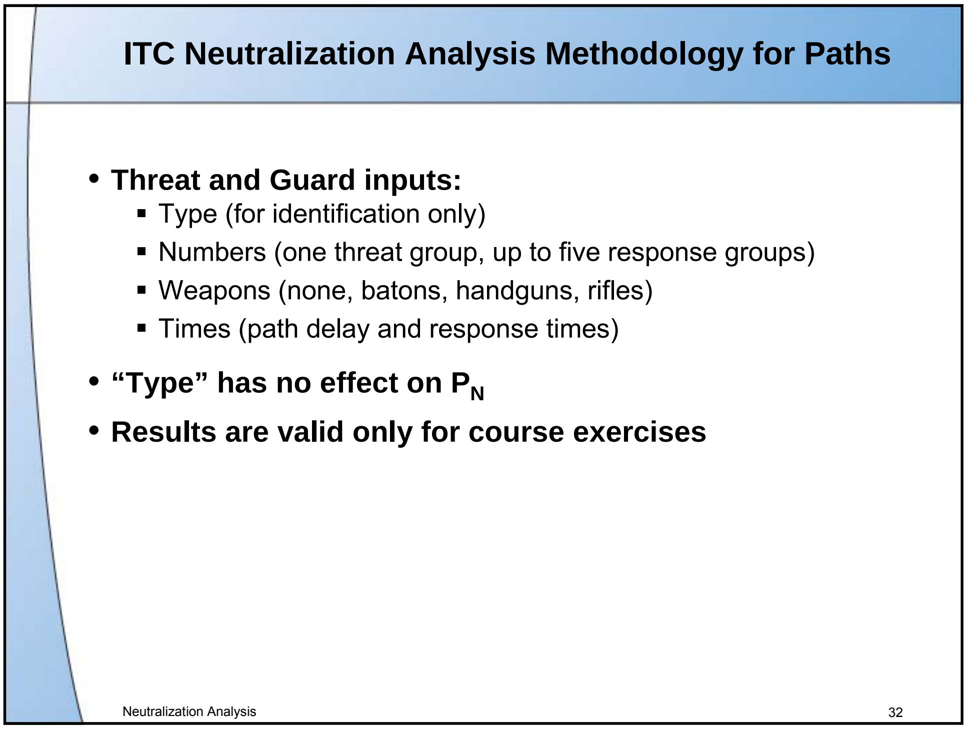
for P_N = 0.50,

1 baton = 2 no weapons

1 handgun = 2 batons

1 automatic rifle = 2 handguns

Neutralization Analysis 31

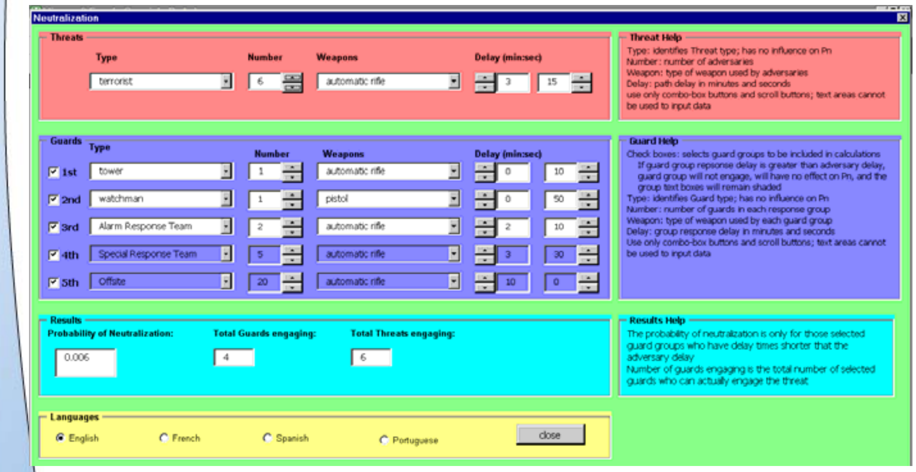


ITC Neutralization Analysis Methodology for Paths

- **Threat and Guard inputs:**
  - Type (for identification only)
  - Numbers (one threat group, up to five response groups)
  - Weapons (none, batons, handguns, rifles)
  - Times (path delay and response times)
- **"Type" has no effect on P_N**
- **Results are valid only for course exercises**

Neutralization Analysis 32

ITC Neutralization Analysis Methodology



Neutralization

Threats

Type	Number	Weapons	Delay (min:sec)	
terrorist	6	automatic rifle	3	15

Threat Help

Type: identifies Threat type; has no influence on Pn
Number: number of adversaries
Weapon: type of weapon used by adversaries
Delay: path delay in minutes and seconds
use only combo-box buttons and scroll buttons; text areas cannot be used to input data

Guards

	Type	Number	Weapons	Delay (min:sec)	
☑ 1st	tower	1	automatic rifle	0	10
☑ 2nd	watchman	1	pistol	0	50
☑ 3rd	Alarm Response Team	2	automatic rifle	2	10
☑ 4th	Special Response Team	5	automatic rifle	3	30
☑ 5th	Offsite	20	automatic rifle	10	0

Guard Help

Check boxes: selects guard groups to be included in calculations
If guard group repsonse delay is greater than adversary delay, guard group will not engage, will have no effect on Pn, and the group text boxes will remain shaded
Type: identifies Guard type; has no influence on Pn
Number: number of guards in each response group
Weapon: type of weapon used by each guard group
Delay: group response delay in minutes and seconds
Use only combo-box buttons and scroll buttons; text areas cannot be used to input data

Results

Probability of Neutralization:	Total Guards engaging:	Total Threats engaging:
0.006	4	6

Results Help

The probability of neutralization is only for those selected guard groups who have delay times shorter that the adversary delay
Number of guards engaging is the total number of selected guards who can actually engage the threat

Languages

● English ○ French ○ Spanish ○ Portuguese

Neutralization Analysis Summary

- Probability of Neutralization (P_N) is a major component of System Effectiveness
- Measure of Response Effectiveness
- Several methodologies available to calculate P_N
- Data required on Threat, Response Forces, and PPS
- Response upgrades should increase P_N
  - Go to the subgroups and use numbers, times, and weapons in practice exercises

Subgroup 20S
Neutralization Analysis

Session Objectives

After the session, the participants will be able to do the following:

1. Identify the Response Force posture for the Institute.
2. Define the Response Strategy and Rules of Engagement for the Response Forces.
3. Determine the Order of Battle for each target set at the Institute.
4. Analyze Response Force/Threat engagements to compute P_N at specific targets.
5. Determine upgrades to increase Response Force effectiveness.

Exercises

1. Response Force Posture
2. Rules of Engagement
3. Order of Battle
4. Neutralization Analysis
5. Response Force Upgrades

Exercise 1 – Response Force Posture

The purpose of this subgroup exercise is to identify the Response Force Posture for the target set at the Institute. The participants will accomplish this by completing the table below, which will provide data needed to perform a neutralization analysis and evaluate the Response Force effectiveness. Completing the table will provide necessary data for a neutralization analysis. The participant will need to use information from Subgroup 15S, Response Force Subgroup, and the *Exercise Data Book* to complete the table. Fill in the cells for Response Force Strategy, P1, and P5.

Target: PTR Reactor Facility								
Adversary Strategy: Sabotage				**Response Force Strategy:**				
Response	**Numbers Available (day/night)**	**Deploy Numbers (day/night)**	**Weapons**	**Body Armor**	**Transport**	**Distance**	**Response Time (vehicle)**	**Response Time (foot)**
P1 Tactical Teams	15	5	AR	Y	car	1100 m	319 s	494 s
	10							
P2 Institute Portal	3	0	HG	N	foot	---	---	---
	1	0	HG	N	foot	---	---	---
P3 Vehicle gate	2	0	HG	N	foot	---	---	---
	1	0	HG	N	foot	---	---	---
P4 Delivery gate	1	0	HG	N	foot	---	---	---
	0	0	HG	N	foot	---	---	---
P5 PTR Outer Portal								
P6 PTR R061	1	1	HG	N	foot	50 m	---	15 s
	0	0	HG	N	foot	---	---	---
P7 PTR SAS	2	1	HG	N	foot	50 m	---	20 s
	1	0	HG	N	foot	---	---	---
P8 NBR Portal	1	0	HG	N	foot	---	---	---
	1	0	HG	N	foot	---	---	---
P9 Rad Waste	1	0	HG	N	foot	---	---	---
	1	0	HG	N	foot	---	---	---
P10 Patrol	2	0	AR	N	foot	---	---	---
	2	0	AR	N	foot	---	---	---
LLEA City Police	10	10	HG	N	car	20 km	20 min	---
	10	10	HG	N	car	20 km	20 min	---
Offsite Army	35	35	AR	N	truck	30 km	30 min	---
	35	35	AR	N	truck	30 km	30 min	---

Exercise 2 – Rules of Engagement

The purpose of this subgroup exercise is to identify the Rules of Engagement that the Response Force will use for the target set at the Institute. The participant will accomplish this by completing the table below, which will provide data needed to perform a neutralization analysis and evaluate the Response Force effectiveness. The participant will need to use information from Subgroup 15S, Response Force Subgroup, and the Exercise Data Book to complete the table.

<table>
<tr><th colspan="5">TARGET: <u> PTR REACTOR FACILITY</u></th></tr>
<tr><th colspan="5">Adversary Strategy: <i>SABOTAGE</i> Response Force Strategy:</th></tr>
<tr><th>Response</th><th>Strategy</th><th>Objective</th><th>Tactic</th><th>Escalation of Force Technique</th></tr>
<tr><td><b>Target Posts</b></td><td></td><td>delay</td><td>Engage at will</td><td></td></tr>
<tr><td><b>Other Posts</b></td><td></td><td>backup</td><td></td><td>Deadly force</td></tr>
<tr><td><b>Patrols</b></td><td></td><td>delay</td><td>Engage at will</td><td>Deadly force</td></tr>
<tr><td><b>Tactical Response</b></td><td></td><td></td><td>Coordinated engagement</td><td>Deadly force</td></tr>
<tr><td><b>LLEA</b></td><td>pursuit</td><td>arrest</td><td>Coordinated engagement</td><td>Deadly force</td></tr>
<tr><td><b>Offsite</b></td><td>containment</td><td>neutralize</td><td>Engage on necessity</td><td>Deadly force</td></tr>
</table>

Strategies:

- Deterrence
- Denial
- Containment
- Pursuit
- Recapture/recovery

Objectives:

- Neutralize
- Interrupt
- Delay
- Observe
- Arrest
- Backup

Tactics:

- Engage at will
- Engage on command
- Engage on necessity
- Coordinated engagement

Techniques:

- Deadly force
- Physical force
- Physical restraint
- Verbal coercion
- Physical presence
- Other

Exercise 3 – Order of Battle

The purpose of this subgroup exercise is to determine the Response Force Order of Battle for the target set at the Institute. The participant will accomplish this by completing the table below, which is necessary to perform a neutralization analysis and evaluate the Response Force effectiveness. The participant will need to use information from the *Exercise Data Book* to complete the table. Consider only the first five groups of responders, in the temporal order in which they might engage the adversary under the Rules of Engagement developed in the previous exercise and in Exercise 1. Fill in the Response Force Strategy, data for P6, the 3rd response, and the 5th response.

<table>
<tr><th colspan="5">Target:<u> PTR Reactor Facility</u></th></tr>
<tr><td colspan="5"><b>Adversary Strategy</b><i>:___Sabotage_________</i> <b>Response Force Strategy:</b></td></tr>
<tr><th>Response</th><th>Location</th><th>Numbers (day/night)</th><th>Weapons</th><th>Times</th></tr>
<tr><td rowspan="2"><b>1st</b></td><td rowspan="2"><b>P5</b></td><td>1</td><td>HG</td><td>12 s</td></tr>
<tr><td>1</td><td>HG</td><td>12 s</td></tr>
<tr><td rowspan="2"><b>2nd</b></td><td rowspan="2"><b>P6</b></td><td>1</td><td></td><td></td></tr>
<tr><td>0</td><td></td><td></td></tr>
<tr><td rowspan="2"><b>3rd</b></td><td rowspan="2"><b>P7</b></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="2"><b>4th</b></td><td rowspan="2"><b>P1</b></td><td>5</td><td>AR</td><td>319 s</td></tr>
<tr><td>5</td><td>AR</td><td>319 s</td></tr>
<tr><td rowspan="2"><b>5th</b></td><td rowspan="2"><b>P1</b></td><td>5</td><td>AR</td><td></td></tr>
<tr><td>5</td><td>AR</td><td></td></tr>
</table>

Notes: The second response group from P1 is called to respond just after the first group arrives at the target. They require 15 seconds for notification, 75 seconds to travel and 90 seconds to deploy.

Exercise 4 – Neutralization Analysis

The purpose of this subgroup exercise is to **compute the probability of neutralization for the Response Force for the target set at the Institute.** The participant will accomplish this by inserting the data requested below into the *Markov Chain Neutralization Estimation* computer program. The adversary numbers and weapons should be taken from the 4S Threat Definition Exercise 2. The adversary task time is the value computed in the Multipath Computer Model subgroup exercise. Other necessary information is from the Order of Battle data from the previous exercise. Use the drop-down boxes and the spin buttons to select the correct input values on the computer menu.

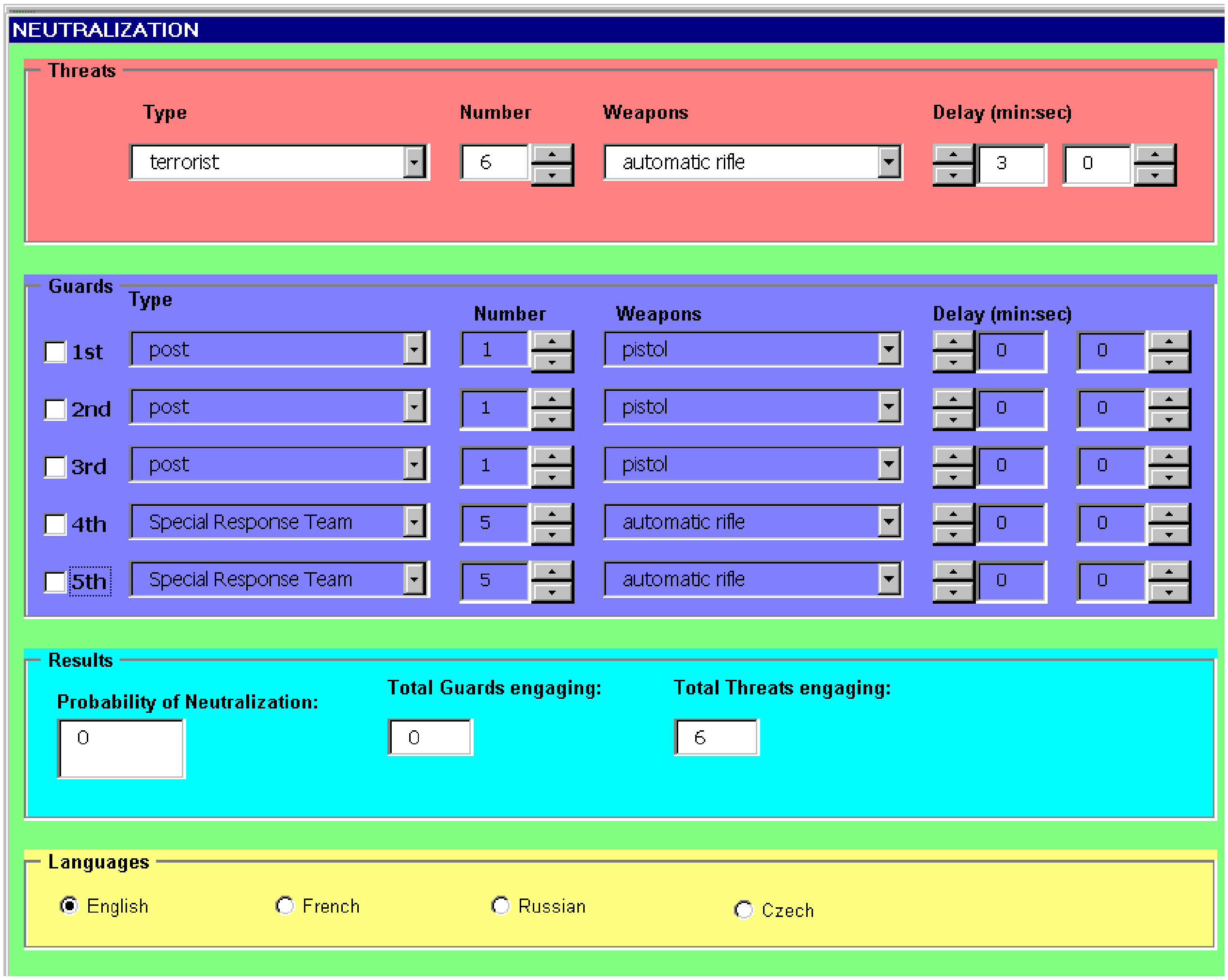
Target:_PTR Reactor Facility

Adversary Strategy:_____________ **Response Force Strategy:** ________________

Adversary Numbers: _____________

Adversary Weapons: _____________

Adversary Task Time: ____________



NEUTRALIZATION

Threats

Type	Number	Weapons	Delay (min:sec)	
terrorist	6	automatic rifle	3	0

Guards

	Type	Number	Weapons	Delay (min:sec)	
□ 1st	post	1	pistol	0	0
□ 2nd	post	1	pistol	0	0
□ 3rd	post	1	pistol	0	0
□ 4th	Special Response Team	5	automatic rifle	0	0
□ 5th	Special Response Team	5	automatic rifle	0	0

Results

Probability of Neutralization: 0

Total Guards engaging: 0

Total Threats engaging: 6

Languages

● English ○ French ○ Russian ○ Czech

Exercise 5 – Response Force Upgrades

The purpose of this subgroup exercise is to investigate the effectiveness of potential Response Force upgrades and determine how to implement them. The participant will accomplish this by using the P_N code to answer the questions below.

1. What is the computed P_N from Exercise 4? _____

2. How can P_N be improved?

3. How can the improvements be accomplished?

4. Perform a sensitivity analysis to determine the minimum number of guards, their weapons, and their maximum response time to meet the P_N design requirement.

Application Questions

Circle the letter of the best answer. Be prepared to provide the rationale for your response.

1. Probability of neutralization P_N is a measure of:
   a) PPS effectiveness
   b) detection effectiveness
   c) delay effectiveness
   d) Response Force effectiveness

2. At a minimum, P_N depends on:
   a) number of guards, weapons, and response times
   b) P_I, delay, and assessment
   c) number of guards, P_I, transport
   d) P_I, delay, and response times

3. Options for increasing P_N include:
   a) more guards
   b) better weapons
   c) reduced response times
   d) all of the above
   e) none of the above

4. Response Force survivability can be enhanced by:
   a) body armor
   b) armored response vehicles
   c) hardened posts
   d) all of the above
   e) none of the above

5. Response Force probability of arrival can be increased by:
   a) multiple communications methods
   b) armored response vehicles
   c) barracks inside the protected area
   d) all of the above
   e) none of the above

21. Scenario Analysis

Abstract. *Confidence that the Physical Protection System (PPS) system effectively protects against a range of adversary attacks is achieved by evaluating the PPS system against a representative set of adversary attack scenarios. To ensure confidence, the scenarios need to cover a range of possible attacks, be based on realistic assumptions about response plans, and be credible as attacks . This section reviews the methods pursued to develop adversary scenarios and provides a framework for succeeding discussions on adversary scenario evaluation.*

21.1 Introduction

Scenarios Analysis Defined

The objective of the physical protection system is to prevent an adversary from achieving an undesirable event (or unacceptable event). It is difficult but important to assess the readiness of the entire protection system – not only the hardware, but also response plans and procedures -- to achieve this objective with high assurance if such an attack were attempted. While previous sections have discussed timely detection or Probability of Interruption as an evaluation metric the security system must perform an additional function – neutralization – to succeed. Scenario analysis is the methodology used for analyzing system effectiveness, P_E, by considering the effect of several alternative possible adversary attacks (scenarios) against the PPS.

Scenarios Analysis Requires More details about the attack and the defense

Evaluating neutralization (and overall effectiveness), in turn, requires more detail about how the adversary attack is conducted than just the path as the attack and site defenses must be simulated, using either computer simulations, tabletop exercises, or Force-on-Force exercises. While path analysis was most concerned with finding the most vulnerable path, scenario analysis is concerned with creating a 1) detailed representative set of adversary scenarios/attack plans, 2) detailed description of site security plans, procedures, and deployment conditions, and 3) performing a simulation of the interaction between adversaries and the PPS that is conducted as honestly and realistically as possible. Scenario descriptions should include:

- What each adversary is doing as a function of time
- Coordination steps between different adversaries (wait until...)
- How much equipment the adversary is bringing and how it will be loaded on adversary transportation equipment
- PPS assumptions at the time of the adversary attack

Thus, multiple timelines are needed, not just one as was the cased with path analysis.

Evaluate Potential Design Basis Threat (DBT) Adversary Scenarios

These scenarios should both be realistic for an adversary constrained within the Design Basis Threat and should cover the range of potential vulnerabilities seen in the PPS. .While the quality of path analysis can drop when a vulnerable path is missed, the quality of scenario analysis can suffer both because vulnerabilities are overlooked in scenario formulation and because unrealistically effective scenarios are simulated against the PPS.

21.2 Comprehensive Scenario Analysis

Analyze Adversary Scenarios

In order to provide confidence that an analysis is comprehensive, it is necessary to follow a systematic, structured approach to identifying scenarios. The steps in one such approach are given below:

1. Identify the key questions to be addressed by the scenario analysis.
2. Identify major drivers of performance in the study and sort these drivers into those that are controllable within the study, such as the capability of the attacking force or security response options, versus those that are uncontrollable, such as the size of the DBT.
3. Collect necessary site data, including performance test data, timeline information from the path analysis, and detailed security plans and procedures.
4. Based on the information collected from steps 1-3, use either a formal approach to creating a set of scenarios using expert attack planners or an informal approach when such experts are not available. (This section will focus on how to accomplish the informal approach.)
5. Assess the system effectiveness, P_E, against the representative scenarios using either Subject Matter Experts (using criteria-based assessments) or one or more simulations – Tabletop analysis, computer simulations, or Force-on-Force exercises.
6. Document results and conclusions along with scenario descriptions

Note: The ITC uses tabletop exercises as a qualitative effectiveness tool as both computer simulations and Force-on-Force are outside the scope of the analysis.

Value of Using Expert Planners and Some Limitations

In a formal application of scenario analysis, one or more experienced attack planners should be used to develop the attack scenarios. Compared to others, such as engineers and security personnel, the expert planner can go a long way to keeping the scenario realistic. Personnel with many of the right skills can be found in military and similar organizations. One criterion for the expert to have is experience in planning missions with forces the size of the design basis threat. It is also important to find planners who appreciate that the adversary will typically carry out an attack lacking some of the capabilities that conventional militaries have. Without considering this limitation, the expert planner may develop plans that are fictitious: they appear to be possible for the threat to carry out but are not.

A Less Formal Approach

Scenario analysis can be performed by engineers and security personnel without using an expert planner. These applications are less formal but may be necessary due to difficulties in locating/engaging expert planners. Such an approach is discussed in 21.3.

21.3 An Informal Approach to Generating Scenario Attack Plans

How to Create an Attack Plan without using Expert Planners

The informal approach described here covers the important topics to consider with devising scenario plans, namely:

- Identify site vulnerabilities across various operational conditions and states
- For promising vulnerabilities (either determined during path analysis or by expert):
  - Create a list of essential tasks for the attack to succeed;
  - Create a sub-plan describing how a team of attackers can perform each task within resource constraints; and
  - Combine sub-plans into several distinct master attack plans/scenario descriptions.

- Review and select final plans/scenarios based on criteria:
  - Are analysis objectives covered that we want covered?
  - Are conditions and states covered adequately?
  - Have we addressed several means of adversary approach from the set {on foot, in land vehicles, on water, or by air} that apply, based on the Design-Basis Threat (DBT)?
- Are paths credible, credibly generated and conducted by threats within the DBT, etc.?

This section discusses these steps in more detail.

Identifying site vulnerabilities

In order to identify site vulnerabilities across various operational conditions and states, consider different::

- Operational conditions (operational versus non-operational)
- Target material configurations (reactor load-out versus operations)
- Response force alert levels and personnel "crews"
- Different upgrade packages

Experts, previous path analyses, and previous vulnerability studies and performance tests can give clues about where vulnerabilities are located.

Creation Process for Scenarios

For promising vulnerabilities (either determined during path analysis or by expert) scenarios can be generated by:

- First creating a list of essential tasks that have to be accomplished for the attack based on that vulnerability to succeed. Such a list might look like the following for a target:
  - Task 1: Enter building XYZ
  - Task 2: Collect 20 Kg of U235 in storage containers
  - Task 3: Leave site with material without pursuit by response forces
  - Task 4: Arrive undetected at safe house in city ABC

- Task 5: Hold off responding units so that tasks 1 through 3 are accomplished

These tasks should be kept as simple as possible.

- Next, creating sub-plans that describe how one or more teams of attackers can perform each task within resource constraints. These sub-plans should describe:
  - 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?

- Finally, combine these sub-plans into a master attack plan/scenario description, adjusting sub-plans to meet overall constraints imposed by the DBT and perhaps the site as well as to achieve synchronization between teams.

Use Path Analysis As a Source of Paths for Main Entry Teams

Path analysis can suggest sub-plans that serve as the main or "direct" part of the attack (direct in the sense of going to the target). Such plans might be based on the minimum delay, minimum P_I, or minimum P_I*P_N paths Details can be added to these path descriptions to fill out the scenario. For example, instead of the step "Penetrate Fence" found in the path analysis, the scenario description might consist of: "Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during a storm. Last adversary monitors radio traffic."

Of course, multiple scenarios can be developed for a single path by slightly varying the method by which the adversary attacks different protection elements along the path.

Be aware, though, the most-vulnerable path (MVP) from path analysis may be a poor basis for creating a scenario. This may occur because typically low PI paths should be corrected with upgrades during the path analysis phase. After such upgrades, the MVP should now have a high P_I rendering that path less desirable At this stage scenario analysis might more profitably consider factors not found in path analysis: preventing neutralization and employing other teams to prevent interruption.

Developing sub-plans

Just as we used a timeline to evaluate the interaction between detection, delay, and response for a single team (see Figure 21-1), we can use a timeline to help plan each sub-team's attack (see Figure 21-2). In the latter diagram, the intent early on is to control the point of detection: being detected earlier than the team planned is not good. At the same time, after detection when planned, sub-plan should allow the adversary team carrying it out to complete its mission without being interrupted (that is T_C falls before T_I). Figure 21-3 depicts several supporting attacks for a main attack on a material vault.

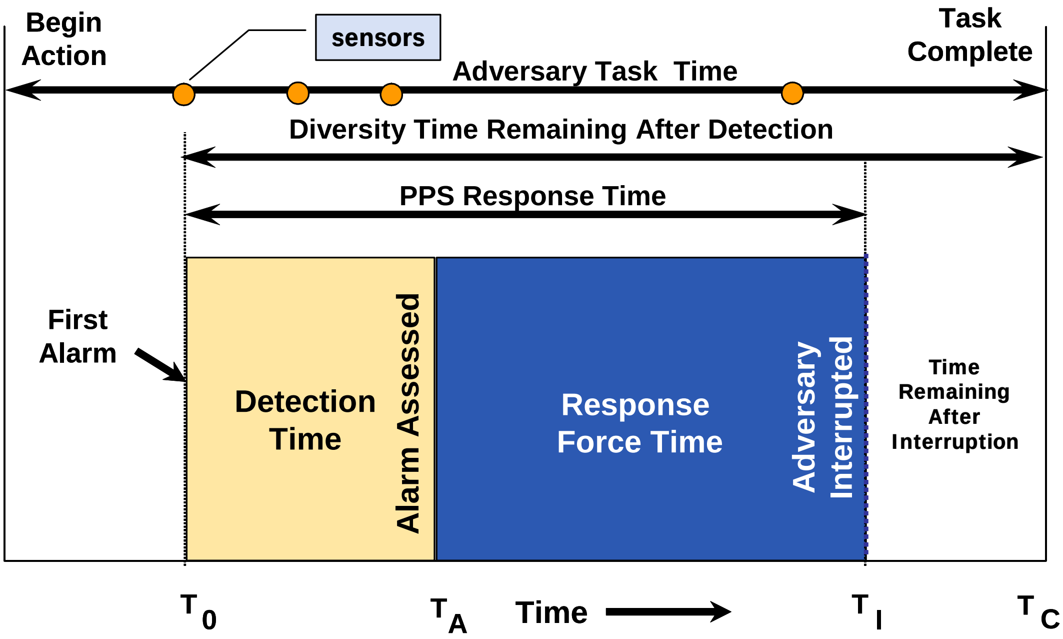


Figure 21-1: Timeline for Single Path Analysis

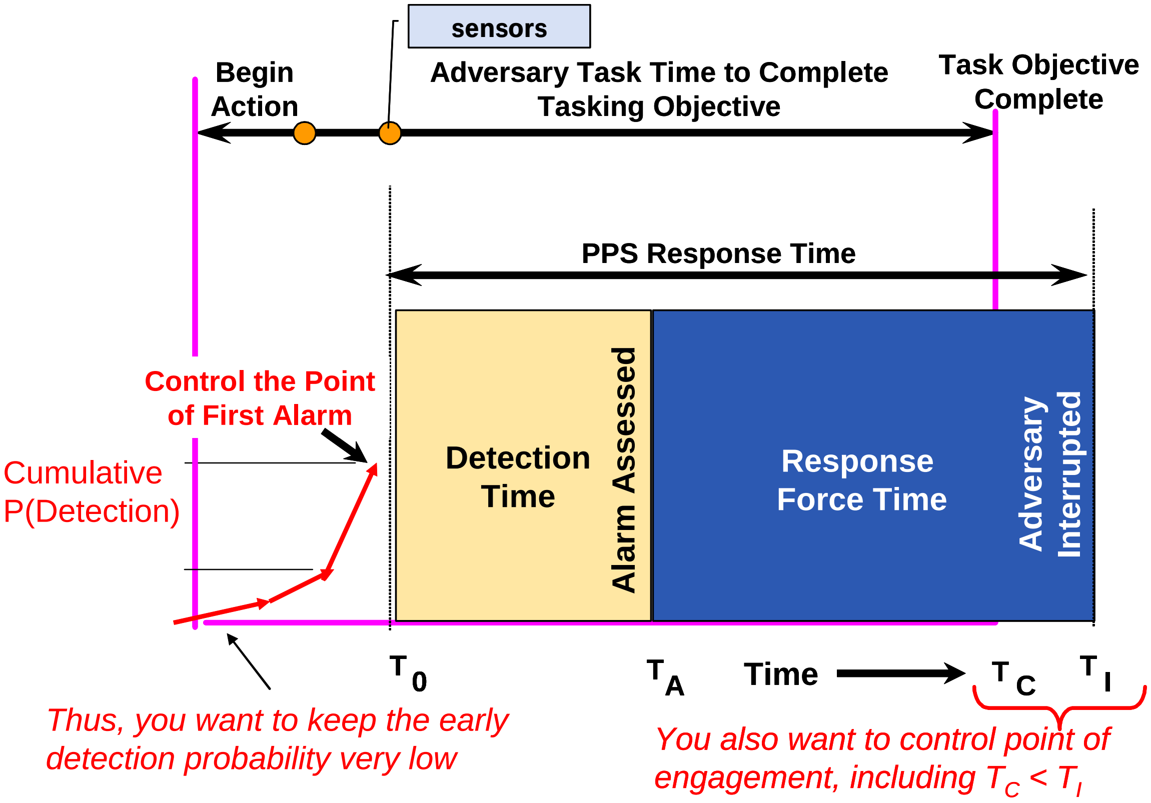

sensors
Begin Action
Adversary Task Time to Complete Tasking Objective
Task Objective Complete
PPS Response Time
Control the Point of First Alarm
Cumulative P(Detection)
Detection Time
Alarm Assessed
Response Force Time
Adversary Interrupted
T_0
T_A
Time
T_C
T_I
Thus, you want to keep the early detection probability very low
You also want to control point of engagement, including $T_C < T_I$

Figure 21-2: Timeline for a Sub-Team Performance:

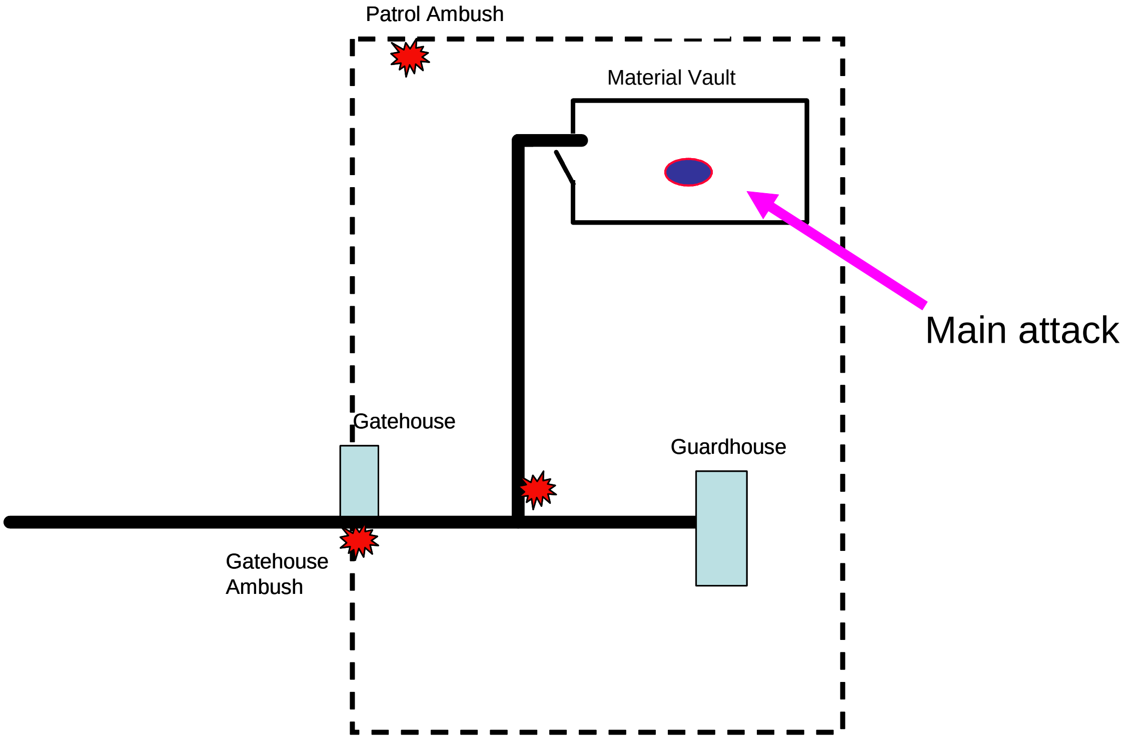


Figure 21-3: Several Supporting Team Targets to aid Main Attack on a Vault:

Adding Supporting Team Sub-Plans to Scenarios

Supporting teams can be assigned to complete other essential tasks or to aid the main team directly. Often, the remaining tasks look like: “Hold off responding units so ...” or “Neutralize offsite response...” Thus, one good use of supporting teams is to delay or incapacitate the response through setting ambushes, creating diversions, and attempting to confuse the response.

Insider Colluding With Outsider Adversary

It is important to recognize that one of the most damaging adversaries to a physical protection element is the insider. Therefore, an insider colluding with outsiders can be a formidable adversary. When determining the impact of a colluding insider on physical protection system effectiveness, consider the access, knowledge, and authority entrusted to the insider, and consider how these might be abused to:

- reduce the probability of detection of a sensor or procedure. *Example: the probability of covert/deceitful entry through an entry portal*
- reduce the delay time offered by barriers. *Example: anything with locks for which the adversary has key access*
- increase the time of response. *Examples: block response doors, disable vehicles, divert response teams, etc.*

decrease the number of respondents. *Examples: detonate pre-positioned explosives, or divert part of the force to another incident.*

The importance of achieving synchronization

Lack of synchronization can result in failure of the attack due to earlier detection than planned or piecemeal attacks on targets. Achieving synchronization requires planning so that multiple teams can coordinate their progress at key steps (e.g., they all are in correct positions when detection occurs, task time estimates are reliable so that some teams don't fall behind others; and surprises (e.g., chance encounters with security or site personnel) are limited.

Complete Credibility Check

When reviewing potential scenarios, credibility and consistency are important considerations for a useful analysis. The credibility implies that although an adversary might be able to successfully perform one or two difficult tasks in a scenario, it would be incredible for him to perform a long series of them. For example, it might be credible for an adversary to employ a hot air balloon to cross a protected area perimeter. It might also be credible for him to rappel from the balloon basket onto the target building ceiling. It might also be credible for him to engage and kill a pair of well-trained guards using a hand gun. However, it would be incredible to propose that an adversary might employ the hot air balloon, rappel onto the building, and, simultaneously engage and neutralize two response force personnel using a handgun.

Defeat Methods In Scenario Should Be Consistent

Consistency implies that the defeat methods pursued along the scenario make sense. For example, it might be possible to consider that an adversary might drive a vehicle through a wall in order to penetrate a building quickly. It would also be credible for an adversary to employ a false badge to deceive a guard posted at a vital area entrance. It would not, however, be credible for the adversary to penetrate the building wall using a vehicle, and then produce a false badge for the guard at the vital area entrance.

Use of Scenarios with maximum equipment

The best scenario for the adversary does not always use all of the equipment allowed within the design basis threat. This may occur because not all of the equipment may provide an advantage to the attackers once training and the need to hide the attack from intelligence services is factored in. Adding equipment may also increase the complexity of the scenario, making it more risky.

Reasons why Scenarios may Fail

Attack scenarios can fail for other reasons than neutralization. Failure may occur due to early detection on the attack plan before that point that adversaries planned to be detected), due to detection by intelligence organizations directly or by populace during the lead-up to the attack. Non-combat failures can also lead to scenario failure due to a variety of reasons:

- inability to get weapons or equipment needed;
- Breakdowns of vehicles, communications equipment
- Exhaustion of team-members during the attack
- Tool/explosive failure to breach
- Timing and synchronization failures
- Wrong plan due to bad information
- Inadequate training and rehearsal

21.4 Physical Protection System (PPS) Effectiveness

Estimate Physical Protection System (PPS) Effectiveness

Once a comprehensive set of credible scenarios has been developed using realistic assumptions about the system and adversary and the defeat strategies have been developed, the effectiveness of the physical protection system (PPS) effectiveness is typically determined by one or more simulations, either table-top, computer simulation, or Force-on-Force exercises. Probability of System Effectiveness, P_{EFF}, can either be determined by estimating P_{EFF} directly or by estimating Probability of Interruption and Probability of Neutralization separately and then using the formula: $P_I \ast P_N = P_{EFF}$.

This course Focuses on tabletops

Table top exercises will serve as the simulation technique taught in this course to determine P_E (qualitatively). Tabletop methodologies, unlike FoF and computer simulations, can be shared with all students.

Combining the Results of Different Simulations

When have a choice of simulations, the best sequence of use is shown below in Figure 21-4. Performance tests typically come first, provide necessary input to Table-tops. Table-top exercises can often foresee the analysis and logistic issues that will arise in computer simulations and FoF exercises. In some cases, issues are identified in table-tops that have to be addressed before other simulations can be performed.

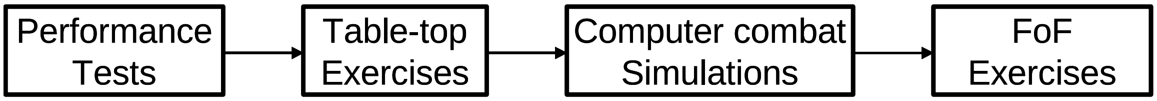


Figure 21-4: Proposed Sequence for Performing Neutralization tool:

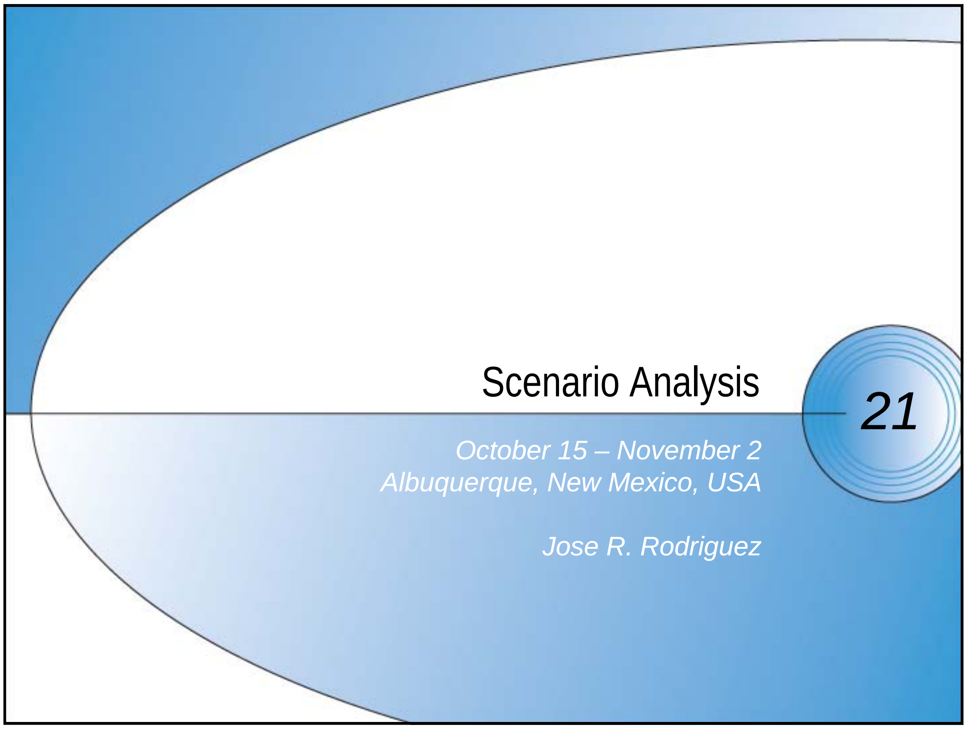
21.5 Summary

Adversary Scenario Analysis Identifies Credible Attack Scenarios

Adversary attack scenario analysis is used to identify a range of representative scenarios an adversary might use that are then employed in simulations to determine how effective the PPS at a facility performs.

Formal and Informal Methods of Identifying Scenarios

Formal scenario analysis typically involves expert scenario planners while Informal scenario analysis, as described here, can be performed when experts are not available or to determine P_E for most-vulnerable P_I paths. Informal scenario analysis employs a structured approach for creating scenarios based on vulnerabilities in the system and most-vulnerable interruption paths.

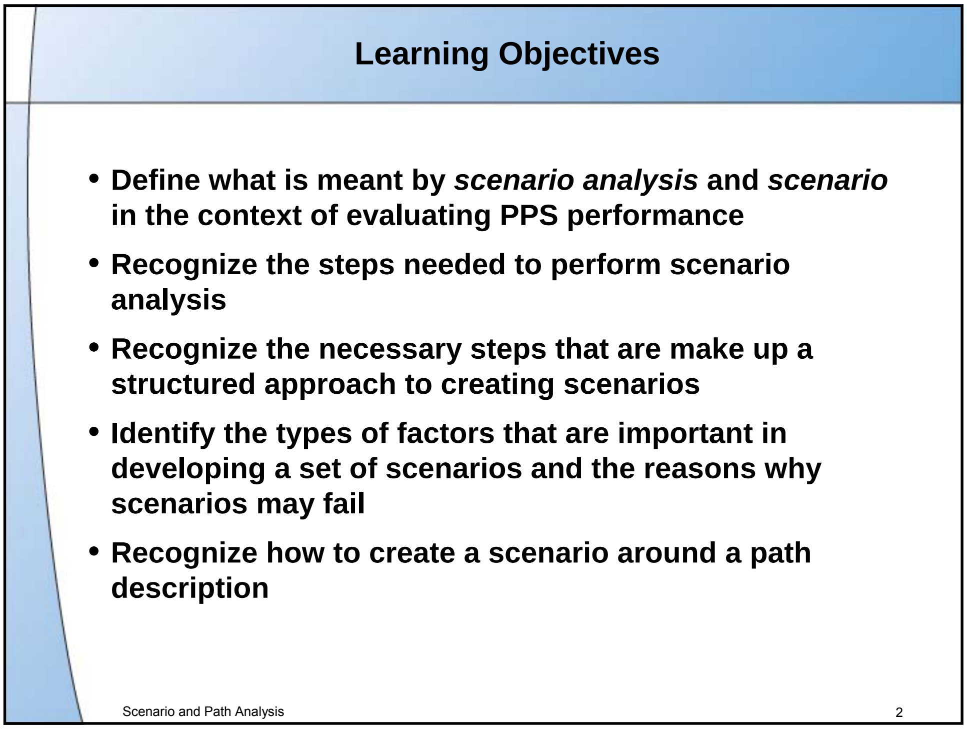


Scenario Analysis

21

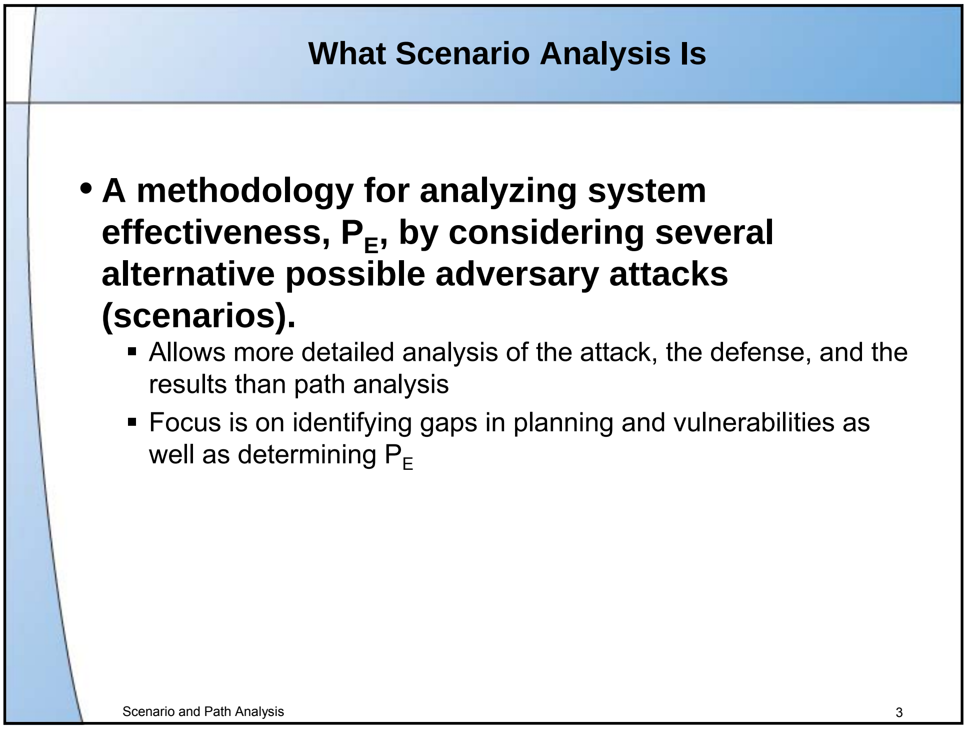
October 15 – November 2
Albuquerque, New Mexico, USA

Jose R. Rodriguez



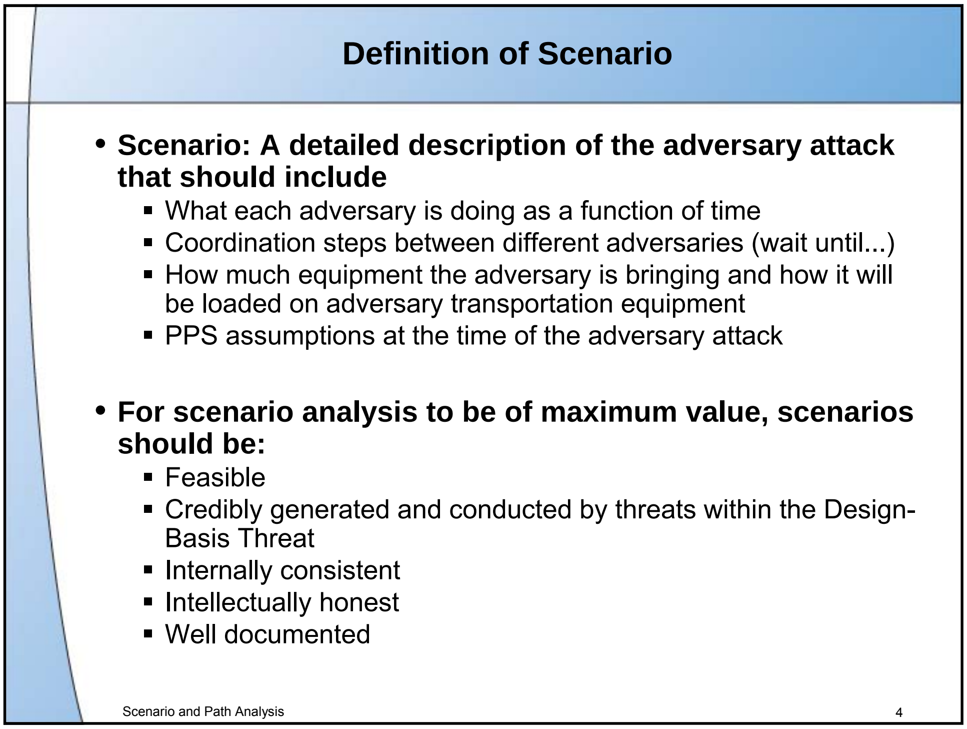
Learning Objectives

- **Define what is meant by *scenario analysis* and *scenario* in the context of evaluating PPS performance**
- **Recognize the steps needed to perform scenario analysis**
- **Recognize the necessary steps that are make up a structured approach to creating scenarios**
- **Identify the types of factors that are important in developing a set of scenarios and the reasons why scenarios may fail**
- **Recognize how to create a scenario around a path description**



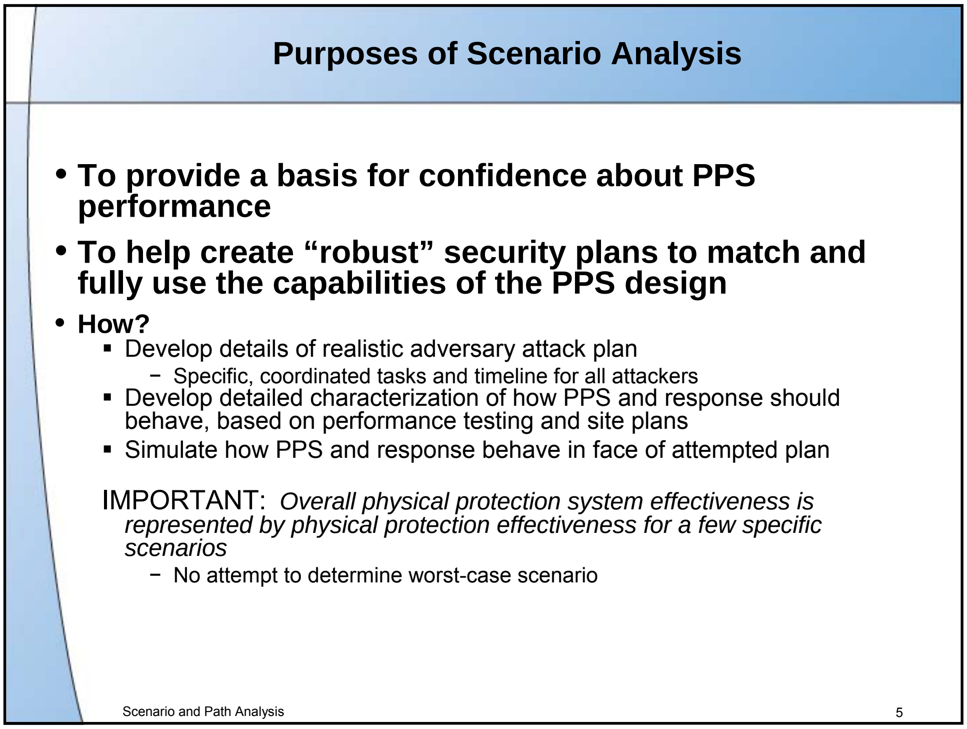
What Scenario Analysis Is

- **A methodology for analyzing system effectiveness, P_E, by considering several alternative possible adversary attacks (scenarios).**
  - Allows more detailed analysis of the attack, the defense, and the results than path analysis
  - Focus is on identifying gaps in planning and vulnerabilities as well as determining P_E



Definition of Scenario

- **Scenario: A detailed description of the adversary attack that should include**
  - What each adversary is doing as a function of time
  - Coordination steps between different adversaries (wait until...)
  - How much equipment the adversary is bringing and how it will be loaded on adversary transportation equipment
  - PPS assumptions at the time of the adversary attack
- **For scenario analysis to be of maximum value, scenarios should be:**
  - Feasible
  - Credibly generated and conducted by threats within the Design-Basis Threat
  - Internally consistent
  - Intellectually honest
  - Well documented

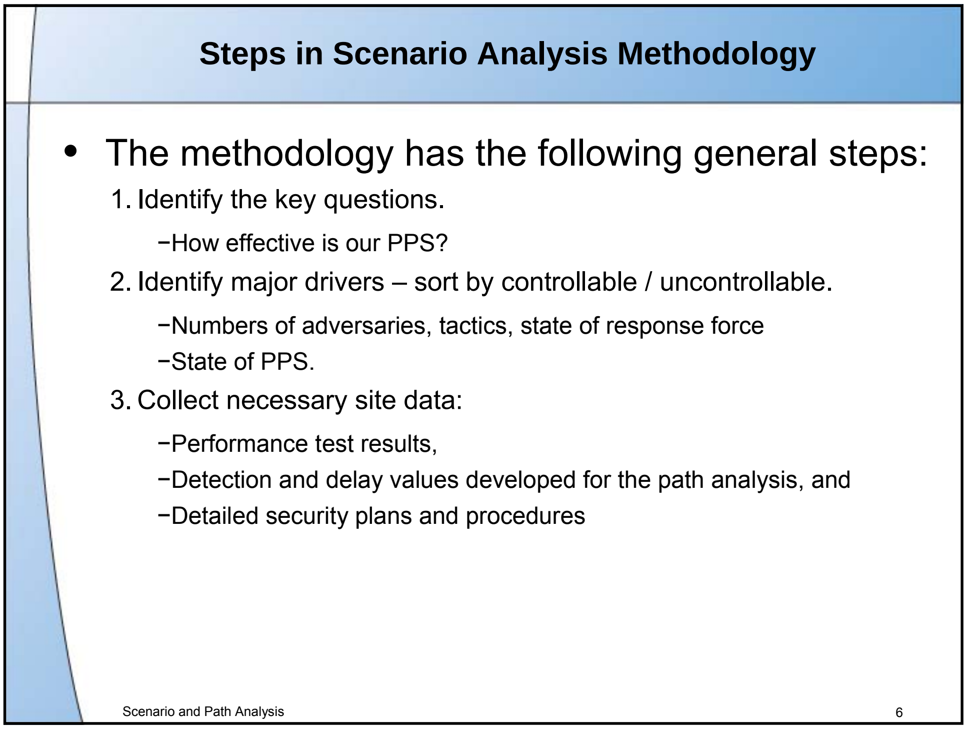


Purposes of Scenario Analysis

- **To provide a basis for confidence about PPS performance**
- **To help 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 in face of attempted plan

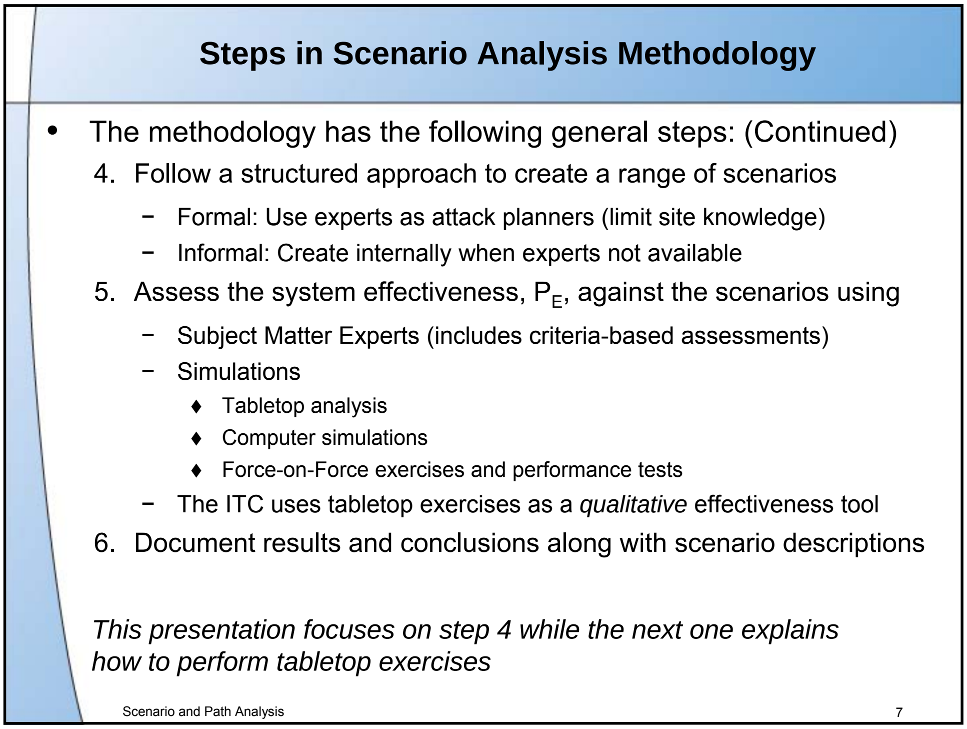
IMPORTANT: *Overall physical protection system effectiveness is represented by physical protection effectiveness for a few specific scenarios*

- No attempt to determine worst-case scenario



Steps in Scenario Analysis Methodology

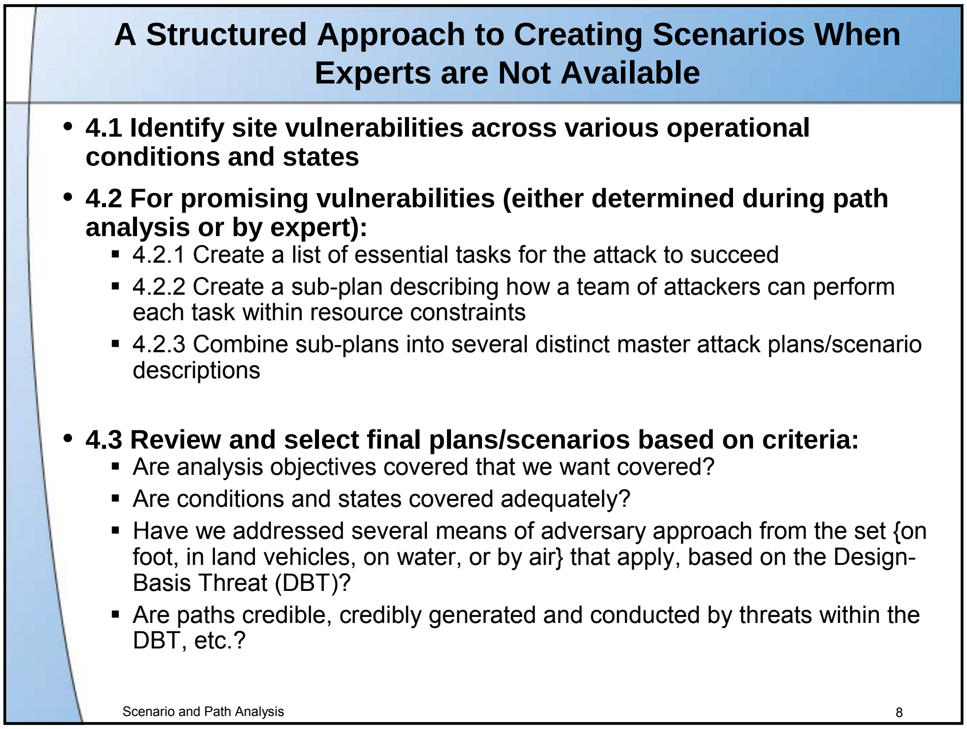
- The methodology has the following general steps:
  1. Identify the key questions.
     - How effective is our PPS?
  2. Identify major drivers – sort by controllable / uncontrollable.
     - Numbers of adversaries, tactics, state of response force
     - State of PPS.
  3. Collect necessary site data:
     - Performance test results,
     - Detection and delay values developed for the path analysis, and
     - Detailed security plans and procedures



Steps in Scenario Analysis Methodology

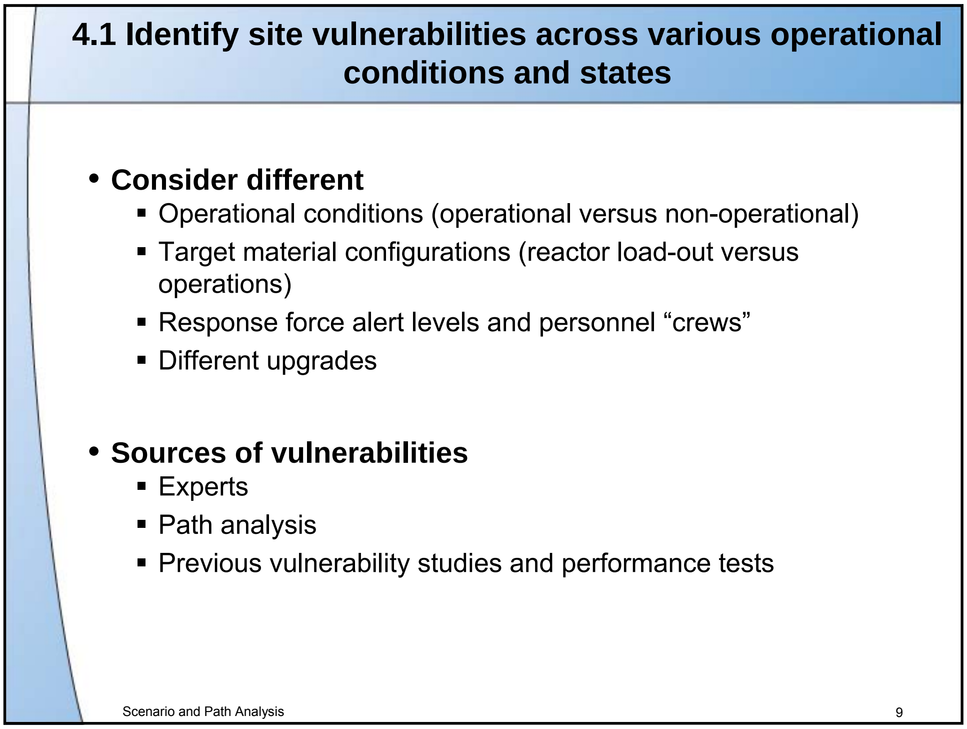
- The methodology has the following general steps: (Continued)
  4. Follow a structured approach to create a range of scenarios
     - Formal: Use experts as attack planners (limit site knowledge)
     - Informal: Create internally when experts not available
  5. Assess the system effectiveness, P_E, against the scenarios using
     - Subject Matter Experts (includes criteria-based assessments)
     - Simulations
       - ♦ Tabletop analysis
       - ♦ Computer simulations
       - ♦ Force-on-Force exercises and performance tests
     - The ITC uses tabletop exercises as a *qualitative* effectiveness tool
  6. Document results and conclusions along with scenario descriptions

This presentation focuses on step 4 while the next one explains how to perform tabletop exercises



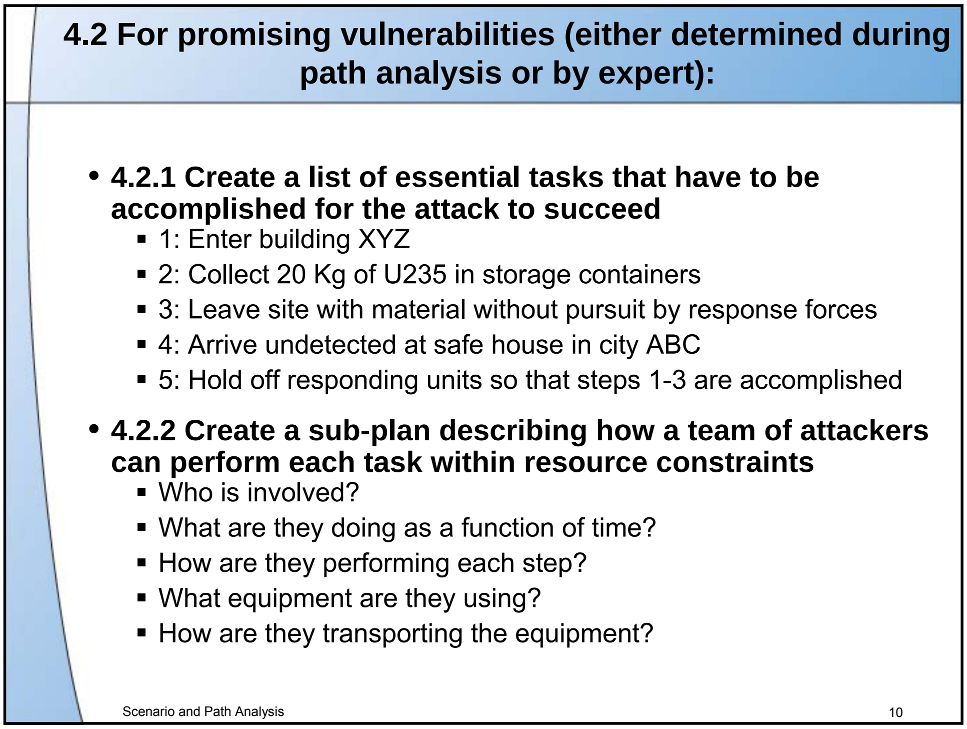
A Structured Approach to Creating Scenarios When Experts are Not Available

- **4.1 Identify site vulnerabilities across various operational conditions and states**
- **4.2 For promising vulnerabilities (either determined during path analysis or by expert):**
  - 4.2.1 Create a list of essential tasks for the attack to succeed
  - 4.2.2 Create a sub-plan describing how a team of attackers can perform each task within resource constraints
  - 4.2.3 Combine sub-plans into several distinct master attack plans/scenario descriptions
- **4.3 Review and select final plans/scenarios based on criteria:**
  - Are analysis objectives covered that we want covered?
  - Are conditions and states covered adequately?
  - Have we addressed several means of adversary approach from the set {on foot, in land vehicles, on water, or by air} that apply, based on the Design-Basis Threat (DBT)?
  - Are paths credible, credibly generated and conducted by threats within the DBT, etc.?



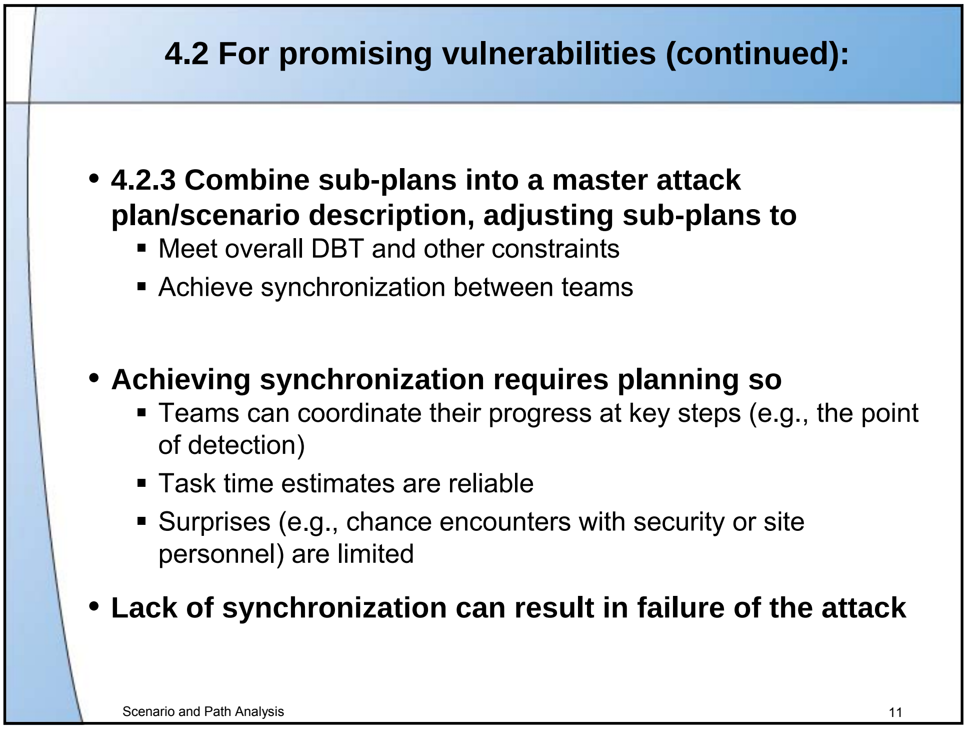
4.1 Identify site vulnerabilities across various operational conditions and states

- **Consider different**
  - Operational conditions (operational versus non-operational)
  - Target material configurations (reactor load-out versus operations)
  - Response force alert levels and personnel “crews”
  - Different upgrades
- **Sources of vulnerabilities**
  - Experts
  - Path analysis
  - Previous vulnerability studies and performance tests



4.2 For promising vulnerabilities (either determined during path analysis or by expert):

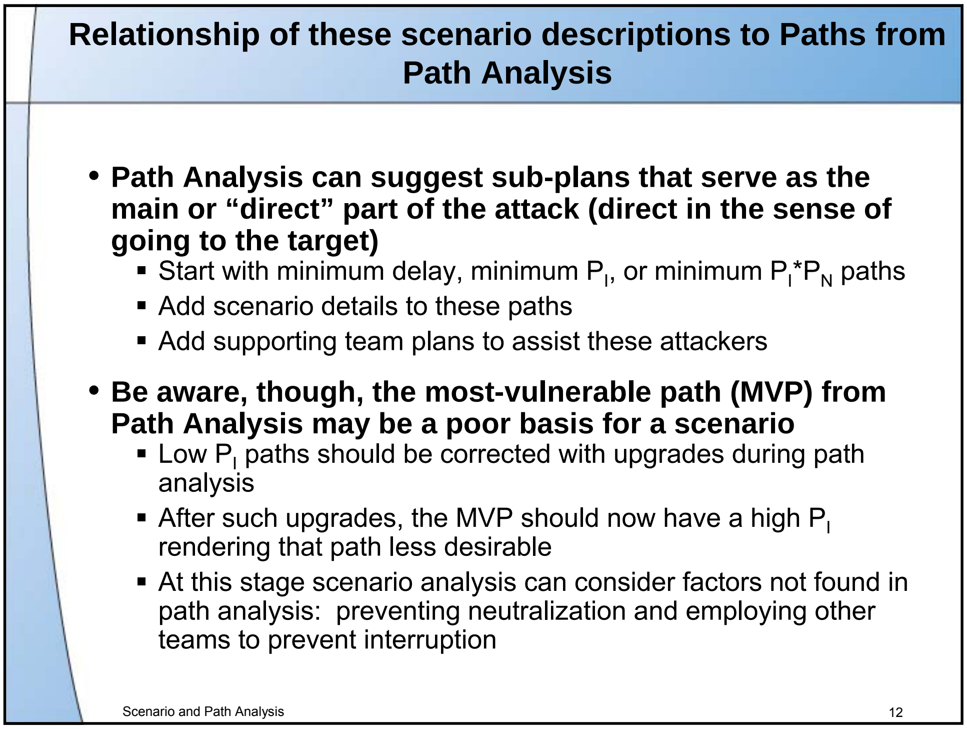
- **4.2.1 Create a list of essential tasks that have to be accomplished for the attack to succeed**
  - 1: Enter building XYZ
  - 2: Collect 20 Kg of U235 in storage containers
  - 3: Leave site with material without pursuit by response forces
  - 4: Arrive undetected at safe house in city ABC
  - 5: Hold off responding units so that steps 1-3 are accomplished
- **4.2.2 Create a sub-plan describing how a team of attackers 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?



4.2 For promising vulnerabilities (continued):

- **4.2.3 Combine sub-plans into a master attack plan/scenario description, adjusting sub-plans to**
  - Meet overall DBT and other constraints
  - Achieve synchronization between teams
- **Achieving synchronization requires planning so**
  - Teams can coordinate their progress at key steps (e.g., the point of detection)
  - Task time estimates are reliable
  - Surprises (e.g., chance encounters with security or site personnel) are limited
- **Lack of synchronization can result in failure of the attack**

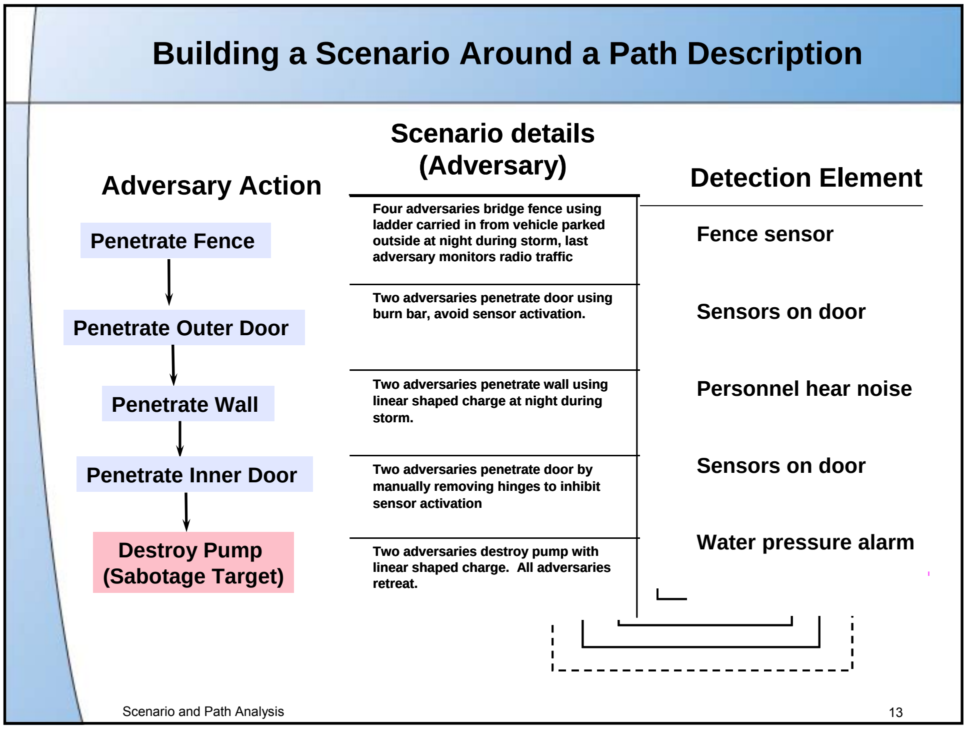
Scenario and Path Analysis 11



Relationship of these scenario descriptions to Paths from Path Analysis

- **Path Analysis can suggest sub-plans that serve as the main or "direct" part of the attack (direct in the sense of going to the target)**
  - Start with minimum delay, minimum P_I, or minimum P_I*P_N paths
  - Add scenario details to these paths
  - Add supporting team plans to assist these attackers
- **Be aware, though, the most-vulnerable path (MVP) from Path Analysis may be a poor basis for a scenario**
  - Low P_I paths should be corrected with upgrades during path analysis
  - After such upgrades, the MVP should now have a high P_I rendering that path less desirable
  - At this stage scenario analysis can consider factors not found in path analysis: preventing neutralization and employing other teams to prevent interruption

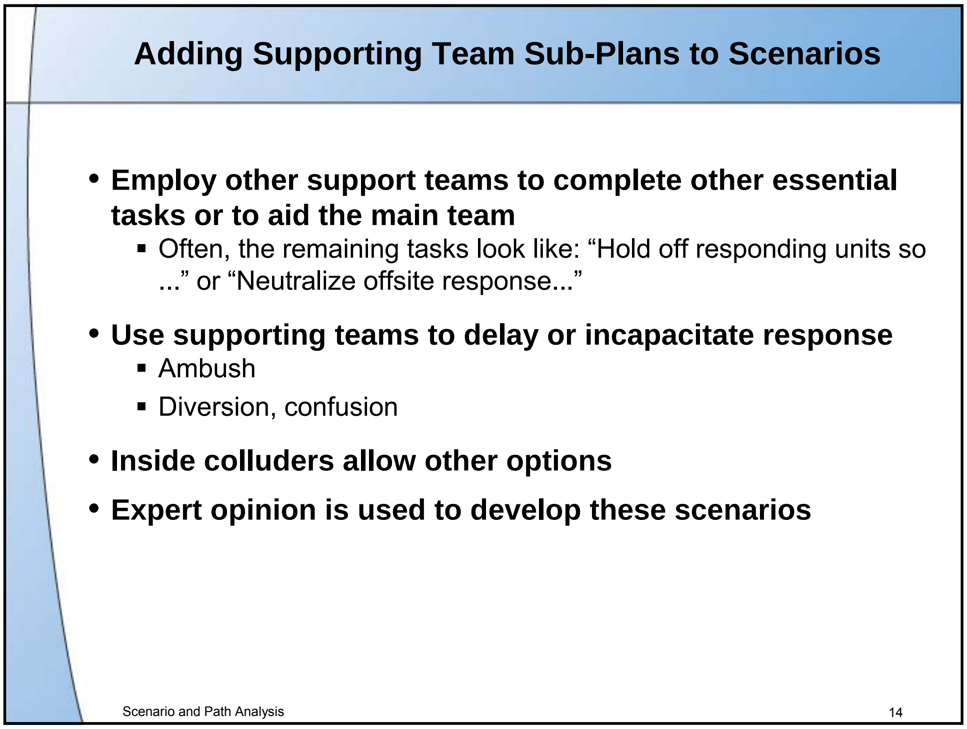
Scenario and Path Analysis 12



Building a Scenario Around a Path Description

Adversary Action	Scenario details (Adversary)	Detection Element
Penetrate Fence	Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during storm, last adversary monitors radio traffic	Fence sensor
Penetrate Outer Door	Two adversaries penetrate door using burn bar, avoid sensor activation.	Sensors on door
Penetrate Wall	Two adversaries penetrate wall using linear shaped charge at night during storm.	Personnel hear noise
Penetrate Inner Door	Two adversaries penetrate door by manually removing hinges to inhibit sensor activation	Sensors on door
Destroy Pump (Sabotage Target)	Two adversaries destroy pump with linear shaped charge. All adversaries retreat.	Water pressure alarm

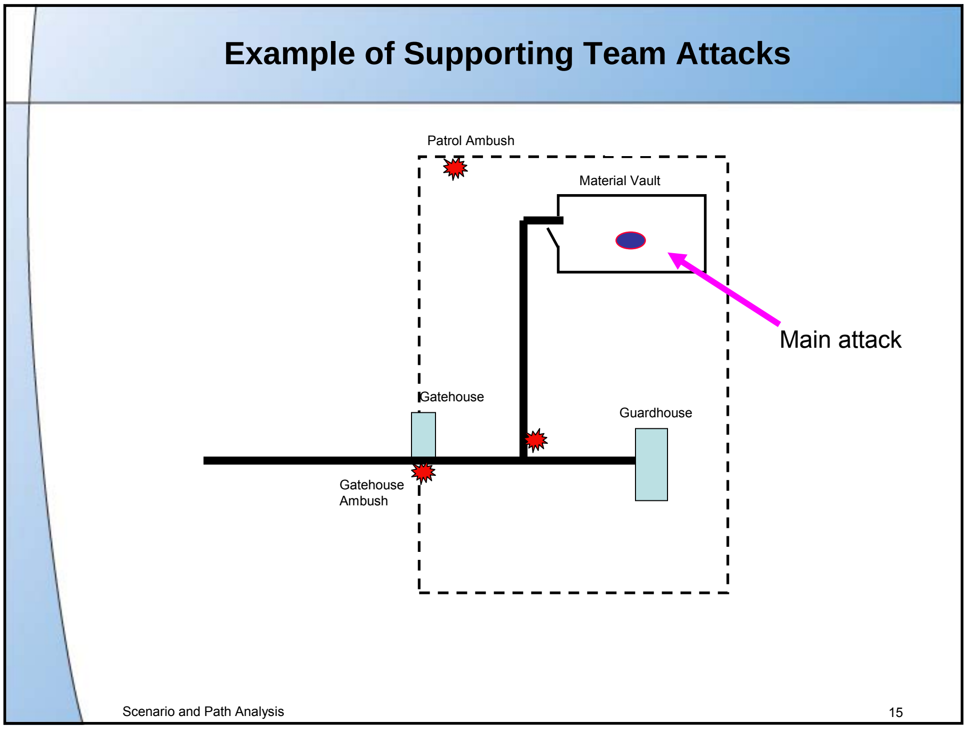
Scenario and Path Analysis 13



Adding Supporting Team Sub-Plans to Scenarios

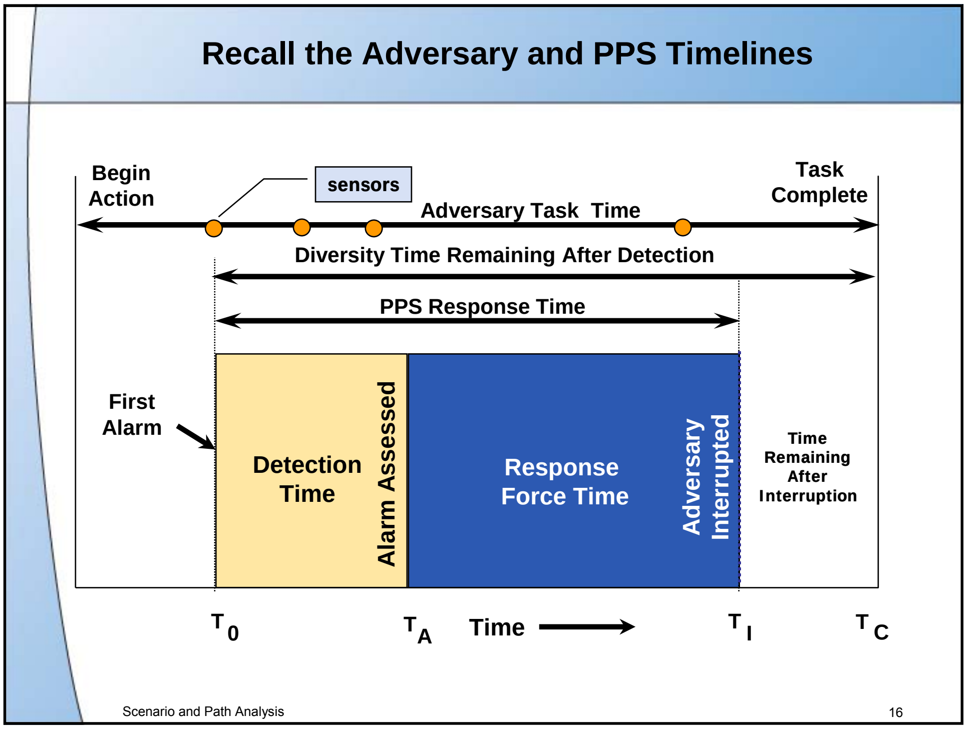
- **Employ other support teams to complete other essential tasks or to aid the main team**
  - Often, the remaining tasks look like: “Hold off responding units so ...” or “Neutralize offsite response...”
- **Use supporting teams to delay or incapacitate response**
  - Ambush
  - Diversion, confusion
- **Inside colluders allow other options**
- **Expert opinion is used to develop these scenarios**

Scenario and Path Analysis 14



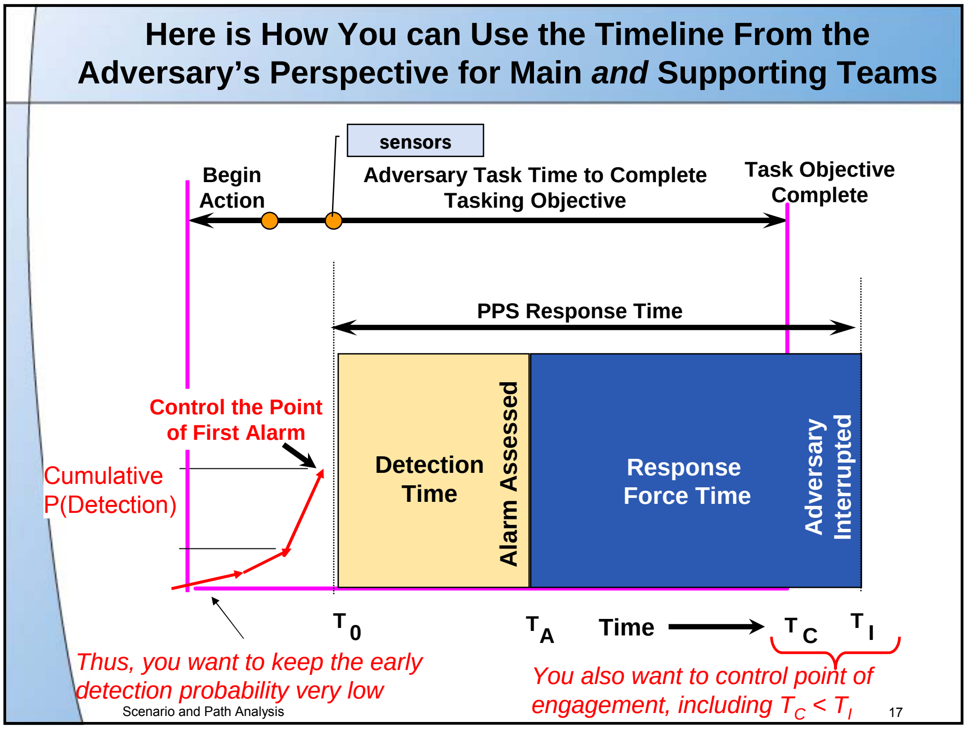
Example of Supporting Team Attacks

Scenario and Path Analysis 15



Recall the Adversary and PPS Timelines

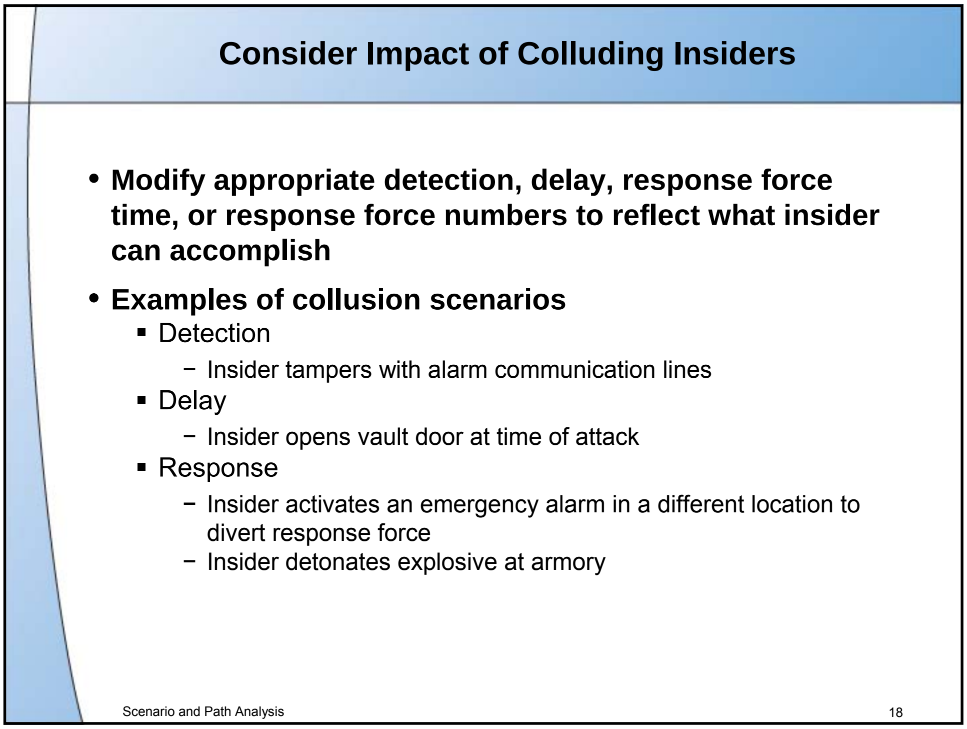
Scenario and Path Analysis 16



Here is How You can Use the Timeline From the Adversary's Perspective for Main *and* Supporting Teams

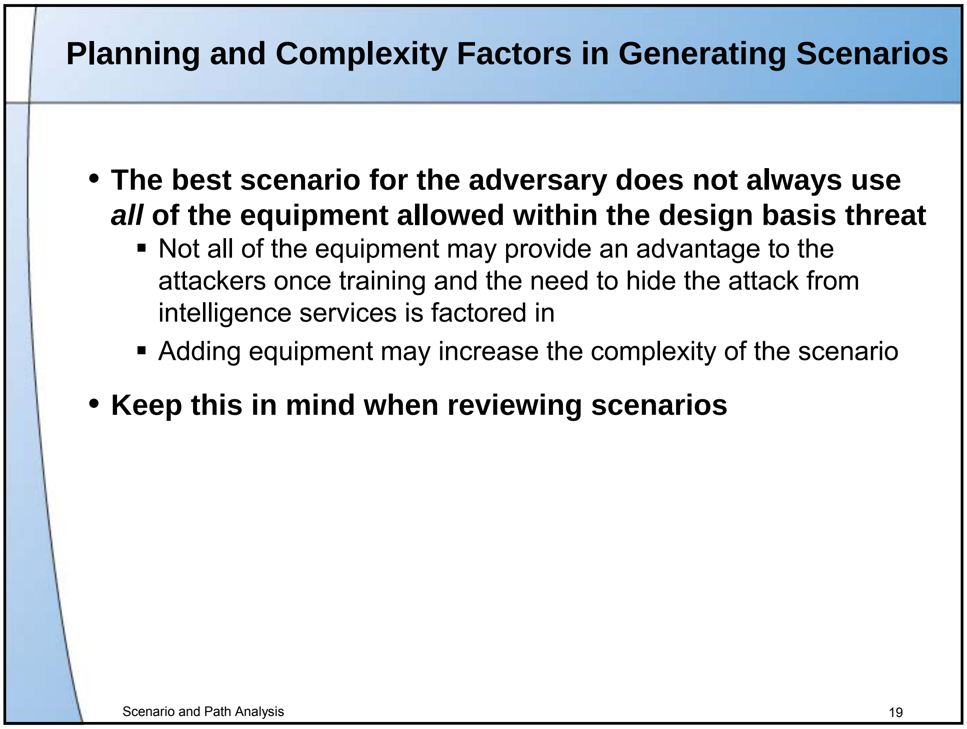
Thus, you want to keep the early detection probability very low

You also want to control point of engagement, including $T_C < T_I$



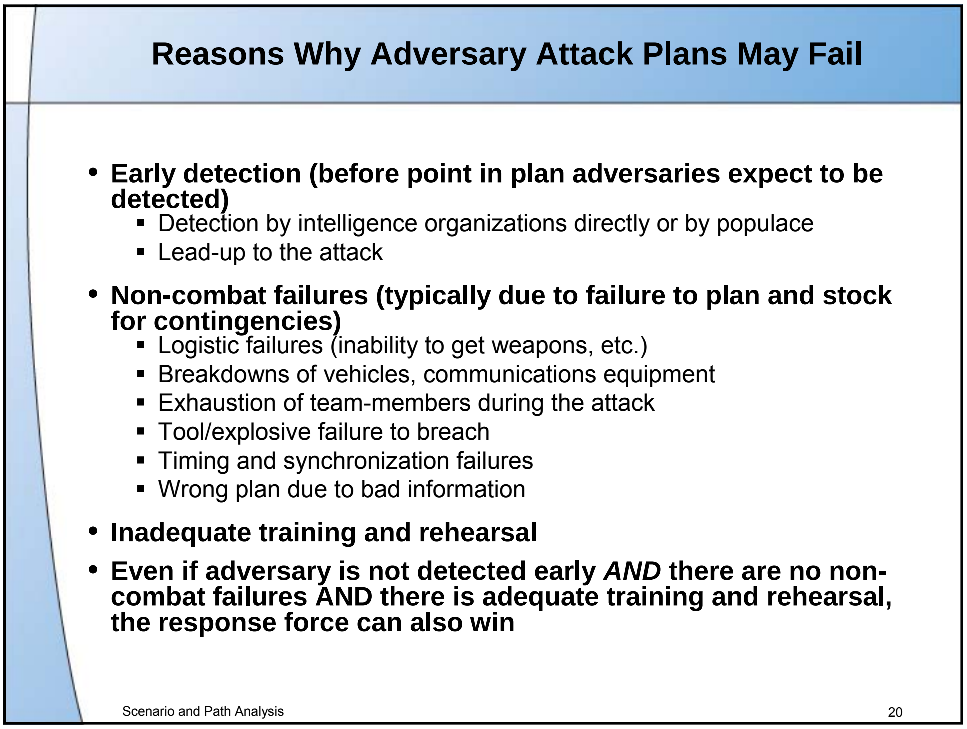
Consider Impact of Colluding Insiders

- **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



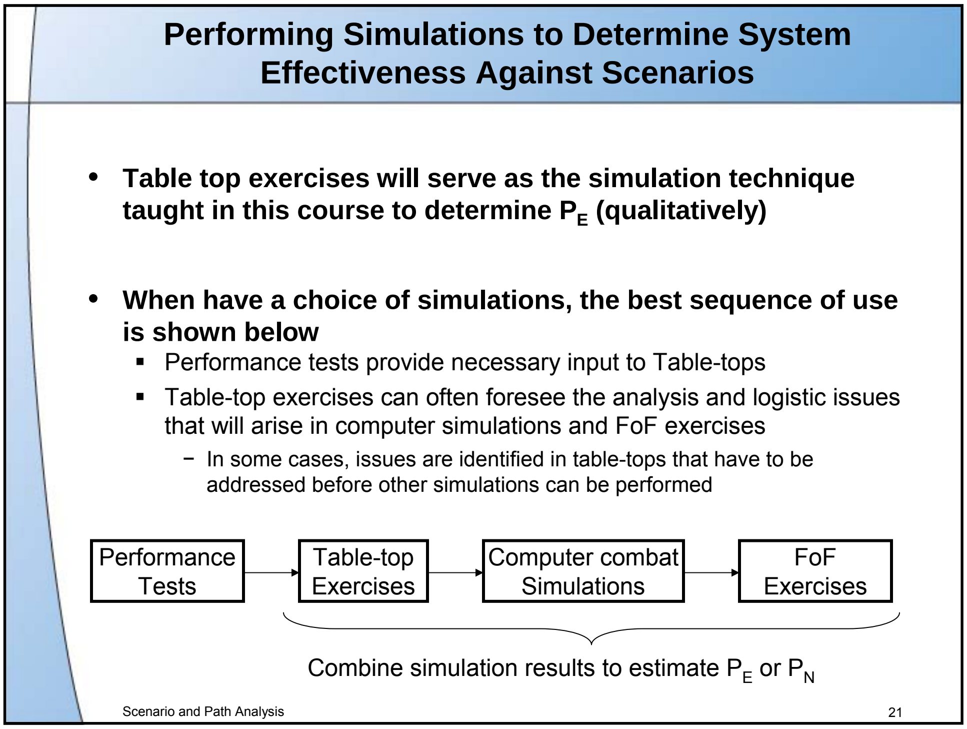
Planning and Complexity Factors in Generating Scenarios

- **The best scenario for the adversary does not always use *all* of the equipment allowed within the design basis threat**
  - Not all of the equipment may provide an advantage to the attackers once training and the need to hide the attack from intelligence services is factored in
  - Adding equipment may increase the complexity of the scenario
- **Keep this in mind when reviewing scenarios**



Reasons Why Adversary Attack Plans May Fail

- **Early detection (before point in plan adversaries expect to be detected)**
  - Detection by intelligence organizations directly or by populace
  - Lead-up to the attack
- **Non-combat failures (typically due to failure to plan and stock for contingencies)**
  - Logistic failures (inability to get weapons, etc.)
  - Breakdowns of vehicles, communications equipment
  - Exhaustion of team-members during the attack
  - Tool/explosive failure to breach
  - Timing and synchronization failures
  - Wrong plan due to bad information
- **Inadequate training and rehearsal**
- **Even if adversary is not detected early *AND* there are no non-combat failures AND there is adequate training and rehearsal, the response force can also win**

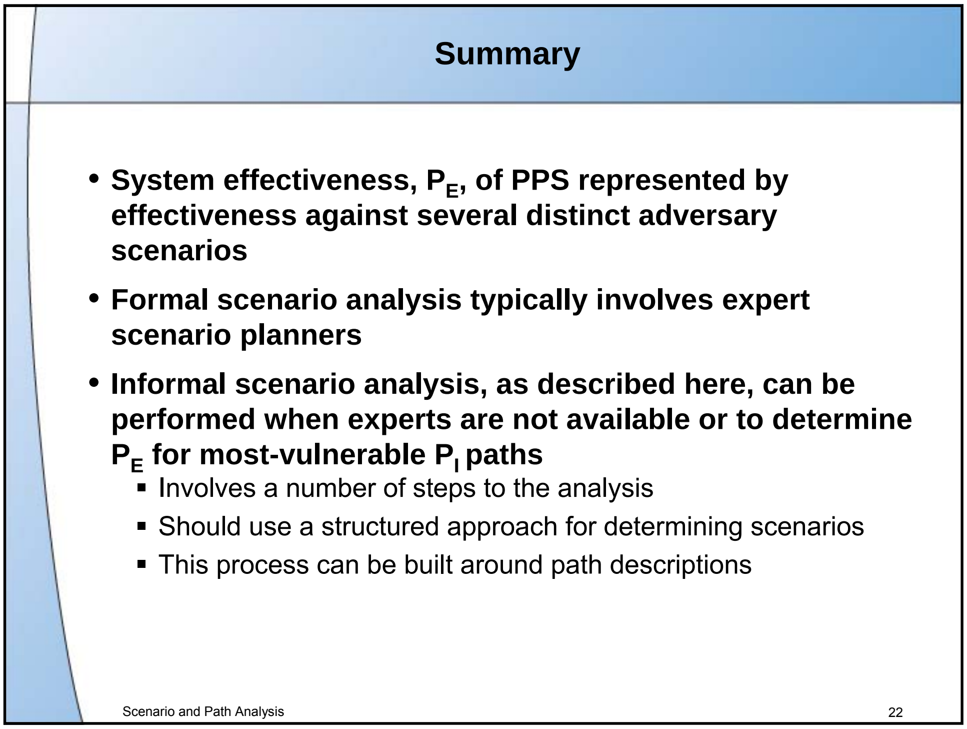


Performing Simulations to Determine System Effectiveness Against Scenarios

- **Table top exercises will serve as the simulation technique taught in this course to determine P_E (qualitatively)**
- **When have a choice of simulations, the best sequence of use is shown below**
  - Performance tests provide necessary input to Table-tops
  - Table-top exercises can often foresee the analysis and logistic issues that will arise in computer simulations and FoF exercises
    - In some cases, issues are identified in table-tops that have to be addressed before other simulations can be performed

Performance Tests → Table-top Exercises → Computer combat Simulations → FoF Exercises

Combine simulation results to estimate P_E or P_N



Summary

- **System effectiveness, P_E, of PPS represented by effectiveness against several distinct adversary scenarios**
- **Formal scenario analysis typically involves expert scenario planners**
- **Informal scenario analysis, as described here, can be performed when experts are not available or to determine P_E for most-vulnerable P_I paths**
  - Involves a number of steps to the analysis
  - Should use a structured approach for determining scenarios
  - This process can be built around path descriptions

23. Insider Analysis

Abstract. *The term "insider" describes any individual with authorized access to nuclear materials or transport who might attempt unauthorized removal of nuclear material or sabotage, or who could aid outsiders to do so. Facilities handling nuclear materials and other attractive targets should consider the possibility of malevolent action by an insider. The insider has unique capabilities compared to the "outsider" adversary, such as authorized access, authority, and knowledge. Insiders may also act in collusion with outsiders. Prevention and protection against the insider threat includes identifying facility-specific insider groups, using a system approach to design relevant preventive and protective measures, and analyzing and evaluating protection system effectiveness.*

23.1 Introduction

Insiders Have Access, Authority, and Knowledge,

An insider adversary could be anyone who has authorized access to the facility, regardless of position of authority or level of knowledge. Insiders present a unique problem for a physical protection system. Insiders could take advantage of their access, complemented by their authority and facility knowledge, to bypass protection elements, including safety, material control and accountability, and operating measures and procedures, and to access controls to perform acts of sabotage or unauthorized removal. Further, as a trusted person, the insider is capable of defeat methods not available to outsiders when confronted with protection elements and access controls. The insider can select the most vulnerable target, the best time to execute the malicious act, and can stretch the malicious act over a long period if advantageous to maximize likelihood of success. This would include, among other things, modifying safety equipment or stealing small amounts of material over an extended period.

Insider Categories

Insiders may be passive or active, violent or nonviolent, internally motivated or externally coerced (see Figure 23-1).

- The ***passive insider*** is nonviolent, limiting his participation to providing information about facility operations and safeguards to a colluding insider or outsider(s). The passive insider provides only the information that he or she can readily obtain and divulge without fear of detection.

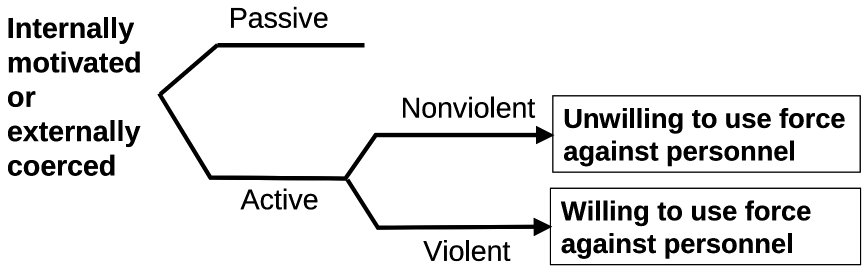

Internally motivated or externally coerced
Passive
Nonviolent
Unwilling to use force against personnel
Active
Willing to use force against personnel
Violent

Figure 23-1. Categories of insiders.

- The ***active insider*** is willing to provide information, perform actions for the adversaries, and may be violent or nonviolent. The active insider is willing to open doors, provide hands-on help, and aid in neutralizing response force personnel.
  - The ***nonviolent active insider*** is not willing to be identified or risk the chance of engaging response forces and may limit his or her activities to tampering with safeguards and security systems.
  - ***Violent*** active insiders may use force regardless of whether it enhances their chances for success or not. The violent insider may be rational or irrational; he may be a psychotic or a criminal.

Types of Insiders

Types of insiders include criminals, disgruntled employees, ideologues, and psychotic individuals.

- The ***criminal insider*** may have a prior history of committing criminal acts. Every day, U.S. businesses lose 70 million dollars to theft, and in 2000 employee theft accounted for 44% of these losses. The insider criminal is a very real threat.
- Typically, the ***disgruntled employee*** is a person who has been employed in their position for several years, but who has become dissatisfied with the working environment. Another employee may be happy with the job, but external influences could cause the employee to act inappropriately at work. The most common cause in these situations is an unhappy domestic life. Employees might be worried about possible layoffs or increased workloads, which could raise stress levels and cause actions against management. Other employee-related problems can include drug abuse and a wide range of psychological problems such as long-term depression.
- Some insiders are motivated by ***ideological beliefs***, such as anti-nuclear activists, who believe so strongly in certain issues that they are willing to defy the law for the sake of their beliefs. These insiders are typically bright individuals who have a committed attitude and a rebellious nature.

23.2 Past Incidents

Insiders Are Difficult to Defend Against

Analysis of past insider incidents indicates that insiders are among the most difficult threats to defend against. In a study of commercial industry incidents, members of the security force represented approximately 41% of insiders who commit acts against the facilities. No similar conclusions can be drawn from the limited data available for the nuclear industry. However, the response force is probably one of the very few groups of individuals that have complete access to any place within the protected area and would not attract any suspicion based on their presence. In addition, they are often some of the lowest-paid employees.

Examples of Disgruntled Employees

In December 1987, an American PSA Flight 1771 crashed and killed everyone aboard. The perpetrator was a former employee who had been fired from the airline for alleged misconduct. Although no longer an employee of the airline, he was able to use his access card to gain entry into the plane with a gun in his possession. Once in the air, the ex-employee gained control of the cockpit and shot the crew. Shortly after the incident, the Director of Security for the Federal Aviation Administration (FAA) was quoted, "*The most difficult problem (in personnel screening at airports) is those with knowledge and access*" (Associated Press, 1987).

An example of a computer-related incident involving a disgruntled employee took place in September 1996. A small Internet provider was virtually destroyed by the former employee who, on the day he was laid off from his job, accessed the company's files and erased all the data and back-up files (USA Today, 1997).

On December 4, 1997, staff at McGuire Nuclear Station, Unit 2 discovered indications of potential tampering with the upper and lower personnel air lock seals. The air lock design incorporates two inflatable seals per door, for a total of four seals per air lock. The damage was identified during the performance of required testing of the air lock seal integrity to support restart of the unit. A sharp instrument was used to damage the seals. The plant staff determined that all of the eight seals had been cut. No additional indications of tampering were identified. Walkdowns of plant systems conducted before this tampering event also identified mispositioned valves. The unit was shut down to replace the steam generators and undertake refueling at that time. The utility speculated that the tampering might have been related to a work-force-reduction announcement.

Examples of Criminal Insider

In Germany, a Slovak engineer was arrested on suspicion of smuggling 6 pounds of radioactive uranium into the country. The uranium was found in a bank safety deposit box in the southern town of Ulm. The 49-year-old man was arrested after Austrian police reported that the man was trying to sell the uranium for $1 million, U.S. currency (CJ Europe, 1996).

Attempted Extortion by Temporary Employee

On Friday, January 26, 1979, a temporary employee of subcontractor working at the General Electric low enriched fuel fabrication plant in Wilmington, North Carolina, stole two 5-gallon containers of low enriched UO_2 (~145 pounds total). The theft was accomplished as follows. After working the day shift, he drove back to the plant at 10:50 p.m. and entered with the night shift. He circumvented the access controls at the entrance gate by showing the guard his Florida driver's license which looked similar to a picture badge authorizing access to the plant area where the UO_2 was processed. His yellow contractor badge would not have permitted access to this area. He had allegedly used his driver's license to gain access to this area on previous occasions. Once inside the plant, the subject would have been guided by gates and fences into a parking area had it not been for the fact that one gate had been removed to allow installation of truck scales. The missing gate made it possible for him to drive to an area adjacent to the building he wanted to enter and park his car. He entered the building and went to his normal workstation, the Chem Tech Lab, entering it using his key. In the lab he picked up his protective clothing, a two-wheel cart used to move 55-gallon drums, and a container used to ship chemicals. The container could hold two 5-gallon cans. He then proceeded to a door leading up a stairwell into the radiation controlled area. The door was normally locked (though there was no regulatory requirement to do so). However, at this time it was slightly ajar due to malfunction of the locking mechanism. Once through the door, he put on his protective clothing and went up the stairs to the Blend Queue Area. He removed two 5-gallon cans of $U0_2$, carried them down the stairs and put them in the shipping container. He then removed his protective clothing and retraced his steps back to his workstation, the Chem Tech Lab.

Once back in the lab he opened one can and removed some of the material, which he intended to use to effect his blackmail scheme. Using the two-wheel cart, he transported the remaining material to his car and loaded it into his trunk. He retraced his steps and left the plant just before midnight on Friday, January 26. (Plant procedures required anyone leaving the plant after midnight to sign out.) He had been in the plant approximately one hour. He had entered the plant with the incoming plant change and had left with the outgoing shift.

At 11:45 a.m. on the following Monday, January 29, the plant General Manager reported to authorities that he had found an extortion letter and a sample of UO_2 at his door when he came to work. The letter stated that the writer had taken two 5-gallon containers of UO_2 from the plant and identified the containers by serial number and gross weight. The letter also stated that sufficient UO_2 had been removed from one of the containers to furnish samples to newspaper editors, Senators, anti-nuclear group leaders, and others if his demand for $100,000 in cash was not met by Thursday, February 1. The writer further threatened that, after the samples had been delivered, if he had not received the money, one container of UO_2 would be dispersed through one unnamed large American city. The UO_2 powder from the second container would be dispersed through another large city if an additional $100,000 was not provided at that time.

As the General Manager was in the process of verifying the authenticity of the container numbers and determining whether they were missing, he received independent notification from the plant near-real-time accounting system that the two containers were not in their assigned locations and could not be accounted for. The Federal Bureau of Investigation (FBI) assumed investigative jurisdiction on January 29 and arrested the perpetrator on February 1, 1979. The perpetrator, a temporary employee, was subsequently convicted and sentenced to 15 years in prison.
(From IE Circular No. 79-08, “Attempted Extortion – Low Enriched Uranium,” May 17, 1979.)

Theft of Fuel Assembly

In August 1992, a 7-meter-long fuel assembly weighing 270 kg and containing 111 kg of 2% enriched LEU was stolen from the Ignalina Nuclear Power Plant, in Ignalina, Lithuania. It was removed from the facility by attaching it to the bottom of a duty bus. The investigation revealed that the reactor operation personnel and the guards had carried out the theft. About 80 kg of the stolen LEU are said to have been recovered on several occasions between 1992 and 2002. (Presentation by Chaim Braun, Fritz Steinhausler, and Lyudmila Zaitseva at the ANS 2002 Winter Meeting.)

Theft of Uranium

In 1992, Russian security agents detained a group of criminals who had been stealing Uranium from the Chepetsk plant in Izhevsk and seized 140 kg of LEU (2% to 4% enrichment). Facility employees stole the material taking advantage of an accounting system weakness that allowed a 4% "loss of inventory" in material balance closures. Based on the incident, an inventory was conducted at the plant and 300 kg were found to be missing. Parts of the diverted material are believed to have been seized in Poland, Belarus, Lithuania, Russia, and Chechnya between 1992 and 2002. (Presentation by Chaim Braun, Fritz Steinhausler, and Lyudmila Zaitseva at the ANS 2002 Winter Meeting.)

23.3 Opportunity, Motivation, and Attempts

Opportunity

The combination of access, authority, and knowledge combine to provide the insider with an opportunity to commit a malevolent act.

- **Access:** Insiders by definition have authorized access to work areas in a facility. They may also have special temporary access, including emergency access by fire, medical, or police responders. They may be escorted or unescorted, and may have other restrictions during access. Because of their knowledge or authority, they may be able to obtain unauthorized access to certain areas. They may have access to protection equipment, process tools, or other special site equipment that they could exploit. They may also know about and gain access to target material during vulnerable conditions of sufficient duration to perform malevolent acts.

- **Authority:** Insider authority may be over personnel, such as designated authority or personal influence, or over tasks and equipment, such as alarm assessment, sensitive documents, or authorization for processes and procedures.

- **Knowledge:** Insider knowledge may comprise target information, security system details, or information about site tools and equipment. Target information includes locations, characteristics, durations, and other details of targets, as well as details of facility layouts. Security system information includes response force capabilities and communications, details of facility and security operations, as well as the location and operational details of safety equipment.

Motivation

Insider motivation may be ideological, financial, revenge, ego, mental stability, or coercion. Motivation is an important indicator for both level of malevolence and likelihood of attempt.

Insider Advantages

- **Unique capabilities:** Insiders can select the best time and strategy to be successful in their task. Because of their unique capabilities, they can exploit time, tools, tests, and collusion to be successful.
- **Time:** Insiders can select the optimum time to implement a plan, and they can extend acts over long periods of time to avoid detection.
- **Tools:** Insiders have the capability to use tools located at work stations, or to introduce contraband tools into the facility.
- **Tests:** Insiders can test the protection system with intentional, normal-looking "mistakes."
- **Collusion:** Insiders may recruit, direct, coerce, or collude with others, including both other insiders and outsiders.

Attempts

The combination of access, authority, and knowledge attributes may provide an insider with an opportunity for the commission of a malevolent act. Opportunity, when combined with motivation, may lead to an actual ***attempt*** to commit a malevolent act. The system to prevent and protect against insiders is predicated on this combination of opportunity and motivation.

23.4 Measures to Prevent and Protect Against Insiders

General Approach

The insider problem must be approached in a different way than that of the outsider. The outsider attacks can only be addressed once they occur but there are several elements of the insider protection system that reduce the likelihood of a malevolent insider presence as well as elements that detect and prevent insider malevolent actions. The insider protection approach can be broken into several sequential phases, as shown in Figure 23-2. The process to prevent and protect against insiders consists of five steps:

1. Exclude potential insiders from obtaining access,

2. Remove potential insiders after they have access,

3. Minimize opportunities for committing malevolent acts,

4. Detect, delay and respond to such acts, and

5. Mitigate consequences from a completed act.

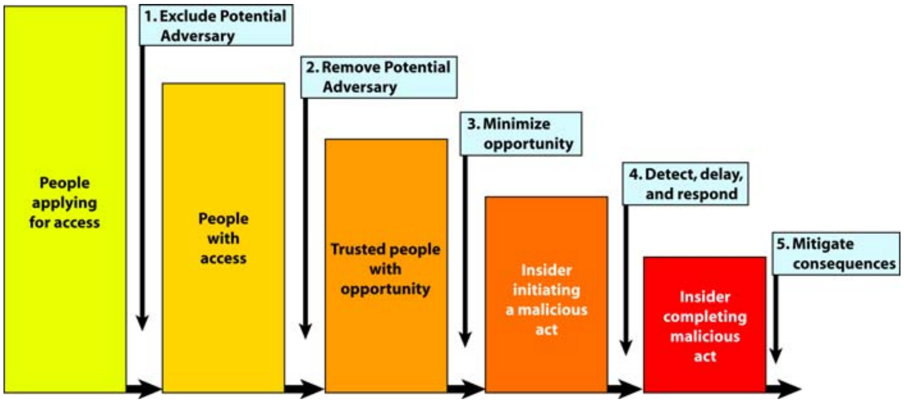

1. Exclude Potential Adversary
2. Remove Potential Adversary
3. Minimize opportunity
4. Detect, delay, and respond
5. Mitigate consequences
People applying for access
People with access
Trusted people with opportunity
Insider initiating a malicious act
Insider completing malicious act

Figure 23-2. Insider protection system approach.

Personnel Security Programs

Personnel security programs address Steps 1 and 2, and include:

- initial access authorization (personnel clearances),
- security education and awareness (security culture),
- control of visits, and
- the Human Reliability Program (HRP).

Physical Security Systems

Physical security systems address Steps 3 and 4. These can include, but are not limited to, the following:

- barriers,
- intrusion detection systems,
- contraband detection,
- access controls to monitor access and exit,
- surveillance,
- response force, and
- contingency plans.

Material control and accountability systems are an important part of both Steps 3 and 4. Physical consolidation of material to reduce the number and location of target material is also important.

23.4.1 Exclude Potential Adversaries with Pre-Employment Checks

Pre-Employment Checks

The first step is to filter potential employees and contractors. A **pre-employment investigation** is a systematic compilation and evaluation of information collected through inquiries made in person, by telephone, or in writing with the intent to establish the general character, trustworthiness, and reliability of prospective employees and contractors. These investigations are not trivial. In the U.S., they are often done by the FBI and cost more than $10,000 for each investigation.

23.4.2 Remove Potential Adversaries After They Begin Activities at the Facility

Develop a Desirable Working and Security Culture

Once a clearance is granted, it should be re-evaluated periodically, for example, every five years. Through a continuing program of security education and awareness, a security culture can be established which tends to minimize malevolent activity. The level of employee satisfaction can be enhanced by good working conditions, well-conducted training, and employee benefits (insurance, holidays, etc.) Operational quality control programs also assist in reducing the motivation and opportunity for malevolence. Finally, special programs for those few individuals who have direct access to critical areas can be put into place. In the U.S., one of these is called the Personnel Security Assurance Program (PSAP). Many facilities worldwide also have “fitness for duty” requirements. All of these programs are intended to reduce the number of potential insider adversaries. If disciplinary action is invoked when malevolence occurs, additional malevolent activities may be deterred.

Educate Employees

Security awareness is an integral element for physical protection systems. Employees are required to attend briefings that apply to their specific access needs. The goal of the security education program is to inform the employees of their security responsibilities, to alert them to actual or potential threats, and to motivate them to maintain a high level of security awareness.

Types of Briefings

In the U.S., types of briefings are used in the Security Education and Awareness Program, as follows:

- Initial Briefing,
- Comprehensive Briefing,
- Annual Refresher Briefing, and
- Termination Briefing.

Information Contained in Briefings

These briefings incorporate the following information:

- applicable Safeguards and Security (S&S) directives and procedures,
- site-specific (and/or operations-specific) Safeguards and Security policies, procedures, and requirements,
- recent espionage cases,

- approaches and recruitment techniques employed by foreign intelligence services, Safeguards and Security incidents and considerations
- Safeguards and Security threats and vulnerabilities.

New Employees Receive an Initial Briefing

The Initial Briefing is provided to individuals approved for unescorted access to security areas and is included as a module in new employee training. Briefing topics may include:

- an overview of Safeguards and Security disciplines, such as personnel security, information security, and physical security,
- local access control procedures and escort requirements,
- protection of property,
- prohibited articles, and
- reporting incidents of a Safeguards and Security concern.

Topics for Comprehensive Briefing

The Comprehensive Briefing is provided to individuals before being granted access to classified information or to special nuclear material (SNM). An employee receives a Comprehensive Briefing after their security clearance has been granted. A Comprehensive Briefing is provided before receiving a cleared security photo badge.

Comprehensive briefing topics could include:

- information security,
- physical security,
- personnel security,
- reporting/notification requirements,
- legal and administration sanctions imposed for incurring a security infraction or committing a violation, and
- general information concerning the protection of SNM.

Annual Reminders

The Annual Security Refresher Briefing is provided annually to cleared employees. The briefing reminds employees of their security responsibilities and outlines updated security policies.

Termination Briefing Describes Post-Job Responsibilities

The Termination Briefing is provided to individuals who are terminating their security clearance. The Termination Briefing is provided on the last day of employment, the last day an individual possesses a security clearance, or the day it becomes known that the individual no longer requires access to classified information or SNM, whichever is sooner. A

Termination Statement is provided to the employee when the cleared security badge is returned to the facility. This briefing clearly explains the person's status (uncleared) and the ongoing responsibility not to divulge important information and data.

HRP Applies to Certain Employees

The Human Reliability Program (HRP) is a continuous evaluation program for individuals who:

- have direct access to, protect, and transport Category I quantities of SNM,
- perform duties as reactor operators, or
- may cause an unacceptable risk to national security.

HRP Activities

Continuous evaluation is accomplished through initial assessment and recurring assessments consisting of supervisory reviews, medical assessments, management evaluation, and security determinations. The HRP also includes training for supervisors in how to recognize aberrant behavior. Aberrant behavior is defined as behavior that deviates from normal or typical behavior that is expected from an individual or behavior that is contrary to socially accepted behavior. HRPs provide for testing for controlled substances or the habitual use of alcohol, which may impair judgment, trustworthiness, and reliability.

The HRP requires an organization that makes this program mandatory for personnel in key positions. Persons in these positions must complete an initial certification and an annual recertification.

Medical Assessment

After the initial training has been completed, the applicant receives a HRP Medical Assessment. The applicant must sign a consent form for the HRP. A physician examines the applicant to ensure there are no concerns (such as substance abuse) that the person might not be trustworthy. This involves:

- a physical examination,
- a random drug screen, and
- a psychological assessment.

Polygraph Examination

The next step in initial certification may be a polygraph examination. The polygraph is limited to the topics of espionage, sabotage, terrorism, intentional unauthorized disclosure of classified information, intentional unauthorized foreign contacts, and deliberate damage or malicious misuse of the government or a defense system. Controls are in place to prevent unwarranted intrusion into the privacy of individuals. Questions will **not** be asked about an individual's thoughts or beliefs that concern conduct that has no counterintelligence implication, or no direct relevance to an investigation.

Substance Abuse Test

Applicants complete an initial substance abuse test for illegal drugs and alcohol.

Certification

Once a person passes these tests, they are enrolled in the Personnel Security Assurance Program (PSAP). In the U.S., these PSAP people have unique color-coded badges or badge holders so everyone in the facility will know that they require special observation.

Ongoing Tests and Oversight by a Supervisor

Annually, all HRP employees have a medical and psychological examination as described above. Random drug tests may occur during the year. A major feature of the HRP is that all supervisors are trained to observe aberrant behavior, and at any indication of the following action must be taken:

- suspicion of excessive alcohol or substance abuse on or off the job,
- psychological or physical disorders that impair performance of assigned duties,
- significant behavioral changes, moodiness, depression, or other evidence of loss of emotional control (i.e., crying bouts, uncontrollable anger),
- inability to deal with stress or the appearance of being under stress,
- hostility or aggression toward fellow workers or authority,
- evidence of a pattern of poor decision making or irresponsibility, or
- failure to follow direct orders or a violation of safety, security, or work procedures.

23.4.3 Minimize Opportunities for Malevolent Activities

Access Authorization

Access authorization is the process of determining eligibility for access. Access can be granted to sensitive information and facilities if the individual meets the requirements for obtaining a security clearance through pre-employment screening and background investigations.

Badges Provide Identification of the Person and Clearance Level

Once a person is cleared, they are issued a badge to identify them and their clearance status. These badges are appropriately colored and coded. They are used and accepted as evidence of an access authorization (or security clearance level). Some sites may require presentation of additional photo identification or further positive personnel identification.

Keep Badges Up to Date

Badges are to be worn conspicuously, photo side out, in a location above the waist and on the front of the body while at the facility. The badges must be maintained in good condition. If a significant change in appearance takes place, such as facial hair, new glasses, and so on, the individual must obtain a new badge with a new photograph. Guard force personnel are authorized to confiscate faded, worn, or damaged badges.

Keep Records of Badges and Maintain a Database

Badge inventories and records are maintained. Such records include, at a minimum: description and serial number of item issued, date of issuance, name, organization, and date of destruction. A record of missing badges and credentials is also maintained. Personnel and/or systems controlling access to security areas are given current information regarding missing badges in order to prevent their misuse. The loss of badges must be reported immediately.

Escorting Visitors

Visitor control procedures ensure that only appropriately cleared individuals gain access to security areas and facilities. Unescorted access onto the site and into the facilities is granted to employees and contractor personnel who have an authorized photo badge. Unescorted access onto the site and into buildings may be granted to visitors or employees with a one-day pass or temporary badge. Visitors must be escorted upon entry to sensitive areas.

Responsibilities of Escorts

Escorts must be knowledgeable of security plan requirements and they must:

- be familiar with areas the escorted person is to visit and also be aware of precautions necessary to prevent unauthorized access to classified matter or special nuclear material,
- not deviate from the exact route when routes are specified,
- not delegate responsibilities to another person unless prior arrangements have been made with appropriate personnel,
- discuss only authorized information,
- not admit visitors to any area or building unless such access is indicated on the visitor’s badge or authorized by appropriate security personnel,
- ensure that personnel being escorted are aware of all security rules and procedures,
- ensure that personnel being escorted remain within sight and normal voice communication at all times,
- maintain a knowledge of escort security plans,
- be thoroughly familiar with the security rules and procedures of the area in which they are performing escort duties,
- where required, properly sign in the persons being escorted before entering security areas, and
- notify security personnel when problems occur.

Responsibilities of Facility Personnel When Visitors Are Present

Persons assigned to the facility to be visited (and responsible for the visitor) must:

- ensure that the visitor has an authorized visitor's badge, where required,
- ensure that the visitor is escorted at all times during the visit while they are inside the facility, and
- ensure that the visitor is not allowed access to classified or sensitive information or equipment, unless the visitor is cleared to the appropriate level and has a "need to know" in the performance of their official duties.

Reduce Number of People with Access

In the design of the facility, special care is taken to reduce the opportunities that workers have for theft or sabotage. Insider direct access to sensitive equipment and nuclear materials must be limited to those who must have access to perform their jobs. Entry control systems provide the capability to restrict access to sensitive areas and materials to only those who have been previously authorized for such access. This approach reduces the number of insiders who can commit malevolent acts in these areas.

Material Consolidation

Material consolidation and inventory reduction can also assist in reducing the theft attempt possibilities of the insider. One measure is to place all SNM in central locations and keep on hand only the amount that is actually needed. The remainder is shipped to a centralized repository.

Strict Procedures

Automated systems require significant pre-planning to ensure that when people arrive at a location to do a critical job, they are scheduled to do the job and are the appropriate people to do it. Making and keeping accurate daily schedules and plans is a significant deterrent to an insider who might depend on confusion and mismanagement to mask his activities.

Deter Insiders with Fear of Being Caught

Although physical security measures are used to limit access and delay intruders, they can also provide deterrence if the insider believes there is a high probability of being caught due to the physical security measures in place. Physical security can include, but is not limited to, barriers, intrusion detection systems, contraband detection, access controls, surveillance, response, and contingency plans.

Compartmentalize the Facility to Prevent Access

To make an internal access control system work well, the facility must be compartmentalized to prevent access by people who are not authorized to handle SNM using the two-person rule. Often older facilities were designed with efficiency of operation in mind (open rooms with smooth flow of process material) and this makes physical security against the insider threat much more difficult. A facility should be segmented as much as possible. Then, access should be carefully controlled in each compartment of the facility to make sure that only the authorized people at the authorized time enter those areas and they do only the authorized activity. Having such careful control within a facility will minimize malevolent attempts because the risk of detection is too high and chance of escape with the material is too low for an insider to attempt a theft.

Closely Monitor Vital Equipment Operations

Knowledgeable oversight of the specific details associated with maintaining and calibrating sensitive equipment minimizes the opportunity for maintenance personnel to commit malevolent acts during the regular course of their duties.

Facility Design

The nuclear safety requirements and the subsequent design of facilities also provide additional measures that tend to preclude insider opportunities.

23.4.4 Detect, Delay and Respond to Malevolent Action

Two-Person Rule

The “Two-Person Rule” is used to minimize opportunities for malevolence and detect such if it occurs. In places where one person could easily have access to SNM or vital equipment, there is an enforceable administrative process to ensure that any person cannot be in that location or do that job without another person present. The two people must remain in full view of each other at all times and must be equally qualified so that each will be able to recognize if the other is performing an unauthorized activity. This process can be enforced manually by posting a guard at a door allowing entry only if the proper two people are present. Automated methods of enforcing this rule such as entry control systems can ensure automatically that the door to the area will not open unless the authenticated credentials of two qualified workers are presented.

Tracking Movements of Employees

Control of personnel in some very sensitive areas may be enhanced even further by sensors in rooms that can record the exact location of each badge in the room. There are technologies to ensure that a badge is actually attached to the person like a fiber optic link around the wrist or around the neck, and therefore the person’s location can be identified. The computer then is programmed with the places that each person can go and the distance that each can be apart and still be able to monitor the activity of the other. If any of the parameters are exceeded, an alarm is sounded and the guard force will investigate the infraction. The data from the location sensors and the data from the door sensors are kept in a secure database, and if unauthorized activity is suspected the tracking data can be reviewed to make a list of potential suspects.

Supervisors Watch

Supervisors are not only supposed to watch the employees for changes in their behavior, but supervisory review of all operations is essential to good protection against the insider threat. A supervisor knows who should be in what areas and how long they should be there, and if anything unusual is happening the supervisor should be able to identify the problem. This, of course, raises the issue of “who watches the supervisor?” because the supervisor could be the insider. Every supervisor has a supervisor and the chain of command watches the people under their control.

Contraband and SNM Detectors

Metal detectors and X-ray machines should be installed at the entrance to areas where insiders should not bring contraband (weapons, etc.).

At the exit from Material Access Areas, install a metal detector and an SNM detector through which all operators must pass. The SNM detector is usually a portal device that is set as sensitively as possible, given the background radiation of the area. Sometimes a timer is required to keep the employees standing in the counter until a statistically significant count is obtained and it is determined that the person is not carrying SNM. A guard force person is usually present to ensure that the rules of the exit portal are followed and to respond if a theft attempt is detected. A metal detector is used in conjunction with an SNM detector because the insider could carry the SNM in a shielded container. The metal detector would alarm if a shielded container were being carried out of the area.

Protect Alarm System from Tampering by Insiders

Other means employed within a facility to prevent theft attempts are supervision techniques of the physical protection signal wires to ensure that no insider can tamper with or deactivate the alarm system. All lines that transmit alarms and physical protection data are supervised either by using direct current (DC) line supervision or a more elaborate active interrogation system. If an insider attempts to deactivate the alarm system to either mask his activities or to assist an outsider to enter the facility without being detected, the supervisory systems would cause an alarm. Fiber optic transmission systems increase the difficulty of the adversary tampering with the signal lines without detection.

Self-Test Systems

Many of the sensors used to detect unauthorized insider activity inside the facility have a self-test feature. This enables the sensor to test its ability to detect from the sensor all the way to the alarm station, and any problems or inoperative equipment will be immediately identified. These self-tests are generally conducted automatically by the computer control system of the alarm system and can detect malevolent actions performed against the security system in preparation for a theft or sabotage attempt.

Material Control and Accounting

Another detection/protection measure is material control and accounting programs. These programs detect losses of material and provide an audit trail to detect the responsible parties.

Monitor Spare Parts

Finally, one area that should be monitored by the security personnel is the spare part inventory for the security and vital equipment. If an adversary were able to obtain unlimited access to a spare sensor or pump that would be used to replace another sensor or pump, then internal modifications could be made to allow the adversary undetected access if the spare part were used. The equipment that is critical to the operation of the security system and the spare parts must be protected from tampering by an insider.

23.4.5 Mitigate Consequences of Malevolent Acts

Emergency Response Plan – Theft

Material inventories are performed often and routinely to identify if any material is missing. If a missing amount is larger than the reasonably expected measurement error of the instruments, or if an item is discovered missing during a physical inventory of items, then an emergency response plan is put into action immediately. This pre-planned operation stops all egress from the facility and tries to locate the missing material if it has not left the site. Part of this plan involves coordination with outside forces to locate material that might have already been removed from the plant. This emergency response plan is practiced often and is kept up to date for two reasons:

1. to ensure that it will be effective if actually needed, and

2. to make it clear to all employees that if material is missing, a significant operation will ensue until the material is found.

Emergency Response Plan – Sabotage

All facilities are usually required by their licensing organization to have an emergency response plan for conditions that may result in off-site dispersal and contamination. These are in place to protect the populace in the event of an accident but are also very useful in the event of an insider-initiated sabotage incident. This pre-planned operation initiates events and actions within the operational system to minimize the effect of safety system compromise. Part of this plan includes coordination with outside emergency responders. This emergency response plan is practiced often and is kept up to date for two reasons:

1. to ensure that it will be effective if actually needed, and

2. to make it clear to all employees that there is significant capability to prevent and/or mitigate the consequences of a sabotage act.

Deter Insiders with Major Personal Consequences

It is also clear to the employees that prosecution after finding the stolen material or ascertaining who caused the incident will be swift and punishment will be sure. In the very few cases in the U.S. of nuclear material being stolen from a plant, the perpetrators were caught and sent to jail with much publicity. Sabotage has been more difficult to ascribe to specific individuals but can be done in many cases. The purpose of these actions is to ensure that no insider will attempt to steal the material or will attempt to sabotage the facility.

23.5 Facility-Specific Insider Analysis Methodology

Method to Analyze Effectiveness Against Insider Threat

The protection system to counter the insider threat must also be evaluated to determine the level of system effectiveness. The estimate of adversary sequence interruption (EASI) model and the systematic analysis of vulnerability to instruction (SAVI)-4 model analyze the outsider probability of interruption (P_I), but similar techniques are available to analyze the insider probability of detection.

Steps for Insider Analysis

The approach to the analysis of the effectiveness of the physical protection system against the insider uses worksheets to guide and document the evaluation. Examples of these work sheets are included in this material. There are six steps in the manual insider analysis and these steps follow the general DEPO process. The steps are:

1. Collect facility or transport information,

2. Identify targets of interest,

3. Define the facility-specific threat (insider groups),

3. Use the system approach for prevention and protection,

4. Evaluate the preventive and protective measures, and

5. Summarize target/threat results.

23.5.1 Collect Facility or Transport Information

Necessary Information

Information about the nuclear facility's layout, organization, operations and systems must be gathered in order to properly characterize the potential vulnerabilities of a facility. This includes the physical protection measures, operating conditions, safety systems, material control and accounting, radiation protection measures, emergency procedures and response. In addition, the organizational chart and personnel responsibilities, operational security awareness, process and procedures, and day-to-day execution of duties must be taken into account.

Information about transport must also be gathered. This includes the physical protection measures (e.g., tracking devices, personnel identity verification, written instructions, confidentiality, etc.), routes and schedules, communications, responsibility of those involved in transport, transportation unit and package characteristics, radiation protection and safety measures, emergency procedures during transport, and response plans.

Conditions Favorable for Insiders

Situations or activities favorable for an insider should be identified, such as:

- The conditions inside the facility or regarding the transport, including work force, labor issues, industrial relation policies, security culture and awareness, trustworthiness programs, previous workers, etc.

- The conditions outside the facility or regarding the environment of the transport routes, including the general attitude of the community, and whether the surrounding area is urban or rural. The presence of organized groups, such as any discontented or disgruntled faction of the population, should be reviewed and special attention should be paid to possible connections between this population and persons with experience in or access to the nuclear facility.

23.5.2 Identify Targets of Interest

Overview

Target identification is an evaluation of what to protect *a priori*, including nuclear material, areas, components, systems, and functions, without consideration of the difficulty of providing protection.

Consideration should be given to:

- safety analysis and the associated Vital Area Identification analysis as the starting point to identify potential sabotage targets, and
- categorization of nuclear material as it applies to the physical protection of nuclear material (INFCIRC/225/Rev 4.) to identify unauthorized removal targets.

The identified targets should be ranked based on the gravity of consequences. Since the objectives of either an unauthorized removal of nuclear material or a sabotage of a nuclear facility are of different natures, the protection goals are also different. Although a specific target may be subject to both unauthorized removal and sabotage, the consequences of these two events may be significantly different. Therefore, a ranking for all unauthorized removal targets should be generated, as well as a separate ranking for all sabotage targets. A unique ranking for both unauthorized removal and sabotage targets together is not generally feasible. This ranking will provide basis for implementing graded preventive and protective measures.

Sabotage Targets

Identifying sabotage targets at a facility begins by using safety analyses to identify potential accident sequences, which, if they occurred, would have significant radiological consequences for workers, the public, or the environment. An accident sequence is a series of events resulting from one or more initiating events (human error or the failure of one or more components or functions) that put the facility into a degraded situation despite its installed engineered safety systems and mitigation devices. However, sabotage is not considered in a safety scenario and therefore some other maliciously initiated events may also lead to significant radiological consequences. For example, in some cases the simultaneous failure of the redundant equipment of a safety-related system, such as the pumps of an emergency cooling system, is not considered probable in the safety analysis, yet this failure can credibly be caused by an act of sabotage and can lead to an act with radiological consequences. Components, systems, or functions that could lead to a degraded situation if they were lost or caused to fail by a malicious action must be identified.

The levels of unacceptable radiological consequences are established by the State or the competent authority mainly from the results of safety analysis studies. These consequence levels may vary from State to State. It is desirable that the consequence levels used for malicious incidents consider those taken from the safety criteria. But levels of unacceptable consequences for malicious acts could differ from those considered in the facility safety analysis and may need to be graded in levels below or above those of the safety analysis.

This approach enables the identification of the most sensitive elements in the facility (components, systems, or functions) and their locations, and suggests ranking the targets in categories according to sensitivity. Figure 23-3 illustrates the identification of vital area sabotage targets. Figure 23-4 illustrates the identification of unauthorized removal targets.

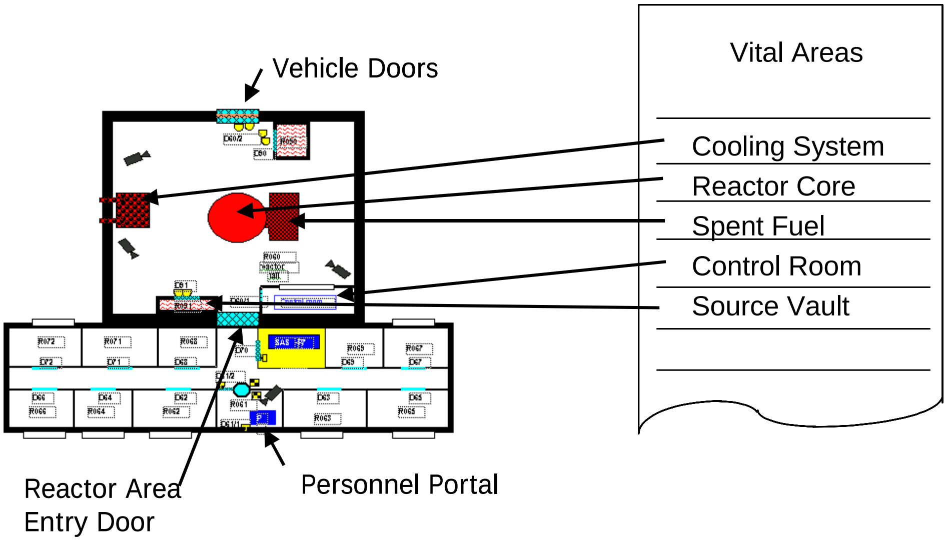


Figure 23-3. Vital area sabotage target identification.

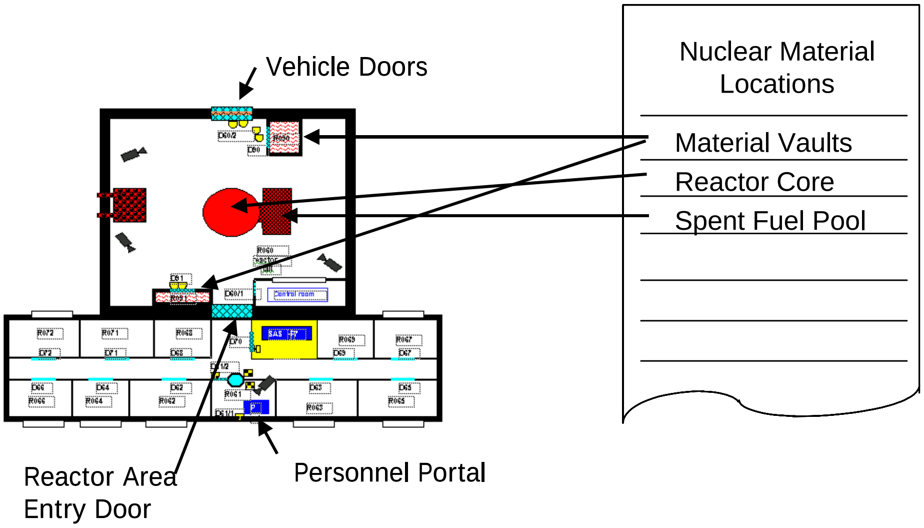


Figure 23-4. Unauthorized removal target identification.

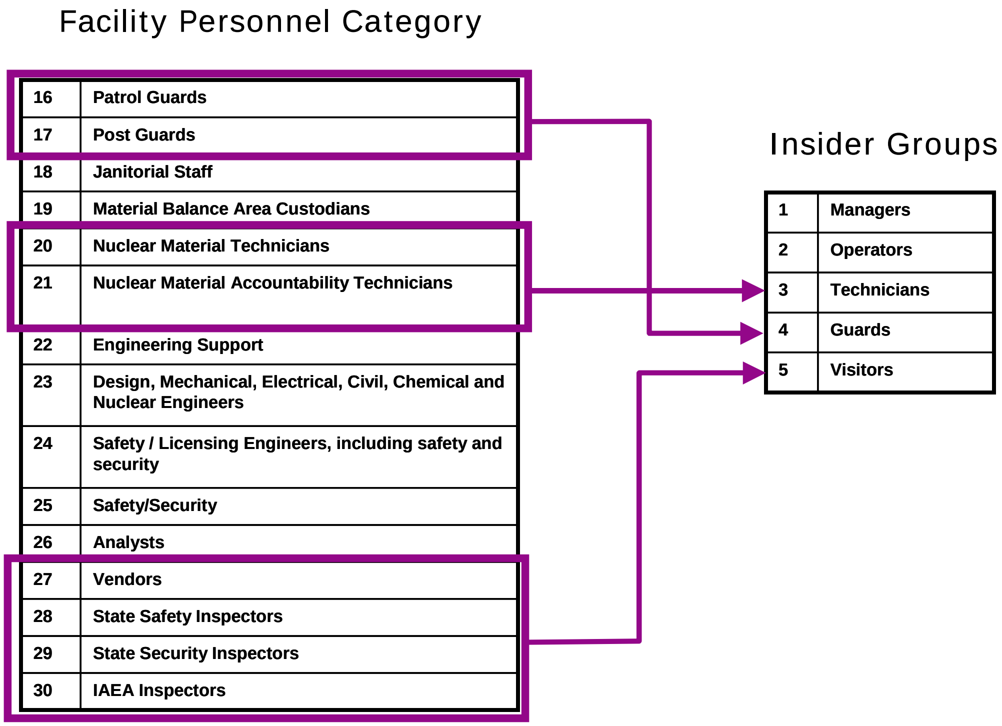
23.5.3 Define the Facility-Specific Threat

Facility-Specific Insider Groups

The State Design Basis Threat (DBT) is the starting point for facility-specific insider definition. The State DBT for insiders may or may not be detailed. Information for a facility or transport should be collected to describe every individual employee or type of potential insider based on levels of access, authority over others, knowledge of the facility operations and other general capabilities that support opportunity for malevolence. Organization charts and job descriptions should be used to determine the levels of access, authority, and knowledge possessed by those engaged in activities at the facility or in the transport. One-on-one discussions and interviews should be conducted with personnel working at the facility or transport to confirm or better understand the levels of access, authority, and knowledge they have.

Other facility or transport characteristics affecting the insider threat attributes should be collected, such as personnel flow and access control, facility state (normal operation, shutdown, maintenance duty, etc.), operational processes, authority structure, general job categories, physical protection features, information characterization, safety and/or radiation protection requirements, and accountancy and control systems for nuclear material.

In addition to potential insiders identified through their authorized access, specific consideration should be given to people with no access to a facility but with sufficient knowledge and/or authority to conduct a malicious act. This large list of potential insiders may be impractical. Since many types of potential insiders may have similar or identical attributes, insider types should be grouped. The grouping should then result in a concise, credible but comprehensive list of insider groups. Figure 23-5 illustrates how the complete list of potential insiders for a facility may be grouped.



Facility Personnel Category

16	Patrol Guards
17	Post Guards
18	Janitorial Staff
19	Material Balance Area Custodians
20	Nuclear Material Technicians
21	Nuclear Material Accountability Technicians
22	Engineering Support
23	Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers
24	Safety / Licensing Engineers, including safety and security
25	Safety/Security
26	Analysts
27	Vendors
28	State Safety Inspectors
29	State Security Inspectors
30	IAEA Inspectors

Insider Groups

1	Managers
2	Operators
3	Technicians
4	Guards
5	Visitors

Figure 23-5. Potential insider groups.

List Attributes

For each of the defined insider groups, characterize their attributes. List the keys that they have, the special privileges that they have, the special knowledge that they have, and the target areas where they have routine access. Continue to list every attribute that might have a bearing on the effectiveness of the security system to counter them as an adversary. Figure 23-6 lists some attributes to consider during the grouping process.

Access	Authority	Knowledge
Limited Areas	Supervisory	Procedures
Protected areas	Supervisory over guards	Processes
Vital areas	Personal vehicle	Locations
Nuclear materials	Exempt searches	Site details
Central alarm station	Exempt metal detector	Physical protection system
Alarms	Exempt nuclear material detector	Frequency of events
Keys	Authorize nuclear material transfers	Potential vulnerabilities
Badging	Verify nuclear material transfers	Tools, equipment
Information management of access system	Verify inventory	Procedure violations
Nuclear material records	Assess alarms	
Nuclear material forms	Issue badges	
Site vehicles	Issue codes	
Tools	Prepare access lists	
Controlled Information	Equipment maintenance	

Figure 23-6. Insider attributes.

23.5.4 Use System Approach for Prevention and Protection

Analysis Process

Preventive measures effectiveness is difficult, if not impossible, to quantify. However, these measures are reasonable and prudent precautions even if their effects cannot be quantified. A systematic review should be performed to indicate which of these measures are in place and properly applied.

The analysis process emphasis is on assessing the effectiveness of the protective measures to counter a malicious act. The approach involves developing credible insider scenarios, including collusion scenarios as appropriate, and then evaluating the protection system effectiveness against them.

The development of credible scenarios consists of identifying the combination of events necessary to accomplish the malicious act. For sabotage, we are concerned with the actions that must be accomplished to initiate a sequence leading to unacceptable radiological consequences. Sabotage scenarios should include both single and multiple target attacks. For unauthorized removal of nuclear material, actions that must be successively accomplished to remove nuclear material from the facility should be identified. Unauthorized removal scenarios should include situations in which the insider leaves the facility directly with the stolen nuclear material or hides this material on site, taking it out later under more favorable circumstances. Both protracted and abrupt theft should be considered.

Action Sequences

Around each target there are a series of protection layers. These are the same layers identified in the development of an adversary sequence diagram during the outsider analysis process. Within each protection layer, there are path elements that the insider might use to move from one area to another. Each path element should have some protection measures to defend against the insider. The development of an insider action sequence is similar to the development of an outsider path. The difference, however, lies in the fact that an insider may attack more than one target to accomplish his goal, and he may bypass many, if not all, of the protection measures. An example will be used here to illustrate the process. The target will be reactor sabotage from the control room. The general action sequence is:

1. Enter the protected area

2. Enter the control room

3. Sabotage the reactor from the control room

    3.1 Trip circuits
    3.2 Disable pumps
    3.3 Open coolant valves

For the first two steps in the sequence, the insider has some path options. To minimize detection in Step 3, the insider has "action" options, such as covertly disabling alarms or defeating closed-circuit television (CCTV) and personnel surveillance, rather than path options. Figure 23-7 illustrates this case.

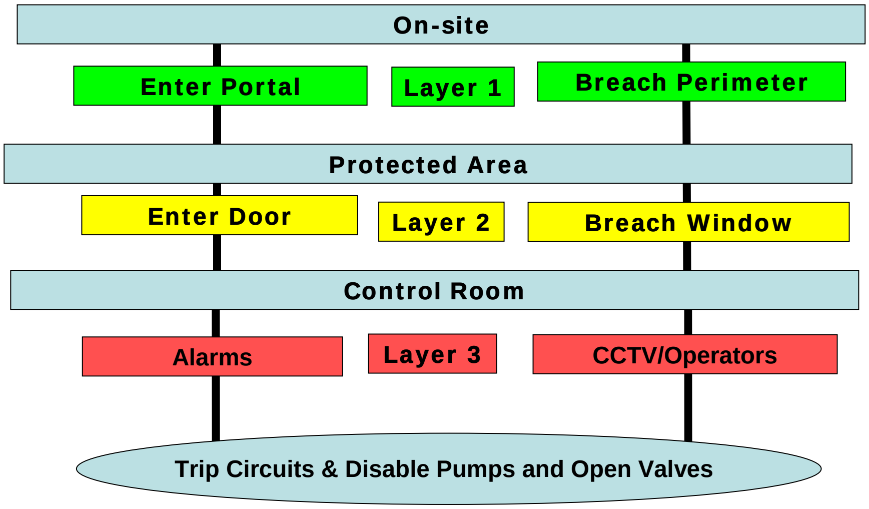


Figure 23-7. Action sequence options.

Protection Measures

The measures used to detect, delay, and respond to malicious acts can be quantitatively analyzed. Likelihood of detection and the timeliness of response are often quantifiable and thus provide a basis for effectiveness analysis. These measures should be identified on the action sequence diagram and listed in a table for evaluation against insider defeat strategies.

Defeat Strategies and Protection Measure Effectiveness

Defeat strategies are developed by considering insider access, authority, and knowledge to overcome the detection, delay, and response features. By examining protection elements characteristics, insider attributes, and potential insider defeat strategies for a required sequence of insider actions, credible insider defeat strategy options can be developed. It should be noted that paths for contraband material into a facility or unauthorized removal of nuclear material from a facility may not be the same as the paths used by the insider himself.

The effectiveness of the specific protection element features against the different potential insider defeat strategies should be assessed quantitatively, as illustrated in Figure 23-8, for each insider group.

Insider Action	Protection measure	Insider Strategy	P_D	Delay
Layer 1	Portal	Normal Entry	0.0	120 sec
	Perimeter	Breach	0.5	300 sec
Layer 2	Door	Normal Entry	0.0	60 sec
		Breach	0.9	300 sec
		Deceit access	0.7	180 sec
	Window	Breach	0.9	90 sec
Layer 3	Alarms	Disable	0.7	2700 sec
		Act surprised	0.9	105 sec
	CCTV/Operators	Disable/kill	0.1	225 sec
		Act surprised	0.9	105 sec

Figure 23-8. Defeat strategies and protection measure effectiveness – "operator" insider attempting control room sabotage.

Credible Scenario Development

The development of credible scenarios consists of identifying the combination of defeat strategies and protection elements with the highest probability of success for the insider to accomplish the malicious act. This is accomplished by superimposing the information from the defeat strategy/protection measures effectiveness table to the action sequence diagram, and then selecting the most advantageous action sequence for the insider. The paths, the sequence of actions along the path, the protective elements encountered, and the optimum defeat strategies are now all taken into consideration. An example is shown in Figure 23-9. Detection probabilities for the optimum defeat strategy for a specific insider are listed in blue at the lower left of the protection element or act. Delay values are listed in red at the lower right of each element. These values are derived from appropriate strategy and effectiveness tables for specific insider groups.

In some cases, the required actions for completion of the malicious act can be performed over an extended period, and may not follow a specific sequence, so the concept of a continuous path may not always be relevant.

For comprehensive insider analyses, pairing all identified targets and all defined insider groups should be considered.

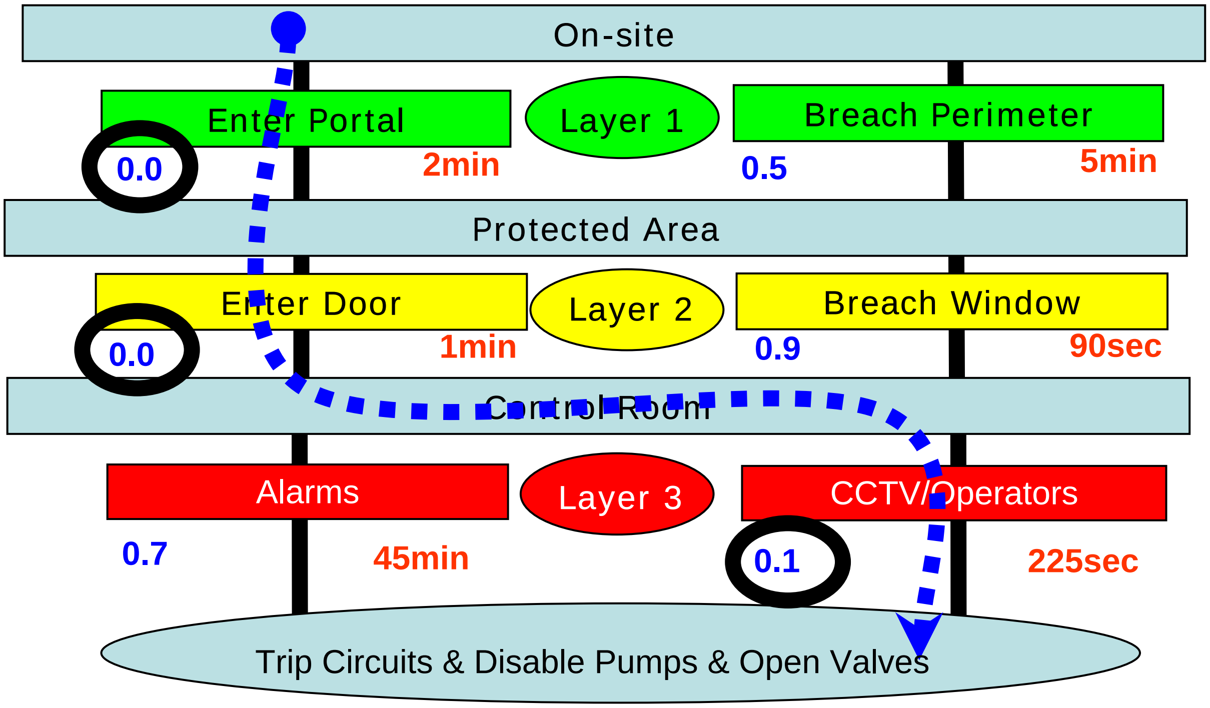


Figure 23-9. Optimum insider scenario.

Incorporate Response and Mitigation

The final step in the analysis is to make a judgment on the effectiveness of the response forces to neutralize a detected adversary. In a theft scenario, the adversary is moving outwards and the security response force is generally moving inwards. Since the response force knows where to go and what to do to contain the adversary, the probability is high that the response force will be able to neutralize the insider. Often the effectiveness of the response force is determined to be 1.00 and therefore the P_D obtained from this analysis is the system effectiveness.

For the case of sabotage, the security response force may not be able to reach a denial position or even to interrupt the insider before completion of the sabotage act. In this event, safety operations may be initiated to mitigate the consequences of the sabotage. This should always be included in the insider analysis.

23.5.5 Evaluate and Summarize Results

Combining Results for Protection System Effectiveness

Once detailed insider scenarios have been developed, the effectiveness evaluation is completed by considering the accumulated detection, assessment, and delay, and by overlaying the response and mitigation on the insider scenarios. The response effectiveness considers both the effectiveness of interrupting and neutralizing the insider, and the effectiveness of preventing or mitigating the consequences. Insider efforts to reduce response effectiveness should be considered.

The evaluation process should be repeated for every credible scenario for all insider groups and target combinations. The protective measures effectiveness should consider the results of all the evaluations above. An example table showing summarized results for five defined insider groups attempting control room sabotage is shown in Figure 23-10.

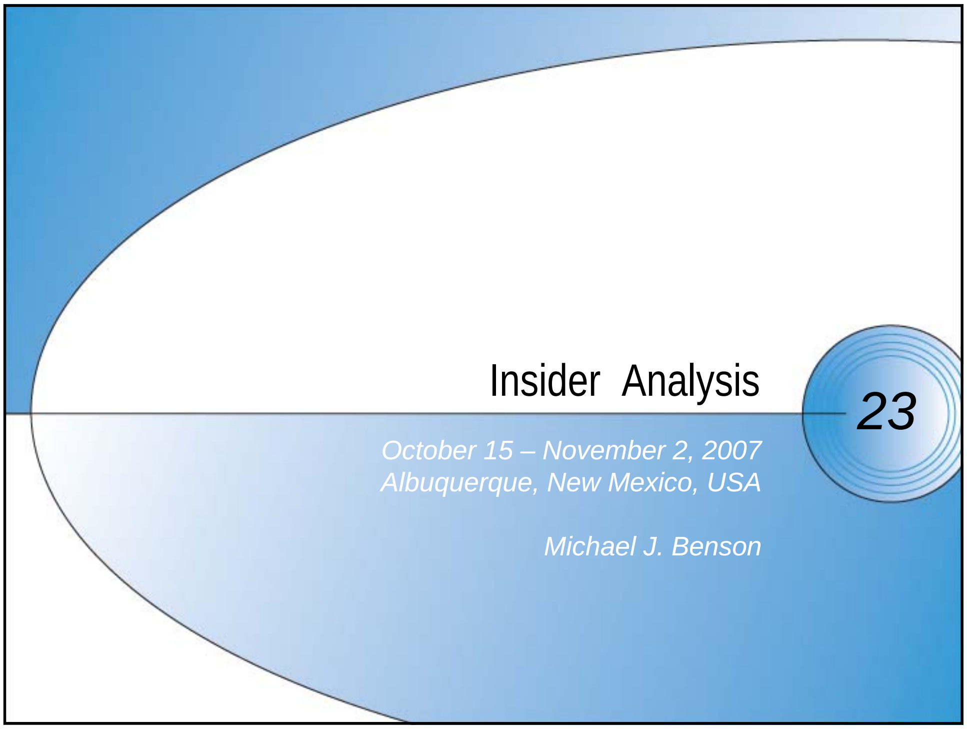
Insider	Layer 1	Layer 2	Layer 3	Combined Pd
Manager	0.0	0.1	0.9	0.91
Operator	0.0	0.0	0.1	0.10
Technician	0.0	0.0	0.5	0.50
Guard	0.0	0.9	0.1	0.91
Visitor	0.5	0.9	0.9	0.995

Figure 23-10. System effectiveness against control room sabotage.

23.6 Summary

Use a Variety of Measures to Counter the Insider Threat

The insider is considered to be one of the greatest threats that a safeguards and security system will encounter because the insider has access, authority, and special knowledge. Therefore, it is imperative that effective measures be taken to prevent insider incidents. A combination of preventive and protective measures offers the best solution to mitigating the insider threat. These include an employee screening process, security awareness education, physical protection systems, and policies and procedures ensuring appropriate handling and controls of attractive target materials.

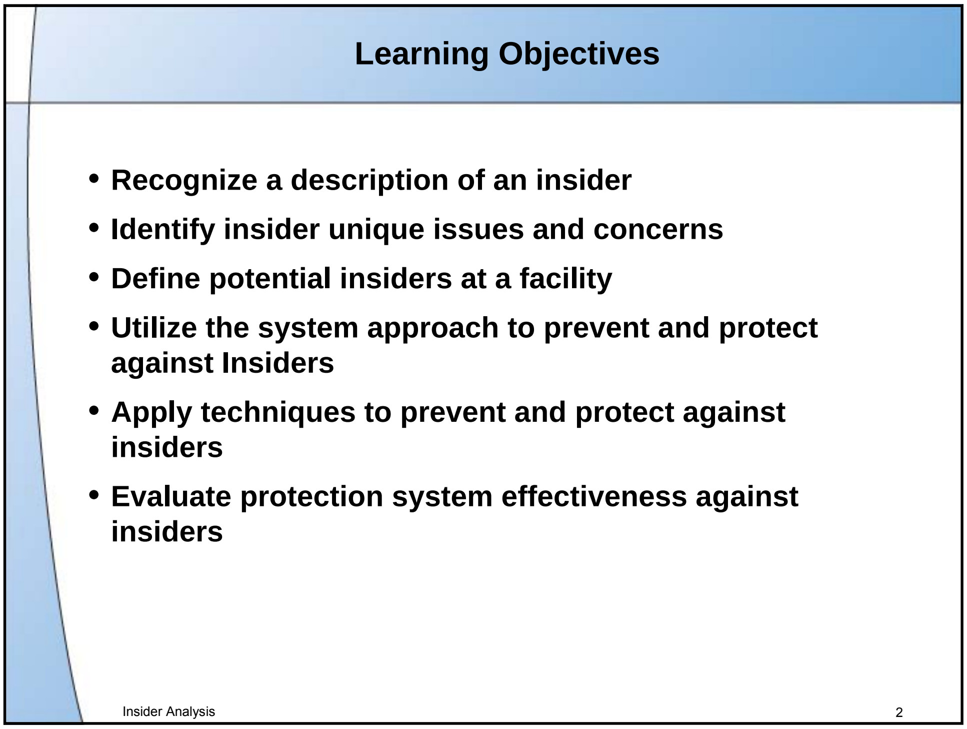


Insider Analysis

23

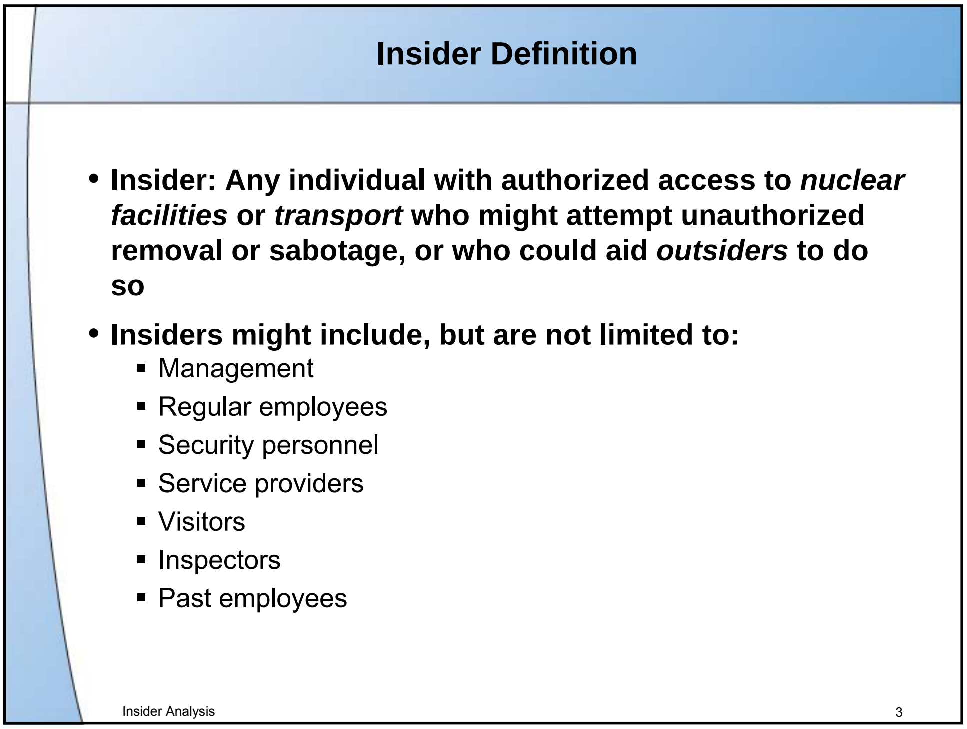
October 15 – November 2, 2007
Albuquerque, New Mexico, USA

Michael J. Benson



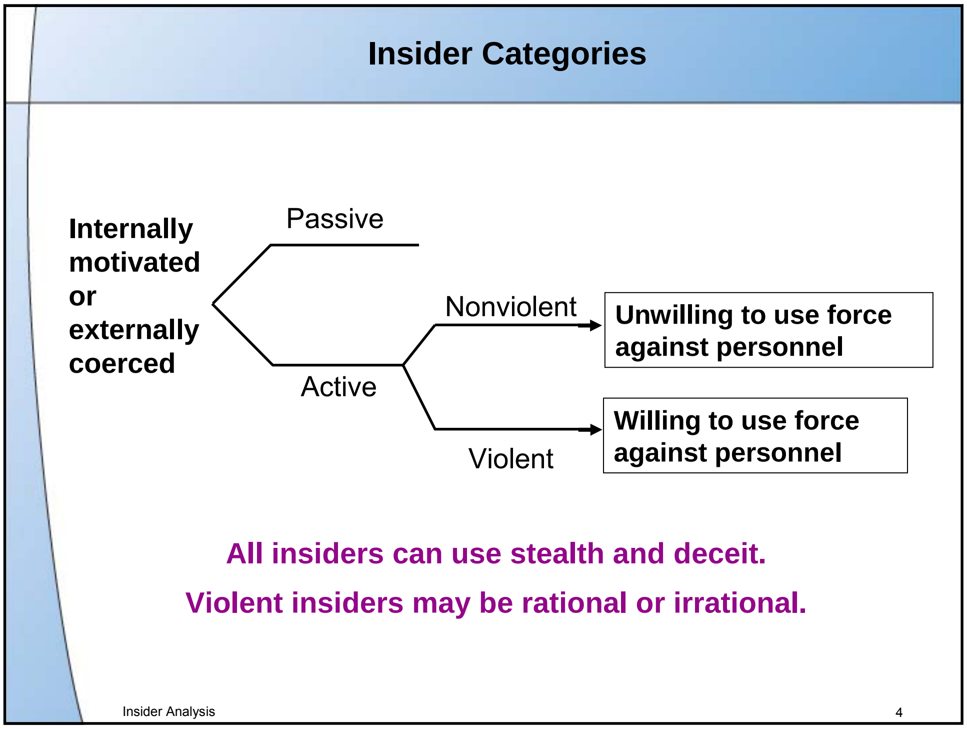
Learning Objectives

- **Recognize a description of an insider**
- **Identify insider unique issues and concerns**
- **Define potential insiders at a facility**
- **Utilize the system approach to prevent and protect against Insiders**
- **Apply techniques to prevent and protect against insiders**
- **Evaluate protection system effectiveness against insiders**



Insider Definition

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



Insider Categories

Internally motivated or externally coerced

Passive

Active

Nonviolent

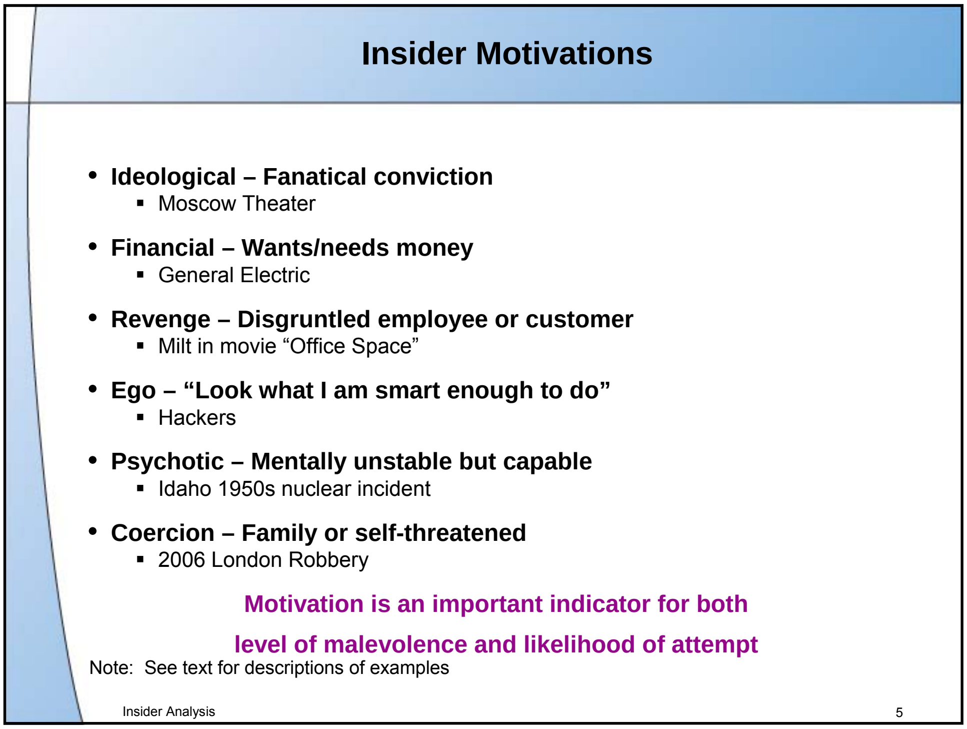
Unwilling to use force against personnel

Violent

Willing to use force against personnel

All insiders can use stealth and deceit.

Violent insiders may be rational or irrational.



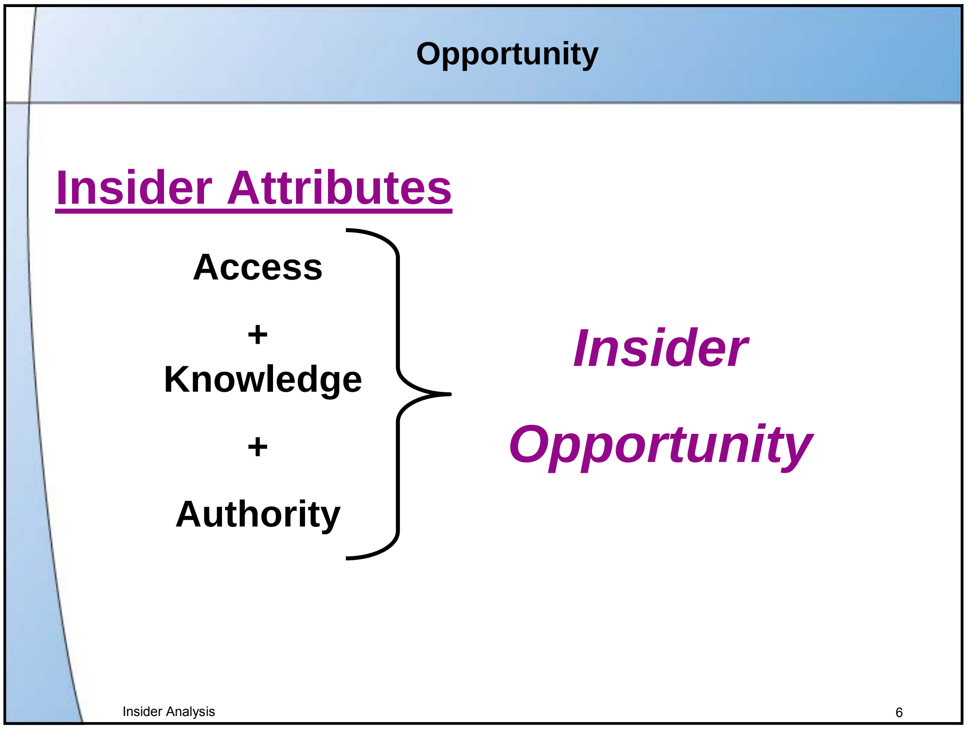
Insider Motivations

- **Ideological – Fanatical conviction**
  - Moscow Theater
- **Financial – Wants/needs money**
  - General Electric
- **Revenge – Disgruntled employee or customer**
  - Milt in movie “Office Space”
- **Ego – “Look what I am smart enough to do”**
  - Hackers
- **Psychotic – Mentally unstable but capable**
  - Idaho 1950s nuclear incident
- **Coercion – Family or self-threatened**
  - 2006 London Robbery

Motivation is an important indicator for both

level of malevolence and likelihood of attempt

Note: See text for descriptions of examples



Opportunity

Insider Attributes

Access

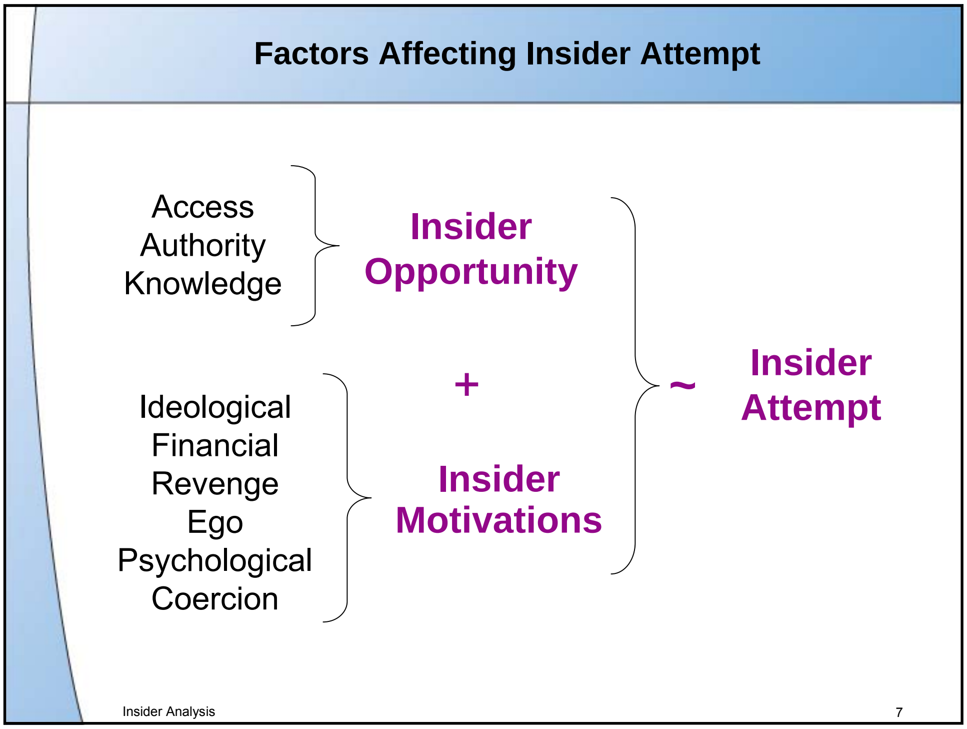
+

Knowledge

+

Authority

Insider Opportunity



Factors Affecting Insider Attempt

Access
Authority
Knowledge

Insider Opportunity

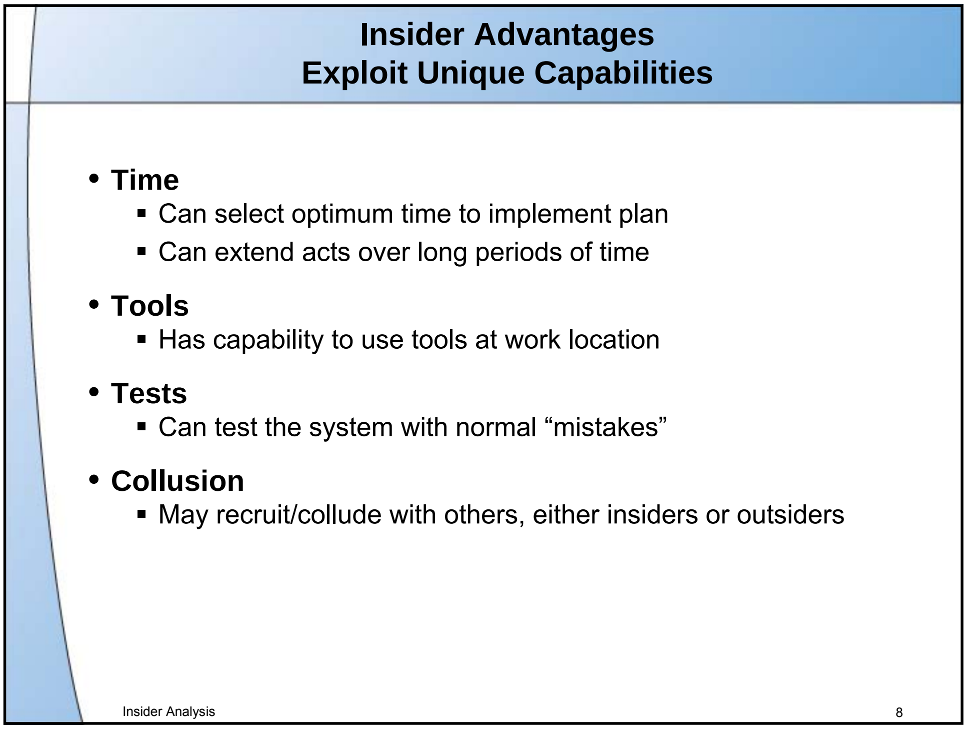
+

Ideological
Financial
Revenge
Ego
Psychological
Coercion

Insider Motivations

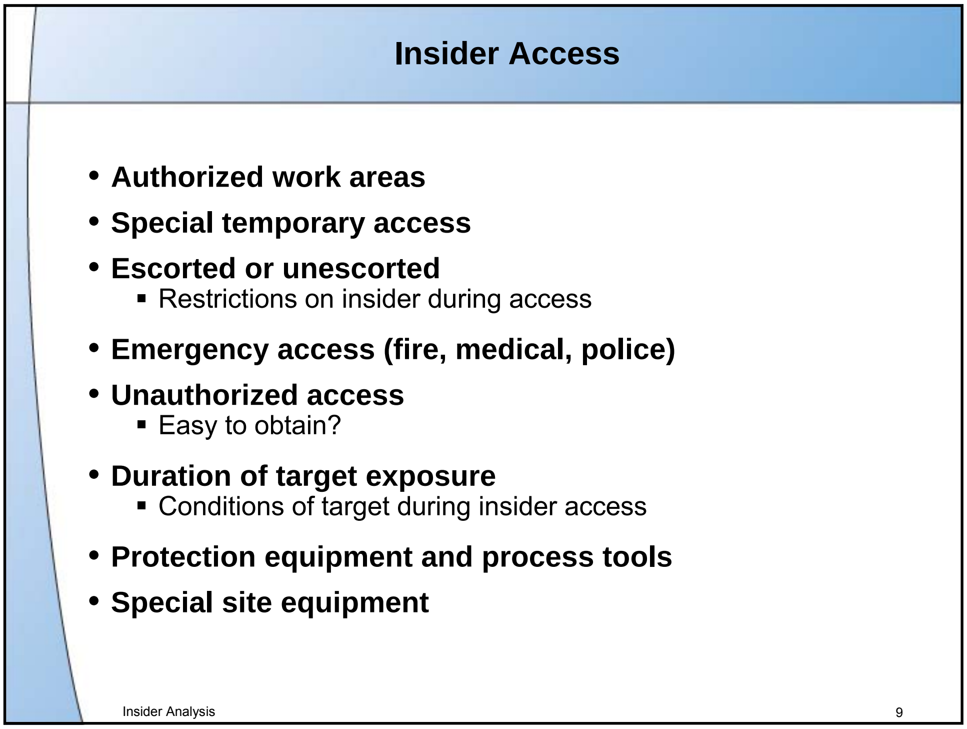
~

Insider Attempt



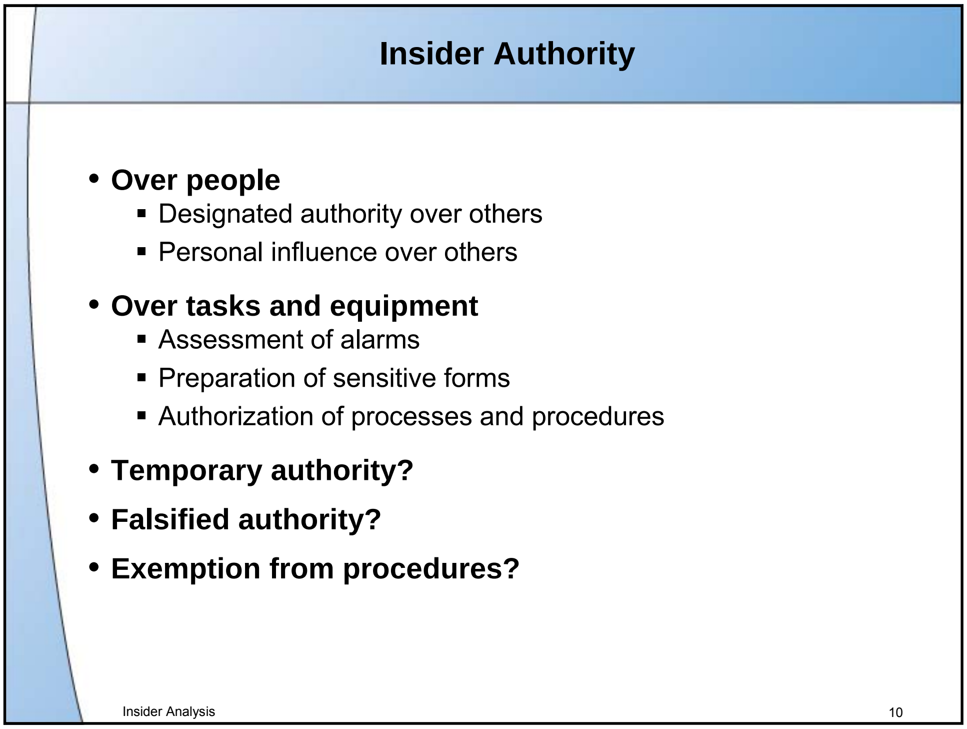
Insider Advantages
Exploit Unique Capabilities

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



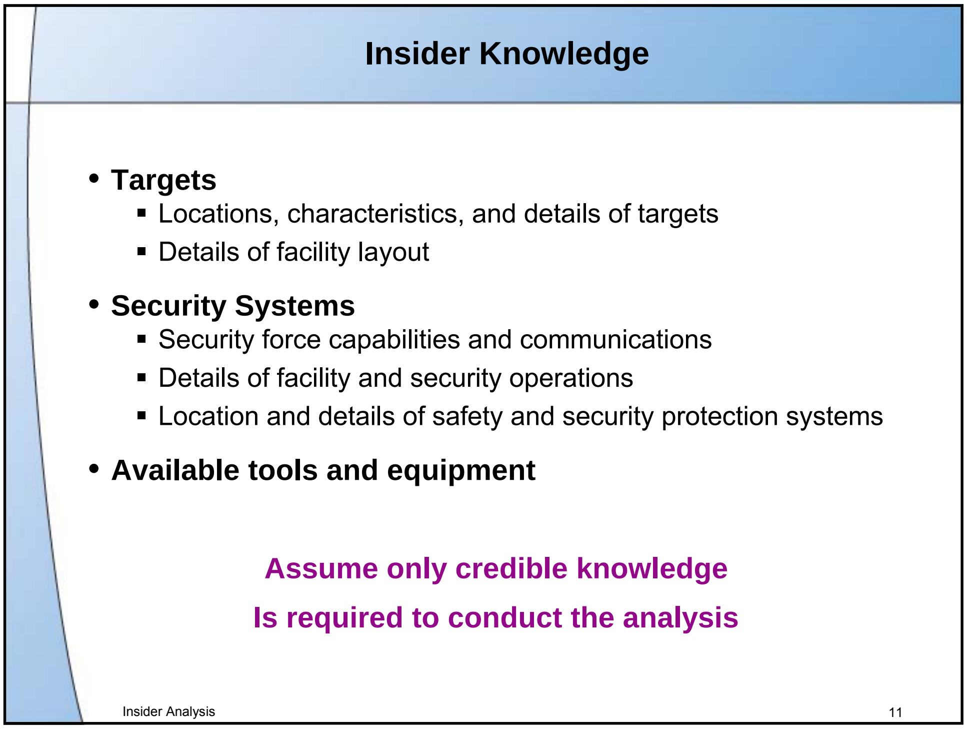
Insider Access

- **Authorized work areas**
- **Special temporary access**
- **Escorted or unescorted**
  - Restrictions on insider during access
- **Emergency access (fire, medical, police)**
- **Unauthorized access**
  - Easy to obtain?
- **Duration of target exposure**
  - Conditions of target during insider access
- **Protection equipment and process tools**
- **Special site equipment**



Insider Authority

- **Over people**
  - Designated authority over others
  - Personal influence over others
- **Over tasks and equipment**
  - Assessment of alarms
  - Preparation of sensitive forms
  - Authorization of processes and procedures
- **Temporary authority?**
- **Falsified authority?**
- **Exemption from procedures?**

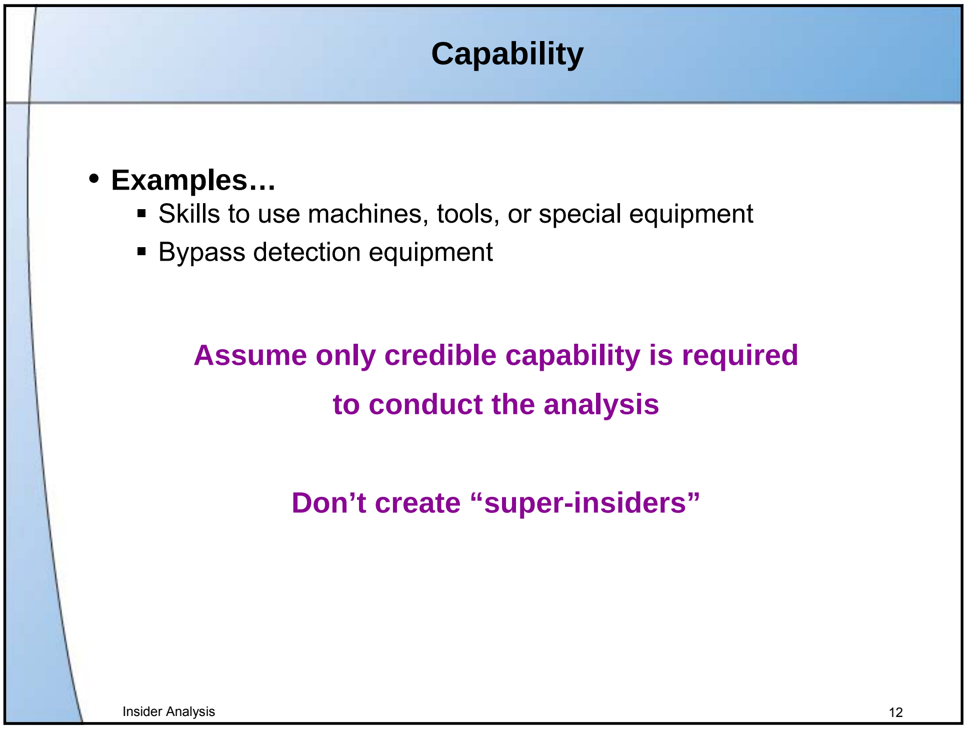


Insider Knowledge

- **Targets**
  - Locations, characteristics, and details of targets
  - Details of facility layout
- **Security Systems**
  - Security force capabilities and communications
  - Details of facility and security operations
  - Location and details of safety and security protection systems
- **Available tools and equipment**

Assume only credible knowledge

Is required to conduct the analysis



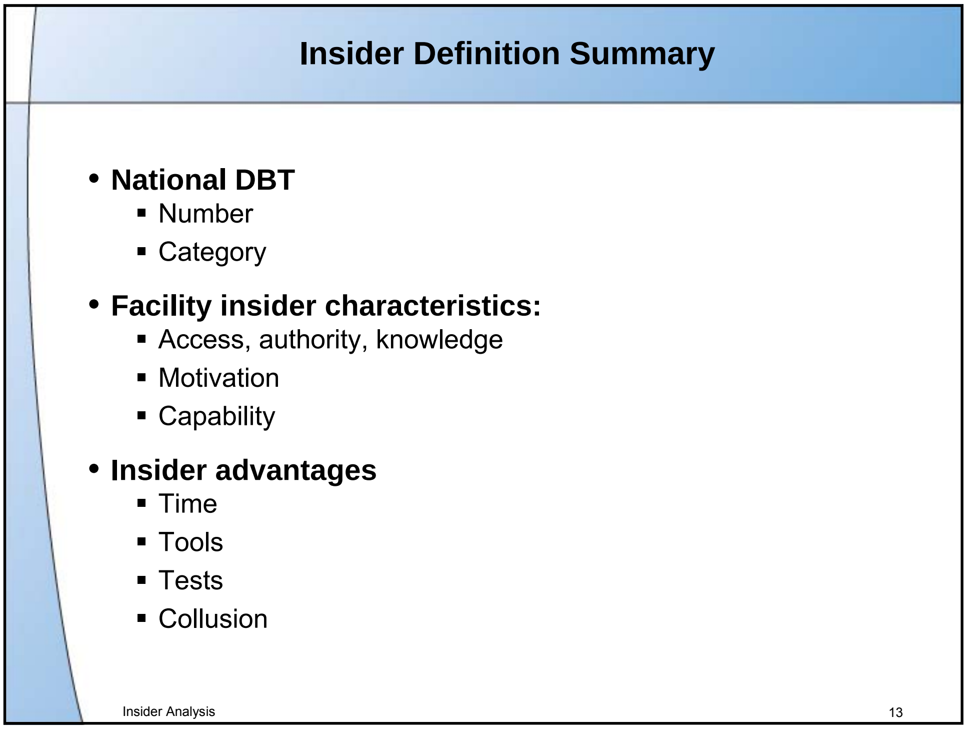
Capability

- **Examples…**
  - Skills to use machines, tools, or special equipment
  - Bypass detection equipment

Assume only credible capability is required

to conduct the analysis

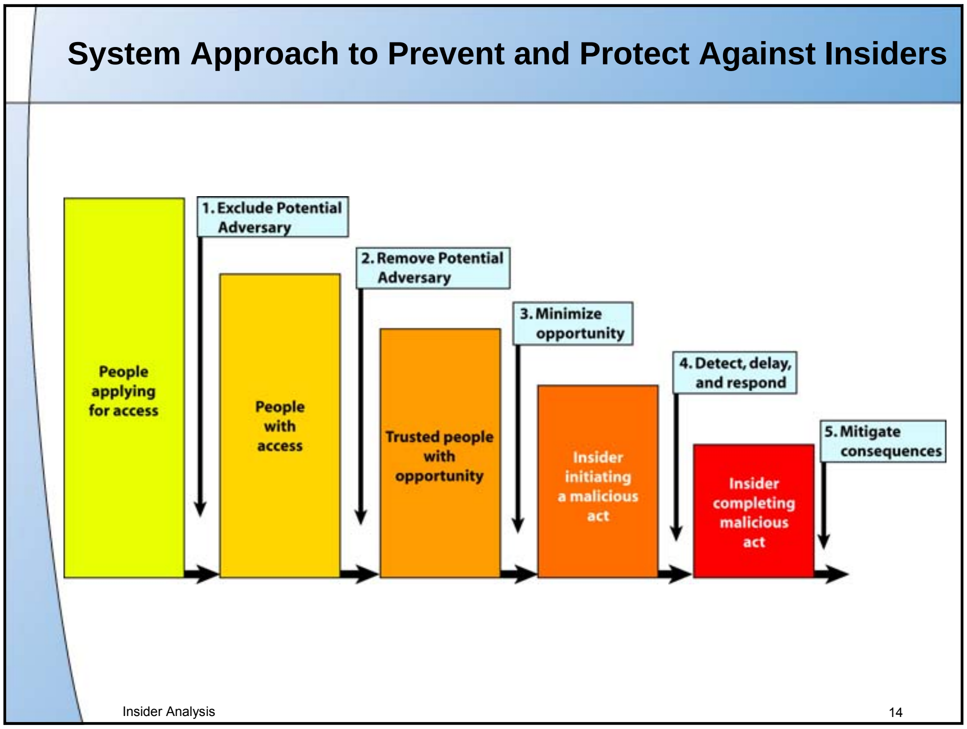
Don’t create “super-insiders”



Insider Definition Summary

- **National DBT**
  - Number
  - Category
- **Facility insider characteristics:**
  - Access, authority, knowledge
  - Motivation
  - Capability
- **Insider advantages**
  - Time
  - Tools
  - Tests
  - Collusion

Insider Analysis 13



System Approach to Prevent and Protect Against Insiders

People applying for access

1. Exclude Potential Adversary

People with access

2. Remove Potential Adversary

Trusted people with opportunity

3. Minimize opportunity

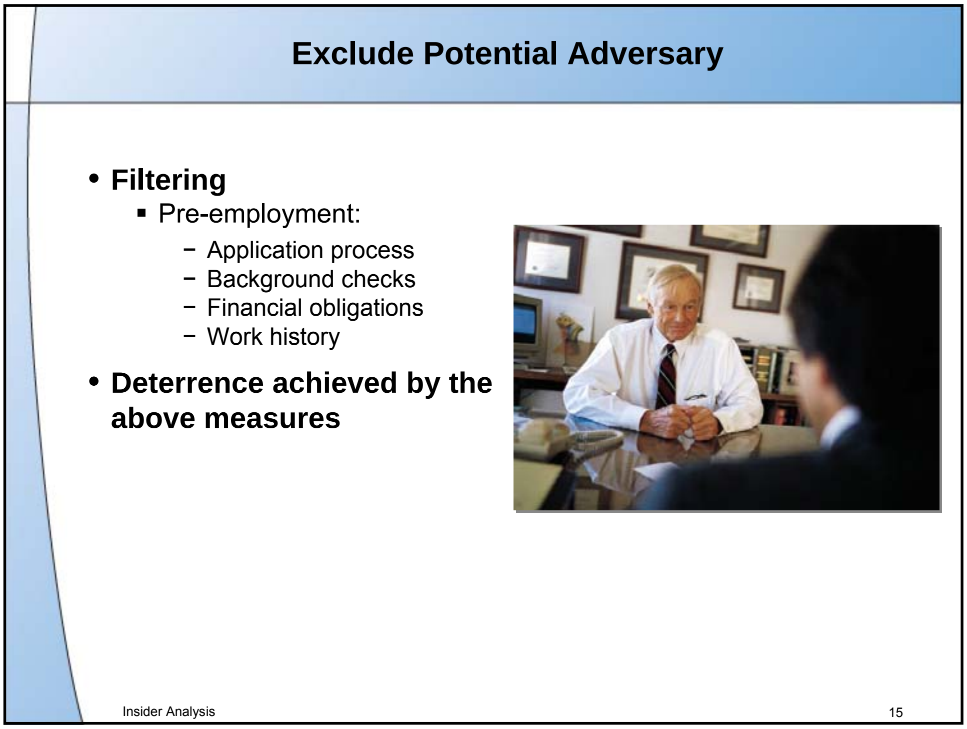
Insider initiating a malicious act

4. Detect, delay, and respond

Insider completing malicious act

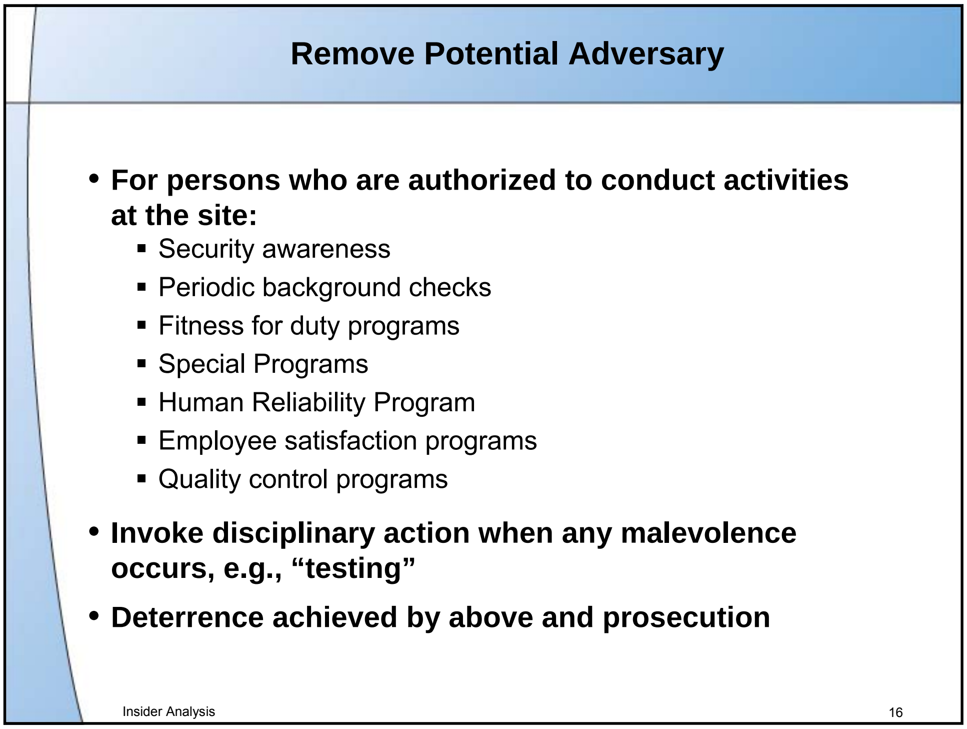
5. Mitigate consequences

Insider Analysis 14



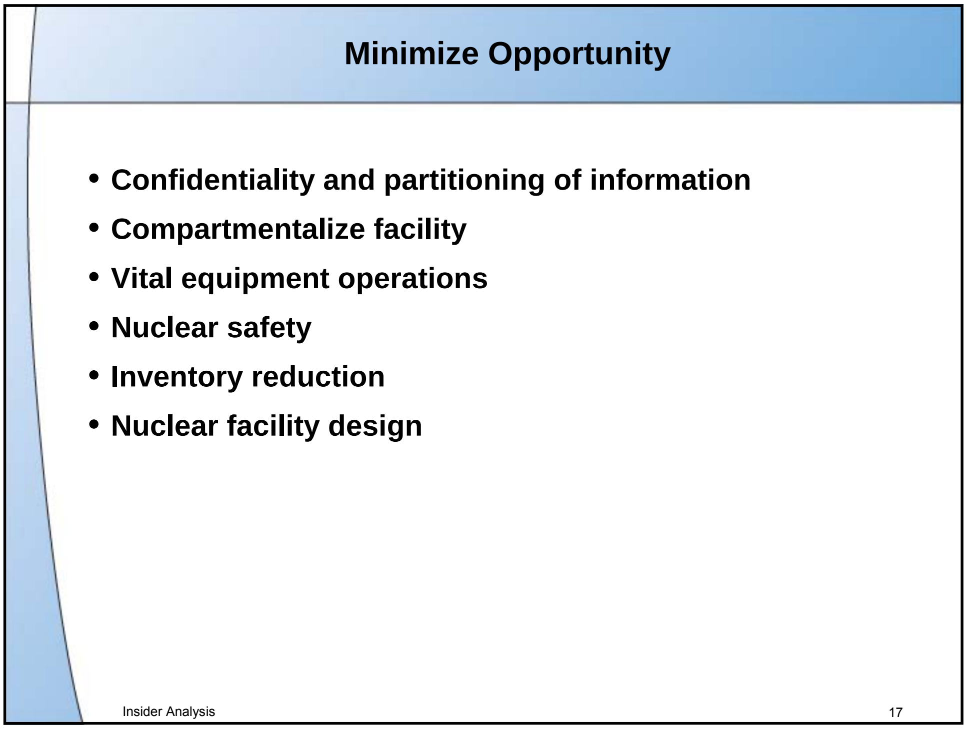
Exclude Potential Adversary

- **Filtering**
  - Pre-employment:
    - Application process
    - Background checks
    - Financial obligations
    - Work history
- **Deterrence achieved by the above measures**



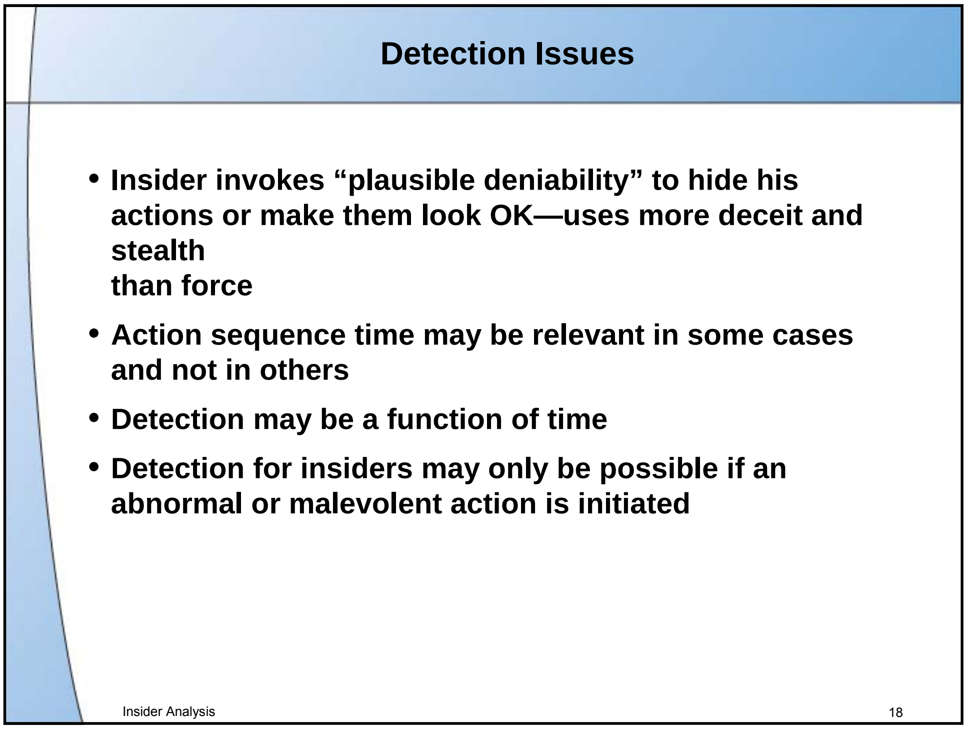
Remove Potential Adversary

- **For persons who are authorized to conduct activities at the site:**
  - Security awareness
  - Periodic background checks
  - Fitness for duty programs
  - Special Programs
  - Human Reliability Program
  - Employee satisfaction programs
  - Quality control programs
- **Invoke disciplinary action when any malevolence occurs, e.g., “testing”**
- **Deterrence achieved by above and prosecution**



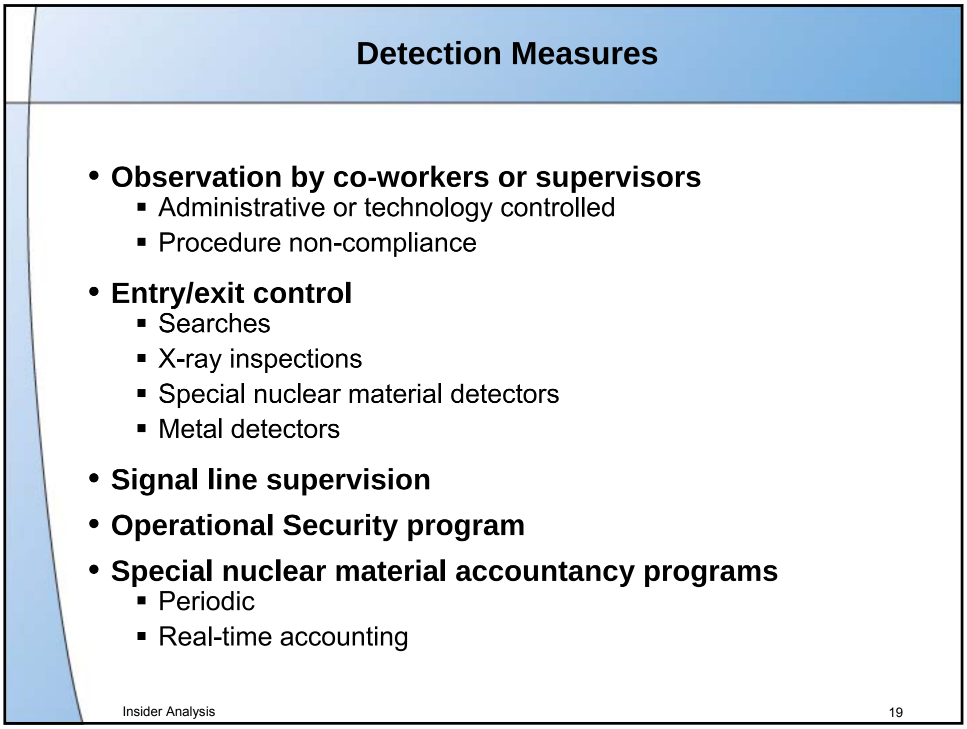
Minimize Opportunity

- Confidentiality and partitioning of information
- Compartmentalize facility
- Vital equipment operations
- Nuclear safety
- Inventory reduction
- Nuclear facility design



Detection Issues

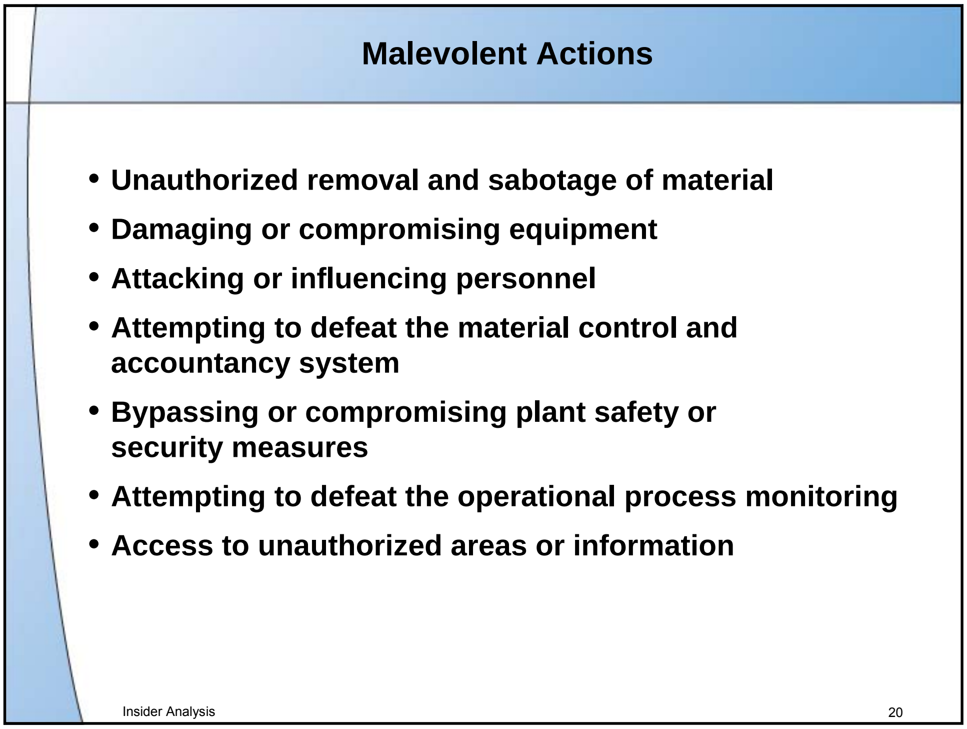
- Insider invokes “plausible deniability” to hide his actions or make them look OK—uses more deceit and stealth
  than force
- Action sequence time may be relevant in some cases and not in others
- Detection may be a function of time
- Detection for insiders may only be possible if an abnormal or malevolent action is initiated



Detection Measures

- **Observation by co-workers or supervisors**
  - Administrative or technology controlled
  - Procedure non-compliance
- **Entry/exit control**
  - Searches
  - X-ray inspections
  - Special nuclear material detectors
  - Metal detectors
- **Signal line supervision**
- **Operational Security program**
- **Special nuclear material accountancy programs**
  - Periodic
  - Real-time accounting

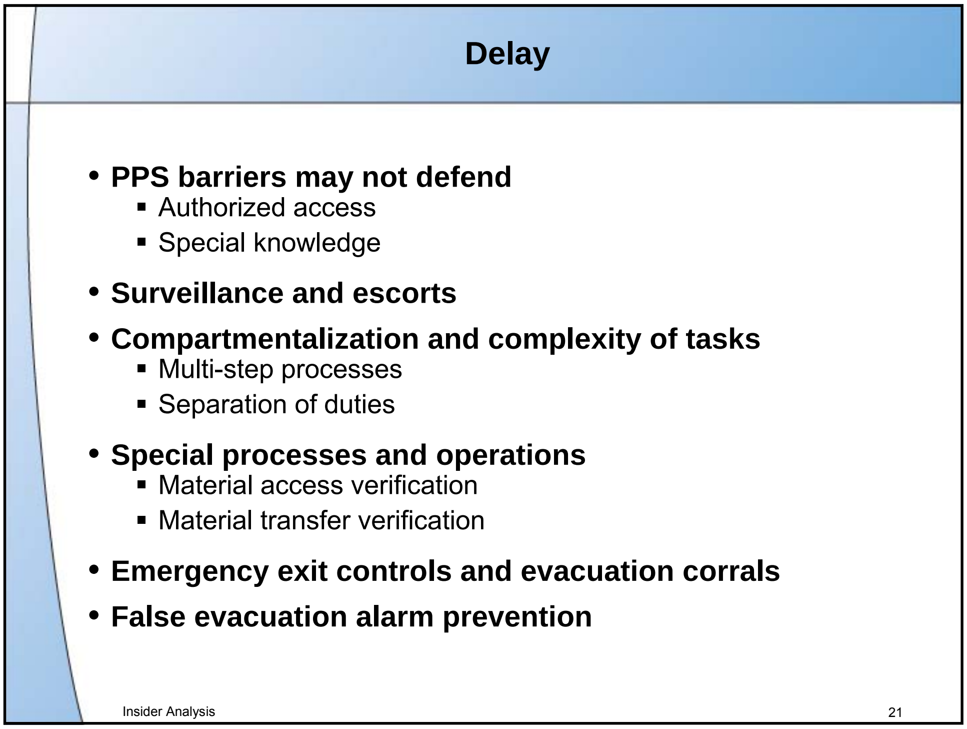
Insider Analysis 19



Malevolent Actions

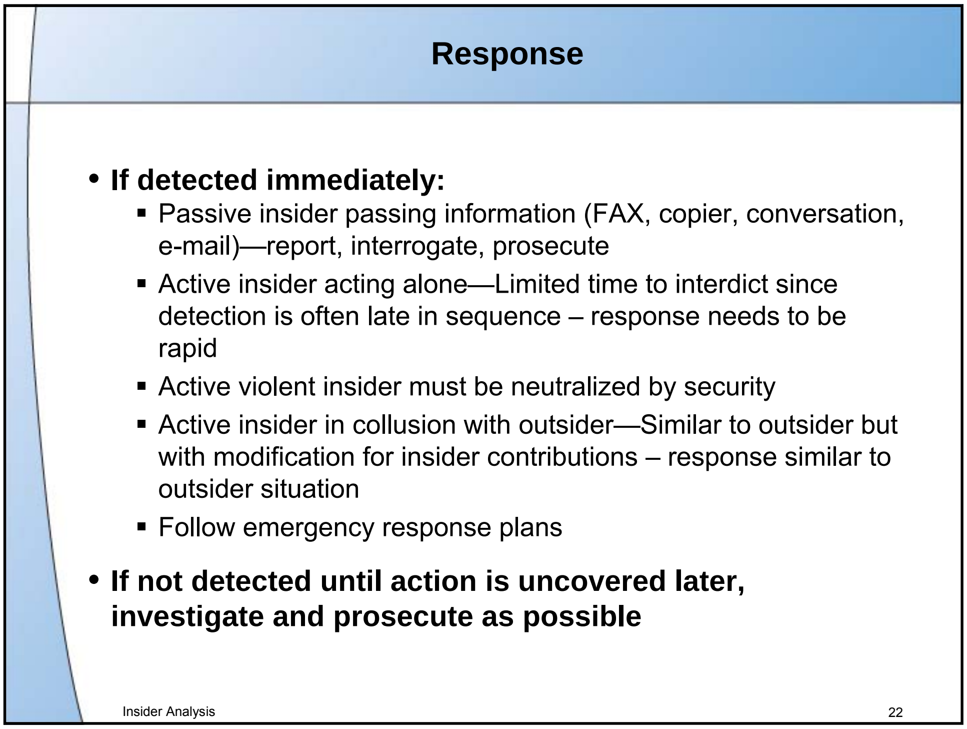
- **Unauthorized removal and sabotage of material**
- **Damaging or compromising equipment**
- **Attacking or influencing personnel**
- **Attempting to defeat the material control and accountancy system**
- **Bypassing or compromising plant safety or security measures**
- **Attempting to defeat the operational process monitoring**
- **Access to unauthorized areas or information**

Insider Analysis 20



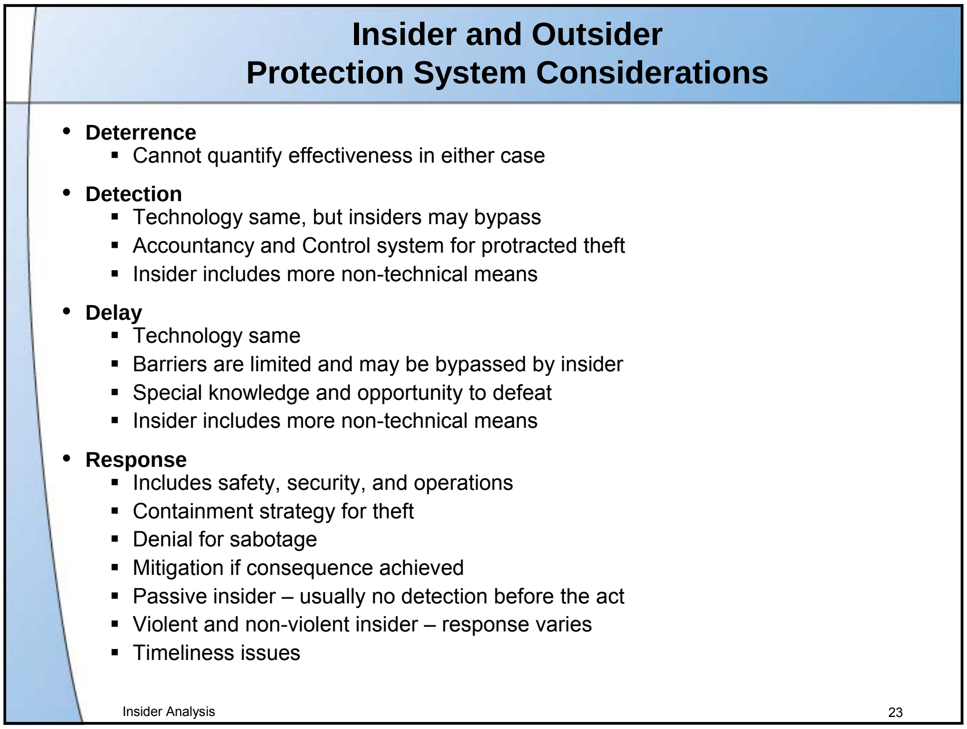
Delay

- **PPS barriers may not defend**
  - Authorized access
  - Special knowledge
- **Surveillance and escorts**
- **Compartmentalization and complexity of tasks**
  - Multi-step processes
  - Separation of duties
- **Special processes and operations**
  - Material access verification
  - Material transfer verification
- **Emergency exit controls and evacuation corrals**
- **False evacuation alarm prevention**



Response

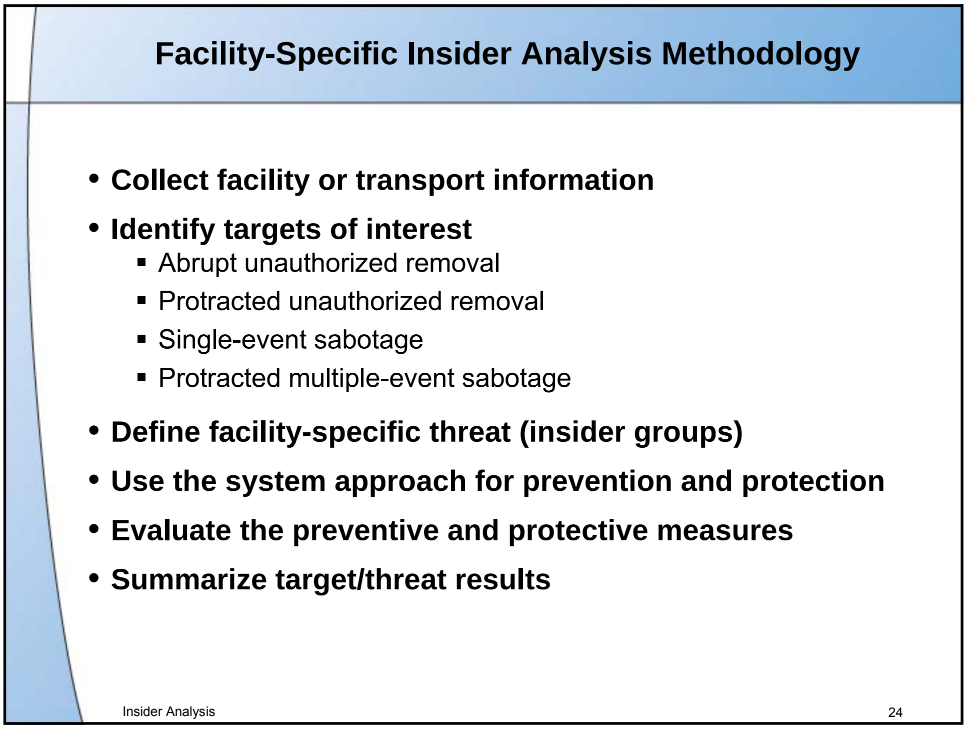
- **If detected immediately:**
  - Passive insider passing information (FAX, copier, conversation, e-mail)—report, interrogate, prosecute
  - Active insider acting alone—Limited time to interdict since detection is often late in sequence – response needs to be rapid
  - Active violent insider must be neutralized by security
  - Active insider in collusion with outsider—Similar to outsider but with modification for insider contributions – response similar to outsider situation
  - Follow emergency response plans
- **If not detected until action is uncovered later, investigate and prosecute as possible**



Insider and Outsider Protection System Considerations

- **Deterrence**
  - Cannot quantify effectiveness in either case
- **Detection**
  - Technology same, but insiders may bypass
  - Accountancy and Control system for protracted theft
  - Insider includes more non-technical means
- **Delay**
  - Technology same
  - Barriers are limited and may be bypassed by insider
  - Special knowledge and opportunity to defeat
  - Insider includes more non-technical means
- **Response**
  - Includes safety, security, and operations
  - Containment strategy for theft
  - Denial for sabotage
  - Mitigation if consequence achieved
  - Passive insider – usually no detection before the act
  - Violent and non-violent insider – response varies
  - Timeliness issues

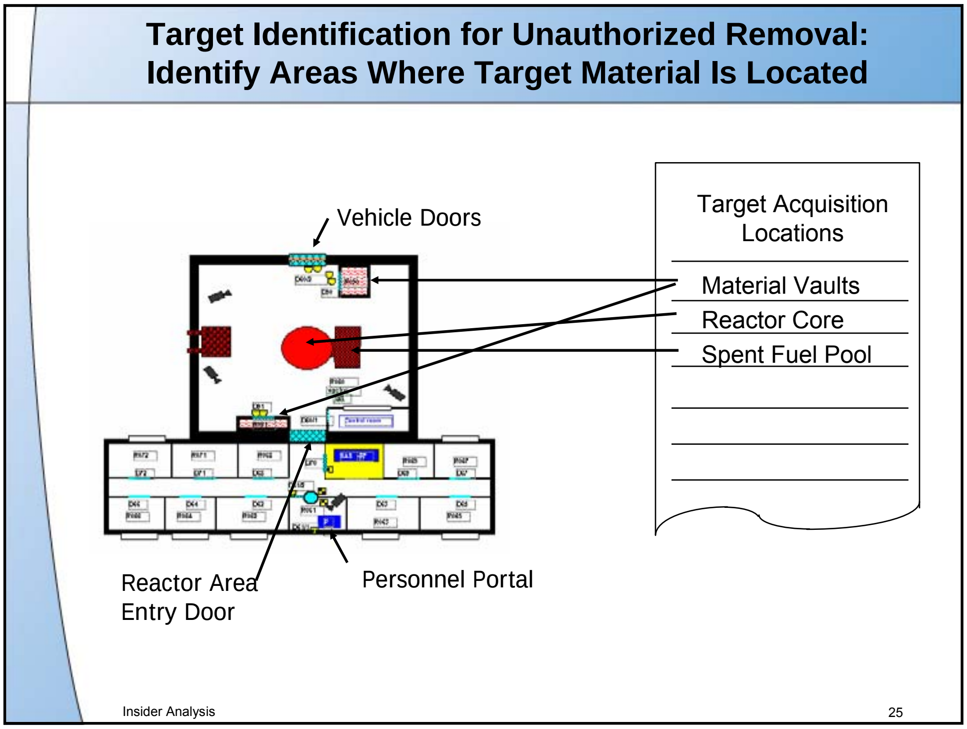
Insider Analysis 23



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)**
- **Use the system approach for prevention and protection**
- **Evaluate the preventive and protective measures**
- **Summarize target/threat results**

Insider Analysis 24



Target Identification for Unauthorized Removal: Identify Areas Where Target Material Is Located

Vehicle Doors

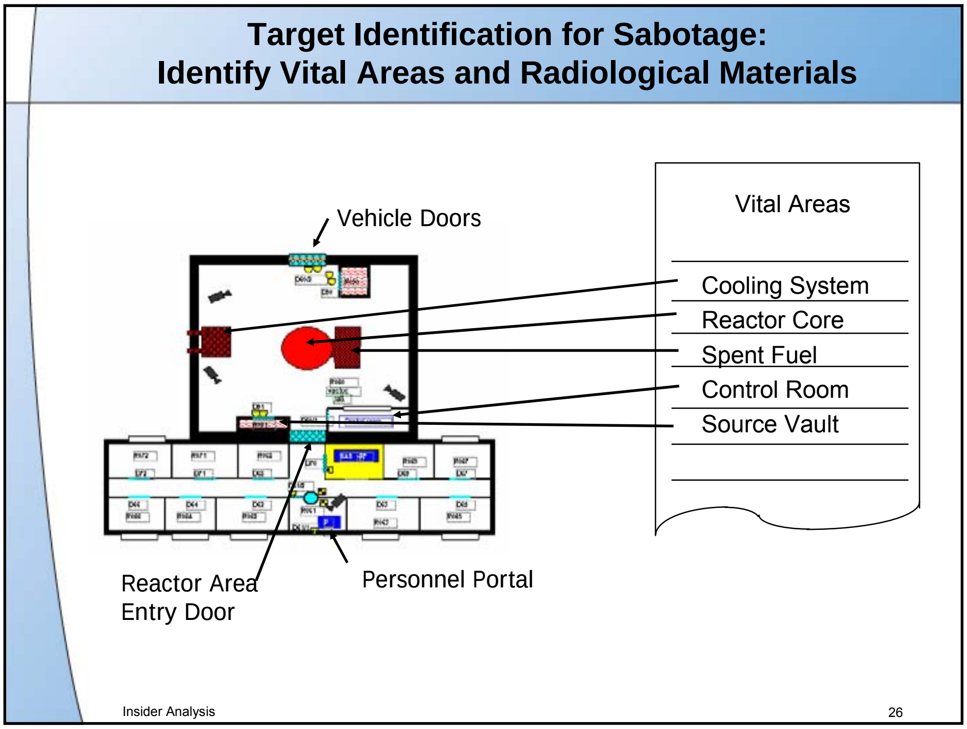
Reactor Area Entry Door

Personnel Portal

Target Acquisition Locations

- Material Vaults
- Reactor Core
- Spent Fuel Pool

Insider Analysis 25



Target Identification for Sabotage: Identify Vital Areas and Radiological Materials

Vehicle Doors

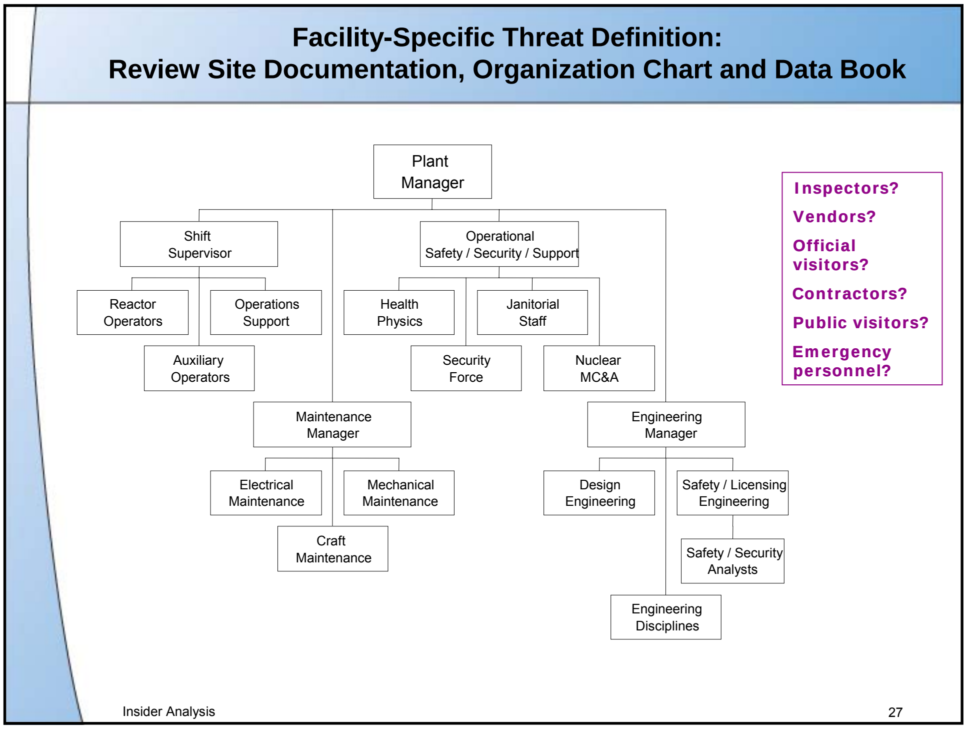
Reactor Area Entry Door

Personnel Portal

Vital Areas

- Cooling System
- Reactor Core
- Spent Fuel
- Control Room
- Source Vault

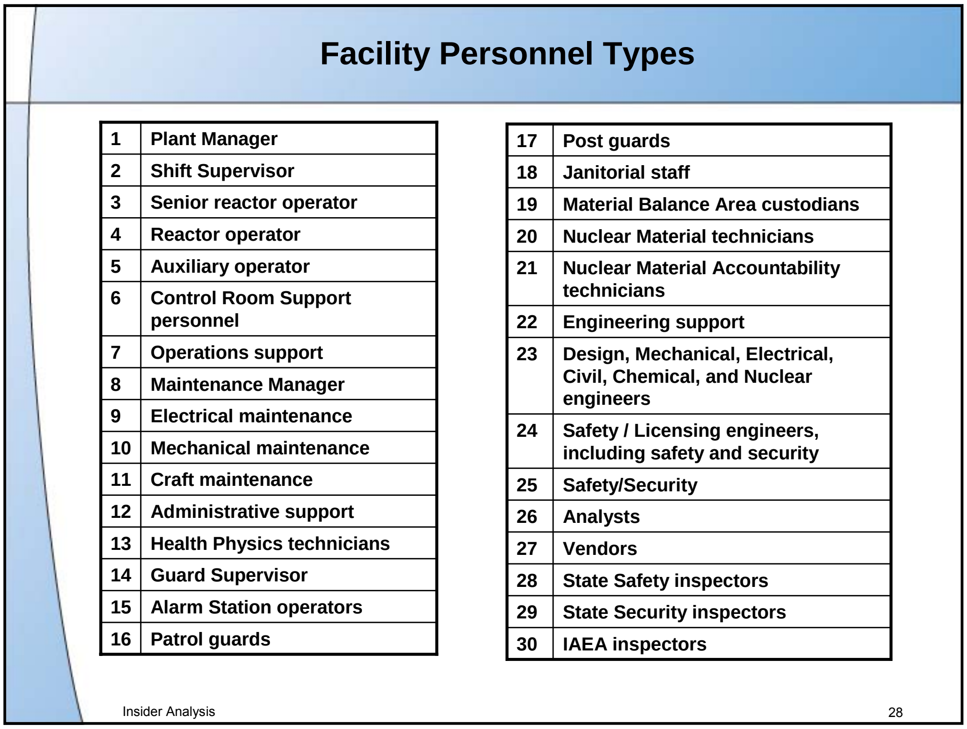
Insider Analysis 26



Facility-Specific Threat Definition: Review Site Documentation, Organization Chart and Data Book

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

Insider Analysis 27

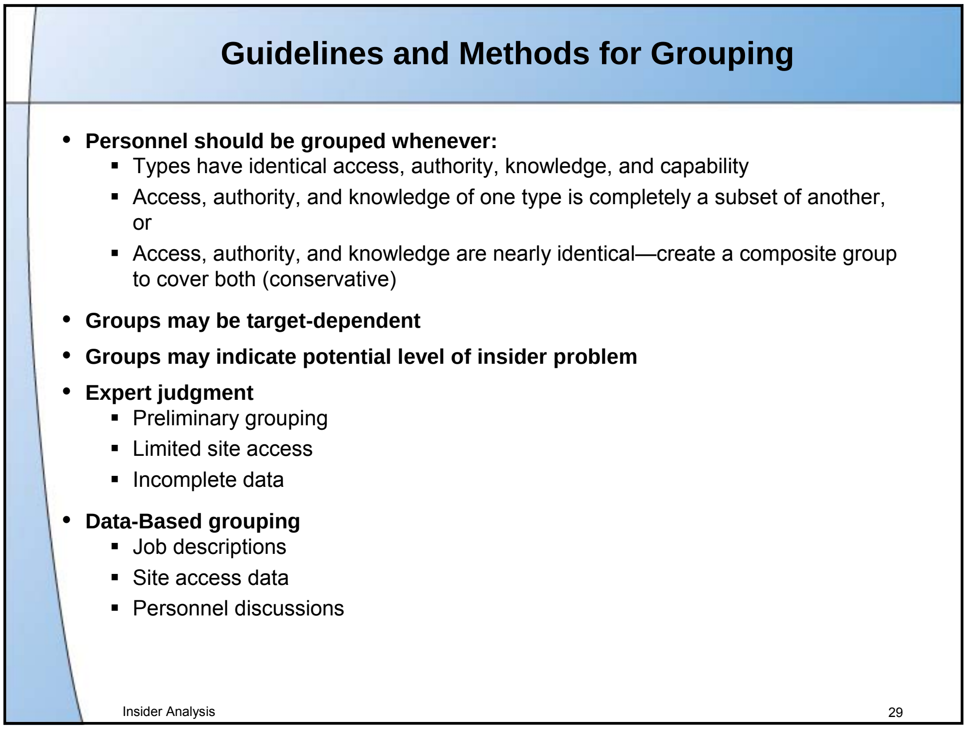


Facility Personnel Types

1	Plant Manager
2	Shift Supervisor
3	Senior reactor operator
4	Reactor operator
5	Auxiliary operator
6	Control Room Support personnel
7	Operations support
8	Maintenance Manager
9	Electrical maintenance
10	Mechanical maintenance
11	Craft maintenance
12	Administrative support
13	Health Physics technicians
14	Guard Supervisor
15	Alarm Station operators
16	Patrol guards

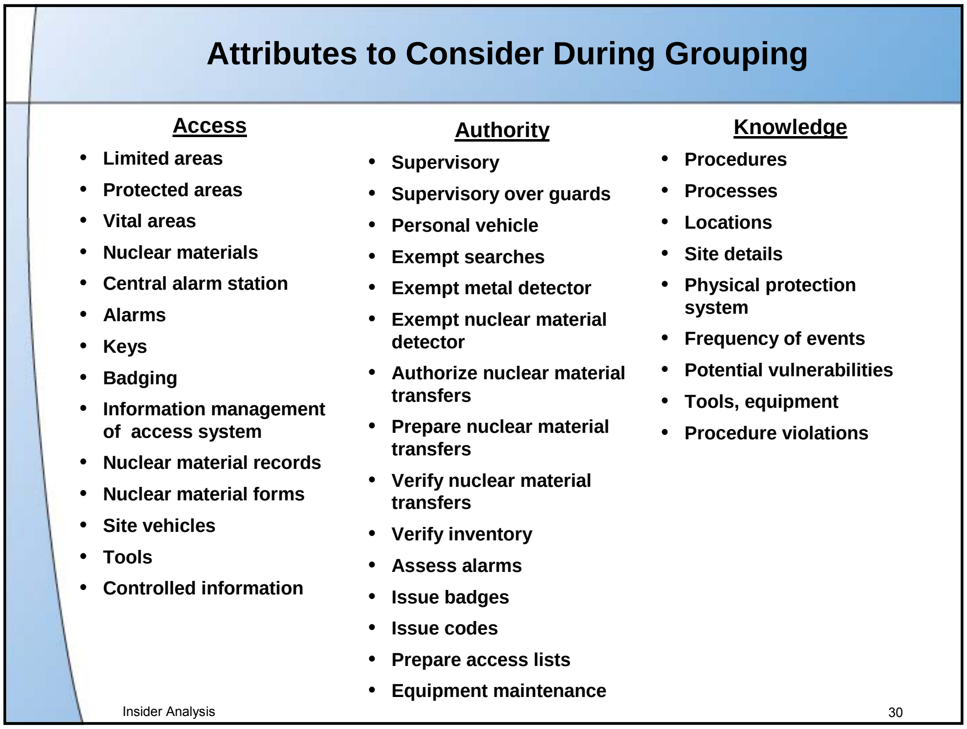
17	Post guards
18	Janitorial staff
19	Material Balance Area custodians
20	Nuclear Material technicians
21	Nuclear Material Accountability technicians
22	Engineering support
23	Design, Mechanical, Electrical, Civil, Chemical, and Nuclear engineers
24	Safety / Licensing engineers, including safety and security
25	Safety/Security
26	Analysts
27	Vendors
28	State Safety inspectors
29	State Security inspectors
30	IAEA inspectors

Insider Analysis 28



Guidelines and Methods for Grouping

- **Personnel should be grouped whenever:**
  - Types have identical access, authority, knowledge, and capability
  - Access, authority, and knowledge of one type is completely a subset of another, or
  - Access, authority, and knowledge are nearly identical—create a composite group to cover both (conservative)
- **Groups may be target-dependent**
- **Groups may indicate potential level of insider problem**
- **Expert judgment**
  - Preliminary grouping
  - Limited site access
  - Incomplete data
- **Data-Based grouping**
  - Job descriptions
  - Site access data
  - Personnel discussions



Attributes to Consider During Grouping

Access

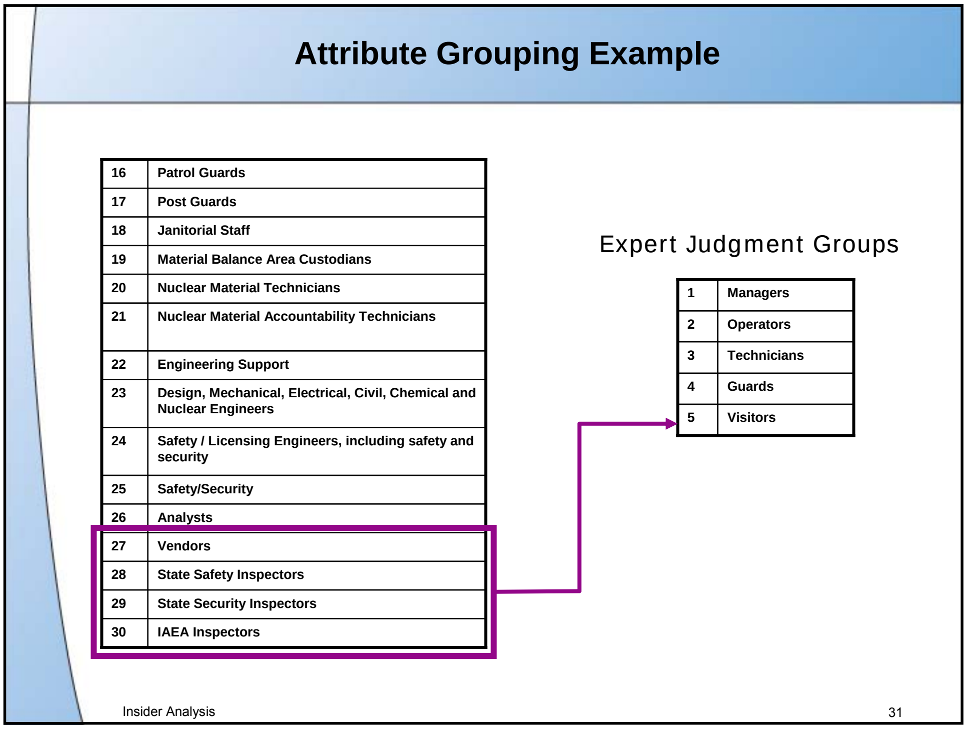
- **Limited areas**
- **Protected areas**
- **Vital areas**
- **Nuclear materials**
- **Central alarm station**
- **Alarms**
- **Keys**
- **Badging**
- **Information management of access system**
- **Nuclear material records**
- **Nuclear material forms**
- **Site vehicles**
- **Tools**
- **Controlled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



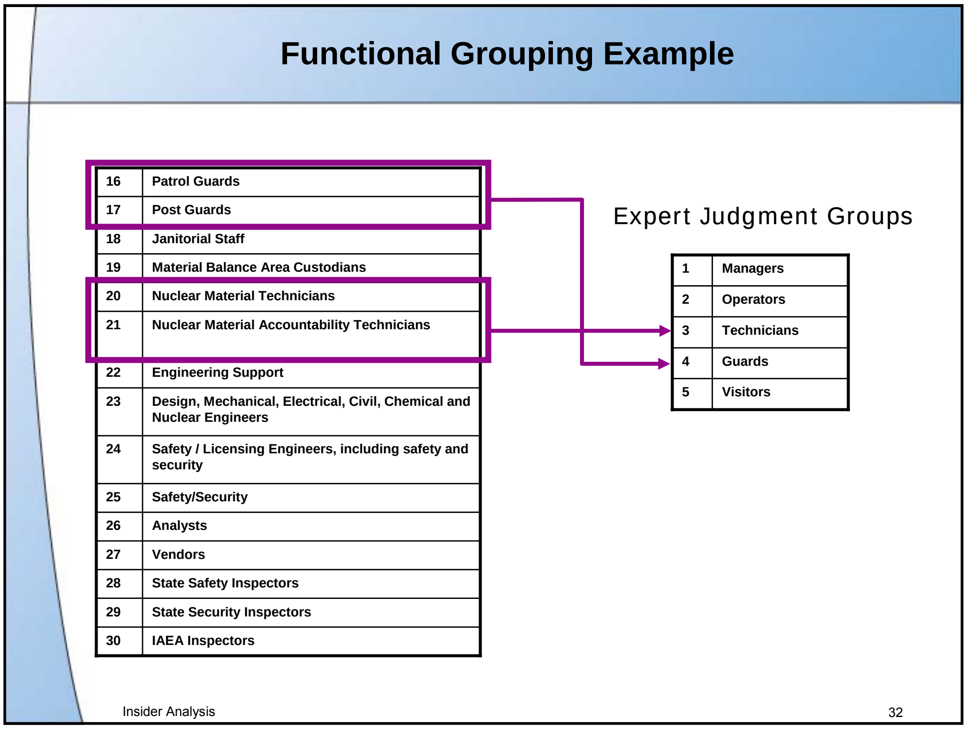
Attribute Grouping Example

16	Patrol Guards
17	Post Guards
18	Janitorial Staff
19	Material Balance Area Custodians
20	Nuclear Material Technicians
21	Nuclear Material Accountability Technicians
22	Engineering Support
23	Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers
24	Safety / Licensing Engineers, including safety and security
25	Safety/Security
26	Analysts
27	Vendors
28	State Safety Inspectors
29	State Security Inspectors
30	IAEA Inspectors

Expert Judgment Groups

1	Managers
2	Operators
3	Technicians
4	Guards
5	Visitors

Insider Analysis 31



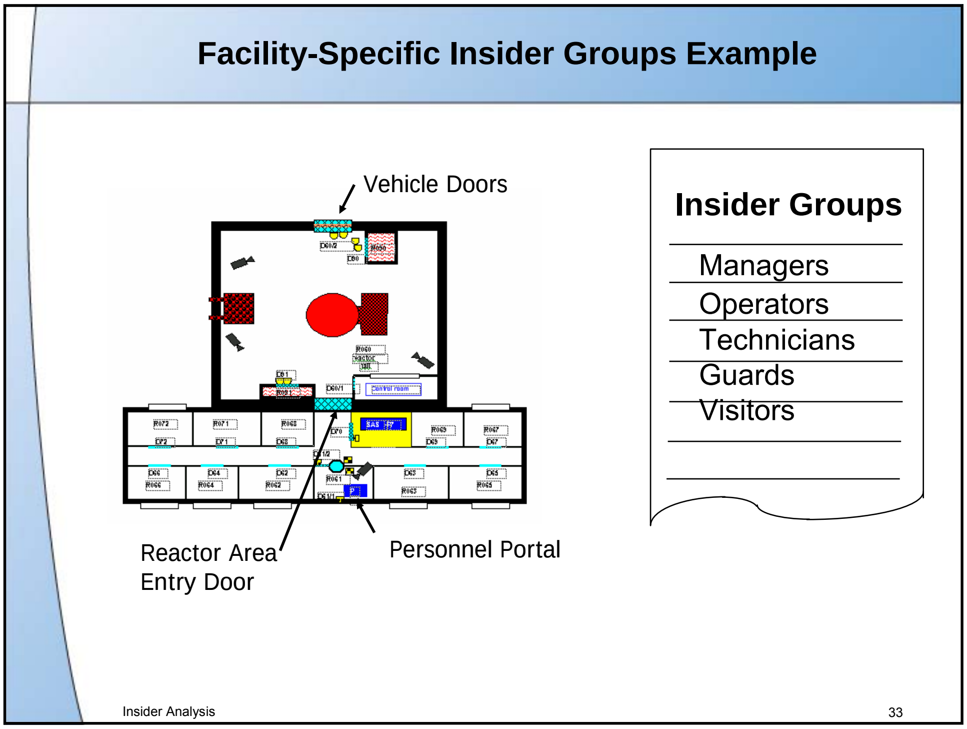
Functional Grouping Example

16	Patrol Guards
17	Post Guards
18	Janitorial Staff
19	Material Balance Area Custodians
20	Nuclear Material Technicians
21	Nuclear Material Accountability Technicians
22	Engineering Support
23	Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers
24	Safety / Licensing Engineers, including safety and security
25	Safety/Security
26	Analysts
27	Vendors
28	State Safety Inspectors
29	State Security Inspectors
30	IAEA Inspectors

Expert Judgment Groups

1	Managers
2	Operators
3	Technicians
4	Guards
5	Visitors

Insider Analysis 32



Facility-Specific Insider Groups Example

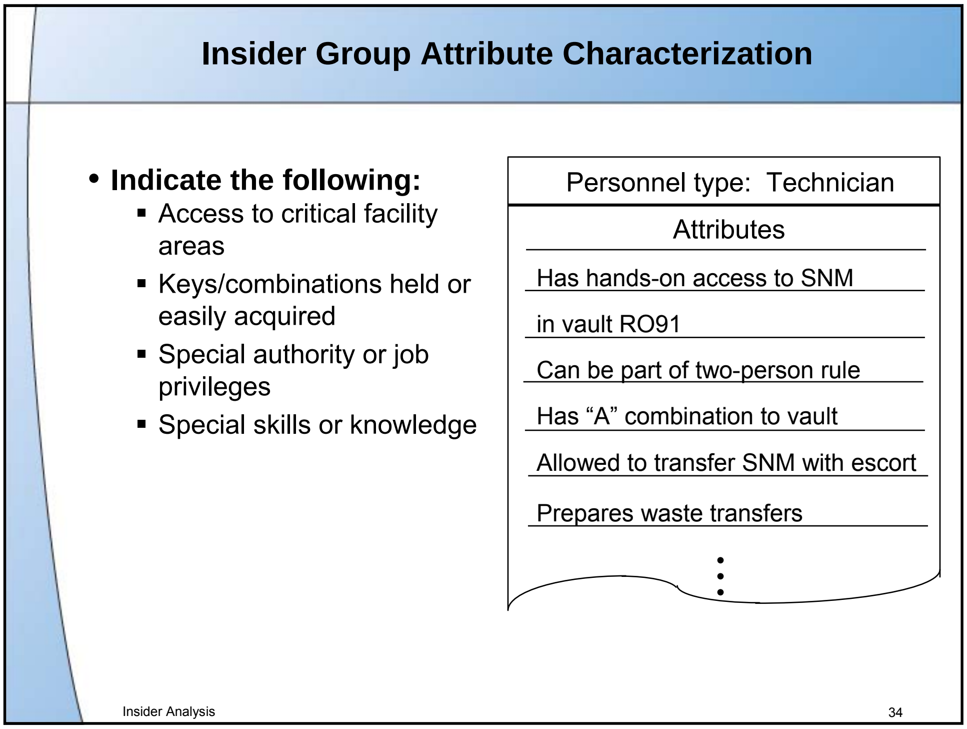
Vehicle Doors

Reactor Area Entry Door

Personnel Portal

Insider Groups

Managers
Operators
Technicians
Guards
Visitors



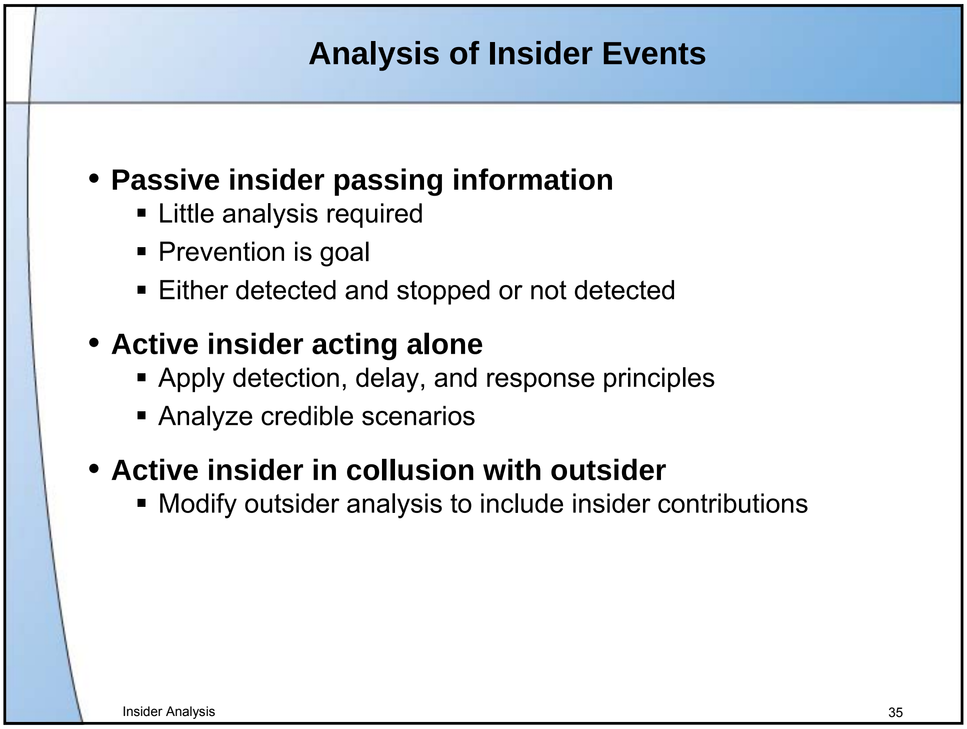
Insider Group Attribute Characterization

- **Indicate the following:**
  - Access to critical facility areas
  - Keys/combinations held or easily acquired
  - Special authority or job privileges
  - Special skills or knowledge

Personnel type: Technician

Attributes

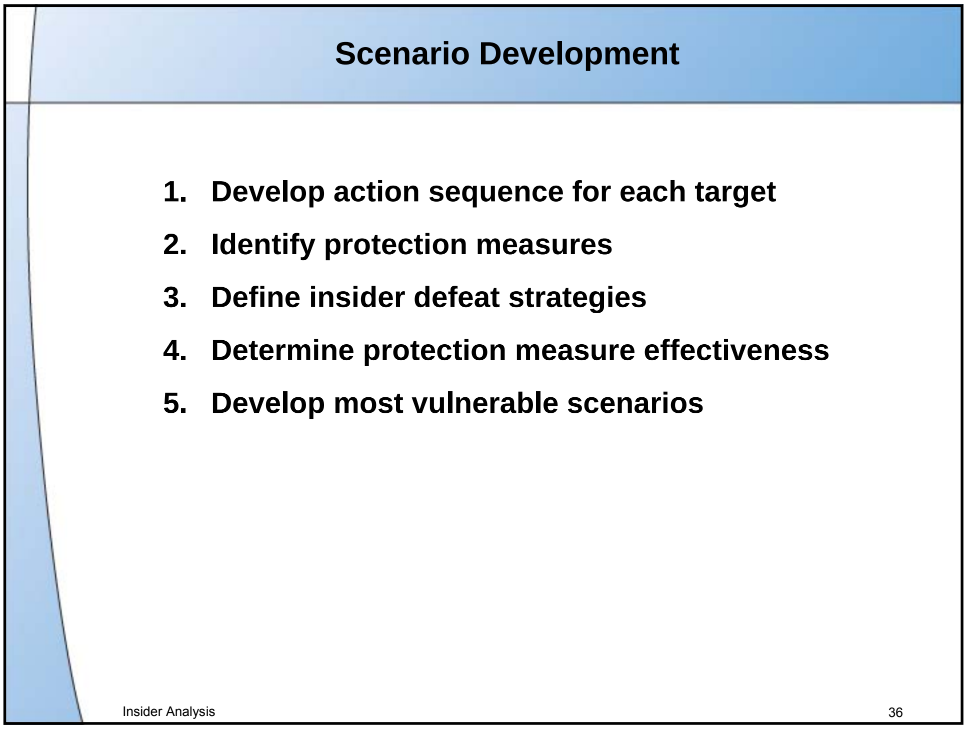
Has hands-on access to SNM
in vault RO91
Can be part of two-person rule
Has “A” combination to vault
Allowed to transfer SNM with escort
Prepares waste transfers
⋮



Analysis of Insider Events

- **Passive insider passing information**
  - Little analysis required
  - Prevention is goal
  - Either detected and stopped or not detected
- **Active insider acting alone**
  - Apply detection, delay, and response principles
  - Analyze credible scenarios
- **Active insider in collusion with outsider**
  - Modify outsider analysis to include insider contributions

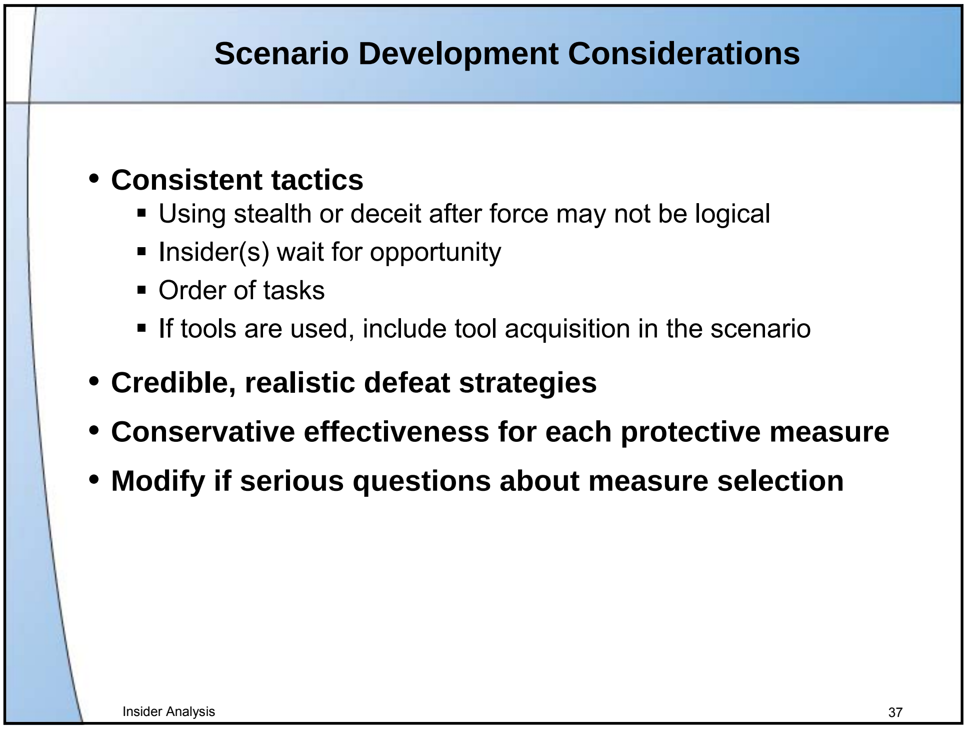
Insider Analysis 35



Scenario Development

1. **Develop action sequence for each target**
2. **Identify protection measures**
3. **Define insider defeat strategies**
4. **Determine protection measure effectiveness**
5. **Develop most vulnerable scenarios**

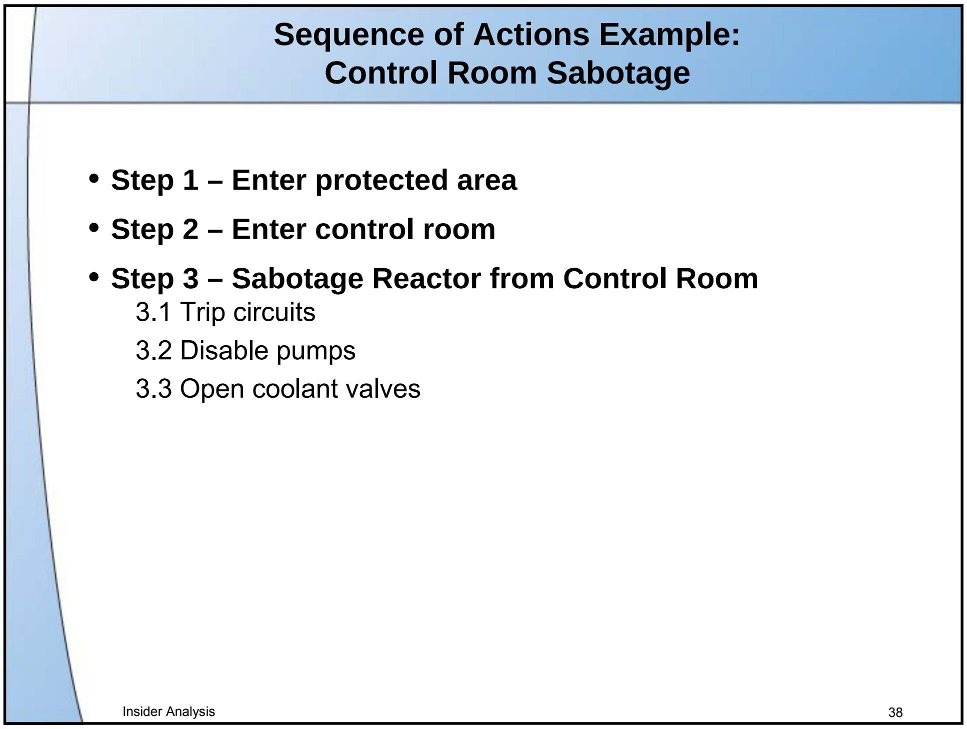
Insider Analysis 36



Scenario Development Considerations

- **Consistent tactics**
  - Using stealth or deceit after force may not be logical
  - Insider(s) wait for opportunity
  - Order of tasks
  - If tools are used, include tool acquisition in the scenario
- **Credible, realistic defeat strategies**
- **Conservative effectiveness for each protective measure**
- **Modify if serious questions about measure selection**

Insider Analysis 37



Sequence of Actions Example: Control Room Sabotage

- **Step 1 – Enter protected area**
- **Step 2 – Enter control room**
- **Step 3 – Sabotage Reactor from Control Room**

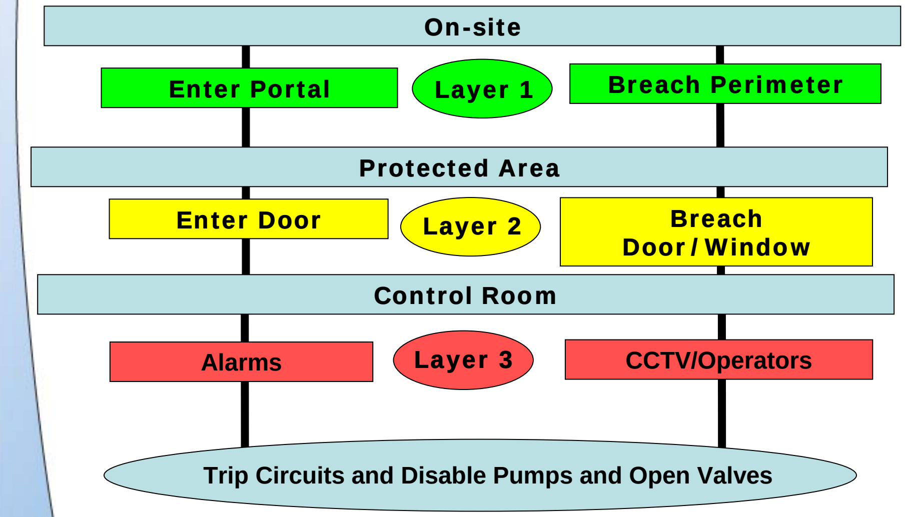
  3.1 Trip circuits

  3.2 Disable pumps

  3.3 Open coolant valves

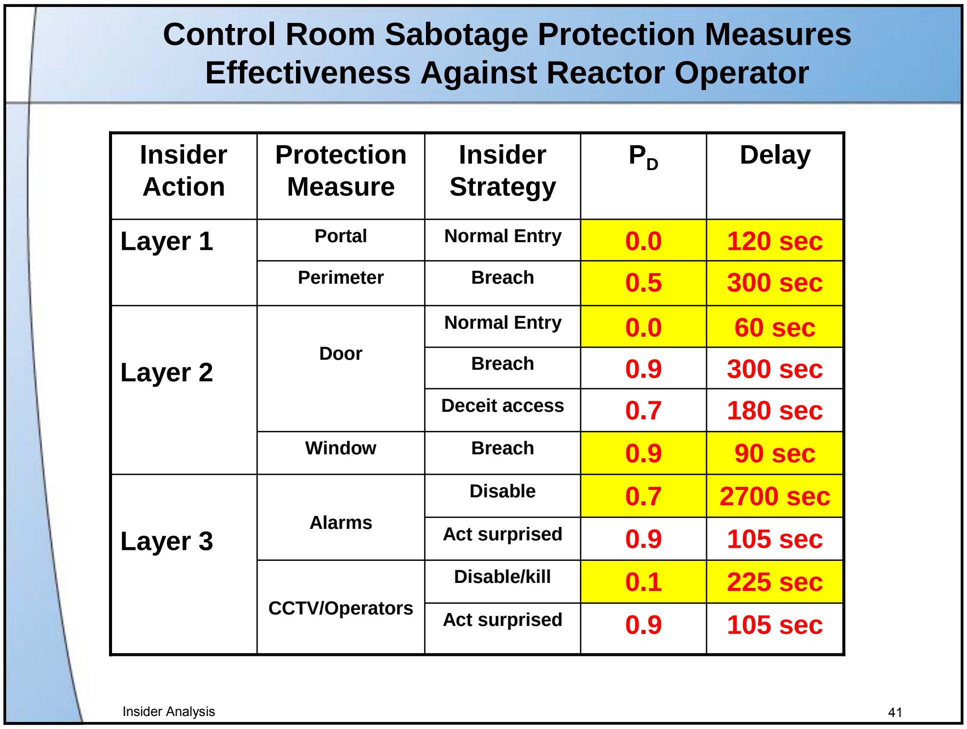
Insider Analysis 38

Adversary Sequence Diagram
Control Room Sabotage



Control Room Sabotage
Protection Measures and Insider Strategies

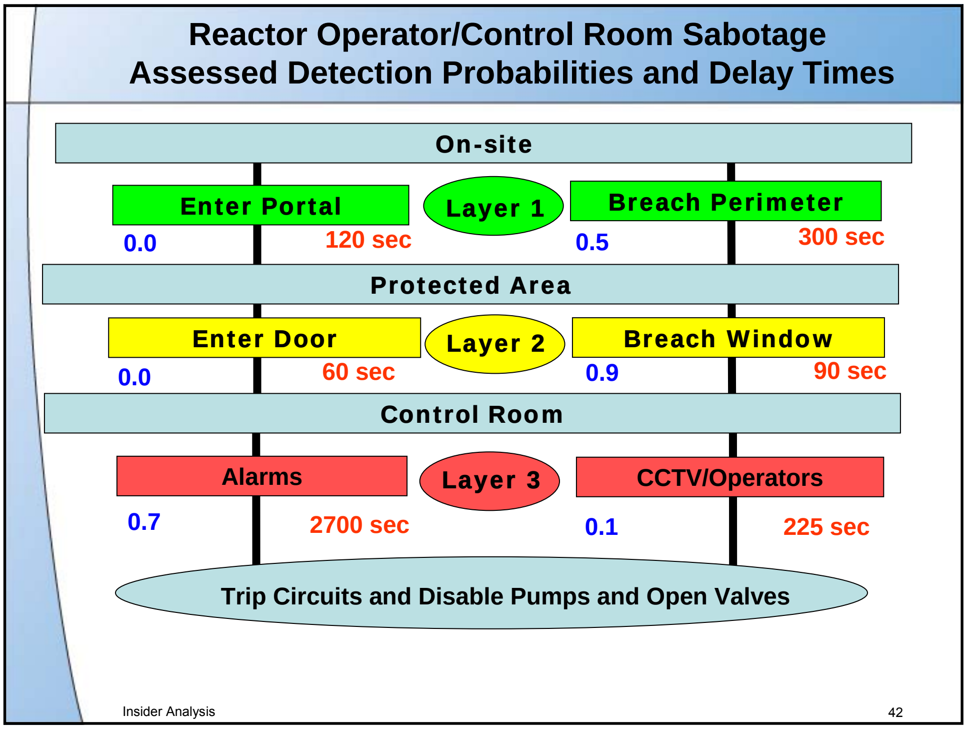
Insider Action	Protection Measure	Insider Strategy		
Layer 1	Portal	Normal Entry		
	Perimeter	Breach		
Layer 2	Door	Normal Entry		
		Breach		
		Deceit access		
	Window	Breach		
Layer 3	Alarms	Disable		
		Act surprised		
	CCTV/Operators	Disable/kill		
		Act surprised		



Control Room Sabotage Protection Measures Effectiveness Against Reactor Operator

Insider Action	Protection Measure	Insider Strategy	P_D	Delay
Layer 1	Portal	Normal Entry	0.0	120 sec
	Perimeter	Breach	0.5	300 sec
Layer 2	Door	Normal Entry	0.0	60 sec
		Breach	0.9	300 sec
		Deceit access	0.7	180 sec
	Window	Breach	0.9	90 sec
Layer 3	Alarms	Disable	0.7	2700 sec
		Act surprised	0.9	105 sec
	CCTV/Operators	Disable/kill	0.1	225 sec
		Act surprised	0.9	105 sec

Insider Analysis 41



Reactor Operator/Control Room Sabotage Assessed Detection Probabilities and Delay Times

On-site

Enter Portal 0.0 120 sec

Layer 1

Breach Perimeter 0.5 300 sec

Protected Area

Enter Door 0.0 60 sec

Layer 2

Breach Window 0.9 90 sec

Control Room

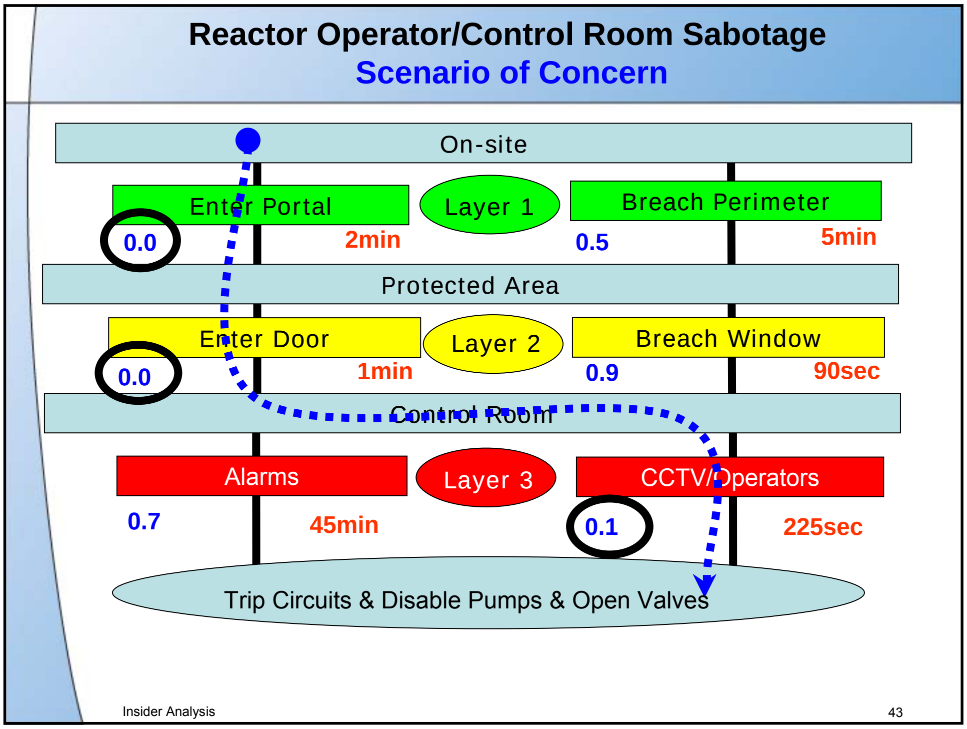
Alarms 0.7 2700 sec

Layer 3

CCTV/Operators 0.1 225 sec

Trip Circuits and Disable Pumps and Open Valves

Insider Analysis 42



Reactor Operator/Control Room Sabotage
Scenario of Concern

On-site

Enter Portal

0.0

2min

Layer 1

Breach Perimeter

0.5

5min

Protected Area

Enter Door

0.0

1min

Layer 2

Breach Window

0.9

90sec

Control Room

Alarms

0.7

45min

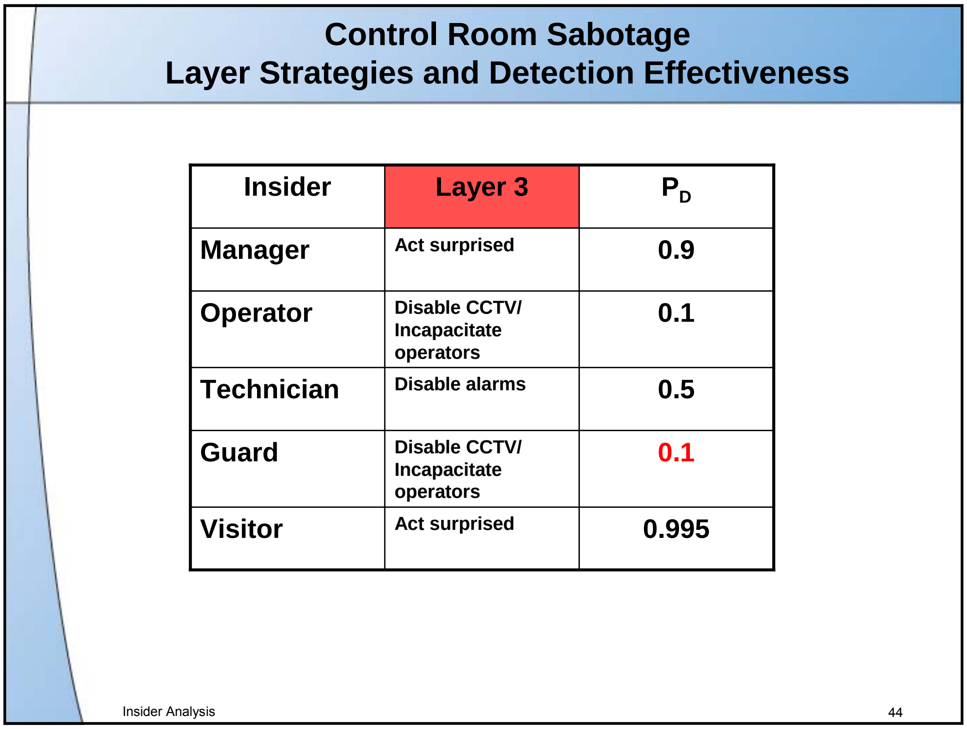
Layer 3

CCTV/Operators

0.1

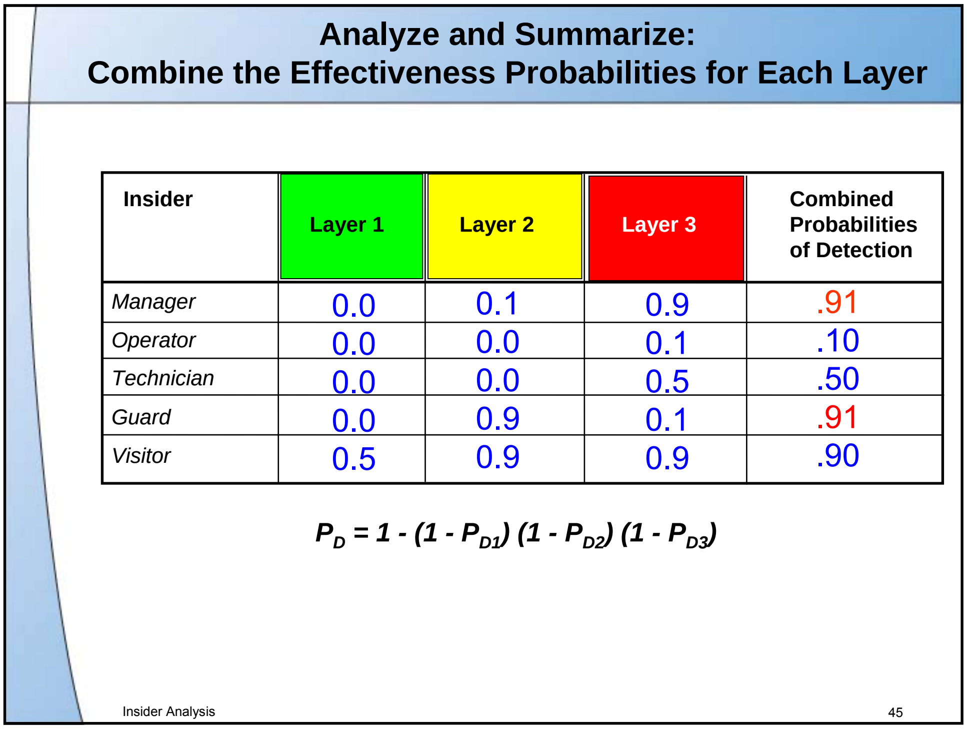
225sec

Trip Circuits & Disable Pumps & Open Valves



Control Room Sabotage
Layer Strategies and Detection Effectiveness

Insider	Layer 3	P_D
Manager	Act surprised	0.9
Operator	Disable CCTV/ Incapacitate operators	0.1
Technician	Disable alarms	0.5
Guard	Disable CCTV/ Incapacitate operators	0.1
Visitor	Act surprised	0.995

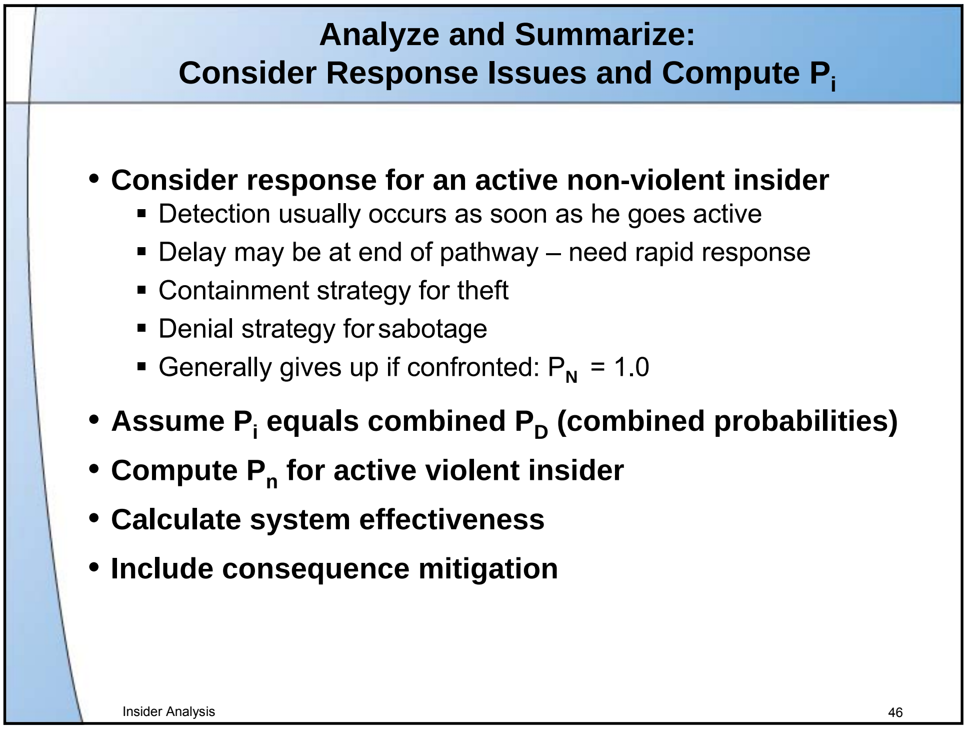


Analyze and Summarize:
Combine the Effectiveness Probabilities for Each Layer

Insider	Layer 1	Layer 2	Layer 3	Combined Probabilities of Detection
Manager	0.0	0.1	0.9	.91
Operator	0.0	0.0	0.1	.10
Technician	0.0	0.0	0.5	.50
Guard	0.0	0.9	0.1	.91
Visitor	0.5	0.9	0.9	.90

$$P_D = 1 - (1 - P_{D1}) (1 - P_{D2}) (1 - P_{D3})$$

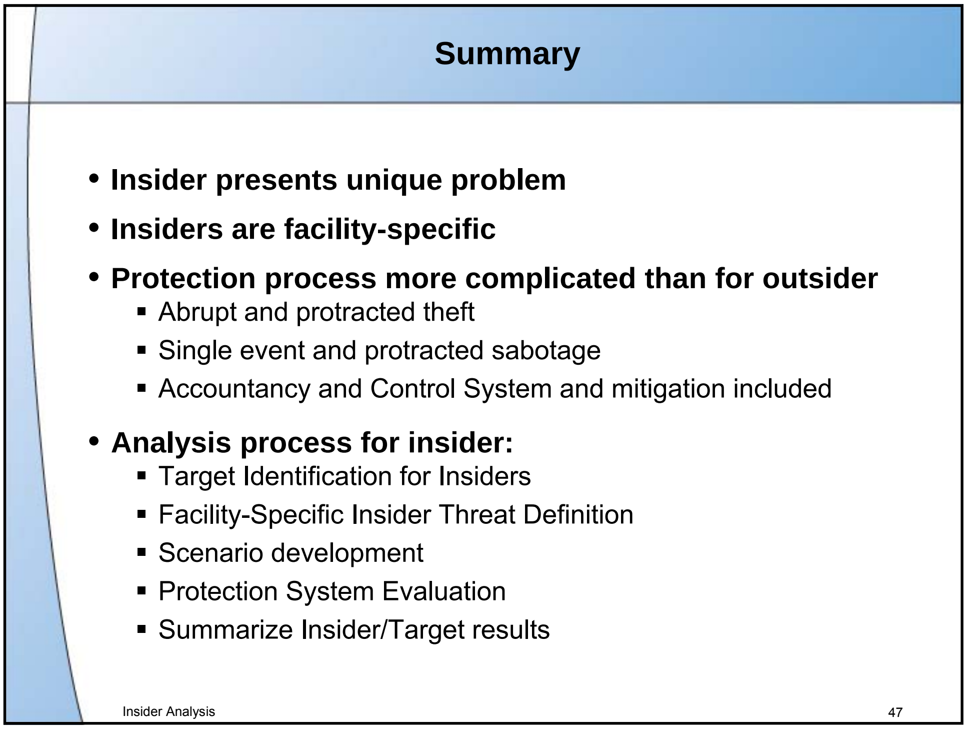
Insider Analysis 45



Analyze and Summarize:
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**

Insider Analysis 46



Summary

- **Insider presents unique problem**
- **Insiders are facility-specific**
- **Protection process more complicated than for outsider**
  - Abrupt and protracted theft
  - Single event and protracted sabotage
  - Accountancy and Control System and mitigation included
- **Analysis process for insider:**
  - Target Identification for Insiders
  - Facility-Specific Insider Threat Definition
  - Scenario development
  - Protection System Evaluation
  - Summarize Insider/Target results

Insider Analysis 47

Subgroup 23S
Insider Analysis

Session Objectives

After the session, participants will be able to do the following:

1. Apply the insider PPS design evaluation technique to the PTR Hypothetical Facility.
2. Use the methodology outlined in Lecture 23, Insider Analysis.
3. Suggest solutions to reduce the vulnerability to the insider threat of theft of special nuclear materials.

Session Instructions

In Exercises 2-7, consider only the Pu experiments in R091 as targets for unauthorized removal by a single active non-violent insider. Begin the analysis on-site but outside of the PTR protected area.

Exercise 8 is a special insider sabotage exercise.

Exercise 1 – Target Identification

In this exercise, use your *Exercise Data Book* Section “3. Material Stored on Site” and section “10. PTR Research Reactor Building Floor Plan” to identify potential Insider theft targets, target acquisition locations, and sabotage Vital Areas. Rank the targets in order of importance to be protected based on consequence and attractiveness. You may use the subjective rankings of Very High (VH), High (H), Medium (M), Low (L), and Very Low (VL), or a ranking scheme of your choice.

Insider Unauthorized Removal Targets

Target Acquisition Locations	Material	Form	Qty	Abrupt theft	Protracted Theft	Consequence of Loss	Rank

Insider Sabotage Targets

Sabotage Vital Areas	Material	Form	Qty	Radiation Level	Consequence of sabotage	Rank

Exercise 2 –Threat Definition: Facility Specific Insider Identification

The objective of this exercise is to define insider groups for subsequent analysis. Information from the facility organization chart and from site visits and interviews has been compiled in Table 23S-1. The table shows job category and access to three facility areas: the PTR protected area, the reactor hall R060, and the plutonium storage vault R091. For each access area in the table, the left column is the number of people per shift with authorized access, and the right column is the number of people allowed access only with a dedicated escort, denoted by a capital "E" after the number. A blank entry means there is no authorized access. R091 is under Two-Person-Rule (TPR) control, which is in addition to the dedicated escort requirement.

Group these personnel for analysis as active non-violent insiders who might attempt unauthorized removal of material from vault R091. Refer to lecture slides 29-34 for grouping guidelines. Use an EXCEL™ spreadsheet if possible during this exercise. You may have more or less than ten groups.

	Insider Group Description	Personnel Categories	Number (Total)	P.A.	R060	R091
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Table 23S-1. PTR Personnel Access List

	Personnel Type	Accesses					
		PTR P.A.		R060		R091	
1	**Plant manager**	1		1			1E
2	Reactor Operations Shift Supervisor	1		1			
3	Senior Reactor operator	1		1			
4	Reactor operator	2		2			
5	Auxiliary Operator	2		2			
6	Control Room Support Personnel	5			5E		
7	Operations Support		2E		2E		
8	Maintenance Manager	1		1			1E
9	Electrical Maintenance	2		2			2E
10	Mechanical Maintenance	2		2			2E
11	Craft Maintenance	2		2			2E
12	Administrative support	4		4			
13	Health Physics Technicians	3		3			3E
14	Guard Supervisor	1		1			
15	Alarm Station Operators	2		2			
16	Patrol Guards	2					
17	Post Guards	3		1			
18	Janitorial Staff	4			4E		4E
19	Material Balance Area Custodians	3		3		3	
20	Nuclear Material Technicians	6		6		6	
21	Nuclear Material Accounting Technicians	2		2		2	
22	Engineering Support	2		2			
23	Design Engineers		2E		2E		
24	Safety	5		5			5E
25	Scientists	6		6		6	
26	Analysts						
27	Vendors		2E				
28	State Safety Inspectors		4E		4E		4E
29	State Security Inspectors		4E		4E		4E
30	IAEA Inspectors		2E		2E		2E

Exercise 3 – Action Sequence for Unauthorized Removal from R091

The objective of this exercise is to develop the action sequence necessary for an active nonviolent insider to complete unauthorized removal of target material from R091. Referring to the PTR site schematic and the adversary sequence diagram that you have developed previously for outsider analysis, develop the action sequence in terms of movement between layers as well as tasks that must be accomplished at each layer. Remember that active nonviolent insiders will use only stealth and deceit, as well as their access, authority and knowledge, and will surrender if detected. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Step	Action
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

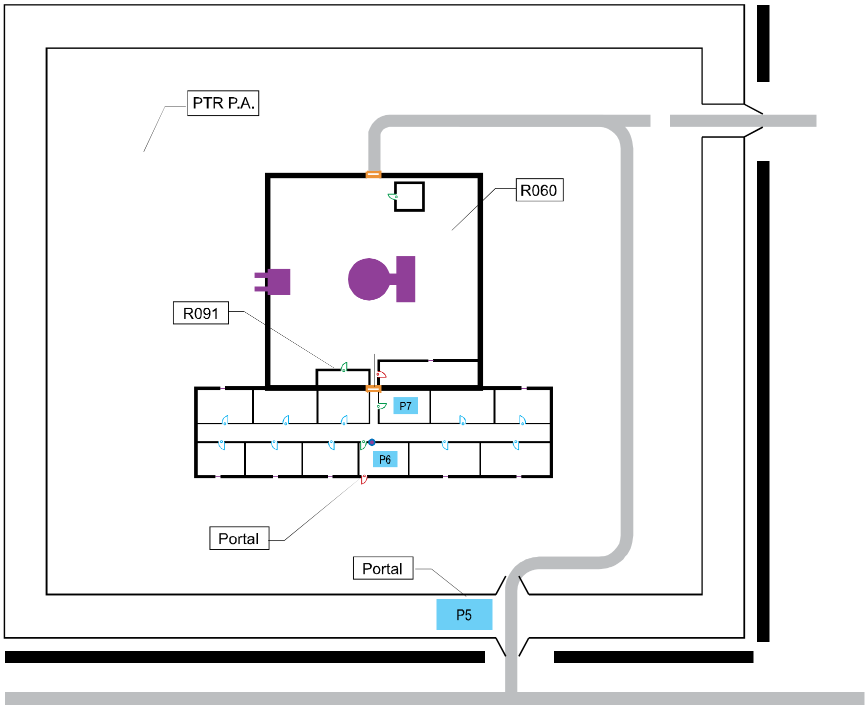


Figure 23S-2. PTR Facility

Exercise 4 – Identify Path Element

The objective of this exercise is to identify path element options and protection measures along the insider action sequence that was developed in Exercise 3. Refer to the PTR site schematic and the adversary sequence diagram that you have developed previously for outsider analysis.

Step	Action	Path Element
1		
2		
3		
4		
5		
6		
7		
8		

Exercise 5 – Define Insider Defeat Strategies

The objective of this exercise is to define possible defeat strategies for the protection measures at each path element or action identified in Exercise 4. Refer to the PTR site schematic to ensure that all PPS elements are accounted for in your defeat strategies. Table 23S-2 lists some defeat strategies. Consider the access, authority, knowledge and capabilities of your insider group list and add other defeat strategies as appropriate.

Action/Location	Path Element	Entry	Exit with target

Table 23S-3. Defeat Strategies

Doors/portals with access control	Normal entry/exit
Doors/portals with alarms	Normal entry/exit
Fences and isolation zones	Climb over
Search and scan detection	Disguise contraband
Target acquisition	Appear authorized
	Distract Two -person Rule
Target removal	Hide on person

Exercise 6 – Determine Path Element Effectiveness

The objective of this exercise is to determine the path element detection probabilities for the strategies at each path element or action identified in Exercise 4. Consider at least two of the insider groups defined in Exercise 2, and be sure that at least one group has authorized access to R091. The detection probabilities may be estimated either quantitatively, as a single digit decimal fraction between 0 and 1.0, or qualitatively, using very high (VH), high (H), medium (M), low (L), or very low (L). However, qualitative values must be converted to quantitative numbers for probability accumulation using the table on the following page. Assume that sensor detection probability for insiders with unauthorized access is 0.9, and that detection by dedicated escorts is 0.7.

Action	Path Element	Strategy	Insider Group P_D				

Action	Path Element	Strategy	Insider Group P_D				

Table 23S-4. Qualitative-to-Quantitative Detection Probability Conversion

Qualitative Effectiveness	Suggested Probability of Detection (P_D)
Very High	0.9
High	0.7
Medium	0.5
Low	0.3
Very Low	0.1

Use this table to convert qualitative probabilities of detection into quantitative values. The suggested quantitative values must reflect the thinking of the evaluators and may not be exactly as shown above. Change the values if necessary.

Exercise 7 – Develop Most Vulnerable Scenarios

The objective of this exercise is to develop the most vulnerable scenarios for insiders trying to acquire and remove target material. Using the results of Exercise 6, find the combination of protection measure and defeat strategy with the lowest probability of detection for each action in the unauthorized removal sequence. This is the most vulnerable scenario for each insider. Calculate the cumulative detection probability for each insider.

Action	**Insider Group __**			**Insider Group ___**		
	Strategy	**P_E**	**P_D**	**Strategy**	**P_E**	**P_D**
Cumulative detection P_i	**-----**	**-----**		**------**	**-----**	

From your analysis, identify the insider group that has the greatest probability of success (lowest P_I) in stealing Pu from the Storage Vault in the PTR (R091).

Insider group with greatest probability of success: ___________________________

Starting with the worst-case insider identified above, for each insider group with P_I less than 0.9, choose one action and suggest at least one upgrade that will increase P_I to at least 0.9. Will this upgrade work for all strategies at that path element? Will the upgrade work for all path elements possible for that action?

____

____

____

____

____

Exercise 8 – Insider Sabotage Analysis

The objective of this exercise is to develop the most vulnerable scenarios for insiders trying to perform a specific sabotage act inside the reactor hall R060. Use all information necessary from Exercises 2-7 in your analysis.

Background: National intelligence agents have conducted a raid on a safe house of terrorist outsider group, which has recently infiltrated the city. Several of the terrorists were killed during the raid, but the leader escaped. The agents obtained hard evidence that the group had plans and necessary materials to conduct a sabotage attack on the reactor. Planning documents indicate that a willing insider has been recruited and active violent insider collusion is part of the attack.

The facility has recently completed a reactor safety analysis review which uncovered a previously unknown safety problem. Analysts have determined that the following operating condition and failure sequence combination can lead to a possible core meltdown and associated radiological release, depending on the time necessary to replace damaged coolant pumps:

1) the reactor is operating at 80% power or greater

2) emergency coolant valve #2 (ECV2) is almost completely closed

3) emergency coolant valve #6 (ECV6) is almost completely closed

4) primary coolant pump #1 (PCP1) fails

5) primary coolant pump #2 (PCP2) fails

The two separate emergency coolant valves are located on the north and west exterior sides of the reactor. Both primary coolant pumps are located inside the coolant exchange area on the west wall of the reactor hall, R060.

Assignment: Using insider information from the previous exercises, estimate the insider risk or probability of success for a single, active, violent insider conducting a sabotage act based on the newly discovered reactor failure mode. Assume that the insider will be provided at least the necessary 0.75 KG of plastic explosive and detonators to destroy both coolant pumps in such a manner that replacement time will exceed consequence mitigation time. Begin your analysis by deciding which potential insider groups would have knowledge of the new failure mode, or be able to use their access and authority to obtain the information. Note that anyone with authorized access to R060 and the required knowledge can conduct the sabotage. What emergency improvements or contingency plans can you suggest to address this threat?

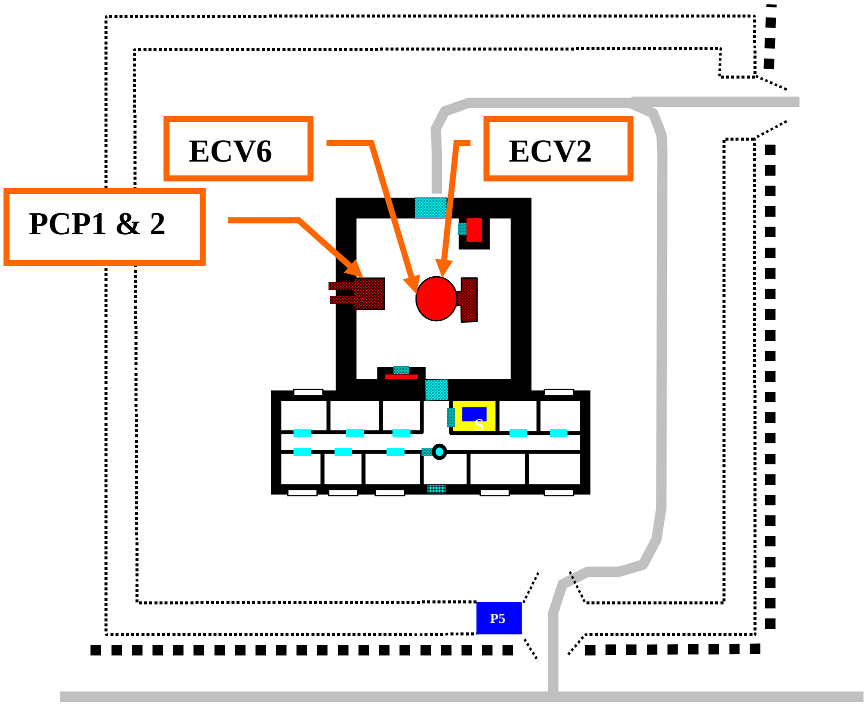


Figure 23-5. Location Of Primary Coolant Pumps And Emergency Valves

24. Transportation Security

Abstract. *The transportation of nuclear materials involves the movement of material from one location to another, often outside the protection boundaries of a fixed-site location. The same physical protection elements (detection, delay, response) are present, but the transportation system being used is continuously exposed to the public, whereas, the fixed site location by its very nature restricts general public access. The material transport system (MTS) can be considered a moving facility. It may consist of several material transports and response force carriers such as military escort vehicles and railcars. The area surrounding the facility (transport mode) automatically changes as the transport moves throughout the designated route. The terrain can change from flat level ground to rolling hills or mountains in a matter of moments. In addition to terrain variations, the transportation operation exposes the MTS to various kinds of public domain, to include urban and country settings.*

24.1 Introduction

Overview

A well-designed physical security system contains elements of detection, delay, and response, all of which are essential for the proper operation of the system. Likewise, a transportation PPS also contains the same elements:

- ***Detection*** initiates an alarm if an unauthorized entry or boundary penetration of the vehicle occurs. Assessment, a part of detection, is the examination of these alarms to determine if they constitute a legitimate security breach. If the alarm is valid, it is essential that the adversaries not be able to complete the sabotage or theft of material before the response force can arrive.

- ***Delay*** is essential to slow down the adversary and give the response force more time to respond. No system by technology alone can withstand an unimpeded, long-term attack.

- A ***response force*** is required to interrupt and stop the attack, which is the third required element of a balanced physical security system.

The synergism that occurs between the guard force and the technology is one of the keys to an effective, balanced security system.

24.2 Transportation Safeguards

Transportation Security System Has Same PPS Elements as a Fixed Site

The same physical protection elements (detection, delay, and response) are provided in a somewhat different manner in a transportation security system. For this discussion, the transportation system is assumed to be a security-hardened material transporter accompanied by at least one separate vehicle carrying additional members of the response force. The transportation system can be described as a movable access control area with built-in delay systems. Instead of being at fixed stations, the guards also move with the convoy. The communication systems, both within the response force itself and to some central command post, become much more complex because of the movements of the various elements of the convoy, as well as the large separation distances that may exist between convoy elements and even larger distances between the convoy and the central command post or off-site response.

Response Force

The response force comes to the adversary versus at a fixed site where an adversary comes to the response force. The effect is that the adversary may pre-position themselves and place personnel devices. The adversary can “own” the position, particularly on remote routes.

Thus, the three basic security elements are still present in the transportation system, although their relative importance changes.

Detection

Access to the transport vehicle when it is moving would be very difficult and, when it is stopped, detection is provided by observation of its exterior by the response force accompanying the shipment. The detection and subsequent assessment will be accomplished primarily by direct human observation rather than relying upon technology, and will frequently occur almost simultaneously when members of the convoy become aware that they are under attack.

Needs for Access Delay Depend on How the Response Force Survives the Initial Attack

The synergistic balance of the technology and response force is important. If the size of the accompanying response force surviving the initial attack is substantial, the need for access delay diminishes. If, however, the number of response force personnel who survive the first portion of the attack is small, there needs to be a greatly increased time between the initiation of the attack and removal of the cargo in order to allow the remaining force time to redeploy to defend the cargo and/or for additional response personnel to arrive.

Differences in Security Imposed by Transportation

In many respects, ground transportation security is more challenging than security at a fixed site. Operation in the public domain is frequently required and the same degree of access limitation is not possible as it is in a protected fixed site. In addition, and perhaps even more importantly, an attack can occur anywhere along a route of up to several thousand miles, giving the adversary a wide choice of potential attack locations. And, in most cases, this choice could be in locations where it will be virtually impossible for any sizeable secondary response force to arrive within a useful period of time. Because of these differences, response force personnel in transit play a more dominant role in the security of a mobile system than they do for a fixed site. In all cases, however, the system time delay that is required to provide the response force the time to react must be provided primarily by transportation vehicle technology elements.

24.2.1 Facility Characterization

Characterize the Transport Vehicle Structure and Existing PPS

In the case of a material transport system (MTS), the facility is the transport system itself. Characterizing the MTS involves the same methodology as a fixed-site, but the components vary. First, the structure of the transport vehicle is characterized in terms of walls, ceiling, and floor. This is most often accomplished with engineering drawings and visual observation. Next, the analyst identifies any physical protection systems, to include operating systems such as communication and alarm annunciation.

Transportation Routes

Transportation routes should be reviewed in detail, with special attention to:

- potential danger zones or choke points
- locations for scheduled stops
- possible adversary infiltration and egress routes
- speed and distance, which affect the timing in which events occur. Vehicles traveling slower up a steep grade offer the adversaries a better target than one moving faster on a level road.

Analysts should perform security surveys prior to the departure of the transport(s).

Understand the Operating States for a Transport System

A transport has various operating states, which include:

- stopped at a scheduled (predetermined) location - day or night,
- stopped at an unscheduled location - day or night,
- rolling to a stop - day or night,
- moving at various speeds - day or night,

Each state may be affected by different types of terrain and environments.

Convoy Configuration

It is important to fully understand the transportation vehicle and the states of the convoy as part of the MTS characterization. The convoy distribution must be balanced between being distributed far enough to survive initial adversary ambush yet close enough to respond, interrupt, and stop the adversary before they can complete their objective. Once this is fully understood the second step of the DEPO, which is the characterization of the existing PPS, may begin.

24.2.2 Detection Requirements

Response Force Provides Detection

All movements of special nuclear material outside the protected area of a fixed site must be accompanied by response force personnel who observe the vehicle at all times. This would require personnel in the material transport vehicle as well as escorts in front of and behind the vehicle. These response force personnel are continuously observing the surface of the vehicle and serve as detection and assessment elements of the security system. Response force capabilities depend on tactics and terrain – rural versus urban. In addition, some effective means of entry control and interior intrusion detection would serve to give an alarm if unauthorized personnel attempt to enter the material transport vehicle. For Category I and II shipments of SNM, it is recommended that the access control system incorporate a two-person rule to minimize threats from the insider.

24.2.3 Delay Requirements

Delay Time Required

An attack may occur in remote areas of the route where sizeable secondary response assistance is not available immediately. The required delay is that time needed by the response forces who accompany the shipment to deploy in the manner to best protect the shipment.

If the analysis shows that response forces external to the convoy are needed, the ***minimum delay time*** is the time estimated to allow this response to arrive before the cargo has been removed from the scene or sabotaged.

Depending upon composition and spacing of the convoy vehicles and the response force tactics, sending additional forces could take several minutes.

Example Delay Techniques

It is difficult to design delay systems that will ensure these types of delays for all possible sets of adversary capabilities and tactics, but such systems, using items such as visual obscurants, vault-like structures, gases, hardened containers, razortape, chains, etc., can be designed that will successfully delay most of these attacks.

Delay and Response Force Are the Main Elements

Without the delay and an effective response provided by the accompanying response force, it is very difficult to design an effective PPS. It is also nearly impossible to develop technology-only security systems that can withstand a well-planned attack for significant amounts of time that will allow for secondary responders to arrive from a more distant location.

Lethal vs. Nonlethal Technology

In this course, we assume that non-lethal deterrents are used in the delay system. Use of lethal deterrents has the potential to significantly increase delay time at a lower hardware cost; however, the social and potential legal costs of accidental or inappropriate activation of these deterrents may outweigh their effectiveness advantage.

24.2.4 Response Requirements

Number of Response Forces Required

The number of guards assigned to transportation depends on:

- their relatively high cost since they must be on duty around the clock and be well trained and highly capable, and
- the estimated size, capability, and objectives of the attacking force.

The defined ratio of defenders to attackers for fixed sites may be somewhat low for ground transportation systems since the engagement will not occur on "friendly ground" and thus will not be as easily defended. In addition, response force personnel may be more vulnerable to a surprise attack while they are exposed to the public.

Communication Requirements

Communications are necessary:

- ***between the various elements of the convoy*** to provide an essential detection and assessment function.

- ***among the members of the security force*** should they have to deploy, for organizing and carrying out a coordinated defense.

- ***between the convoy and the central control station*** for reporting back to the central station to notify authorities that an incident has occurred and for summoning secondary response force reinforcements, if needed.

The relative degree of importance of each of these systems depends on procedures, composition of the convoy, and where it operates. It must be determined on a case-by-case basis.

24.3 Transport Vehicle

Access Delay Also Provides Ballistic Protection

The design of the material transport vehicle (transporter, see Figure 24-1) must provide sufficient access delay so the convoy response force can respond to an attack and defeat the adversary before the adversary task is accomplished. An enhanced transporter can provide increased access delay and ballistic protection together with enhanced safety, while potentially reducing the required number of accompanying security escorts. In addition, vehicle entry control and response force communication capabilities are essential to protect nuclear material in transit.

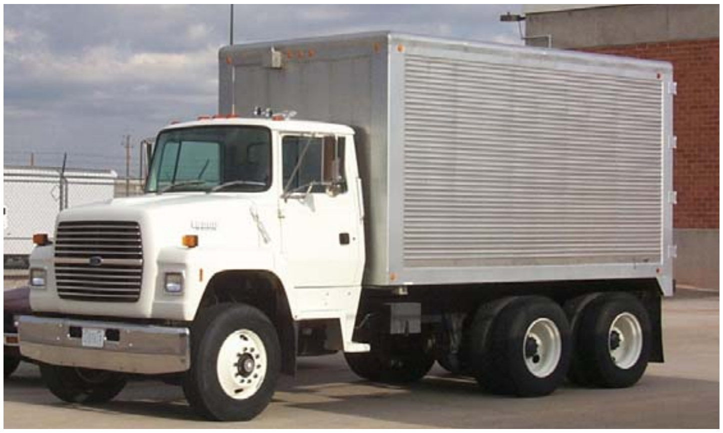


Figure 24-1. Example of a Transporter

24.3.1 Basic Vehicle Requirements

Ballistic Protection, Entry Control, and Access Delay

The primary security requirements for the transporter vehicle are ballistic protection, access control, and access delay for the vehicle. Methods include:

- a very strong vault wall panel design
- robust access doors for the cargo compartment
- two-person entry controls
- vehicle immobilization hardware.

Safety Enhancements

Safety enhancements are required to help reduce impact effects in an accident, especially to reduce the risks from fire during an accident. For example, specific design goals could be to provide thermal protection for vault cargos for 20 minutes in a 1000° C fire. Design features include:

- a strong vault structure,
- strong cargo tie downs,
- new insulating foam materials, and
- limited vehicle fuel capacity.

These basic design features are passive, which substantially reduce concerns with safety and premature initiation or failure of any active delay systems.

24.3.2 Vault

Construction

The vehicle vault should be an integral structure incorporating panels of multi-layer steel corrugated armor, rigid foam, inner and outer stainless steel skins, and other barrier materials on a tubular steel frame. The vault structure should be designed “fracture-tough” with special steels for primary load members. The corrugated armor together with the overall thickness of the wall panels provide access delay and ballistic protection for the cargo.

Vault Cargo Volume

The vault cargo volume should be designed to accommodate as broad a range of container sizes and weights as possible. The vehicle capacity is dependent upon the truck chassis selected for the vehicle and whether the cab armor option is selected. Aircraft-type cargo tie down tracks should be provided in the vault floor and perhaps on the vault sidewalls, and roof. This arrangement allows flexible cargo tie down schemes for containers, palletized loads, or sidewall racks.

24.3.3 Entry Control

Use Two-Person Rule and Hardware for Entry Control

An entry control system is needed to control authorized access to the cargo vault area. The system should provide for two-person access control. An example would be a three to eight digit individual code entry from a plug-in, limited-view, scramble pad pendant. An electronic lock that can accommodate up to 1000 valid user codes with limited try features, and easy code entry and recode is recommended.

Electromechanical Door Lock

Output from the entry control system should control an electromechanical door lock incorporated into the door. This type of mechanism incorporates aircraft-quality actuators for operating a locking block upon receipt of a valid entry code. The locking block drives multiple, distributed locking pins that physically secure the door to the vault frame. A passive locking wedge should provide hinge-side locking. The door lock should also use stressed glass and thermal relockers to provide additional forced entry protection.

24.3.4 Chassis

Design Considerations

The cargo vault could be installed on essentially any vehicle chassis capable of carrying the necessary payload. A heavy-duty front axle allows for the additional weight of cab armor if required. The vehicle should:

- meet all legal requirements for operation on public streets and all applicable federal regulations.
- have an engine powerful enough to allow cruising at 88 km/hr and operation on 10% grades.
- include air brakes, air suspension, and a cold weather starting package.

24.3.5 Immobilization

Prevent Adversaries from Driving Vehicle

Immobilization capabilities can prevent an adversary from simply driving the vehicle away if it is captured. The vehicle incorporates a number of chassis immobilization features that can be activated from the vehicle cab or remotely from one of the escort vehicles.

Immobilization Methods

Chassis immobilization methods could include:

- an engine fuel shutoff device,
- a turbo air shutoff valve,
- an accelerator linkage disablement device, and
- controlled braking of the vehicle to bring it to a stop in several seconds after initiation.

The immobilization system may be reversible either by a variable timer or by manual resets.

24.4 Analysis of System Effectiveness

Path Analysis Not as Useful for Mobile Application; Use Scenario Analysis

The third step of the DEPO is to analyze the effectiveness of the PPS to ensure that the level of risk is acceptable. For a fixed facility, it is recommended that a combination of a path analysis and a scenario analysis be used to evaluate a PPS. However, for an MTS, there are limited layers of protection that an adversary team must penetrate to gain access to the target. This situation makes a path analysis less suitable for analyzing the effectiveness of the PPS of a material transportation system. A more effective tool for systems with limited layers of protection is the scenario analysis. The process of a scenario analysis is covered in greater detail in *Scenario and Path Analysis,* Session 17, of this course. The methodology for conducting a scenario analysis is the same for a fixed site as it is for a MTS.

Adversary Defeat Methods

In general terms, the analyst must determine the defeat methods the adversary may use:

- to stop the vehicle (if is not already stopped).
- penetrate the transporter vault.

- acquire or sabotage material.
- defeat the response force.

Considerations in Scenario Development

In scenario development, consider:

- likely locations and times of the attack
- use of diversion, vehicle bomb, attacks on the response force during meal breaks
- the transporter could be separated from the response force and therefore reduce the probability of interruption of the adversary.

Number of Adversaries

The level of detail in the scenario must be sufficient to ensure all adversary tasks are fully understood and credible. Questions to consider include:

- How many adversaries will be used to breach the vehicle?
- How many adversaries will be required to acquire and move target material?
- Will the adversary use assault teams to engage the response force?

Engagement Analysis

Once the scenarios are fully understood and defined, an engagement analysis should be conducted to determine if the response force is able to deploy effectively and then interrupt and neutralize the adversary team. This is typically conducted with computer models, subject matter expertise, and force-on-force exercises.

24.5 Summary

PPS Considerations for Transport Vehicle: Detect, Delay, Respond

Just as the physical protection system for a fixed site requires a careful balance of detection, delay, and response elements, so does a physical protection system for a transport vehicle carrying special nuclear material:

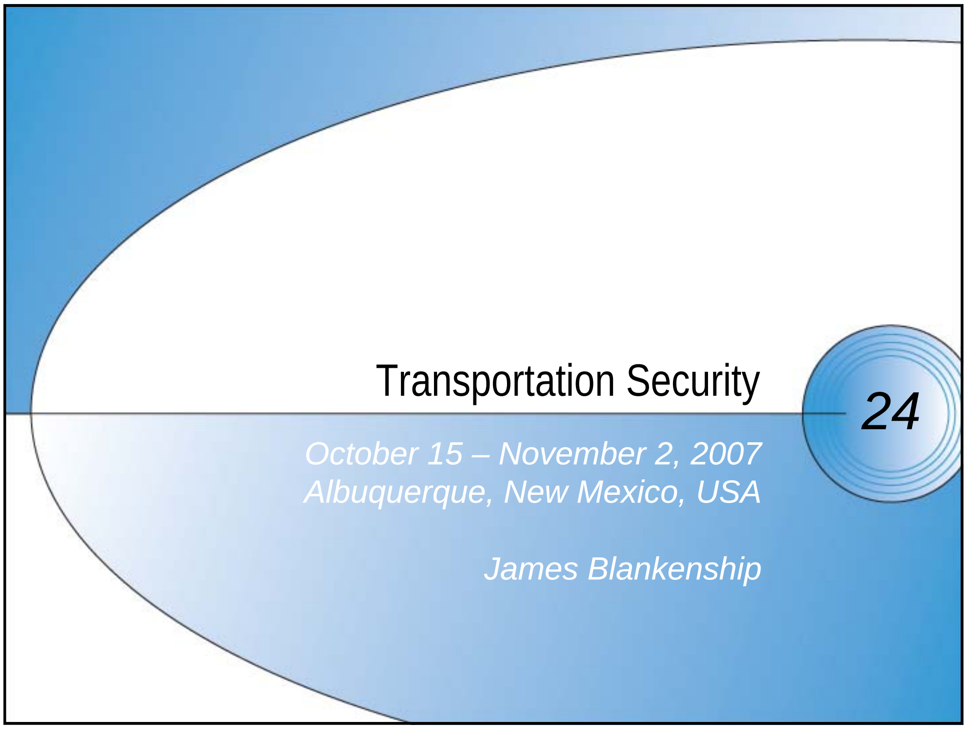
- ***Detection*** is accomplished by convoy observation or by interior intrusion detection devices.
- ***Delay*** can be effected by building a vault-type enclosure on a truck frame.
- ***Response*** will be from convoy response forces and should be relied upon in conducting engagement analysis since local law enforcement may not be available at the time and/or location of an attack.

Analysis methods may be used to determine if the overall safeguards elements fit together to provide a level of safeguards that is determined to be adequate. *The Convention on the Physical Protection of Nuclear Material* (INFCIRC/274 published by the IAEA) clearly places the responsibility on the State to provide the required level of physical protection of all nuclear material in international transport, but preserves the sovereign right of States to determine the manner by which they will provide that level of protection. The three principal international documents that provide guidelines for the physical protection of nuclear materials in transit are:

- *The Guidelines of the Nuclear Exporters Group* (INFCIRC/254);

- *The Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225); and

- The Convention on the Physical Protection of Nuclear Material (the CPPNM, INFCIRC/274)

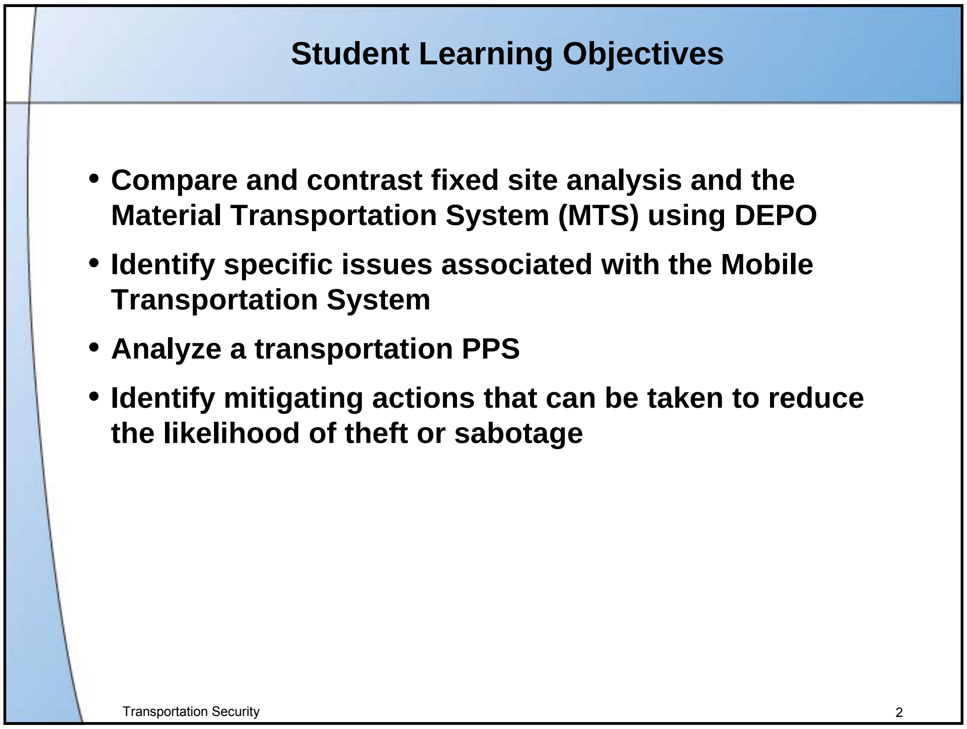


Transportation Security

24

October 15 – November 2, 2007
Albuquerque, New Mexico, USA

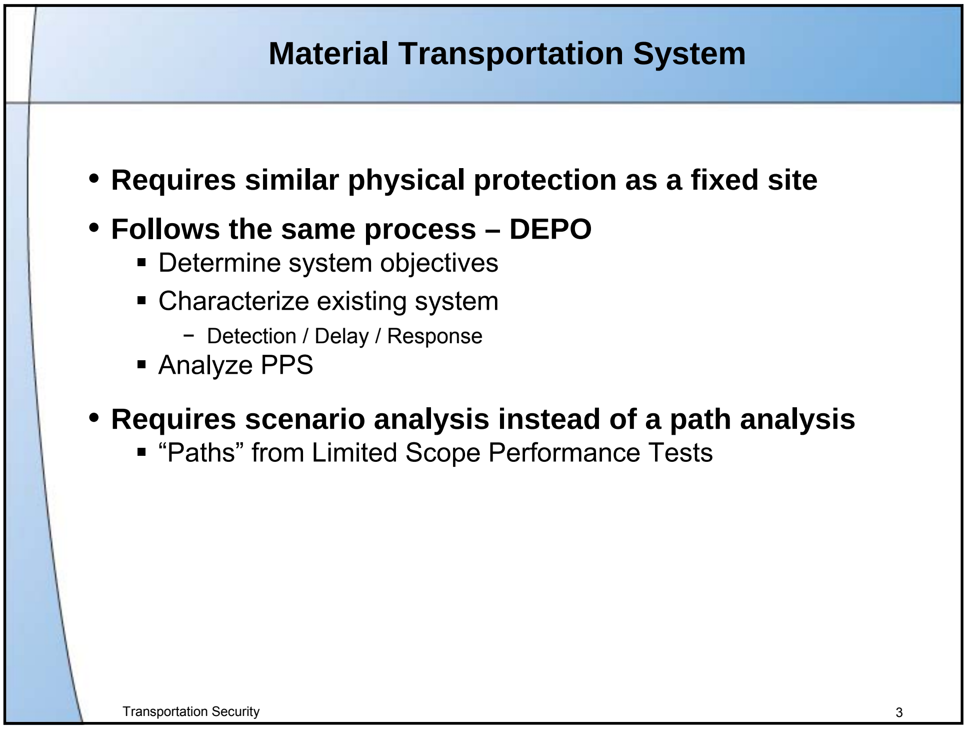
James Blankenship



Student Learning Objectives

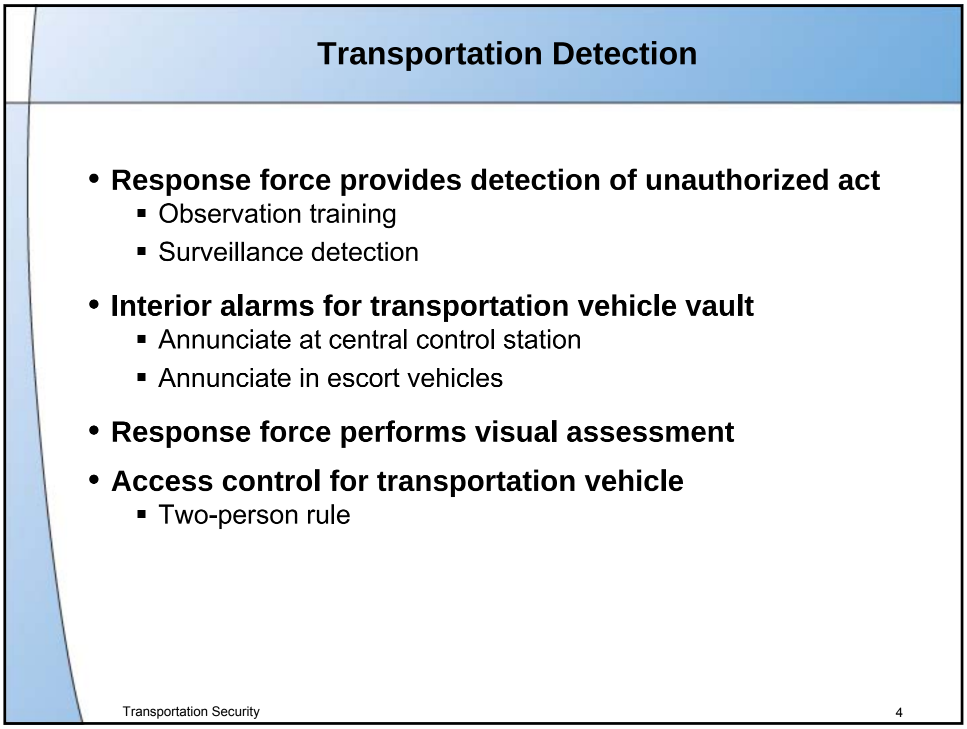
- **Compare and contrast fixed site analysis and the Material Transportation System (MTS) using DEPO**
- **Identify specific issues associated with the Mobile Transportation System**
- **Analyze a transportation PPS**
- **Identify mitigating actions that can be taken to reduce the likelihood of theft or sabotage**

Transportation Security 2



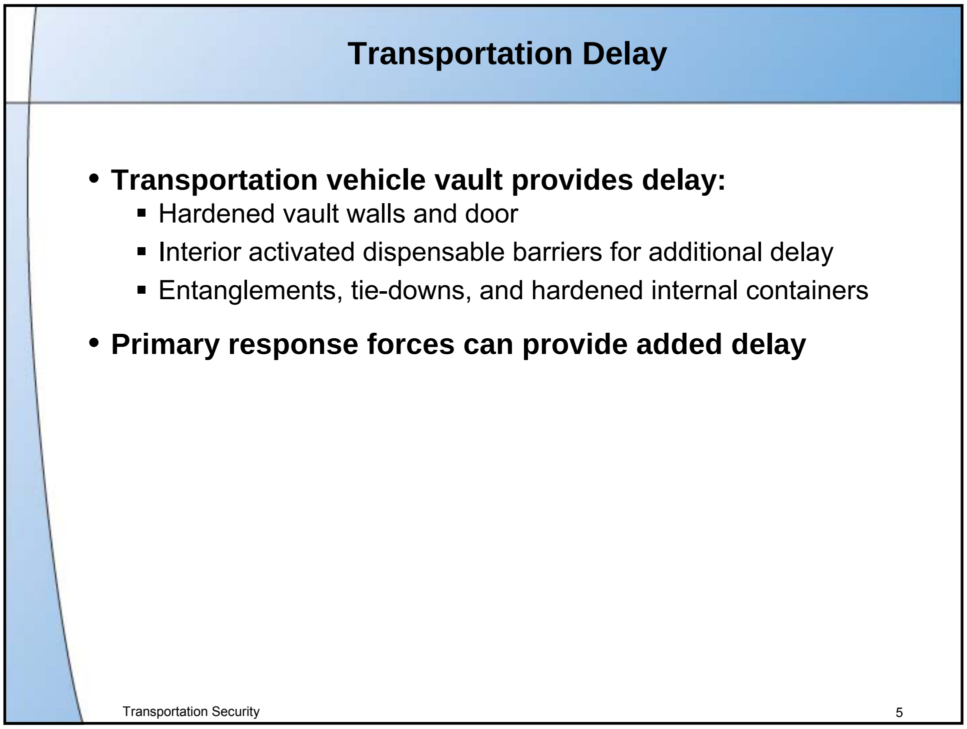
Material Transportation System

- **Requires similar physical protection as a fixed site**
- **Follows the same process – DEPO**
  - Determine system objectives
  - Characterize existing system
    - Detection / Delay / Response
  - Analyze PPS
- **Requires scenario analysis instead of a path analysis**
  - “Paths” from Limited Scope Performance Tests



Transportation Detection

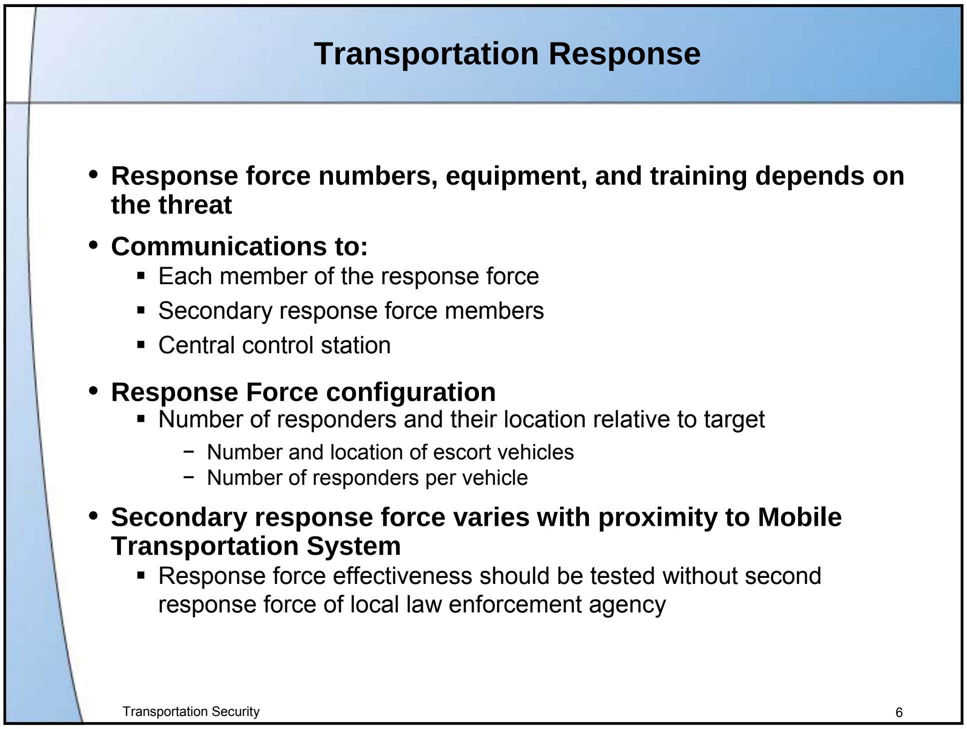
- **Response force provides detection of unauthorized act**
  - Observation training
  - Surveillance detection
- **Interior alarms for transportation vehicle vault**
  - Annunciate at central control station
  - Annunciate in escort vehicles
- **Response force performs visual assessment**
- **Access control for transportation vehicle**
  - Two-person rule



Transportation Delay

- **Transportation vehicle vault provides delay:**
  - Hardened vault walls and door
  - Interior activated dispensable barriers for additional delay
  - Entanglements, tie-downs, and hardened internal containers
- **Primary response forces can provide added delay**

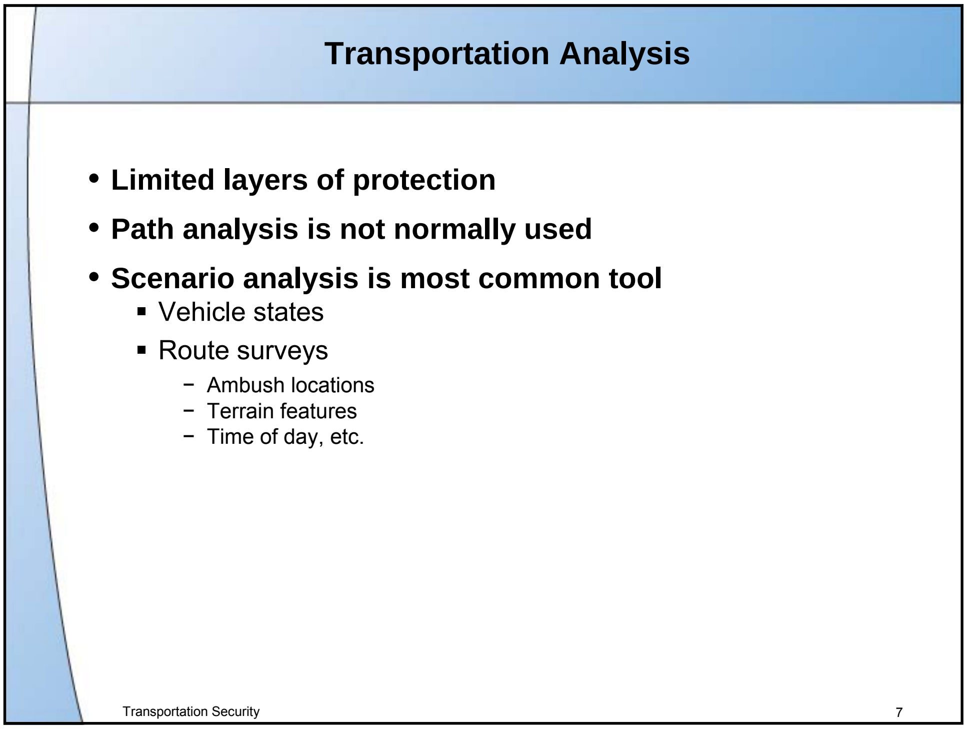
Transportation Security 5



Transportation Response

- **Response force numbers, equipment, and training depends on the threat**
- **Communications to:**
  - Each member of the response force
  - Secondary response force members
  - Central control station
- **Response Force configuration**
  - Number of responders and their location relative to target
    - Number and location of escort vehicles
    - Number of responders per vehicle
- **Secondary response force varies with proximity to Mobile Transportation System**
  - Response force effectiveness should be tested without second response force of local law enforcement agency

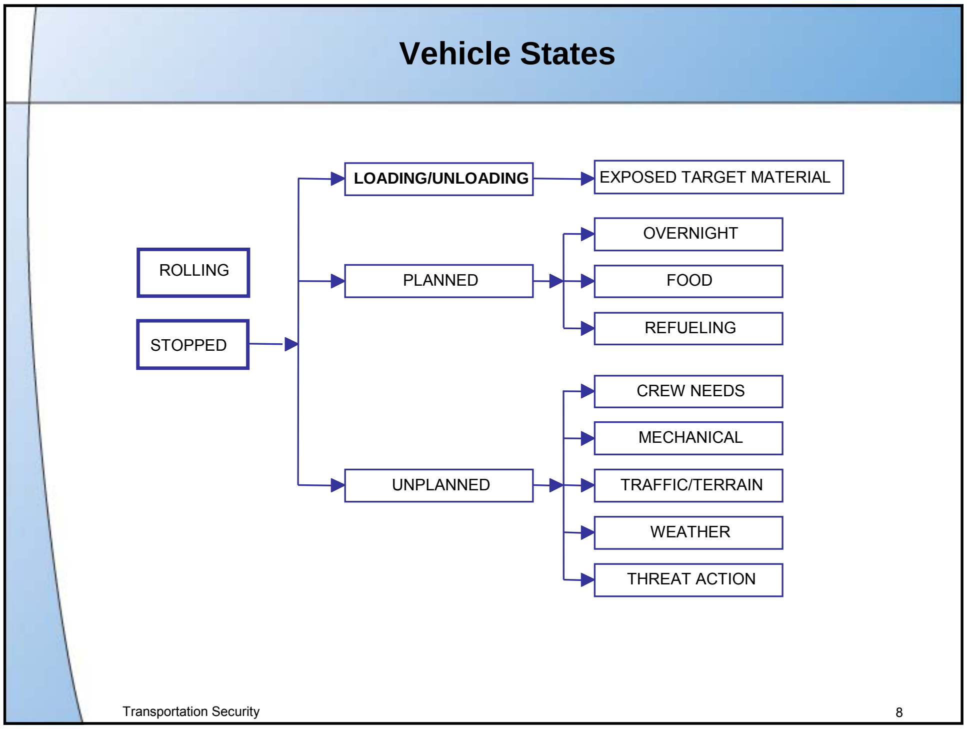
Transportation Security 6



Transportation Analysis

- **Limited layers of protection**
- **Path analysis is not normally used**
- **Scenario analysis is most common tool**
  - Vehicle states
  - Route surveys
    - Ambush locations
    - Terrain features
    - Time of day, etc.

Transportation Security 7



Vehicle States

ROLLING

STOPPED

LOADING/UNLOADING

EXPOSED TARGET MATERIAL

PLANNED

OVERNIGHT

FOOD

REFUELING

UNPLANNED

CREW NEEDS

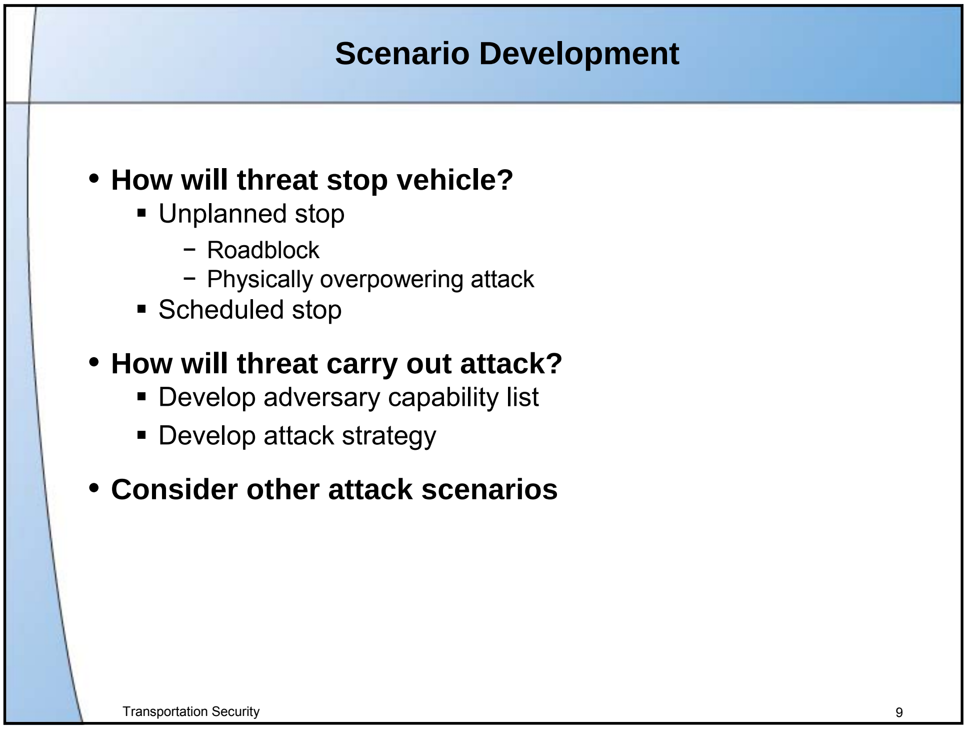
MECHANICAL

TRAFFIC/TERRAIN

WEATHER

THREAT ACTION

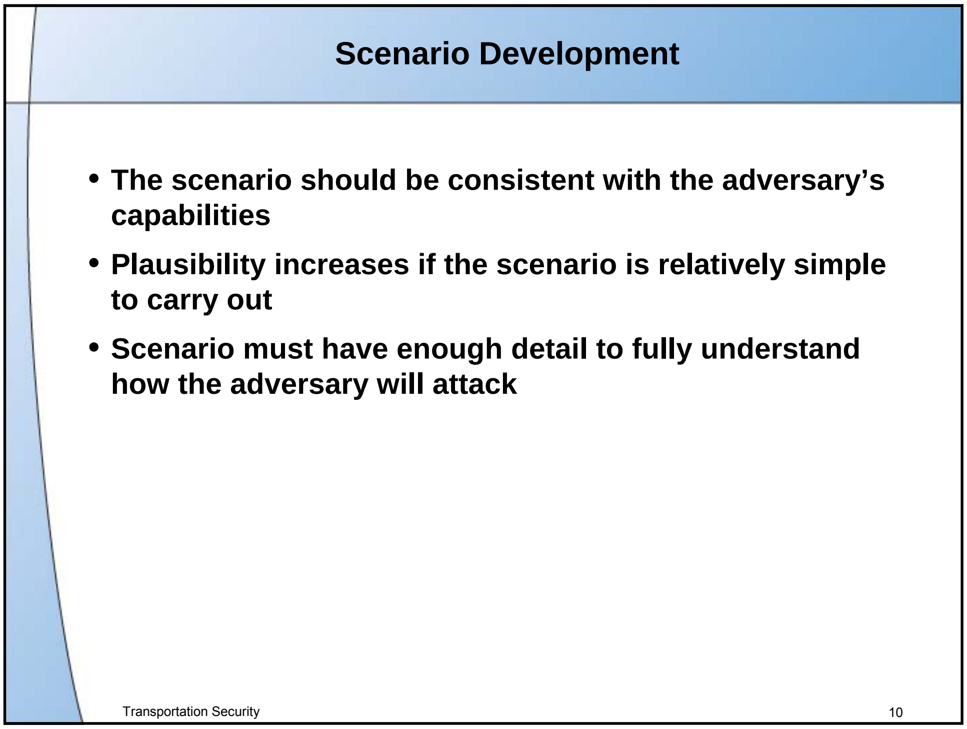
Transportation Security 8



Scenario Development

- **How will threat stop vehicle?**
  - Unplanned stop
    - Roadblock
    - Physically overpowering attack
  - Scheduled stop
- **How will threat carry out attack?**
  - Develop adversary capability list
  - Develop attack strategy
- **Consider other attack scenarios**

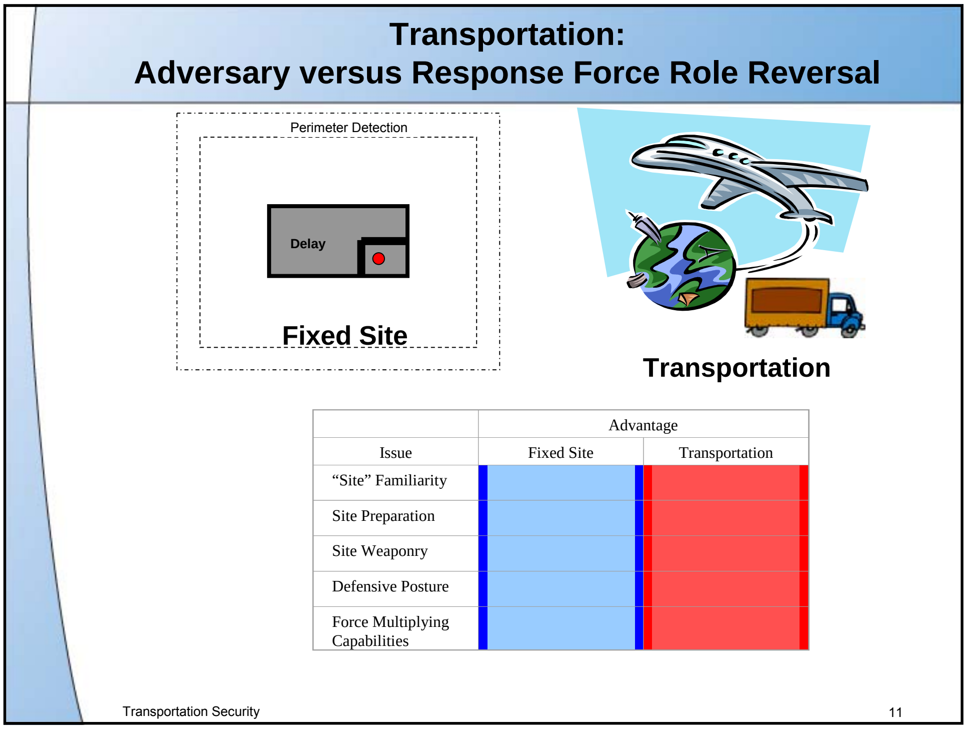
Transportation Security 9



Scenario Development

- **The scenario should be consistent with the adversary's capabilities**
- **Plausibility increases if the scenario is relatively simple to carry out**
- **Scenario must have enough detail to fully understand how the adversary will attack**

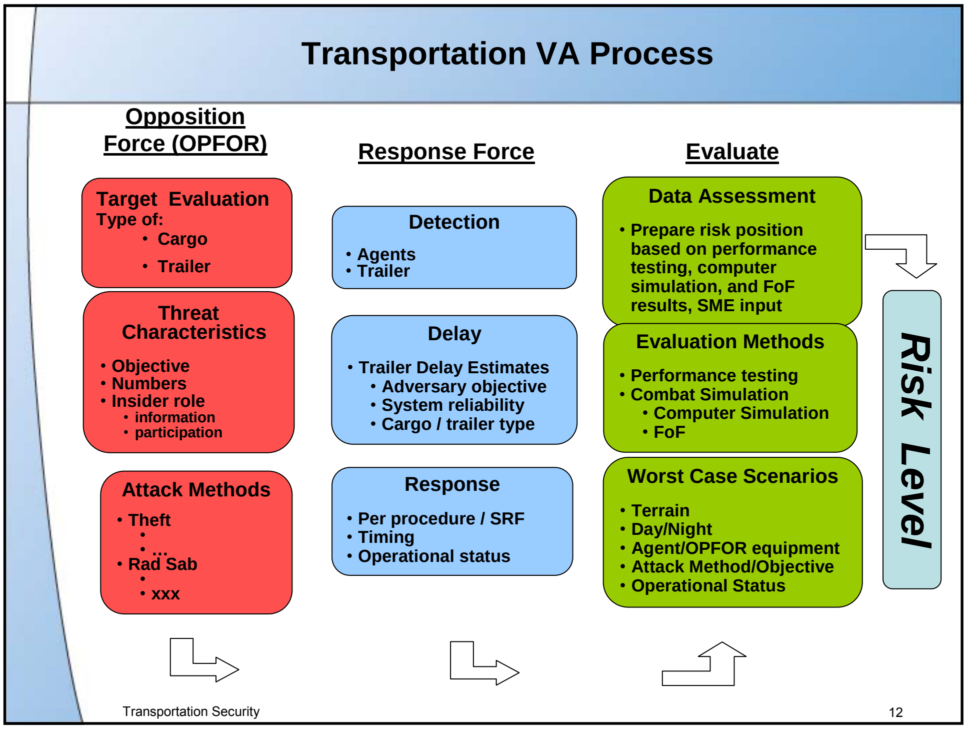
Transportation Security 10



Transportation: Adversary versus Response Force Role Reversal

	Advantage	
Issue	Fixed Site	Transportation
“Site” Familiarity	🟦	🟥
Site Preparation	🟦	🟥
Site Weaponry	🟦	🟥
Defensive Posture	🟦	🟥
Force Multiplying Capabilities	🟦	🟥

Transportation Security 11



Transportation VA Process

Opposition Force (OPFOR)

Target Evaluation
Type of:
- Cargo
- Trailer

Threat Characteristics
- Objective
- Numbers
- Insider role
  - information
  - participation

Attack Methods
- Theft
  -
  - ...
- Rad Sab
  -
  - xxx

Response Force

Detection
- Agents
- Trailer

Delay
- Trailer Delay Estimates
  - Adversary objective
  - System reliability
  - Cargo / trailer type

Response
- Per procedure / SRF
- Timing
- Operational status

Evaluate

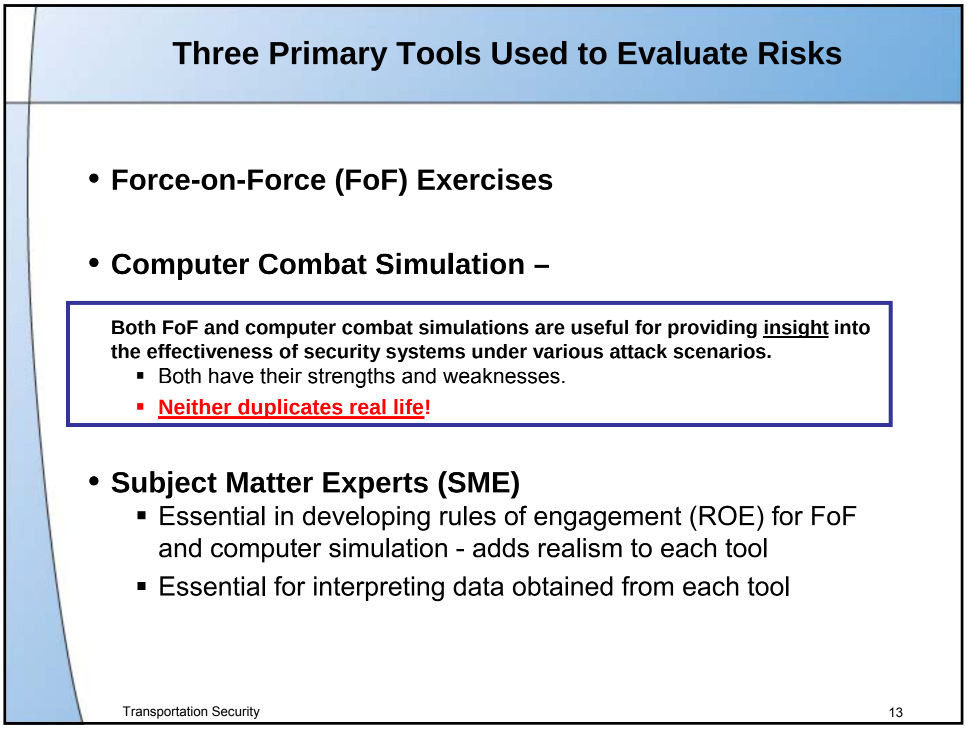
Data Assessment
- Prepare risk position based on performance testing, computer simulation, and FoF results, SME input

Evaluation Methods
- Performance testing
- Combat Simulation
  - Computer Simulation
  - FoF

Worst Case Scenarios
- Terrain
- Day/Night
- Agent/OPFOR equipment
- Attack Method/Objective
- Operational Status

Risk Level

Transportation Security 12



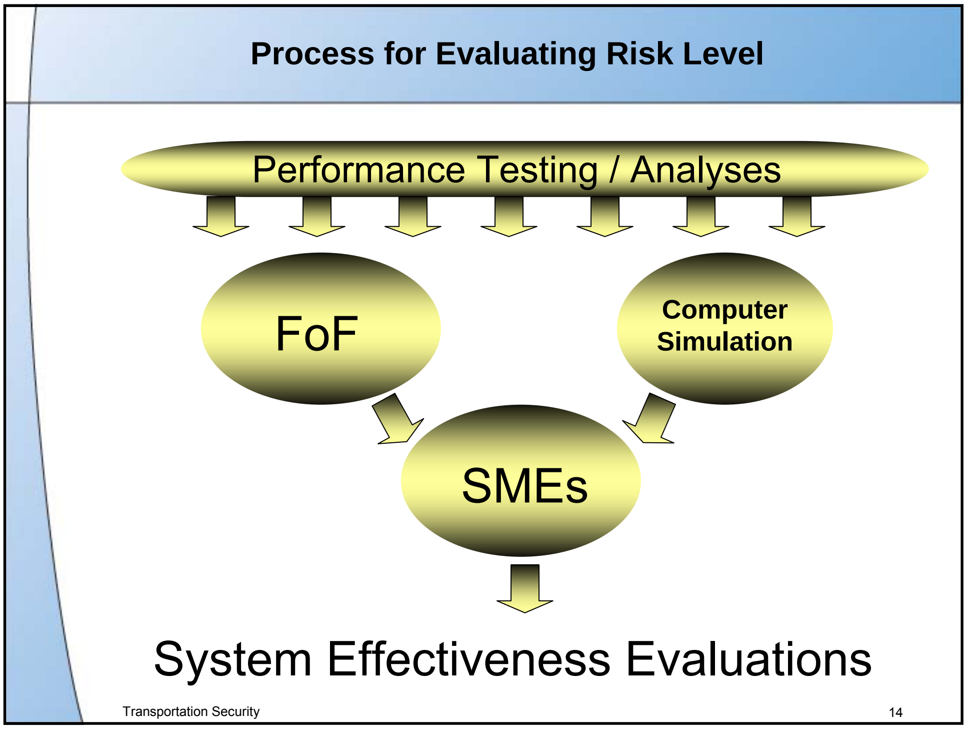
Three Primary Tools Used to Evaluate Risks

- **Force-on-Force (FoF) Exercises**
- **Computer Combat Simulation –**

Both FoF and computer combat simulations are useful for providing <u>insight</u> into the effectiveness of security systems under various attack scenarios.

- Both have their strengths and weaknesses.
- **<u>Neither duplicates real life</u>!**

- **Subject Matter Experts (SME)**
  - Essential in developing rules of engagement (ROE) for FoF and computer simulation - adds realism to each tool
  - Essential for interpreting data obtained from each tool



Process for Evaluating Risk Level

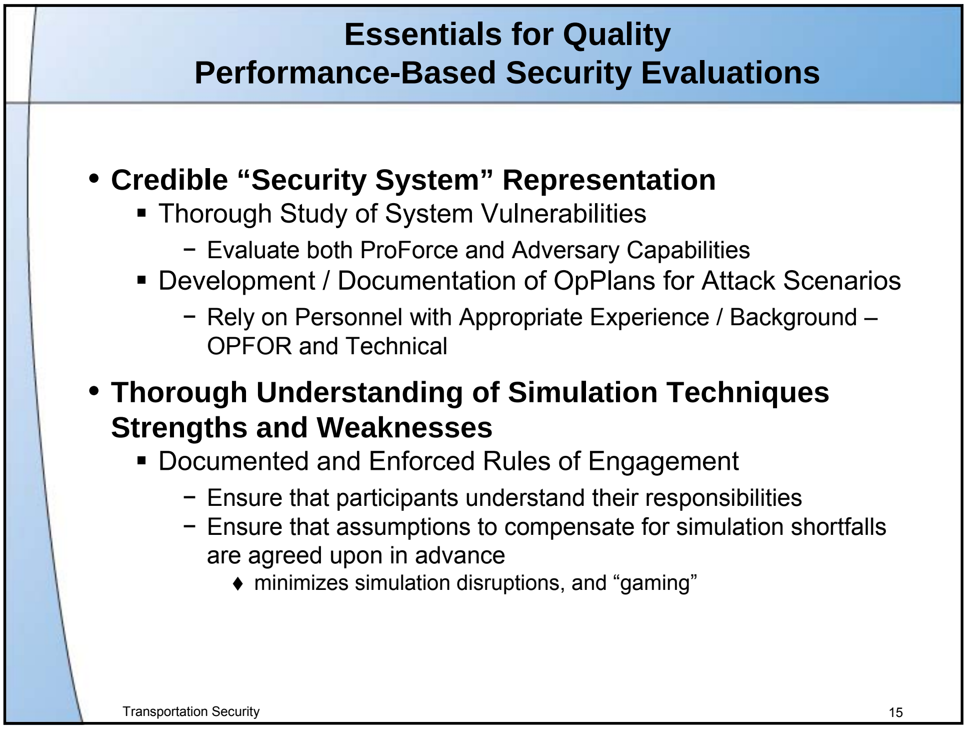
Performance Testing / Analyses

FoF

Computer Simulation

SMEs

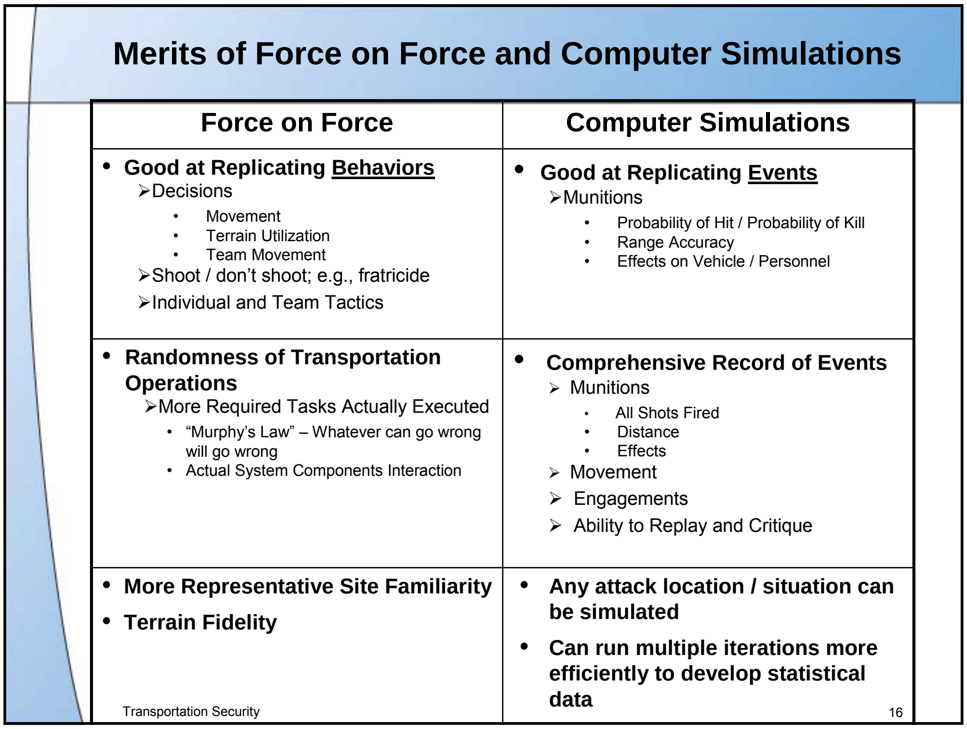
System Effectiveness Evaluations



Essentials for Quality Performance-Based Security Evaluations

- **Credible "Security System" Representation**
  - Thorough Study of System Vulnerabilities
    - Evaluate both ProForce and Adversary Capabilities
  - Development / Documentation of OpPlans for Attack Scenarios
    - Rely on Personnel with Appropriate Experience / Background – OPFOR and Technical
- **Thorough Understanding of Simulation Techniques Strengths and Weaknesses**
  - Documented and Enforced Rules of Engagement
    - Ensure that participants understand their responsibilities
    - Ensure that assumptions to compensate for simulation shortfalls are agreed upon in advance
      - ♦ minimizes simulation disruptions, and "gaming"

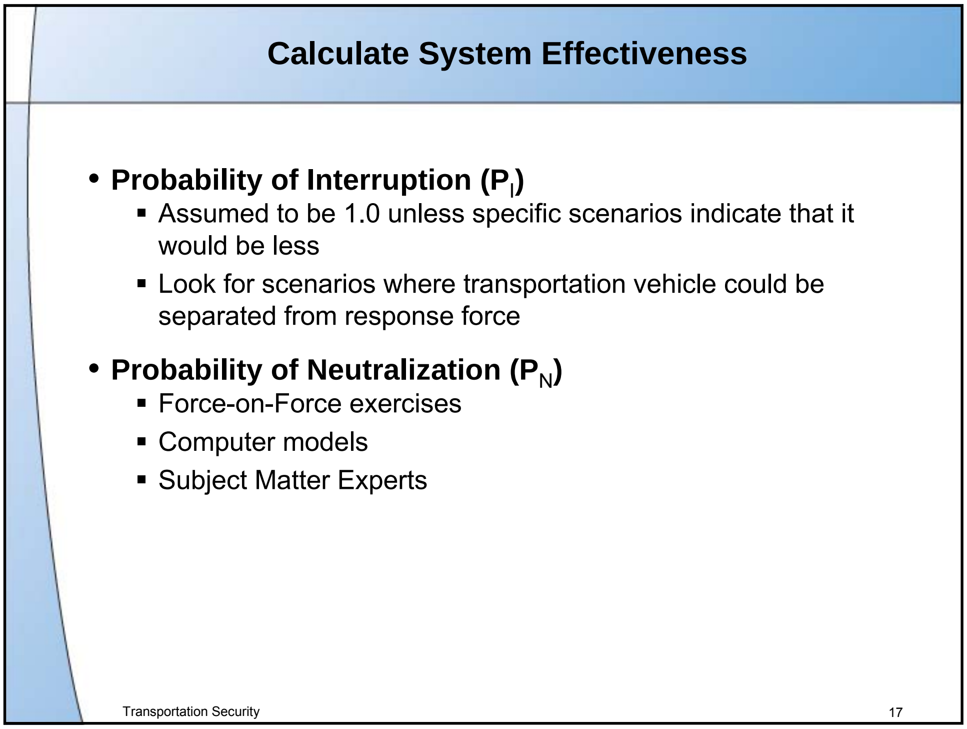
Transportation Security 15



Merits of Force on Force and Computer Simulations

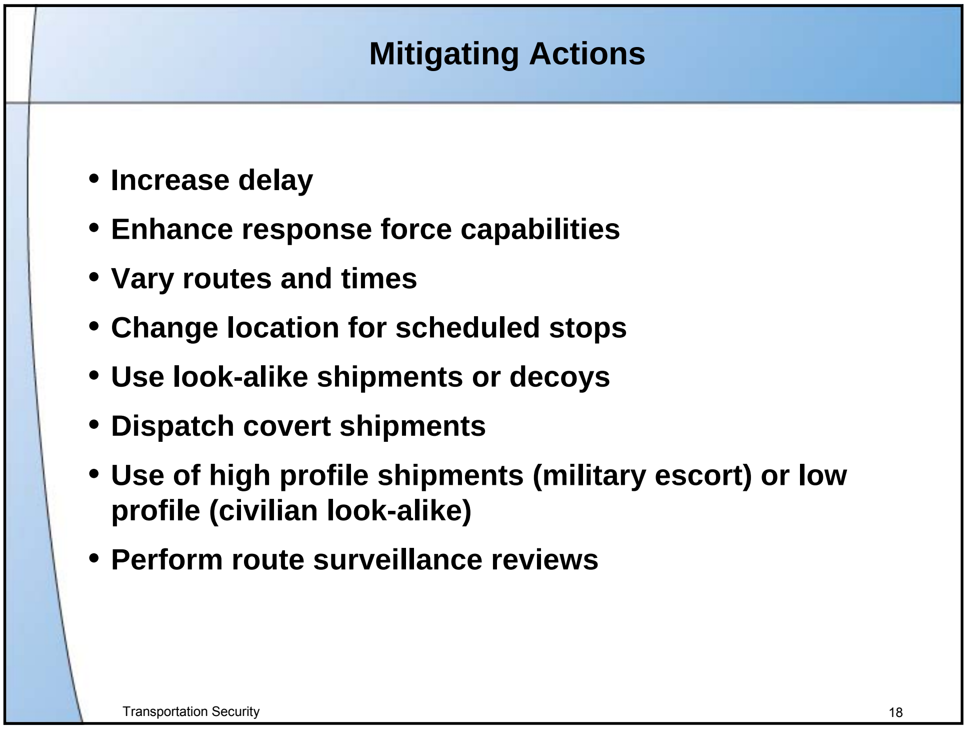
Force on Force	Computer Simulations
• **Good at Replicating <u>Behaviors</u>** ➢Decisions • Movement • Terrain Utilization • Team Movement ➢Shoot / don't shoot; e.g., fratricide ➢Individual and Team Tactics	• **Good at Replicating <u>Events</u>** ➢Munitions • Probability of Hit / Probability of Kill • Range Accuracy • Effects on Vehicle / Personnel
• **Randomness of Transportation Operations** ➢More Required Tasks Actually Executed • "Murphy's Law" – Whatever can go wrong will go wrong • Actual System Components Interaction	• **Comprehensive Record of Events** ➢ Munitions • All Shots Fired • Distance • Effects ➢ Movement ➢ Engagements ➢ Ability to Replay and Critique
• **More Representative Site Familiarity** • **Terrain Fidelity**	• **Any attack location / situation can be simulated** • **Can run multiple iterations more efficiently to develop statistical data**

Transportation Security 16



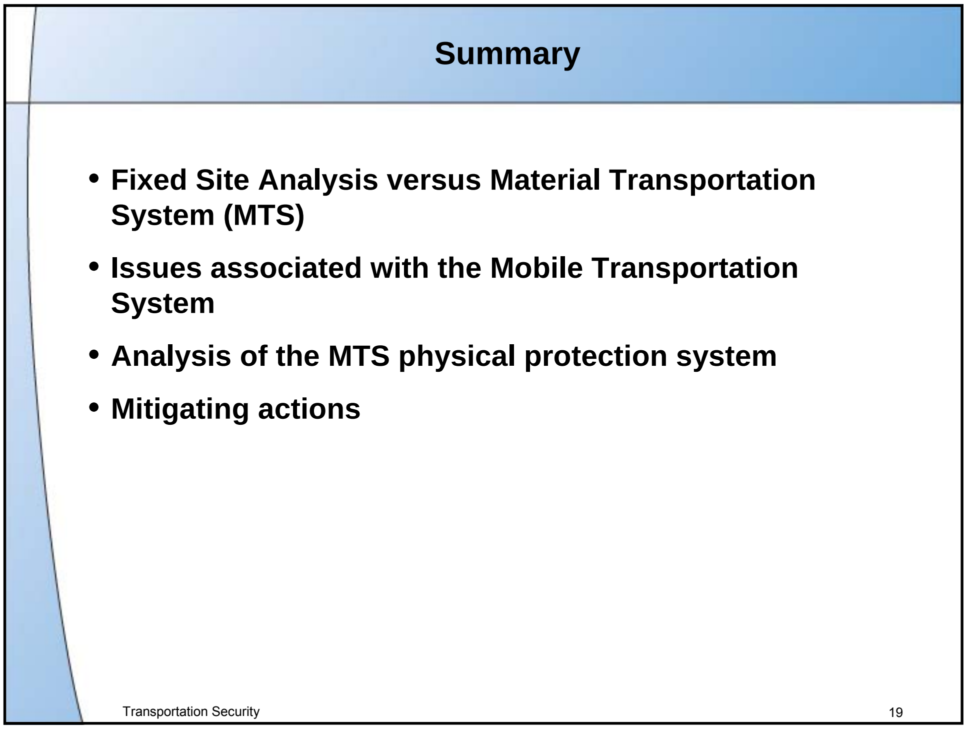
Calculate System Effectiveness

- **Probability of Interruption (P_I)**
  - Assumed to be 1.0 unless specific scenarios indicate that it would be less
  - Look for scenarios where transportation vehicle could be separated from response force
- **Probability of Neutralization (P_N)**
  - Force-on-Force exercises
  - Computer models
  - Subject Matter Experts



Mitigating Actions

- **Increase delay**
- **Enhance response force capabilities**
- **Vary routes and times**
- **Change location for scheduled stops**
- **Use look-alike shipments or decoys**
- **Dispatch covert shipments**
- **Use of high profile shipments (military escort) or low profile (civilian look-alike)**
- **Perform route surveillance reviews**



Summary

- Fixed Site Analysis versus Material Transportation System (MTS)
- Issues associated with the Mobile Transportation System
- Analysis of the MTS physical protection system
- Mitigating actions

Transportation Security 19

Subgroup 24S
Transportation Security

Session Objectives

After the session, the participants will be able to do the following:

1. Recognize that the systems analysis approach to physical protection works for mobile targets in addition to fixed targets.
2. Contrast the importance of detection, delay, and response elements between fixed sites and mobile targets.
3. Use a scenario analysis to measure the effectiveness of a PPS for a mobile target.
4. State the universal applicability of the DEPO process to all parts of the nuclear fuel cycle, including transportation.

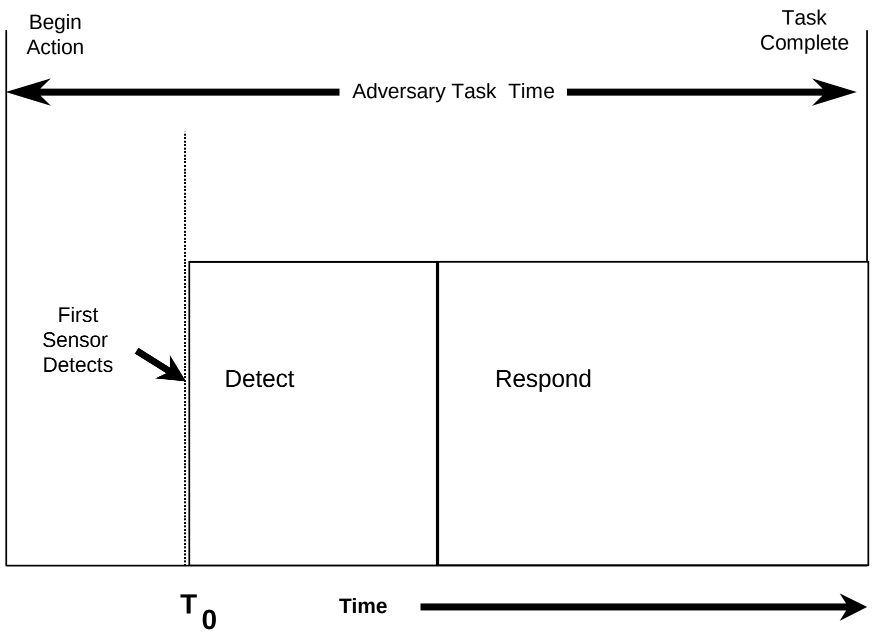
Exercise 1 - Contrasting Detection / Delay / Response

Many of the PPS elements that are present in a transportation physical protection system are present in the PPS of a fixed site. Because of the different "facility" characteristics the three PPS elements (detection, delay, and response) take a different importance. In the table below, list the methods of accomplishing detection, delay, and response for a transportation PPS analysis.

	Fixed Site	Transportation
Detection	Isolation zone	
	Exterior intrusion sensors	
	Roving patrols	
	CCTV alarm assessment	
	Access Control	
	Interior intrusion sensors	
Delay	Distances	
	Hardness of walls and doors	
	Response Forces	
	Task time to sabotage or acquire target	
	Activated Barriers	
Response	On-site response force	
	Police assistance	
	FBI and military if necessary	
	Radio communication and telephone	

Exercise 2 – Relationship Diagram of PPS for Transportation

Recall the diagram below of the relationship of detection, delay, and response for a fixed site. Draw over the top of that diagram, a similar diagram for a transportation PPS.



Exercise 3 – Scenario Analysis of a Material Transportation System

For this exercise, the following transportation system should be used:

Assumptions:

- The transportation of Category I Special Nuclear Material, which is a viable theft target.
- The consequence of theft for this target is 0.7 as defined by the Competent Authority.

Delay and Detection

Material Storage—The material is stored in a heavy-duty shipping cask designed to provide a limited amount of delay. This shipping cask is stored in the vehicle with four sets of tie-down chains with high security padlocks on each tie-down.

Cargo Vault—The cargo vehicle is equipped with a cargo vault. The vault is constructed to provide a significant degree of delay on the walls, ceiling, and floor.

- There are **no** activated dispensable barriers in the vault.
- The doors to the vault are high-security vault doors equipped with locking pins and protected hardware.
- There is a two-person access control system installed on the vault doors.
- There are no interior alarms on the vault.
- The response force members in the convoy provide all detection and assessment.

Response Force

A trained response force member drives the transportation vehicle and three other vehicles escort the vehicle with two responders in each vehicle. Each response force member is highly trained in military tactics and equipped with an automatic rifle, a pistol, and a two-way radio. The escort vehicles are never more than 60 kilometers away from the transporter at any time and at least two of the escort vehicles must have visual contact with the transporter at all times.

Adversary task times (seconds)	
Breach vehicle vault	180
Defeat each shipping cask tie-down	30 (30 x 4 = 120)
Open cask and acquire material	60
Exit vehicle vault	10

Your task is to refer to the DBT developed in the Threat Definition Subgroup (5) and develop a credible scenario that this adversary team could use to attempt the theft of SNM being shipped. Assume the attack occurs during daylight hours and that the convoy has been stopped by a staged traffic accident. Assume that the P_I for this scenario is "1" because of the proximity of the response force. Use the computer model provided in Session 24 Neutralization Analysis to evaluate the P_N for this scenario.

Describe scenario here

Time	Adversary Action	PPS Action	Notes
0:00			

Conduct P_N analysis and document results here

Calculate System Effectiveness

$P_E = P_I*P_N$

Can you identify any specific vulnerabilities?

What upgrade would you suggest to improve this PPS?

Application Considerations

1. The example solution to this problem assumes that the convoy guards are vulnerable to attack. Could they be better protected?

2. Do we need a higher ratio of guards to adversaries to protect material in transportation versus at a fixed facility?

3. What could be done to improve the response time from other agencies? Do you think the improvements would be worth the cost?

4. If transportation were by airplane, what changes would there be in detection, delay, and response?

5. If transportation were by ship on the ocean, what changes would there be in detection, delay, and response?

6. What would be the advantage of using dummy or secret shipments? What factor(s), if any, in evaluating risk would be changed by using secret shipments?

This page intentionally left blank

25. Introduction to the Final Exercise

Abstract. *Before beginning the comprehensive design and evaluation exercise, it is important to reconsider the design and review process that was presented in detail in this course. Basically, the designer or evaluator must determine the PPS objectives, design a new system or characterize an existing system, and then evaluate the PPS design. If the design is judged inadequate, then it must be upgraded and evaluated again. This process is repeated until an effective system is engineered. As an aid, the design and evaluation process has been broken down into steps. The first step is to characterize facility operations and conditions that influence physical protection. Next, define threats to determine what the protection must guard against. Also, identify targets or areas and materials that need to be protected. Then, identify the physical protection system or design a system to protect against the defined threats and to protect the identified targets. Finally, evaluate the physical protection effectiveness to determine whether or not upgrades or modifications are necessary. The computer models SAVI-4, EASI, or both may be used along with the Neutralization tool in this analysis.*

25.1 Introduction

PPS Design and Analysis Methodology

This course presents a methodology for designing and evaluating a physical protection system. As an exercise in the application of the methodology, each subgroup will work on a comprehensive design and evaluation problem, which will require the use of all material that was taught in the course.

Design and Evaluation Is a Cycle

The process begins by determining the PPS objectives. Then the new PPS is designed or the existing PPS is characterized. Next, the effectiveness of the system is evaluated to determine if the PPS is adequate. If the answer is yes, the designers can move on to the Final PPS design (see Figure 25-1). If the answer is no, the system must be redesigned to improve weaknesses and the evaluation is repeated. The cycle is repeated until an effective design is achieved.

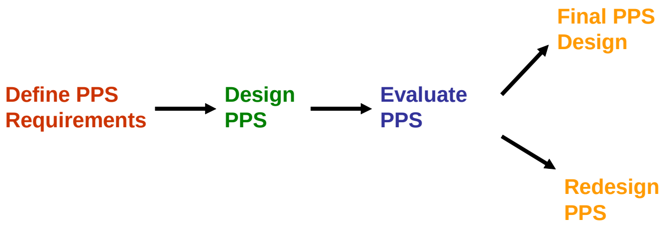


Figure 25-1. Design and Evaluation Cycle

25.2 Exercise Procedure

Use Systems Approach

In previous sessions, the design and evaluation methodology was described. The course material is organized around this process, also called the "systems approach to PPS." Subgroup Session 25S requires the participants to perform a design and evaluation exercise using the following steps:

Determine Requirements

Determine Physical Protection System Requirements:

- ***Characterizing Facility Operations and Conditions***—First study the existing facility or facility plans to identify all of the operations, conditions, and important physical features that have an impact on the physical protection system.

- ***Defining Threats***—Conduct a study of the range of adversaries that the physical protection system must successfully protect against and create a design basis threat.

- ***Identifying Targets***—Identify the most important areas and/or materials, which must be protected from the adversary.

Characterize the Existing System and Design the New PPS

Design/Characterize Physical Protection System:

- ***Identify the existing physical protection elements*** and design a new protection system to protect the facility or materials. This is generally a two step process if the facility is poorly designed (as is the case of this exercise). First make a preliminary design (the minimum that is absolutely needed) and then this will be the base case.

Evaluate the Design

Evaluate Physical Protection System Design:

- Given the information about the facility, the threat, the targets, and the minimum physical protection system***, use accepted analysis techniques to obtain a measure of the protection system's effectiveness***. You could use SAVI, and EASI along with the Neutralization tool to do this.

25.2.1 Using SAVI to Analyze the PPS Design

Use SAVI to Analyze the Design

SAVI-4 Method:

The steps generally to be followed in using SAVI-4 for the path analysis and redesign process are as follows:

a) **Create an ASD** that fully details the layers of protection and associated protection elements for each specific target that must be protected.

b) ***Input the existing facility design*** or the new design into the Facility Module of SAVI-4 to fully describe the performance characteristics of each layer and protection element. Be sure to examine every input value to the very end of the menu-train, and examine the generic input diagram for each type of Physical Protection Elements to ensure that the data is properly entered.

c) ***Run the Outsider Module*** of SAVI-4 using the Facility Module as data, with appropriate numbers of response force times and path considerations (10 × 10 is recommended).

d) ***Determine the Probability of Neutralization*** using the Neutralization tool. Enter the appropriate data into the tool to describe the response force and the adversary team. The tool will provide an estimated Probability of Neutralization that should be used in this analysis. It is helpful to validate this P_N with performance data, subject matter expert advice, and force of force exercises.

e) ***Conduct a scenario analysis*** as described earlier in this course. Determine if an adversary team could use a tactic or strategy that significantly reduces the effectiveness of a protection element(s). The revised performance characteristics will need to be entered into the SAVI module and Neutralization tool to accurately reflect the new data.

f) ***Calculate System Effectiveness*** using the P_I and P_N developed in the previous steps. If the system effectiveness is acceptable, then the analysis is complete and should be documented in a comprehensive report.

g) ***Consider doing an EASI Calculation*** on the most vulnerable path.

h) ***Determine specific vulnerabilities if the system effectiveness is not acceptable.*** The analyst should strive to understand specific vulnerabilities that contribute to the system's weaknesses, focusing on the sub-functions of detection, delay, and response. Specific upgrades should be developed to address the identified vulnerabilities.

i) ***Reanalyze upgrades.*** After deciding on the most effective upgrades, design the upgrades, reenter the data into the Facility Module, and again run the Outsider Module using the new facility design to determine if system effectiveness now is sufficient. Due to time constraints in this course, it may be necessary to enter the upgrades in the Outsider Module and evaluate their effectiveness without completely revising the Facility Module.

25.2.2 Using EASI to Analyze the PPS Design

Use EASI to Analyze the ASD

EASI Method: The steps generally to be followed in using EASI for the analysis and redesign process are as follows:

a) ***Identify a single target and the adversary objectives*** that were identified earlier and draw an ASD. Label the areas and elements, however, for this ASD, add the probability of detection for both stealth and deceit strategies, the delay afforded by the element, and whether the detection occurs at the beginning, middle, or end of each of the elements. Indicate the same information for crossing the areas such as the limited area and the protected area. It is recommended that you write the table shown below beside each element or area and then complete the data.

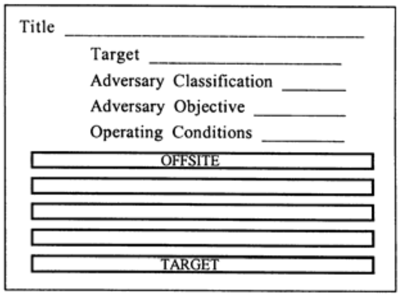
$P_{D\text{ (Stealth or Deceit)}}$ = ___________

Delay $_{\text{(Minimum)}}$ = ___________

B = beginning
M = middle
E = end

Detection $_{(Where)}$ =_________B, M, or E

Note that the data may be different for operational or non-operational periods, for different adversary objectives, for different targets, and for different classes of adversaries. Therefore, a title to identify the ASD is necessary, as shown on the illustration below.



Adversary Strategy (Theft or Sabotage)

What Determines a "Win" for the Adversary?

ASD Shows All Paths to the "Win"

b) ***Adversary Strategy.*** If the adversary tactic or strategy is ***theft***, then an exit path must be drawn on the ASD as well and the data attached to that exit path. The exit path may contain the same elements as the entry path or it may contain different elements if the adversary uses a different path to exit the facility. If the adversary exit path is the same as the entry path, delay elements may be much lower on the way out, in comparison to the entry path (for example, if elements were destroyed on the way in, such as breaching a door or cutting a hole in a fence.)

Also, some determination must be made on what represents a "win" for the adversary. At what point in the exit path is the adversary expected to "break" containment and be outside the response force's ability to prevent the theft of material? The ASD must illustrate all possible paths from the time that the adversary starts the attack on your facility to where the adversary is considered to have won.

If the adversary tactic or strategy is ***sabotage***, then obtaining access to the sabotage target and accomplishing the act of destroying or exploding the target, represents a "win" for the adversary. An exit path is not needed.

Response Force Data

c) ***Response Force Data.*** To accomplish the calculation of P_I using the principle of "timely detection," a crucial part of the data concerns the response force. It should be clear that this time is very dependent on the target and on the adversary objectives.

If the adversary is attempting ***theft***, then the response force can arrive and deploy to contain the adversary and prevent their escape. If the adversary is attempting ***sabotage***, then the response force must deploy to interrupt the progress of the adversary and prevent them from gaining access to the target. The EASI model requires the total response force time from the moment that an alarm is triggered to when a sufficient number of response force personnel are deployed in the most effective position to counter the adversary. This time consists of six parts which should be added and used in EASI, as shown on the following table.

Time (seconds)
Alarm Communication Time ________
Assessment of Alarm Time ________
Communicate to Response Force ________
Preparation Time ________
Travel Time ________
Deployment Time ________
TOTAL ________

Probability of Communication

d) ***Probability of Communication.*** The EASI model also requires the entry of the probability of communication from the central alarm station or secondary alarm station to the response force. This probability must consider the quality of the communications means and the capabilities of the design basis threat to defeat that communication. The probability of effective communications must be consistent with the communication time indicated in the response force total time. It should be clear that a very short communication time (a few seconds) would not produce a high probability of effective communications.

Apply EASI to the 3 Most Vulnerable Paths

e) ***From the ASD that was drawn earlier***, choose the three (3) most vulnerable paths by selecting lowest delay after the critical detection point (CDP) and lowest probability of detection before the CDP. This is assuming the design basis threat is attacking you, and then apply EASI to those paths.

f) **Determine the Probability of Neutralization** using the Neutralization tool. Enter the appropriate data into the tool to describe the response force and the adversary team. The tool will provide an estimated Probability of Neutralization that should be used in this analysis. It is helpful to validate this P_N with performance data, subject matter expert advice, and force-on-force exercises.

g) **Conduct a scenario analysis** as described earlier in this course. If it is determined that an adversary team could use a tactic or strategy that significantly reduces the effectiveness of a protection element(s), the revised performance characteristics will need to be entered into the SAVI module and Neutralization tool to accurately reflect the new data.

h) **Calculate System Effectiveness** using the P_I, and P_N and developed in the previous steps. If the system effectiveness is acceptable, then the evaluation is complete and should be documented in a comprehensive report.

i) **If the system effectiveness is not acceptable, determine specific vulnerabilities**. The analyst should strive to understand specific vulnerabilities that contribute to the system's weaknesses, focusing on the sub-functions of detection, delay and response. Specific upgrades should be developed to address the identified vulnerabilities. The performance characteristics of these enhancements should be entered into the computer models (EASI, and the Neutralization tool) to determine their effect on the system's performance.

It is a sound practice to evaluate these enhancements one at a time or in different combinations to fully understand how they effect the P_I and P_N of the system. It may also be possible to mitigate some the consequences of the undesirable event and reduce the level of consequence used in the risk equation.

25.3 Neutron Burst Reactor (NBR)

Design and Evaluate a PPS for the NBR Pulse Reactor

In this final exercise, you will use the entire DEPO process to design and evaluate the PPS at the NBR Pulse Reactor. Many of the LIMP site characteristics will be well known by this time because you have been working exercises on the PTR reactor which is on the same site.

Description

The NBR is a gun-type highly enriched uranium (HEU) fueled pulse reactor. In Soviet times, when the Republic of Lagassi was a member of the Soviet Union, the reactor was used for military research and radiation testing of weapon components. The reactor is now used primarily for testing of spacecraft components and commercial reactor components. The Institute has a number of foreign clients including the Japan Space Agency, Ariane, the European Space Agency, and Russia.

Operations

The NBR pulse reactor is capable of very short duration pulsed operation for neutron burst experiments. The reactor core is formed by 10 cylindrical plate-like disc fuel elements stacked together and the reactor is controlled by momentarily decreasing the gaps between the fuel element discs. The fuel material is HEU metal alloyed with 9%-10% molybdenum, with uranium enriched to 93 percent. Each fuel disc is approximately 228 mm in diameter, 31 mm thick, and contains a total of 14 kg of uranium in all disks. The reactor is air cooled by natural convection.

Fuel

Irradiated fuel elements for the NBR are manually transferred to a used fuel storage container in locked storage boxes. Used fuel discs are stored in the used fuel locker in the fuel vault, R102, in the reactor building lower level. The surface dose rate of spent fuel disc is approximately 2-3 rem/hr (.02 to .03 Sv/hr).

Fresh fuel discs are manufactured on-site. Fuel discs are stored in storage lockers in the fuel vault, R102, in the reactor building lower level. The storage vault can hold up to 50 discs. Cotton gloves are worn when directly handling the fuel discs.

Consult the Exercise Data

For more data about the NBR pulsed reactor, you should read carefully the NBR Section in the Exercise Data book.

25.4 Summary

DEPO Methodology Provides Framework

A methodology for the design and analysis of a physical protection system is illustrated in Figure 25-2. This figure illustrates the major steps required to successfully design and analyze a physical protection system.

Final Exercise

The final subgroup problem is a 2-day design and evaluation exercise. Each subgroup should use this methodology to design and evaluate physical protection of the NBR Pulse Reactor at the Lagassi Institute . During the evaluation phase each group has the option of using SAVI-4, EASI, or both.

Presentation of Results

At the completion of the exercise, each subgroup will give a 20-minute, final presentation to an evaluation panel of physical protection experts.

Design and Evaluation
Process Outline (DEPO)

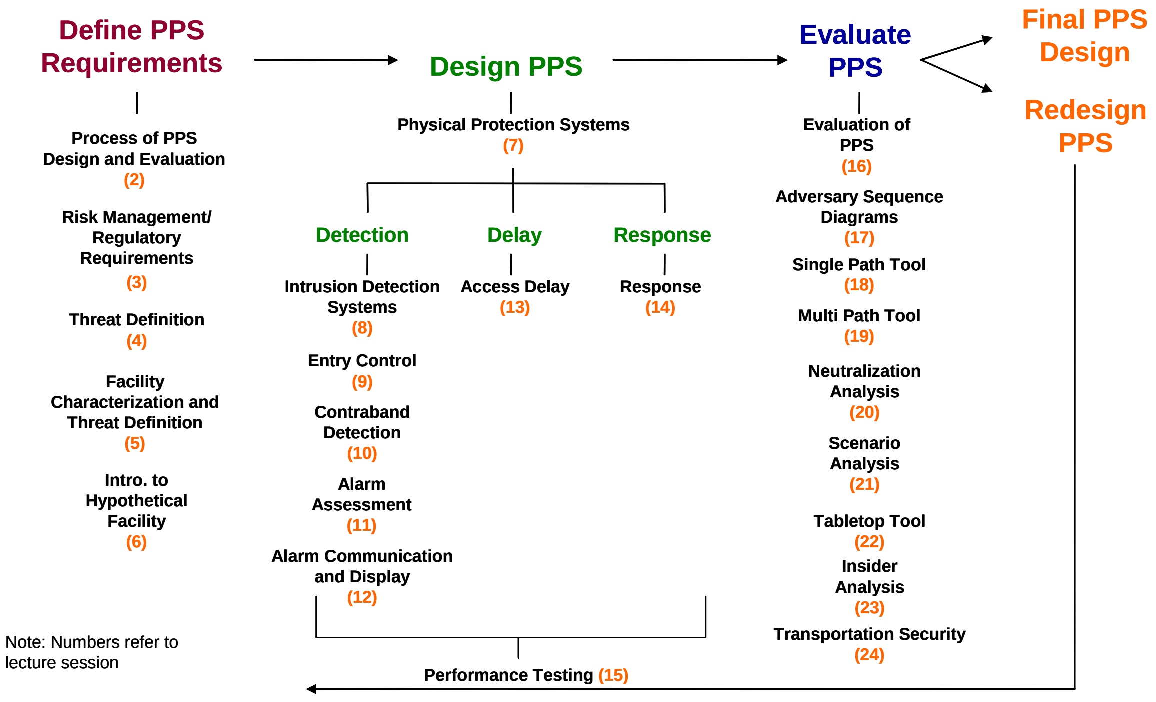
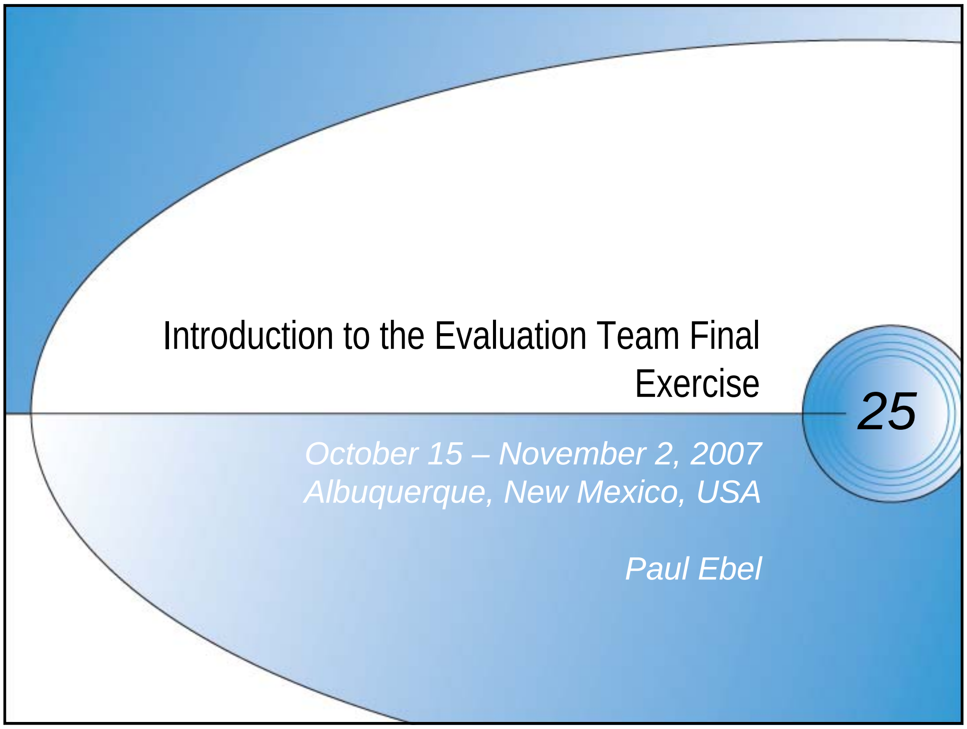

Define PPS Requirements
Process of PPS Design and Evaluation (2)
Risk Management/ Regulatory Requirements (3)
Threat Definition (4)
Facility Characterization and Threat Definition (5)
Intro. to Hypothetical Facility (6)
Design PPS
Physical Protection Systems (7)
Detection
Intrusion Detection Systems (8)
Entry Control (9)
Contraband Detection (10)
Alarm Assessment (11)
Alarm Communication and Display (12)
Delay
Access Delay (13)
Response
Response (14)
Performance Testing (15)
Evaluate PPS
Evaluation of PPS (16)
Adversary Sequence Diagrams (17)
Single Path Tool (18)
Multi Path Tool (19)
Neutralization Analysis (20)
Scenario Analysis (21)
Tabletop Tool (22)
Insider Analysis (23)
Transportation Security (24)
Final PPS Design
Redesign PPS
Note: Numbers refer to lecture session

Figure 25-2. Design and Evaluation Process Outline (DEPO)

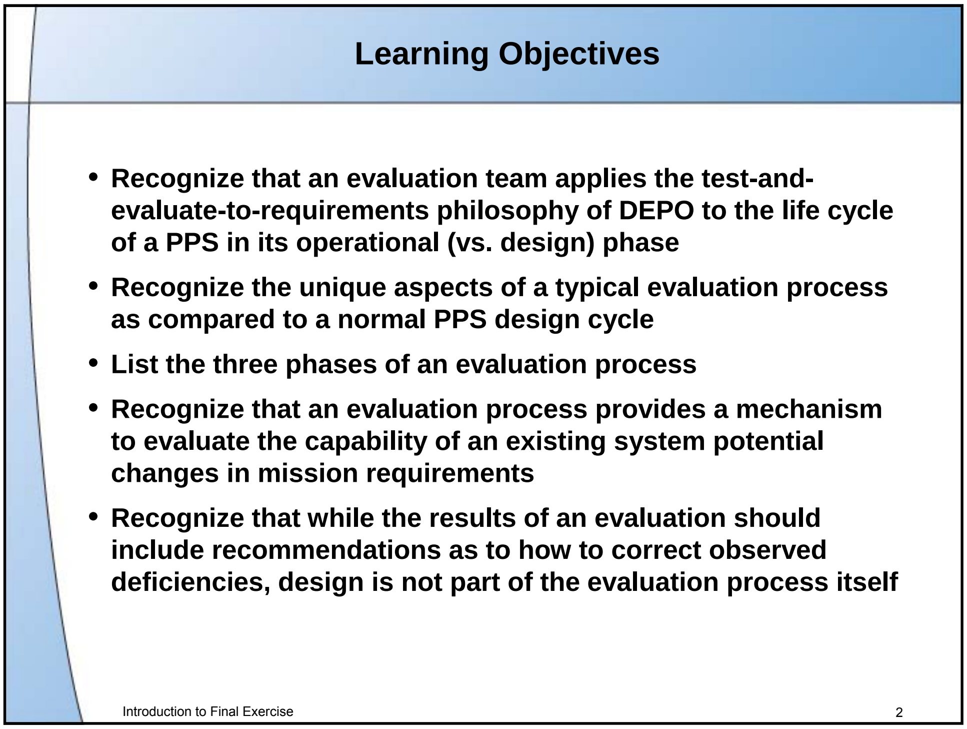


Introduction to the Evaluation Team Final Exercise

25

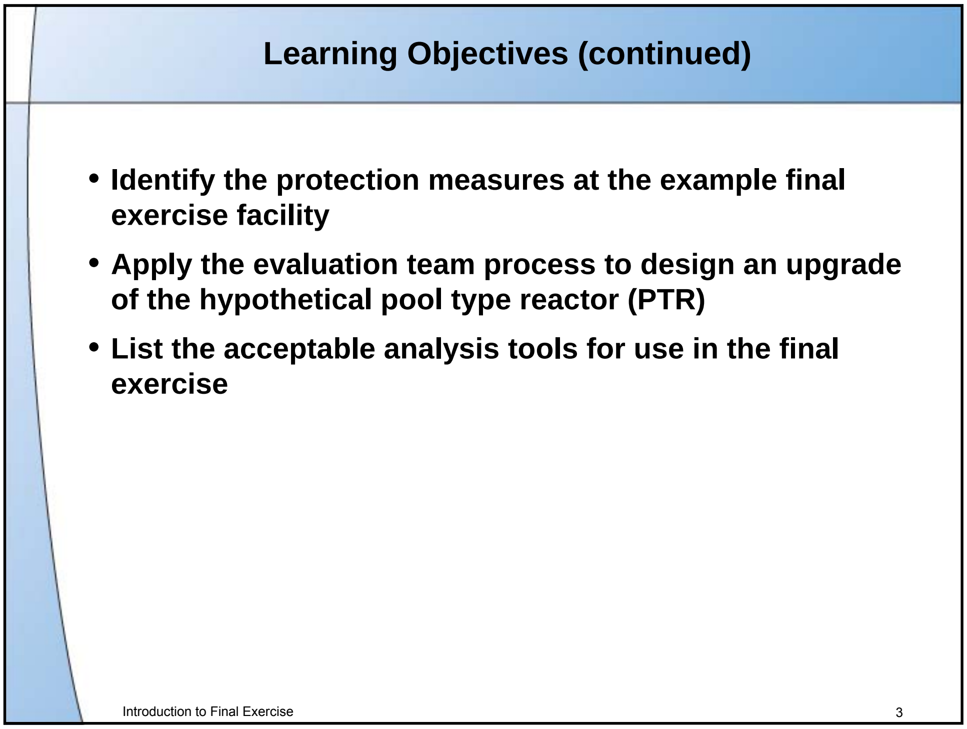
October 15 – November 2, 2007
Albuquerque, New Mexico, USA

Paul Ebel



Learning Objectives

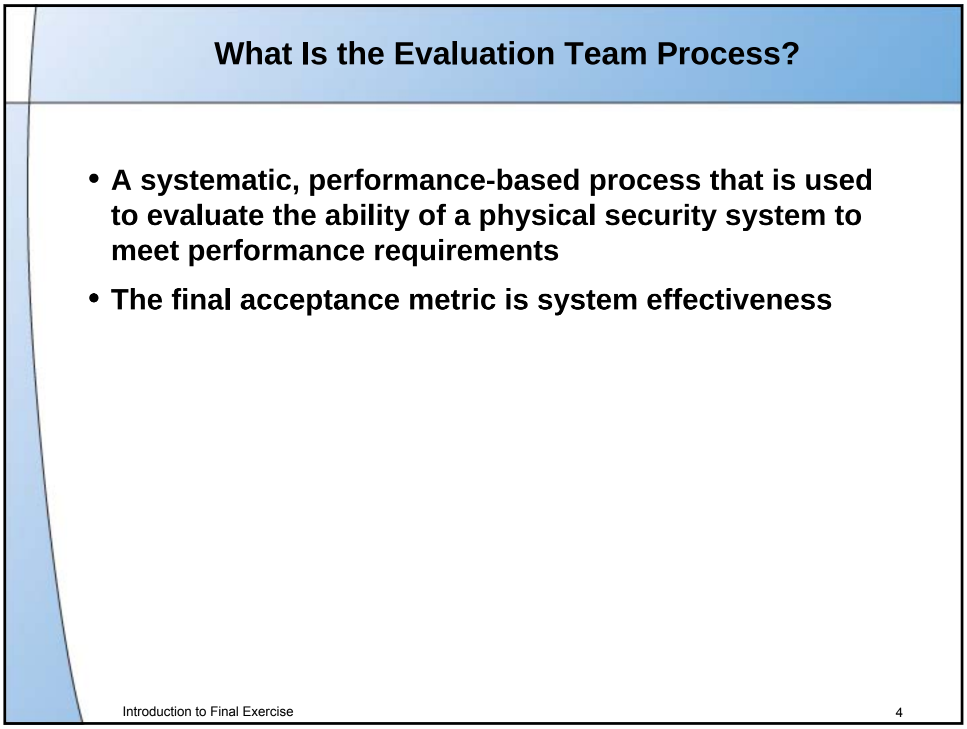
- Recognize that an evaluation team applies the test-and-evaluate-to-requirements philosophy of DEPO to the life cycle of a PPS in its operational (vs. design) phase
- Recognize the unique aspects of a typical evaluation process as compared to a normal PPS design cycle
- List the three phases of an evaluation process
- Recognize that an evaluation process provides a mechanism to evaluate the capability of an existing system potential changes in mission requirements
- Recognize that while the results of an evaluation should include recommendations as to how to correct observed deficiencies, design is not part of the evaluation process itself



Learning Objectives (continued)

- Identify the protection measures at the example final exercise facility
- Apply the evaluation team process to design an upgrade of the hypothetical pool type reactor (PTR)
- List the acceptable analysis tools for use in the final exercise

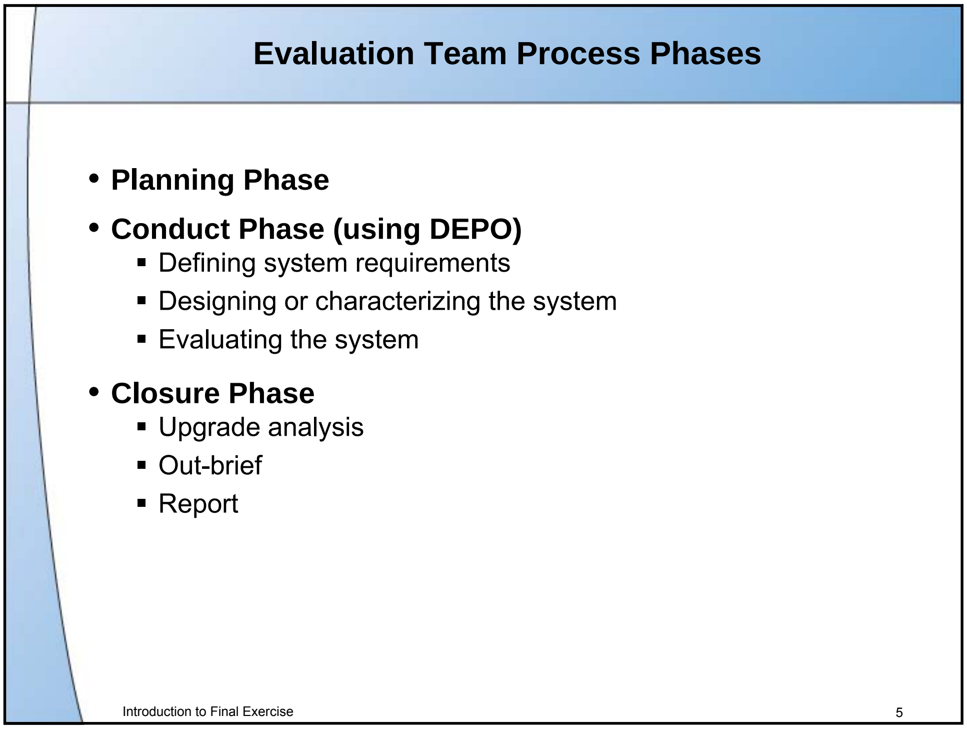
Introduction to Final Exercise 3



What Is the Evaluation Team Process?

- A systematic, performance-based process that is used to evaluate the ability of a physical security system to meet performance requirements
- The final acceptance metric is system effectiveness

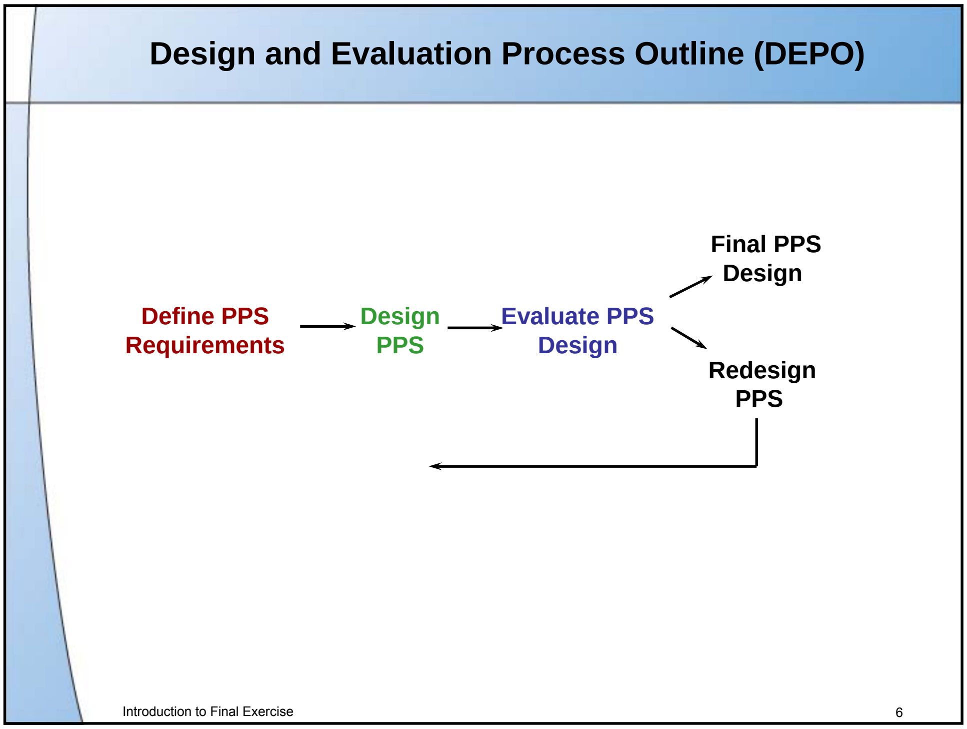
Introduction to Final Exercise 4



Evaluation Team Process Phases

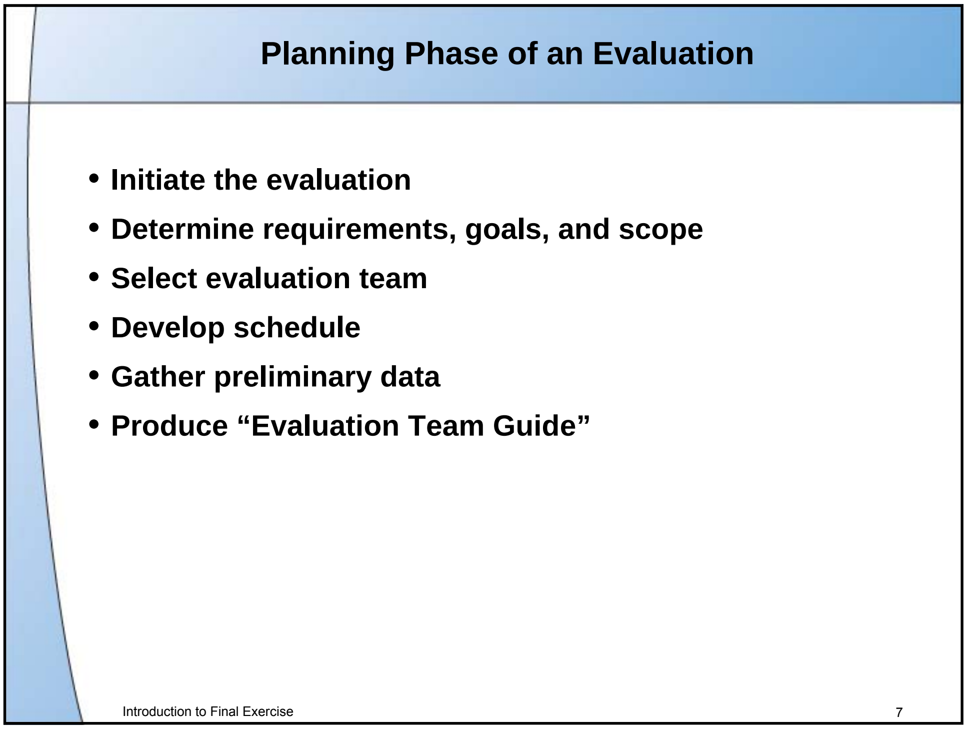
- **Planning Phase**
- **Conduct Phase (using DEPO)**
  - Defining system requirements
  - Designing or characterizing the system
  - Evaluating the system
- **Closure Phase**
  - Upgrade analysis
  - Out-brief
  - Report

Introduction to Final Exercise 5



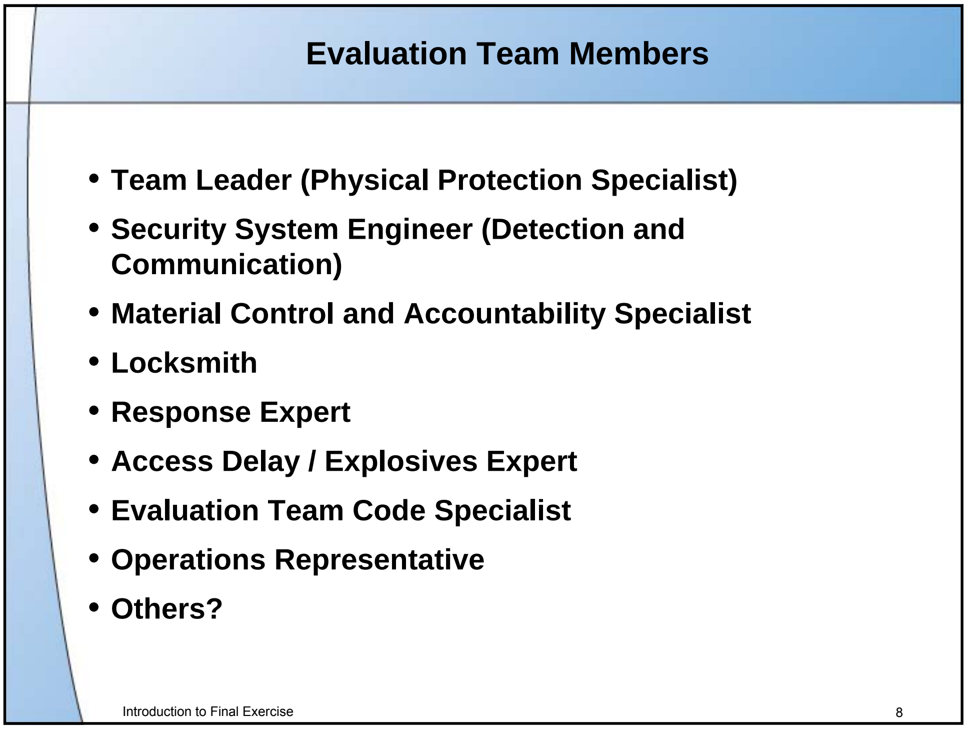
Design and Evaluation Process Outline (DEPO)

Introduction to Final Exercise 6



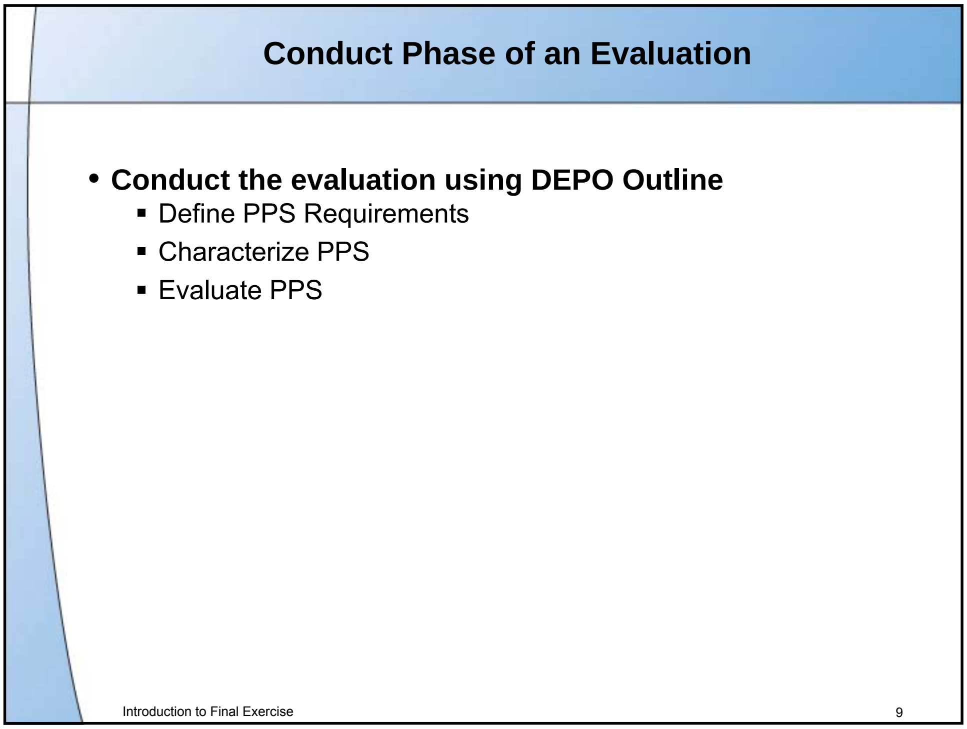
Planning Phase of an Evaluation

- Initiate the evaluation
- Determine requirements, goals, and scope
- Select evaluation team
- Develop schedule
- Gather preliminary data
- Produce “Evaluation Team Guide”



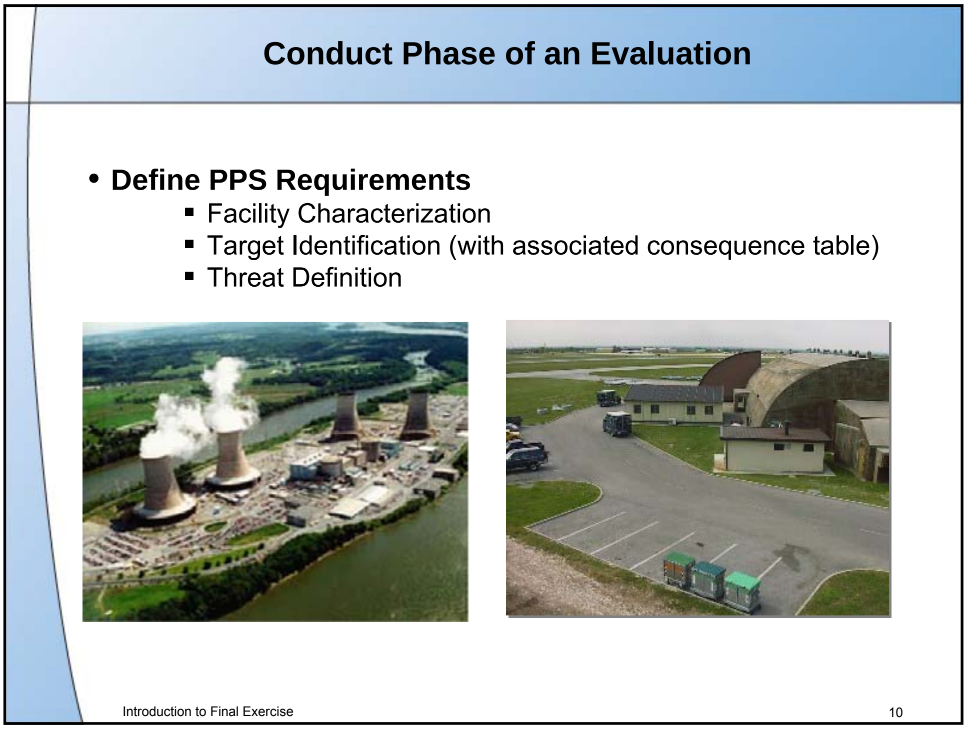
Evaluation Team Members

- Team Leader (Physical Protection Specialist)
- Security System Engineer (Detection and Communication)
- Material Control and Accountability Specialist
- Locksmith
- Response Expert
- Access Delay / Explosives Expert
- Evaluation Team Code Specialist
- Operations Representative
- Others?



Conduct Phase of an Evaluation

- **Conduct the evaluation using DEPO Outline**
  - Define PPS Requirements
  - Characterize PPS
  - Evaluate PPS



Conduct Phase of an Evaluation

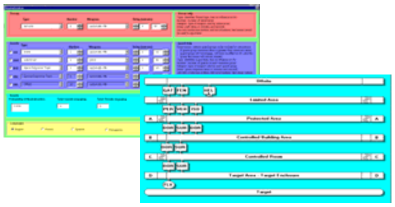
- **Define PPS Requirements**
  - Facility Characterization
  - Target Identification (with associated consequence table)
  - Threat Definition

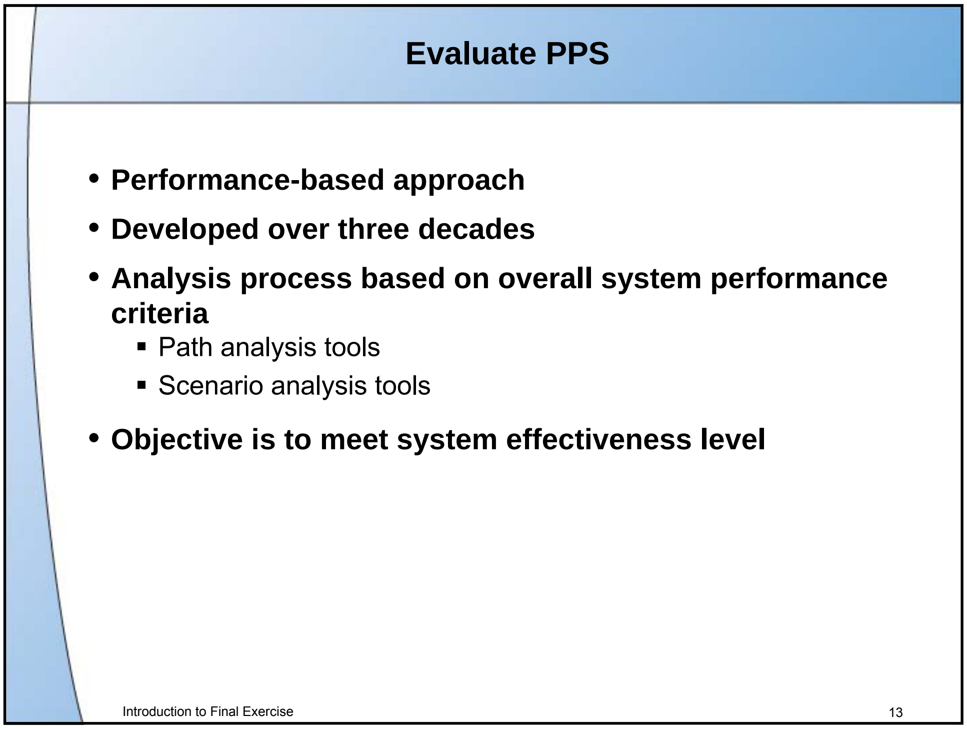
Conduct Phase of an Evaluation

- **Characterize PPS**
  - Detection
  - Delay
  - Response
  - Tours and observations
  - Document review
  - Interviews
  - Data validation

Conduct Phase of an Evaluation

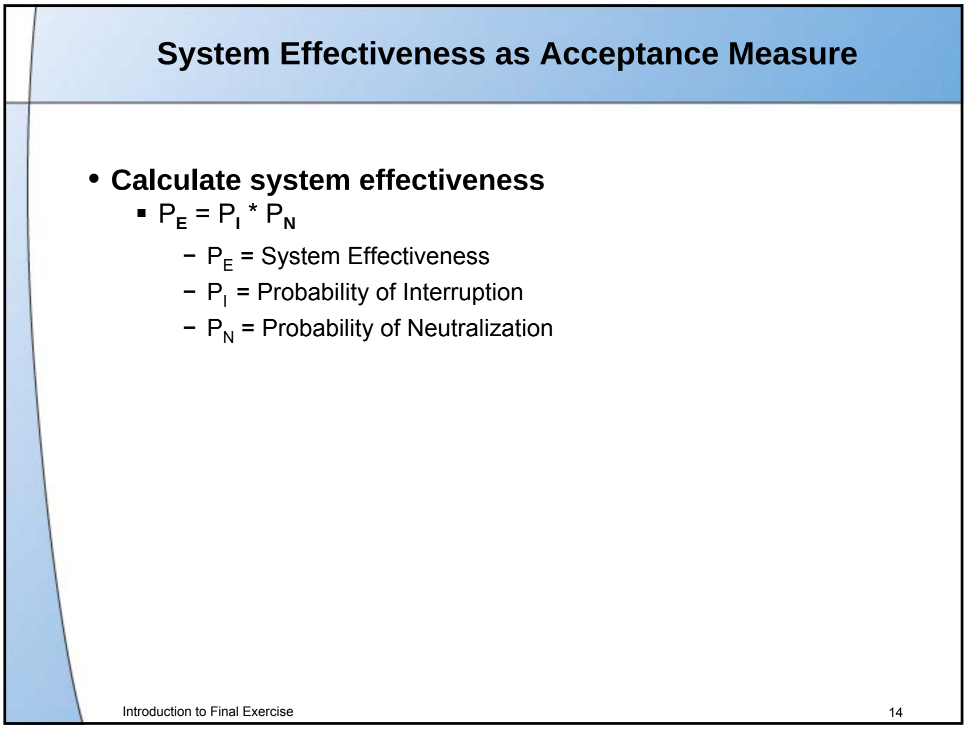
- Evaluate PPS
  - Performance-based tools
  - System effectiveness is final acceptance metric





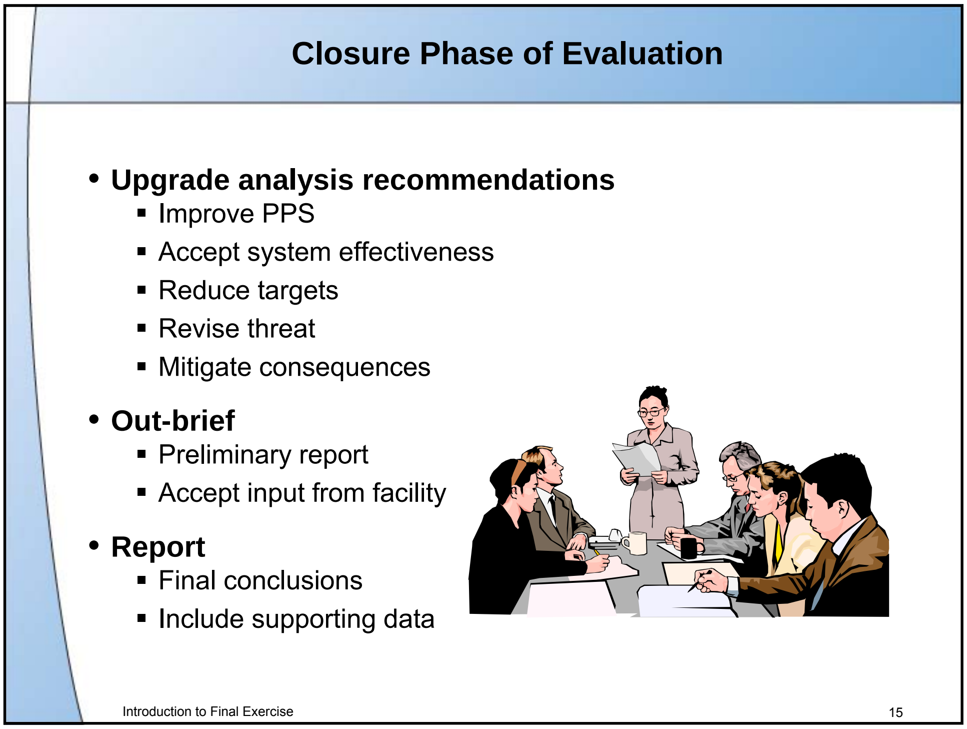
Evaluate PPS

- **Performance-based approach**
- **Developed over three decades**
- **Analysis process based on overall system performance criteria**
  - Path analysis tools
  - Scenario analysis tools
- **Objective is to meet system effectiveness level**



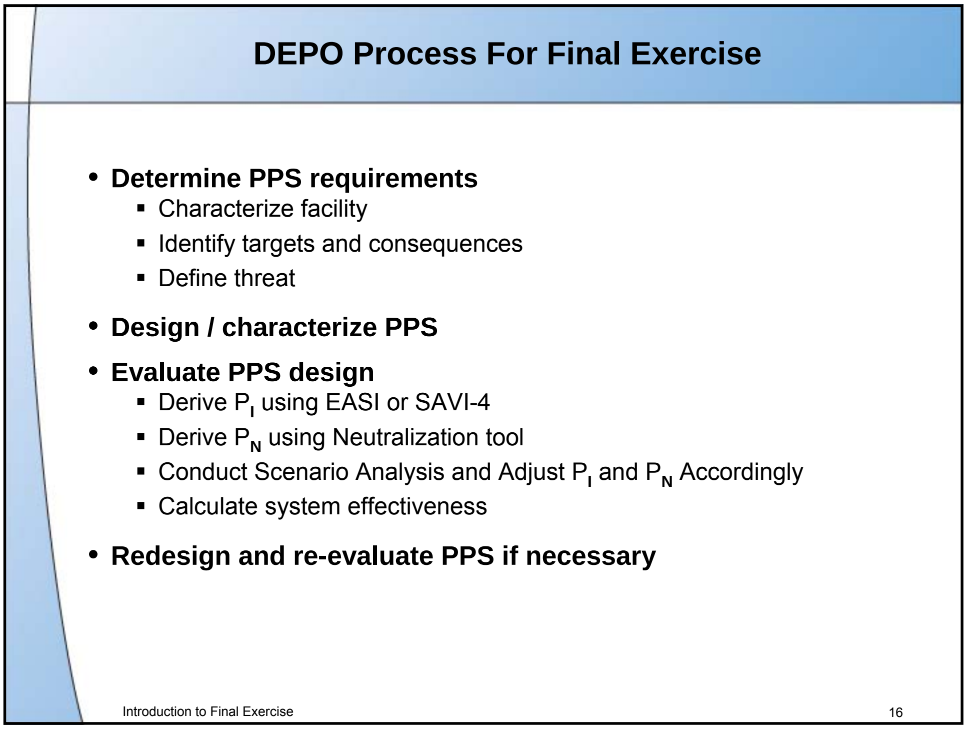
System Effectiveness as Acceptance Measure

- **Calculate system effectiveness**
  - $P_E = P_I * P_N$
    - P_E = System Effectiveness
    - P_I = Probability of Interruption
    - P_N = Probability of Neutralization



Closure Phase of Evaluation

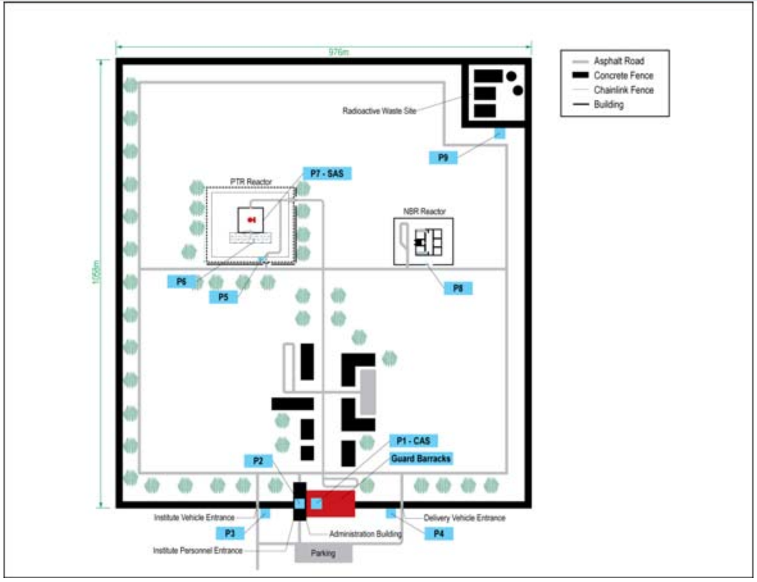
- **Upgrade analysis recommendations**
  - Improve PPS
  - Accept system effectiveness
  - Reduce targets
  - Revise threat
  - Mitigate consequences
- **Out-brief**
  - Preliminary report
  - Accept input from facility
- **Report**
  - Final conclusions
  - Include supporting data



DEPO Process For Final Exercise

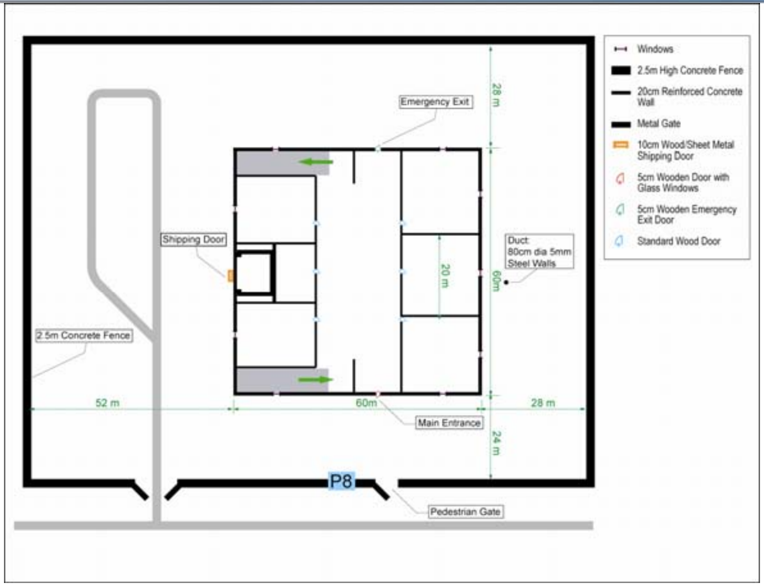
- **Determine PPS requirements**
  - Characterize facility
  - Identify targets and consequences
  - Define threat
- **Design / characterize PPS**
- **Evaluate PPS design**
  - Derive P_I using EASI or SAVI-4
  - Derive P_N using Neutralization tool
  - Conduct Scenario Analysis and Adjust P_I and P_N Accordingly
  - Calculate system effectiveness
- **Redesign and re-evaluate PPS if necessary**

LIMP Site and Response Force Locations



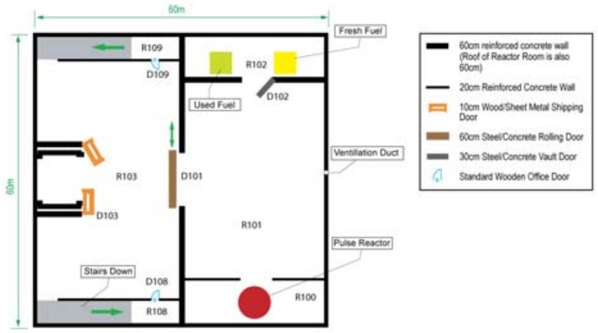
Introduction to Final Exercise 17

NBR-Above-Ground Wall Thicknesses and Distances

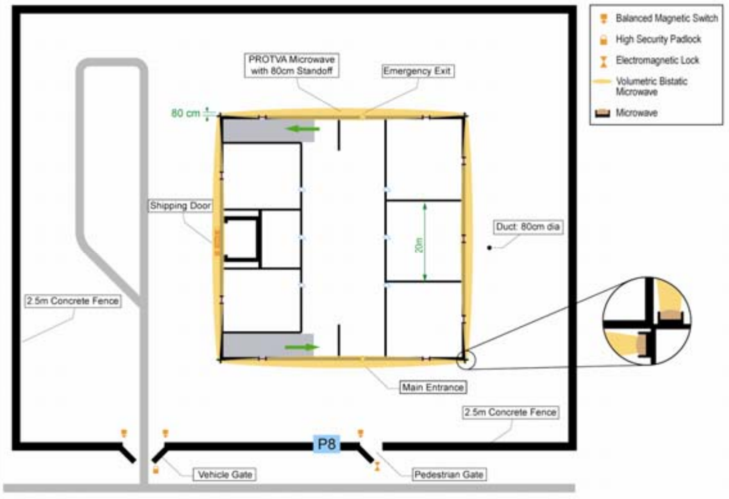


Introduction to Final Exercise 18

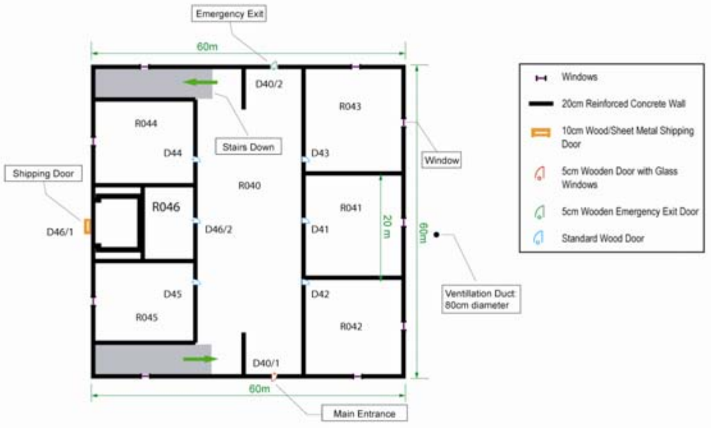
NBR Below-Ground Building Floor Plan


60m
60m
Fresh Fuel
R109
D109
R102
Used Fuel
D102
R103
D101
D103
R101
Ventilation Duct
Pulse Reactor
Stairs Down
D108
R108
R100
▬ 60cm reinforced concrete wall (Roof of Reactor Room is also 60cm)
— 20cm Reinforced Concrete Wall
10cm Wood/Sheet Metal Shipping Door
60cm Steel/Concrete Rolling Door
30cm Steel/Concrete Vault Door
Standard Wooden Office Door

NBR Exterior Physical Protection Elements

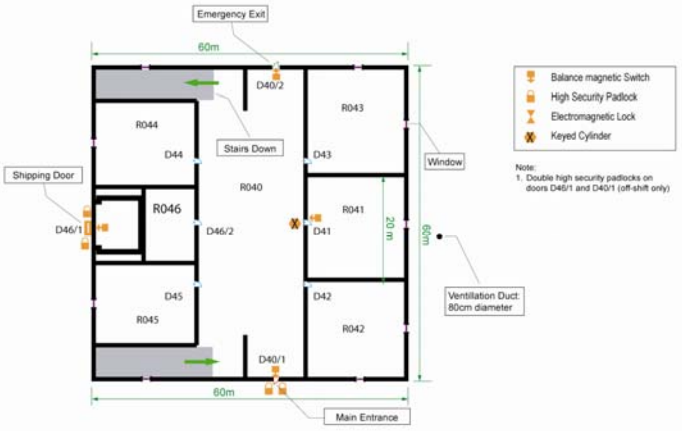


NBR Above Ground Building Floor Plan



Introduction to Final Exercise 21

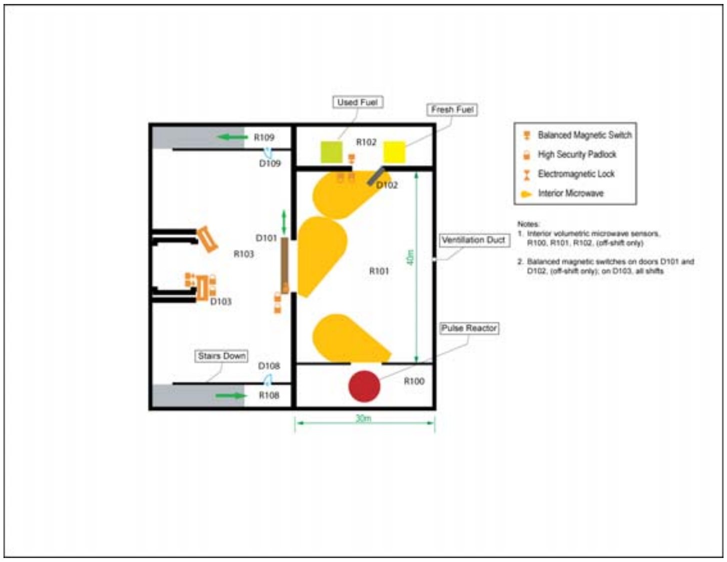
NBR---Above Ground Interior Physical Protection Elements



Note:
1. Double high security padlocks on doors D46/1 and D40/1 (off-shift only)

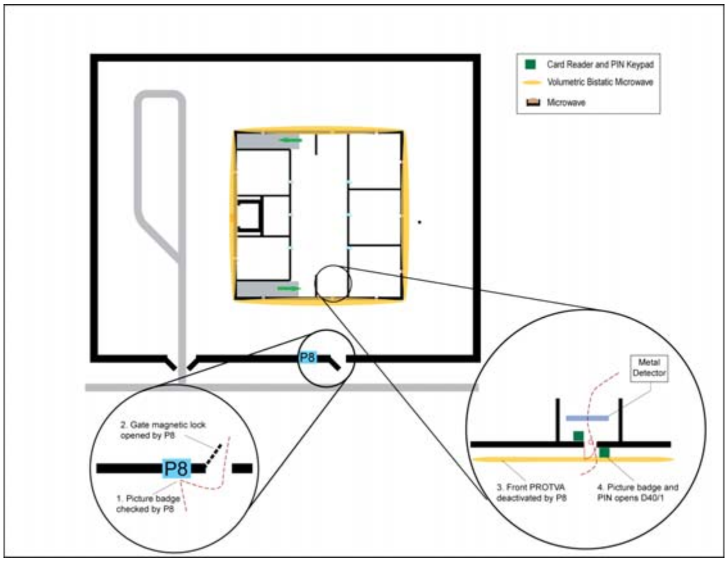
Introduction to Final Exercise 22

NBR---Below Ground Interior Physical Protection Elements



Notes:
1. Interior volumetric microwave sensors, R100, R101, R102, (off-shift only)
2. Balanced magnetic switches on doors D101 and D102, (off-shift only); on D103, all shifts

NBR---Above Ground Access Control

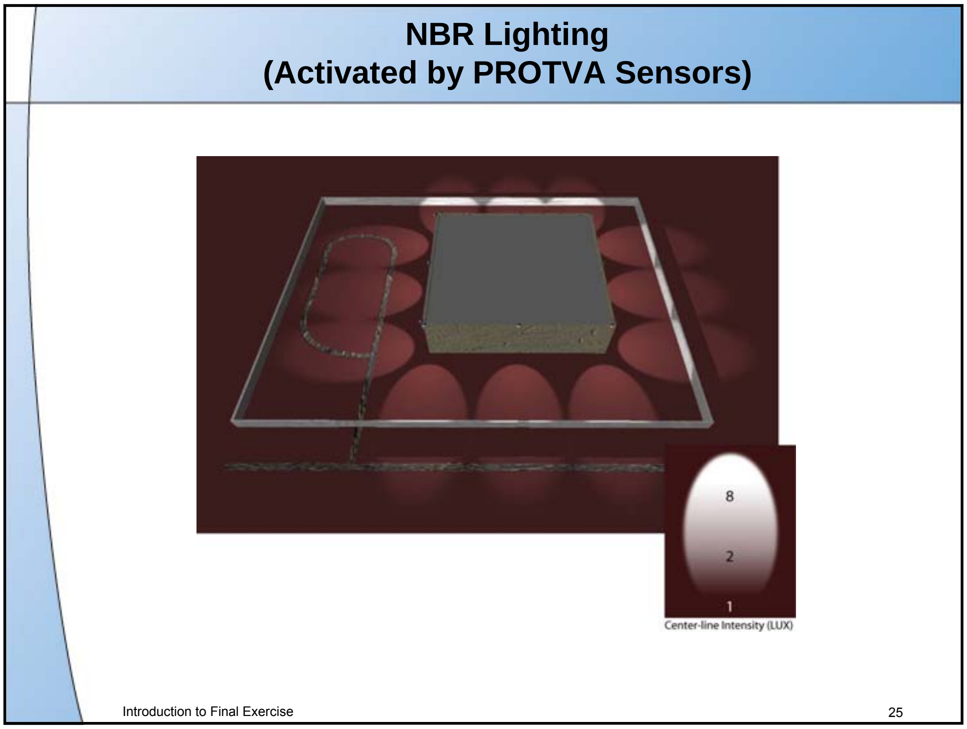


2. Gate magnetic lock opened by P8

1. Picture badge checked by P8

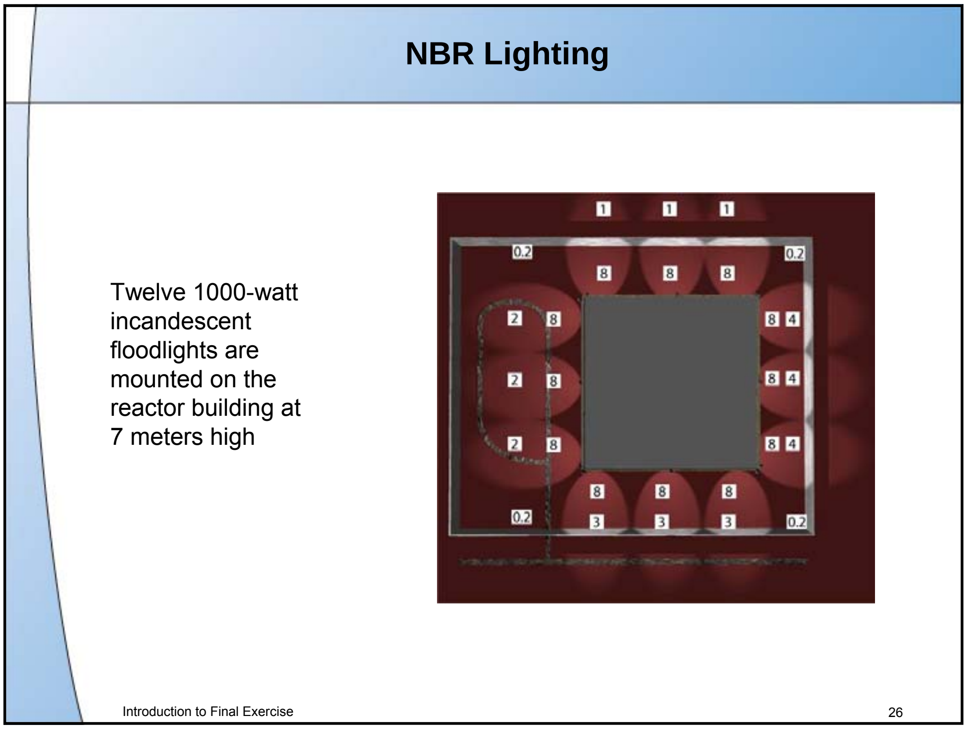
3. Front PROTVA deactivated by P8

4. Picture badge and PIN opens D40/1



NBR Lighting (Activated by PROTVA Sensors)

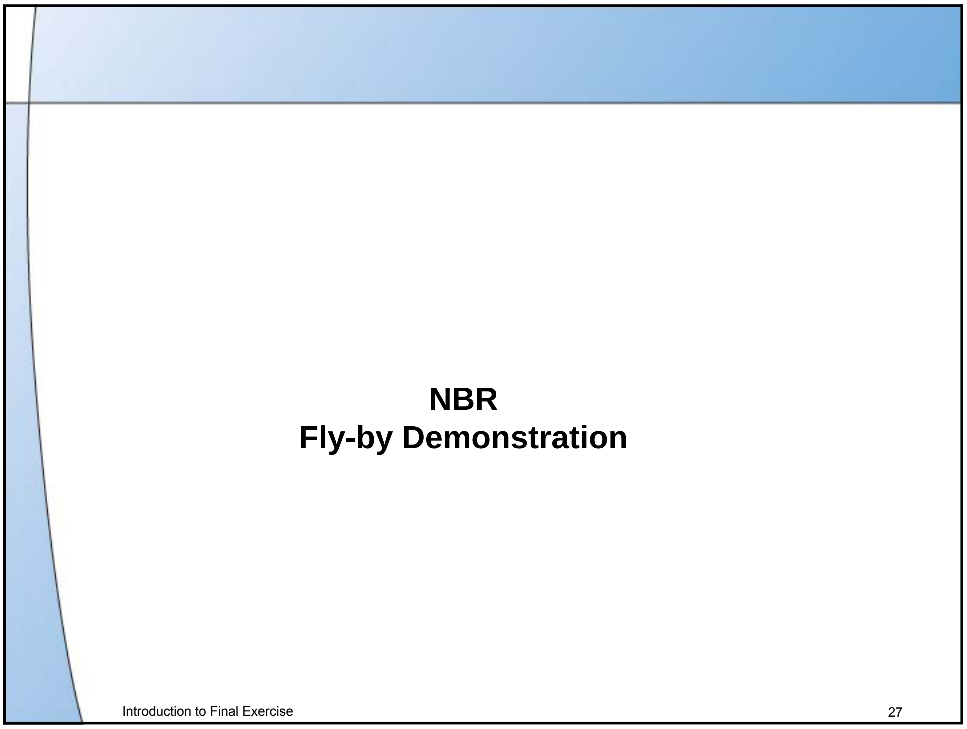
Introduction to Final Exercise 25



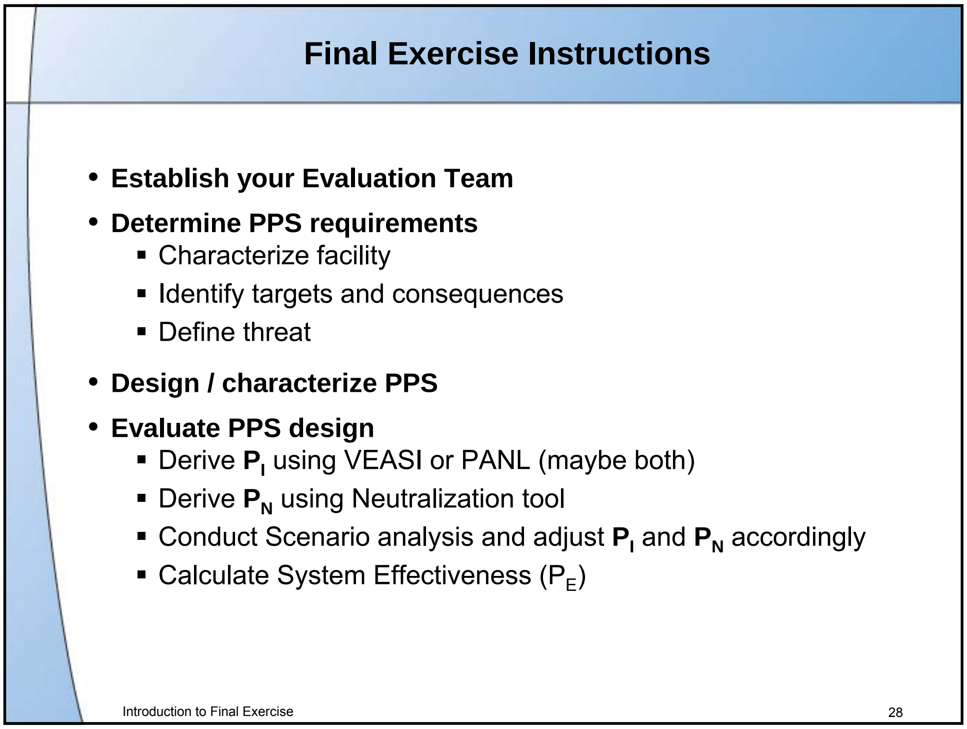
NBR Lighting

Twelve 1000-watt incandescent floodlights are mounted on the reactor building at 7 meters high

Introduction to Final Exercise 26

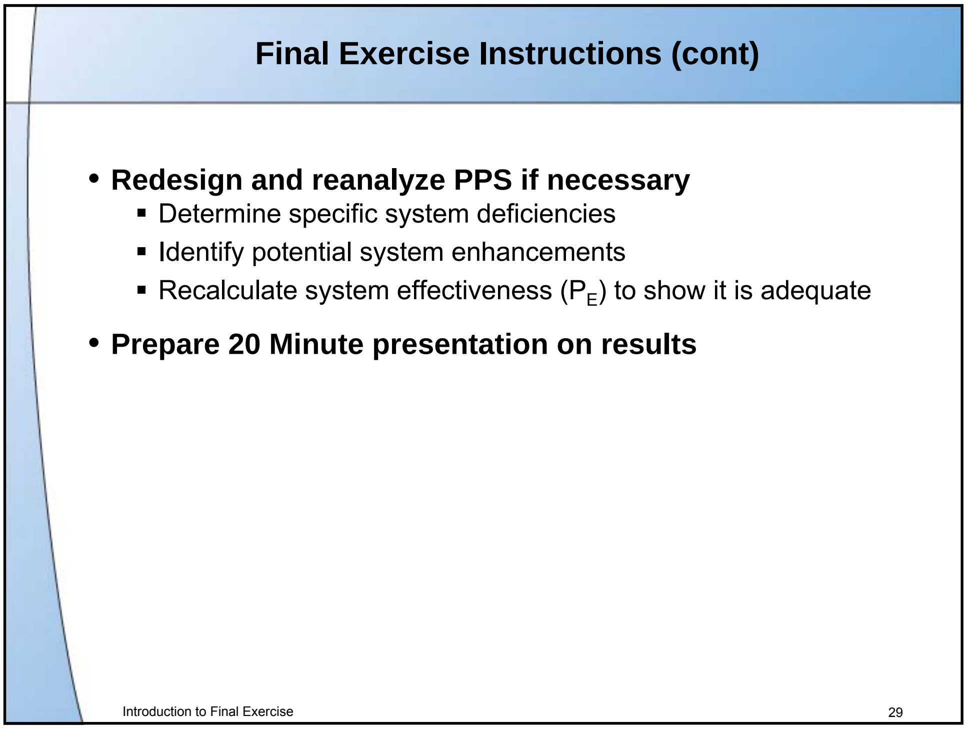


NBR
Fly-by Demonstration



Final Exercise Instructions

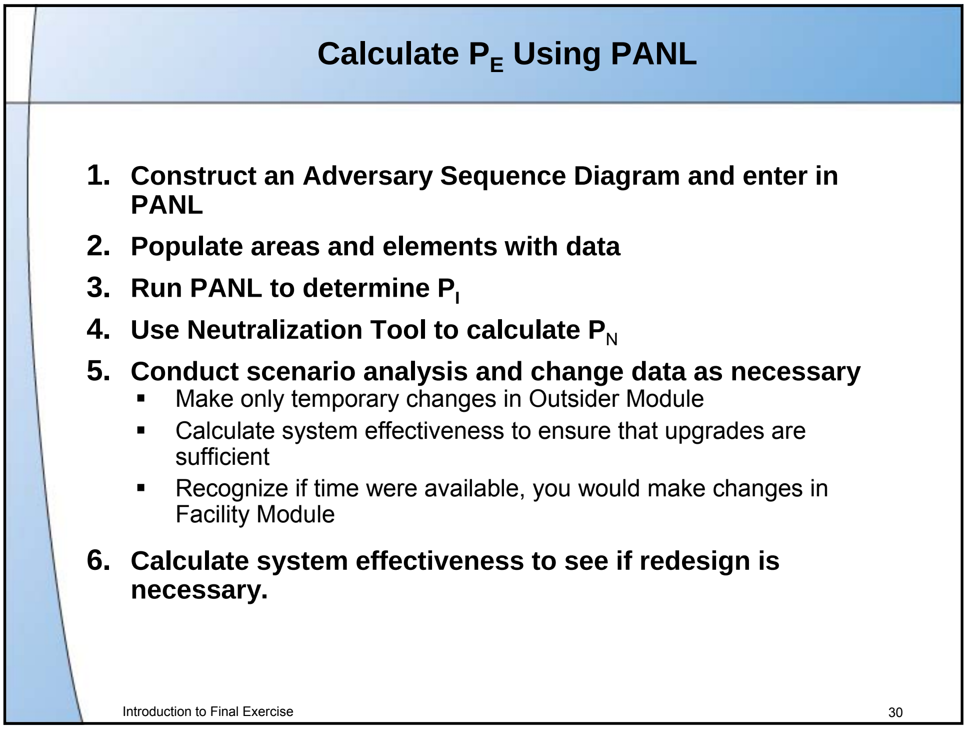
- **Establish your Evaluation Team**
- **Determine PPS requirements**
  - Characterize facility
  - Identify targets and consequences
  - Define threat
- **Design / characterize PPS**
- **Evaluate PPS design**
  - Derive $\mathbf{P_I}$ using VEASI or PANL (maybe both)
  - Derive $\mathbf{P_N}$ using Neutralization tool
  - Conduct Scenario analysis and adjust $\mathbf{P_I}$ and $\mathbf{P_N}$ accordingly
  - Calculate System Effectiveness (P_E)



Final Exercise Instructions (cont)

- **Redesign and reanalyze PPS if necessary**
  - Determine specific system deficiencies
  - Identify potential system enhancements
  - Recalculate system effectiveness (P_E) to show it is adequate
- **Prepare 20 Minute presentation on results**

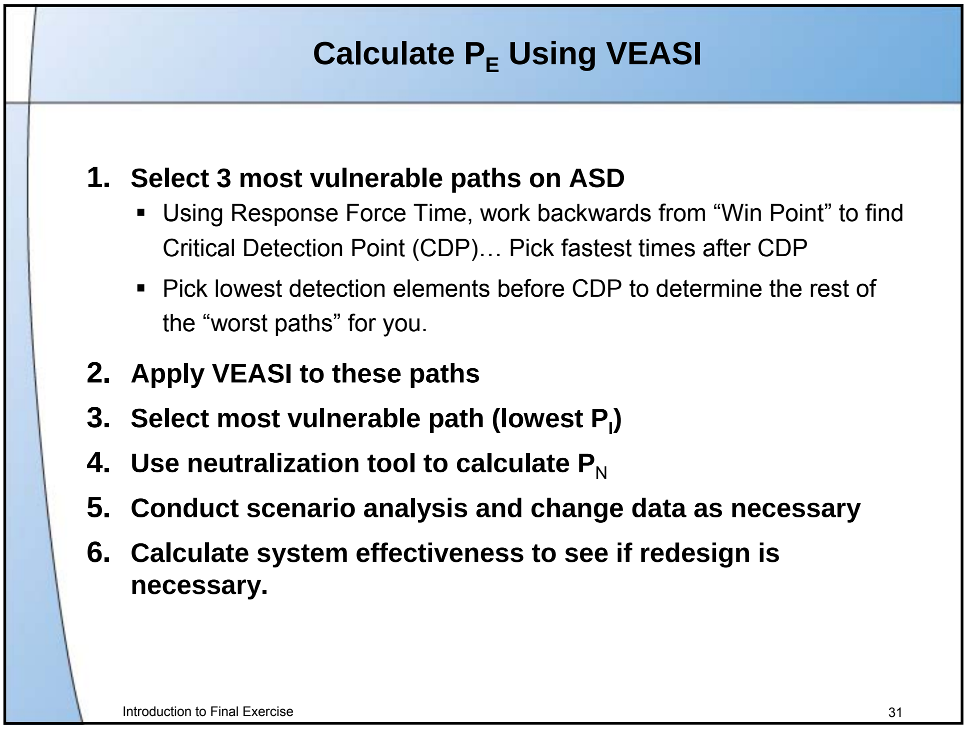
Introduction to Final Exercise 29



Calculate P_E Using PANL

1. **Construct an Adversary Sequence Diagram and enter in PANL**
2. **Populate areas and elements with data**
3. **Run PANL to determine P_I**
4. **Use Neutralization Tool to calculate P_N**
5. **Conduct scenario analysis and change data as necessary**
   - Make only temporary changes in Outsider Module
   - Calculate system effectiveness to ensure that upgrades are sufficient
   - Recognize if time were available, you would make changes in Facility Module
6. **Calculate system effectiveness to see if redesign is necessary.**

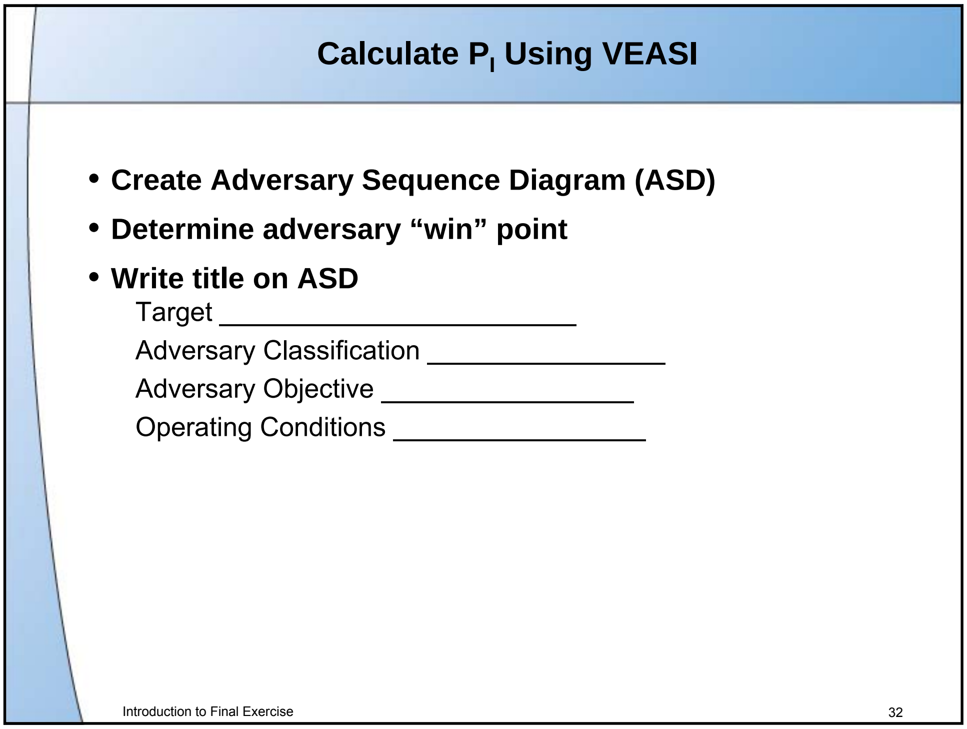
Introduction to Final Exercise 30



Calculate P_E Using VEASI

1. **Select 3 most vulnerable paths on ASD**
   - Using Response Force Time, work backwards from “Win Point” to find Critical Detection Point (CDP)… Pick fastest times after CDP
   - Pick lowest detection elements before CDP to determine the rest of the “worst paths” for you.
2. **Apply VEASI to these paths**
3. **Select most vulnerable path (lowest P_I)**
4. **Use neutralization tool to calculate P_N**
5. **Conduct scenario analysis and change data as necessary**
6. **Calculate system effectiveness to see if redesign is necessary.**

Introduction to Final Exercise 31



Calculate P_I Using VEASI

- **Create Adversary Sequence Diagram (ASD)**
- **Determine adversary “win” point**
- **Write title on ASD**

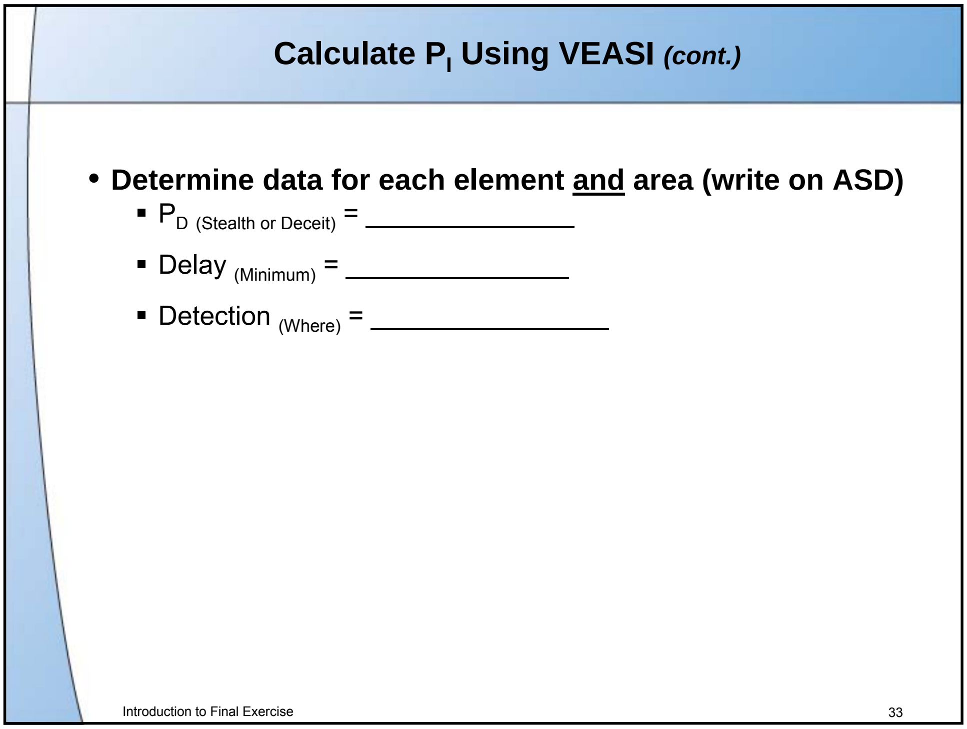
Target _________________________

Adversary Classification ________________

Adversary Objective _________________

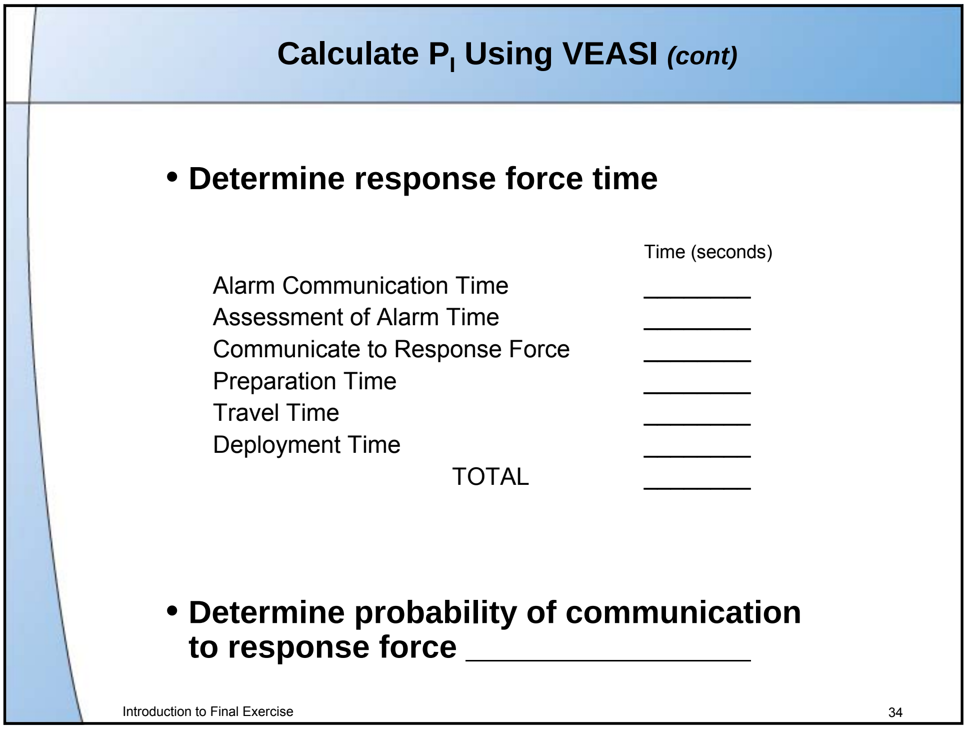
Operating Conditions _________________

Introduction to Final Exercise 32



Calculate P_I Using VEASI *(cont.)*

- **Determine data for each element <u>and</u> area (write on ASD)**
  - P_D (Stealth or Deceit) = ________________
  - Delay (Minimum) = _________________
  - Detection (Where) = __________________

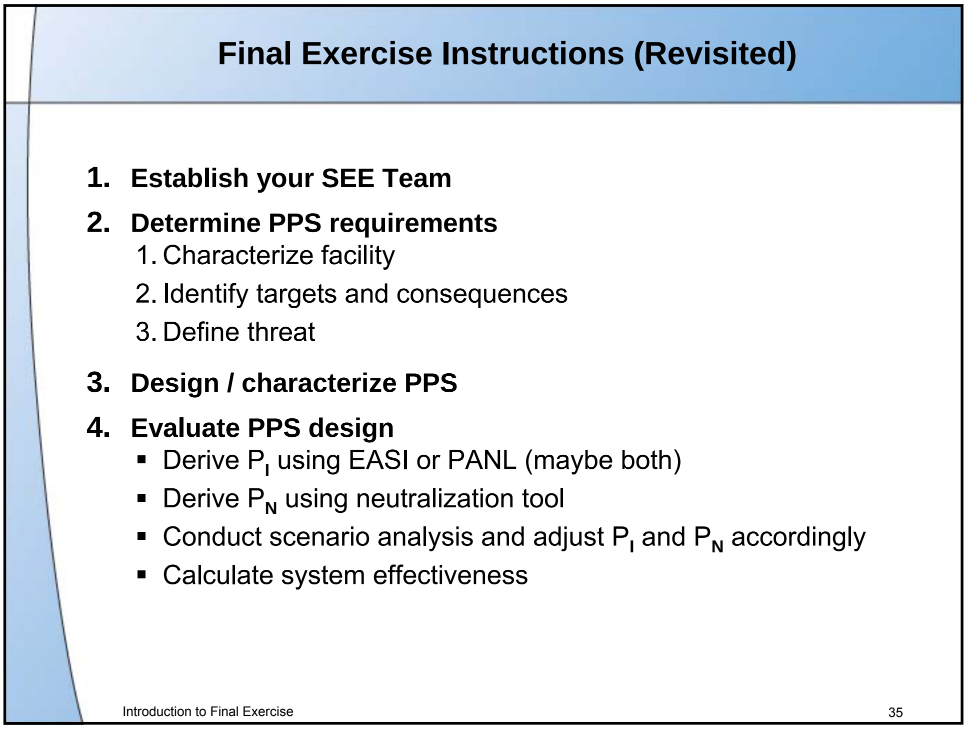


Calculate P_I Using VEASI *(cont)*

- **Determine response force time**

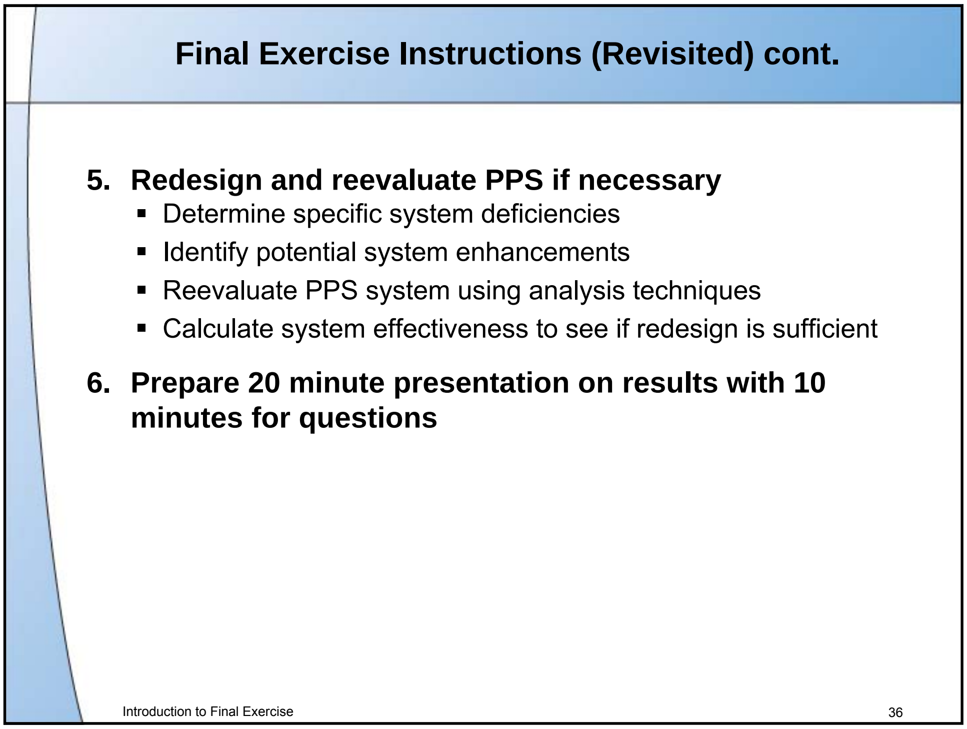
	Time (seconds)
Alarm Communication Time	________
Assessment of Alarm Time	________
Communicate to Response Force	________
Preparation Time	________
Travel Time	________
Deployment Time	________
TOTAL	________

- **Determine probability of communication to response force ______________________**



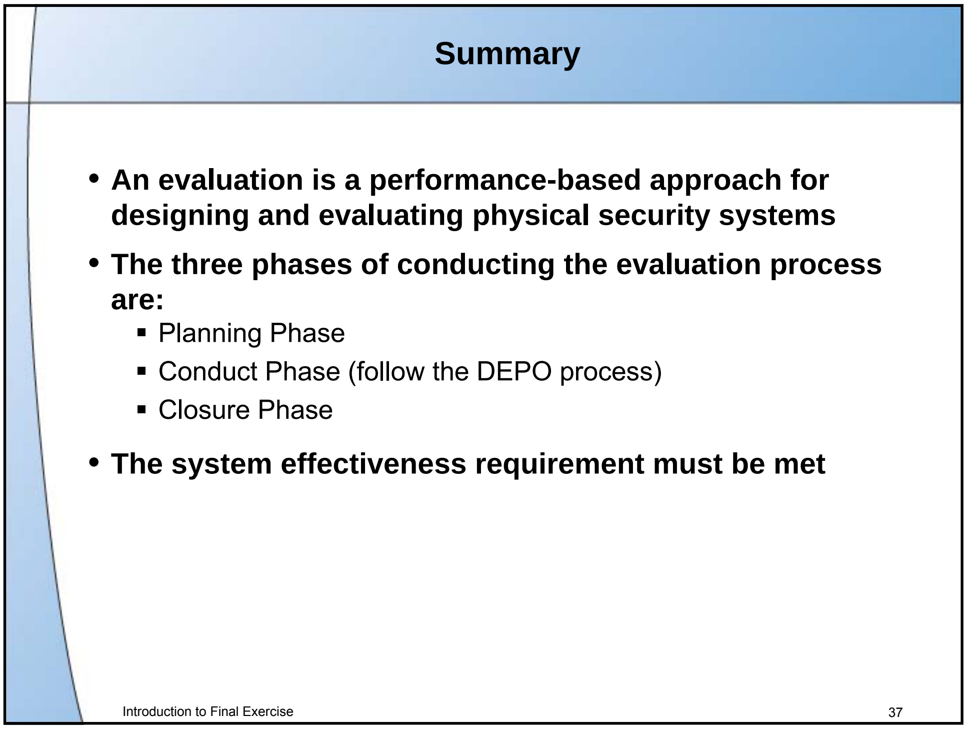
Final Exercise Instructions (Revisited)

1. **Establish your SEE Team**
2. **Determine PPS requirements**
    1. Characterize facility
    2. Identify targets and consequences
    3. Define threat
3. **Design / characterize PPS**
4. **Evaluate PPS design**
    - Derive P_I using EASI or PANL (maybe both)
    - Derive P_N using neutralization tool
    - Conduct scenario analysis and adjust P_I and P_N accordingly
    - Calculate system effectiveness



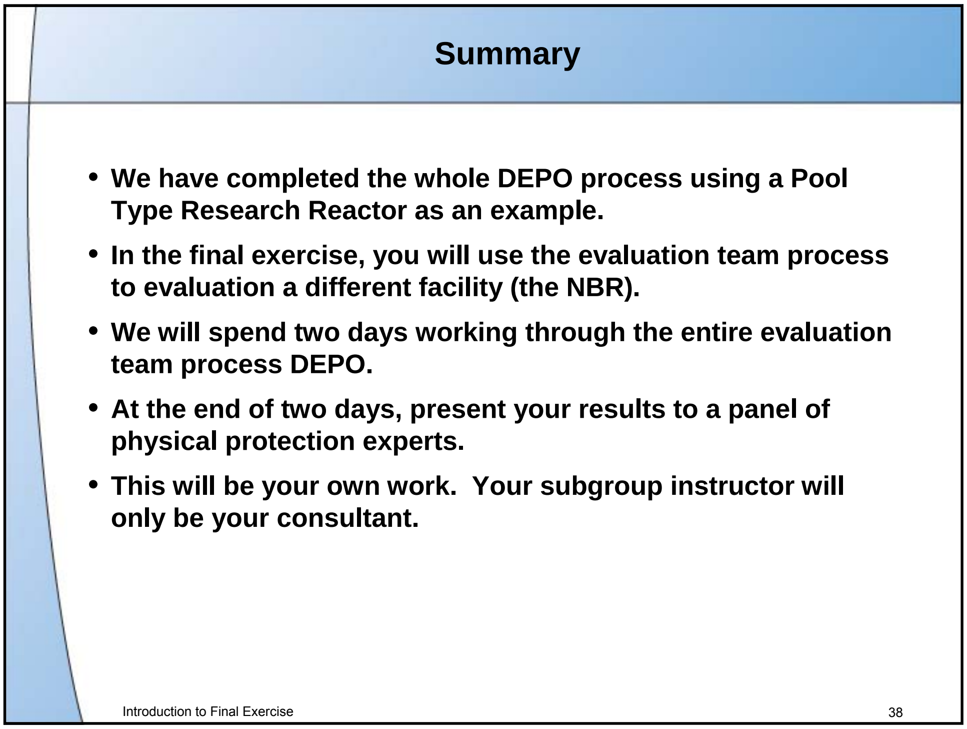
Final Exercise Instructions (Revisited) cont.

5. **Redesign and reevaluate PPS if necessary**
    - Determine specific system deficiencies
    - Identify potential system enhancements
    - Reevaluate PPS system using analysis techniques
    - Calculate system effectiveness to see if redesign is sufficient
6. **Prepare 20 minute presentation on results with 10 minutes for questions**



Summary

- **An evaluation is a performance-based approach for designing and evaluating physical security systems**
- **The three phases of conducting the evaluation process are:**
  - Planning Phase
  - Conduct Phase (follow the DEPO process)
  - Closure Phase
- **The system effectiveness requirement must be met**



Summary

- **We have completed the whole DEPO process using a Pool Type Research Reactor as an example.**
- **In the final exercise, you will use the evaluation team process to evaluation a different facility (the NBR).**
- **We will spend two days working through the entire evaluation team process DEPO.**
- **At the end of two days, present your results to a panel of physical protection experts.**
- **This will be your own work. Your subgroup instructor will only be your consultant.**

Subgroup 25S
Introduction to Final Exercise

Session Objectives

After the session, the participants will be able to do the following:

1. Apply the procedure presented in this course to evaluate a physical protection system for the Neutron Burst Reactor (NBR).
2. Utilize the analysis tools (PANL or VEASI and Neutralization) presented during the ITC to analyze the system that the subgroup designed
3. Recommend upgrade steps to correct any identified deficiencies.
4. Prepare to present the results of the PPS design and evaluation to a panel of physical protection experts.

Exercise 1 - Define Problem and Determine PPS Requirements (3 1/2 hours)

During the remaining subgroup sessions, the class participants will work in their subgroups to apply the techniques learned in this course. The subgroup will design and evaluate its own PPS for the NBR. This first exercise is devoted to defining the problem and identifying the PPS requirements by defining the facility, threats, and targets. You may use up to 3.5 hours to complete this exercise. Refer to the Exercise Data Book.

Tasks to accomplish in this exercise:

- Identify a way to complete the exercise and assign areas of responsibility among subgroup members. Remember that you will need to give a 20-minute presentation to a panel of experts.
- Specify any preliminary assumptions.
- Characterize the facility; check off each of the items under Facility Characterization on the DEPO as you consider them (drawings of the facility are provided in the Exercise Data Book). Draw an ASD.
- Identify the critical targets; consider and check off each item on the DEPO under the heading Target Identification. Consider consequence and System Effectiveness Goals.
- Specify the threat (attributes, tactics, and intent) as discussed in Threat Definition Module 5; consider and check off each item on the DEPO under the heading Threat Definition. Determine the worst threat recognizing that eventually you will have to test your solution against all the threats.

Exercise 2 - Design/Characterize PPS (4 1/2 hours)

For this exercise, use the Exercise Data Book. At this time, you are ready to make a preliminary assessment and then to design your own PPS using the physical protection technologies explained in the ITC. Manage your time so that you can complete this task within the 4.5 hours provided.

Tasks to accomplish in this exercise:

- Identify the existing PPS at the facility.
- Describe any equipment or procedures used for
  - intrusion detection (exterior sensors and interior sensors)
  - alarm assessment
  - alarm communication and display
  - entry control
  - access delay
  - response force
- Put Data on the ASD. Include title, strategy, data on elements and areas.
- Describe the response force time and communication probability.
- Consider and check off each item on the DEPO for the above areas.
- It will be clear that any analysis will result in a very low P_I and P_N. Therefore, make a preliminary design (the minimum that is obviously needed) and this will be the Base Case to be analyzed and improved, if necessary.

Exercise 3 - Evaluate PPS and Redesign, if necessary (5 hours)

Evaluate the effectiveness of the PPS you have just finished designing. The PANL or the VEASI technique should be used to perform path evaluations on the PPS. (See Tasks below.) Any vulnerabilities identified in the analysis should be addressed and the system redesigned or upgraded to correct these vulnerabilities. Analyze the upgraded PPS once again using the PANL or VEASI technique along with the neutralization tool and determine the final design of the PPS. Conduct a Scenario Analysis that will be used to modify the most vulnerable paths that were identified in the PANL or VEASI exercises. Five hours are provided for completing this exercise.

<u>Tasks To Accomplish In This Exercise</u>

- Evaluate effectiveness of the PPS by using the PANL or VEASI technique (or both).

  <u>PANL</u>

  - Evaluate using PANL
  - Calculate P_N using neutralization tool
  - Conduct a scenario analysis
  - Modify PANL and Neutralization data as appropriate
  - Identify any vulnerabilities
  - Upgrade the PPS if system effectiveness does not meet your design goals
  - Evaluate the upgraded PPS.
  - Evaluate using PANL -
  - Determine the final design of the PPS.
    - Determine upgraded system effectiveness

    - Redesign and re-analyze if not acceptable

  <u>VEASI</u>

  - Create ASD
  - Determine adversary "win" point
  - Determine detection and delay value for all elements and areas
  - Determine response force time
  - Determine probability of communication to response force
  - Select the 3 most vulnerable paths on ASD
  - Apply VEASI to these paths; Find P_I
  - Calculate P_N using neutralization tool
  - Conduct a scenario analysis
  - Modify VEASI and Neutralization data as appropriate
  - Upgrade the PPS if system effectiveness does not meet design goals
  - Calculate conditional risk

- Decide on detection, delay, and response upgrades
- Apply upgrades one-at-a-time
- Calculate new system effectiveness
- Redesign and re-analyze if not acceptable

Exercise 4 - Summary Presentation (2 hours)

Each group will present a summary presentation of your PPS and the associated analysis to a panel of ITC instructors for evaluation.

Each group will have 30 minutes total, consisting of:

- 20 minutes (or less) to present your summary. If possible, you should have all members of your group participate in the presentation.
- 10 minutes to answer questions from the panel.

Application Considerations

1. What part of the PPS design do you feel the most confident about?

2. What part of the PPS design worries you the most? What part is the least predictable?

3. Does the PPS design need to be better thought out before starting to design details?

4. What happens if the threat changes with regard to

   - Fire power (ammunition and weapons)?
   - Number of outsiders?
   - Number of insiders?
   - Site knowledge?
   - PPS knowledge?
   - Threat objectives?

5. What other methods, if any, would you use to assess the PPS capability?

6. What are the strengths and weaknesses of both PANL and VEASI analysis?

7. Which values of P_I (PANL or VEASI) do you have most confidence in and why?

8. What problems does the PPS of your facility have that were not solved in this workshop?

9. How will you use this technology in your current work assignment?

Definitions of Selected PANL Database Terms

Table of Contents

Dimensions

Distance Across

This dimension indicates the distance that the adversary must traverse to pass through the element. The default is 0 meters. If the distance across the element varies, as can happen for perimeter isolation zones, use either the average or minimum distance across the element.

Transit Speeds

PANL assumes the following transit speeds:

- Adversaries on foot travel at 4 meters/second (m/s)
- Adversaries in land vehicles travel at 16 m/s
- Adversaries in helicopters travel at 40 m/s

Path Element Characteristic Questions

There is one type of characteristic: Alarm Assessment.

Alarm Assessment

The Alarm Assessment choice applies to all intrusion detectors, including general observation. This choice will not affect performance for access control, contraband and SNM detection, and Security Officer (SO) components.

Assessment can be performed either by SO teams (SO Assessment) or Closed-Circuit Television (CCTV). CCTV Assessment choices are distinguished by whether there is automatic video recording (“instant replay”) of the sensor zone at or only after the alarm is generated. SO Assessment includes Posted SOs station at or overlooking the element and delayed and timely deployment to the element by Assessment teams. Assessment by a posted SO with a duress alarm is typically superior to deployed Assessment teams.

Choices

A. No Assessment—Alarms are ignored. All intrusion alarms at this element have a Probability of Detection of 0.

B. Delayed Deployment—This occurs if an Assessment team is deployed but their deployment is not timely.

C. Timely Deployment—This assumes the Assessment team catches the adversary in the act or that substantial, clear evidence of an adversary act, such as a demolished wall, is present when the team arrives.

D. CCTV without Instant Replay—The camera covering the sensor’s zone is turned on and the view is displayed at the alarm station. This assumes the guards at the alarm station manually switch cameras as a worst-case response.

E. CCTV with Instant Replay—A video recording of the sensor zone occurs simultaneously with or just after the alarm is generated (e.g., “frame grabbers”).

F. Posted SO with Duress Alarm—The guard posted at the element can quickly signal to the alarm station that an unauthorized adversary action is occurring.

G. Automatic Deployment of Response Force—Certain sensors may be so strategically important and may have a low false-alarm rate that any alarm is considered to be a real attack and response forces are automatically deployed. This assumes a full-sized response is sent after an alarm—not just an Assessment team—without waiting for an Assessment.

PANL assumes that detections by Security Officers, through reports or duress alarms, are always treated as real and are not assessed as such. Sensing of abnormal conditions by access control, contraband, SNM detectors, and material transfers are assumed sufficient to impede forward passage of the insider and deceitful passage by the outsider so the Probability of Assessment equals one for such components.

Passage Classes

There are three passage classes —Persons, Packages/Shipments, and Vehicles—that correspond to the types of items that pass through elements that allow authorized passage, such as doors and portals.

Definitions

Persons

This passage class has two groups: Pedestrians and Drivers.

- Pedestrians are authorized personnel who pass through a door, portal, or gate on foot apparently without a vehicle.
- Drivers are those who accompany a vehicle as it passes through an element. Because a vehicle cannot accompany a person through a personnel portal, drivers are not allowed through personnel portals.

Packages/Shipments

There are four groups that fall under this class: Personnel Possessions, Packages, Tools/Equipment, and Shipments/Cargo.

- Personnel Possessions are items such as lunchboxes, handbags, and briefcases that are normally carried by a person.
- Packages are sealed boxes brought in by persons.
- Tools/Equipment are items normally carried by facility employees.
- Shipments/Cargo are items brought in by vehicles.

Vehicles

This passage class can three groups of vehicles: personal vehicles, site vehicles, and shipment/delivery vehicles. The term "vehicle" typically refers to automobiles, trucks, or buses.

- Personal vehicles are offsite vehicles operated by employees or visitors coming into the facility.
- Site vehicles belong to the facility and are generally not used to transport material offsite.
- Shipment/delivery vehicles are offsite vehicles associated with shipments, supply trucks, or emergency vehicles such as ambulances or fire trucks.

Modeling Passage of Persons and Vehicles Through Vehicle Gates and Portals

The Persons passage class has two groups: pedestrians and drivers. This section will define pedestrians and drivers and discuss how they should be modeled at vehicle gates and vehicle portals.

Pedestrians are persons who pass through a vehicle gate or portal on foot and do not declare that they have a vehicle. To indicate that an adversary using a scenario is on foot, indicate “Foot” under transportation on the element strategy page. Drivers are persons in vehicles passing through a vehicle gate or portal. Drivers may stay in the vehicle, pass through the vehicle gate or portal on foot, or pass through an adjacent personnel portal on foot while their vehicle passes through the vehicle portal or gate.

Correct modeling at vehicle gates and portals is more complex than at a personnel door or portal because the analyst must consider several factors:

- How do both drivers and vehicles normally pass through the vehicle gate or portal?
- Are pedestrians also allowed through?
- Do drivers stay with their vehicle at the vehicle gate or portal or are they are required to leave the vehicle and be checked at an adjacent personnel portal?

In this last case, the analyst must define the vehicle gate or portal in such a way that outsider “force paths” through the vehicle portal and “deceit paths” through the personnel portal are both modeled at the vehicle gate or portal element. To do this, the user must define at the vehicle gate or portal all components that apply to the driver, even if these components are physically located at another PE. This is explained in more detail below.

Table 1 summarizes the various pedestrian, driver, and vehicle passage combinations and how these are modeled in PANL. Some of these combinations are considered to be inconsistent, such as vehicles allowed but no drivers, and should not normally be modeled; if modeled, however, the Table shows how these combinations are handled.

Modeling of Specific Vehicle Gateway or Portal Cases

There are two ways that drivers and their vehicles may pass through a vehicle gateway or portal:

The driver accompanies the vehicle through the vehicle gateway and is subjected to whatever ID and contraband checks that exist at the gateway, or

The driver is required to leave the vehicle and submit to the ID and contraband checks at a nearby personnel portal before he is allowed to return to the vehicle gateway to drive the vehicle through it. The correct modeling of each of these cases is described below.

For Case 1, Drivers Allowed and Vehicles Allowed is selected from the passage classes. As in all other PEs, the components at the vehicle portal or gateway are selected and applied.

For Case 2, Drivers Allowed and Vehicles Allowed is selected from the passage classes, as Case 1. All of the components at the vehicle portal or gateway should also be selected and applied. Additionally, the personnel ID check, contraband, and SNM components that are actually located at the personnel portal should be defined at the vehicle gateway or portal. They should also be defined at the central location of the vehicle portal or at the inner location of the vehicle gate.

At some sites pedestrians are allowed through a vehicle gateway or portal even though they do not have a vehicle. If this is the case, then Pedestrians Allowed is selected for passage.

Modeling of Consistent Cases

Passage Allowed?			**INTERPRETATION**	
Pedestrians	Drivers	Vehicles	**THREATS WITH VEHICLE**	Threats on Foot
Yes	Yes	Some	Adversary can 1) pass as a driver with a vehicle; or 2) pass as an apparent pedestrian and smuggle contraband on a vehicle driven by another person. PANL calculates the best way to bring in the contraband.	Adversary can pass as a pedestrian.
No	Yes	Some	Adversary can pass as a driver with a vehicle.	No authorized passage, so the adversary must use force/stealth to defeat the PE.
Yes	No	None	Adversary must abandon his vehicle at this element and pass as a pedestrian. He obtains a site vehicle in the next area.	Adversary can pass as a pedestrian.
No	No	None	No authorized passage so the adversary must use force/stealth to defeat the element.	No authorized passage so the adversary must use force/stealth to defeat the element.
Modeling of Inconsistent Cases				
Yes	No	Some	Adversary can pass as an apparent pedestrian and smuggle contraband on a vehicle driven by another person.	Adversary can pass as a pedestrian.
Yes	Yes	None	Adversary must abandon his vehicle at this element and pass as a pedestrian. He obtains a site vehicle in the next area.	Adversary can pass as a pedestrian.
No	Yes	None	No authorized passage, so the adversary must use force/stealth to defeat the PE.	No authorized passage, so the adversary must use force/stealth to defeat the PE.
No	No	Some	No authorized passage, so the adversary must use force/stealth to defeat the PE.	No authorized passage, so the adversary must use force/stealth to defeat the PE.

Interpretation of Persons—Vehicle Passage Cases in PANL

Components Section—Overview

The Components section has all information associated with the components in a path element or target location element. Components are organized into six component categories: Access Control, Contraband Detection, SNM Detection, Intrusion Detection, Access Delay, and Security Officers. The categories available in an element report change depending on the type of element. For example, fence lines and surfaces do not offer access control components.   The components may be located at several component locations in the element, designated as Outer, Central Outer, Central, Central Inner, and Inner. Installed components are marked on the left with a check. No components are installed when a new element is created.

Expansion/Compression Boxes—Expanding a component class heading reveals all of the components in this class that can be installed in the element.

Activity Boxes—Each component line also has a pair of checkboxes at the far right to indicate if the component is active on entry to, or exit from, the facility. These checkboxes are similar to those found in the Passage section, and are grayed out until the component is installed. Components which may be active against some passage groups and not others are called passage dependent. Some Contraband Detection components, such as metal and explosives detectors, are passage dependent, since a metal detector might be used to check pedestrians but not packages. These components display a pair of “diamond boxes” at the far right. A diamond box with a full black diamond indicates that the component is active against all passage groups in the corresponding direction while a half-full diamond indicates that the component is active against at least one but not all passage groups in the corresponding direction. An empty diamond box indicates that the component is not active against any passage group in the given direction.

Terms and Concepts for Components Categories

Equipment Categories

This section defines the adversary equipment categories found in the PANL database, used by the PANL module of the PANL code. PANL uses the following categories of adversary equipment in its database:

Independent (INDP)

No Equipment (NOEQ)

Contraband

- Metal Contraband
- Radioactive Contraband

Defeat/Breaching Tools

- Hand Tools
- High Explosives
- Land Vehicle (as a ram)
- Power Tools

Transportation

- Land Vehicle
- Helicopter

Weapons

- Small Arms
- Light Anti-tank Weapons (LAWs)

There is another category allowed in the database—visible contraband—that is currently not used by any component.

Independent

The “Independent” equipment category assigns the same probability of detection or delay time for every adversary, regardless of what set of equipment (contraband, breaching tools, transportation, or weapons) they bring. For example, ID Checks, such as badge checks, have probabilities that do not depend on what other equipment the adversary brought, but would depend, presumably, on forgery or theft of badges before the attack.

No Equipment

The “No Equipment” category assumes that the adversary does not bring tools (besides his own hands) that might help defeat this component if it is a barrier; does not bring contraband that might set off this metal, explosive, or SNM detector if the component is a contraband detection component; comes in on foot if the issue is transit time; and does not bring weapons if the component depends on adversary weapons equipment.

Contraband Detection

- Metal Contraband (METL)—This indicates that the threat is carrying metal contraband that can set off metal detectors. This is assumed to be the case when the adversary threat has hand tools, power tools, small arms, or LAWs but it could be assumed when none of these are present.
- Radioactive Contraband (RDEM)—This indicates that the threat is carrying radioactive material (e.g., uranium or plutonium) that can be sensed by SNM detectors.

Defeat/Breaching Tools

For most component choices, delays are listed for the following categories of attack tools:

1. No Equipment (NOEQ)
2. Hand Tools (HTLS)—sledges, axes, bolt cutters, wrecking bars, metal cutters, ladders, etc.
3. Power Tools (PTLS)—powered hand tools (hydraulic boltcutters, abrasive saws, electric drills, rotohammers) and thermal cutting tools (oxyacetylene torches or oxygen lances)
4. Explosives (EXPL)—bulk, tamped, linear- and conical-shaped charges, platter charges
5. Vehicles (VEHI) used as rams

Weapons

SOs at Post or in Towers have delays that depend on whether the adversary has LAWs; Small Arms (ARMS); or NOEQ, which assumes none of these weapons are used by the adversary.

Notes on the Delay Values in the PANL Database—The delays represent mean delay times and are displayed in units of seconds. Some entries in the PANL database listings deserve comment. PANL represents actual delays as integers between 0 and 9999 seconds. Any delay of 30000 seconds or more is truncated to 30000 seconds and it is assumed that the adversary cannot penetrate such a barrier. The acronym DNA indicates that the type of adversary equipment listed “Does Not Apply” to this component—that type of adversary equipment is not considered when determining delays. In practical terms, a “DNA” is equivalent to a delay of 30000 seconds.

The delays in the PANL database are representative estimates, most of them produced by a barrier expert at Sandia. This expert used a slightly different categorization of attack tools:

1. Hand Tools
2. Power Tools
3. Thermal Tools
4. Explosives—Used alone
5. Hand, Power, and Thermal Tools, and Explosives

6. Vehicles

To create the PANL database from the expert's numbers, the Hand Tool and Vehicle estimates were unchanged and the expert's Power tool and Thermal tool estimates were combined into the Power Tool category by taking the lower of the two. The Hand, Power, and Thermal Tools and Explosives estimates typically represent the smallest delay of the Hand Tool, Power Tool, Thermal Tool, and Explosives categories as well as considering the use of all these tools to penetrate concrete walls. The Explosives category in the PANL database generally corresponds to the Hand, Power, and Thermal Tool and Explosives estimate rather than the Explosives (alone) estimate, when these differ.

The No Equipment estimates were created by the PANL development team because of the need for delays for adversaries who were not carrying contraband. Very few tests—mostly defeat of perimeter fences—have been conducted by Sandia without using equipment because this is below the standard US DOE threat. Lacking this experimental database, the PANL development team set these No Equipment delays as 30000 seconds (barrier not penetrable) with the following exceptions:

1. Perimeter chain link fence delays are based on test data
2. Vehicle barrier delay is set to 0, representing no delay to adversaries on foot
3. Half-height turnstile delays are set to 1 second, representing that an adversary could jump over them
4. The bars on aluminum turnstiles could be bent by an adversary.
5. The windows and doors with window panels consisting of 1/4" tempered or laminated glass or acrylic plastic could be kicked in.
6. Relatively weak wall barriers, such as wood studs and plywood, could be kicked in.
7. Standard or reinforced gloves could be torn off.
8. The minimal task time was set at the uniformly low value of 15 seconds across all equipment categories.

For most barriers in the database, the barrier is clearly not penetrable. The window, door, and wall delays that are assumed to be penetrable may not be, depending on the capabilities of the assumed threat and local construction. Others that are assumed to be impenetrable, such as steel turnstiles, might be penetrable without using equipment, depending on the adversary's strength.

Access Control Components (including locks)

These describe controls that control movement for different types of persons and types of vehicles.

Comparisons

Lock Versus Lock A and Lock B

Lock—One key or combination serves to open a door or gate.

Lock A, Lock B—Two locks with independent control of each key or combination (or two independent keys to one lock) are required to open a door or gate. Both need to be installed at the same time.

Distinction—Use a lock when a single key or combination will open the door or gate and use both Lock A and Lock B when control over entry has been divided between personnel by using two means of control—keys or combinations.

Definitions and Choices

ID Verification

An ID verification is a component to control access based on identity that is not directly associated with a lock. It can be used at an open passageway where an SO checks the person's ID before he is allowed through. It can also be used in conjunction with a Lock component (e.g., padlock or combination lock) at an element that is locked with a conventional lock, at which the person is not allowed to proceed unless he passes the ID Check.

Choice Lists for:		
ID Check	ID Actuated Lock	Choice Definitions for Identity Verification Components
A	A	Casual recognition—Guard looks at person to make sure there is nothing suspicious about them. No check of identity per se.
B	B	Credential—A code on a card or badge is checked.
C	C	Credential and Personal Identification Number (PIN)—A code on a card or badge is checked and the person enters a PIN unique to him.
D	D	Picture badge—The person’s face is checked against that on their badge that is taken out of the area.
E	E	Picture badge and PIN—The person’s face is checked against the photo on the badge that is taken out of the area. The person must also run a credential through a reader and enter a PIN.
F	F	Exchange picture badge—The person’s face is checked against the photo on the badge that is taken out of the area. The person is then issued a badge that is surrendered when the person leaves the site.
G	G	Exchange picture badge and PIN—The person’s face is checked against the photo on the badge that is taken out of the area. The person also enters a PIN to receive a badge that is surrendered when the person leaves.
H	H	Retinal scan and PIN—The pattern of blood vessels on the person’s retina is checked against a pattern stored in a database. The person must also enter a PIN.
I	I	Hand geometry and PIN—The pattern of spacing and sizes of fingers on one of the person’s hands is checked against a pattern stored in a database. The person must also enter a PIN.
J	J	Speech pattern and PIN—The pattern of speech that a person uses to repeat certain phrases is checked against a pattern stored in a database. The person must also enter a PIN.
K	K	Signature dynamics and PIN—The pattern of movement and pressure that a person uses to write certain phrases is checked against a pattern stored in a database. The person must also enter a PIN.
L	L	Fingerprint and PIN—The patterns on a person's fingerprint are checked against a pattern stored in a database. The person must also enter a PIN.

Lock

If a door or gate is locked with a single conventional lock using a combination or key, then the Lock component is selected.

Lock A, Lock B*

If a door or gate is locked with two locks with independent control of different keys or combinations, (or one lock with two independent keys), then two components—Lock A and Lock B—need to be recorded.

Choice Lists For:				
Glove Port Lock	Lock, Lock A, Lock B	Window Lock	Window Barrier Lock	Choice Definitions for Conventional Lock Components
A	A	A	A	Padlock—Consists of a locking mechanism within a padlock body, a shackle (a “U”-shaped piece of metal) controlled by the locking mechanism, and a hasp (a metal fastener with a minimum of two sections attached to the barrier). When the barrier is locked, the sections of the hasp are positioned together in such a way that the shackle is inserted between both sections to fasten them together.
B	B	B	B	High security padlock*—A padlock in which the shackle is shrouded by a hardened barrier. Includes a changeable cylinder and a dead bolt-locking mechanism.
C	C	C	C	Keyed cylinder—Door locks that consist of a cylinder case containing a cylinder plug or core. The proper key forces pins into a position so that the cylinder plug can be rotated.
D	D	D	D	Combination—Door locks that open when the proper combination is entered by spinning a dial and stopping at the correct numbers.
-	E	-	-	Mechanically coded—This refers to a self-contained door lock operated by push-buttons. The lock controls a bolt or latch.
-	F	-	-	Electronically coded—This is a lock that stores electronic codes in firmware that, when accessed, allows a mechanical assembly to be operated.
-	G	E	E	Inaccessible—This is a lock that an adversary cannot reach to attack (choice forces adversary to attack door itself).

* The keyed cylinder and combination locks refer here to door locks when these locks can also be found in padlocks. Use the padlock choice where a keyed-cylinder or combination lock is used as part of a padlock.

Vehicle Authorization Checks

These components verify that a vehicle has the right to enter or exit the facility. Because personnel vehicles may be checked differently than site or shipping and delivery vehicles there are three components that can be selected—Vehicle Authorization Check 1, Vehicle Authorization Check 2, and Vehicle Authorization Check 3.

Choice Lists for:	
Vehicle Authorization Check 1, 2, 3	Choice Definitions for Vehicle Verification Components
A	Visual check of insignia/license plate—The guard checks that the vehicle has a correct type of license plate, sticker, or insignia on it before letting it pass.
B	Authorization form check—The vehicle driver brings a form W signed by appropriate site management, which allows entry.
C	Serial number verification—Serial numbers etched into the vehicle are checked against an access list.

Contraband Detection Components

These components describe checks for contraband—guns, explosives, attack tools—on different types of persons, types of packages, and types of vehicles.

Comparisons

Hand-Held versus Portal Detectors

Hand-held detectors are employed by SOs to scan people or packages.

Portal detectors are "walk through" and typically scan people (e.g., airport metal detectors).

Definitions and Choices

Metal Detectors

Hand-held units are used by SOs to scan people or packages while portal detectors are "walk-through" units similar to those at airports.

Choice Lists for:		
Handheld Metal Detector	Portal Metal Detector	Choice Definitions for Metal Detector Components
A	A	Ferrous materials only—Does not detect any lead shielding.
B	B	Ferrous and solid lead materials—Does not detect other types of lead shielding.
C	C	Ferrous materials and all forms of lead—Detects all types of lead shielding.

X-Ray Inspection

Choice Lists for:	
X-Ray Inspection	Choice Definitions for X-Ray Inspection Components
A	Standard—An x-ray unit with the sensitivity equivalent to those found at airports

Item Inspection

Choice Lists for:	
Item Search	Choice Definitions for Item Search Components
A	Cursory—The package containing the item is opened and its contents viewed.
B	Rigorous—All of the items in the package are removed and carefully inspected.

Vehicle Search

Choice Lists for:	
Vehicle Search 1	Choice Definitions for Vehicle Search 1 Components
A	Cursory—The doors, trunk, and hood of the vehicle are opened and the interior is viewed. In buses, the guard enters the bus and walks down the length of the bus, looking under seats.
B	Rigorous, including cargo—This search is a cursory search, plus use of mirrors under the vehicle and a careful search for hidden compartments. All items in the vehicle are removed and carefully inspected.

SNM Detection Components

These components describe checks for special nuclear material (SNM) on different types of persons, types of packages, and types of vehicles.

Comparisons

Hand-Held versus Portal and Drive-Through Detectors

Hand-held detectors are employed by SOs to scan people or packages.

Portal detectors are “walk through” and typically scan people.

Drive-through detectors scan vehicles.

Definitions and Choices

SNM Detectors

These detectors detect SNM.

Choice Lists for:			
Drive-Through SNM Detector	Hand-held SNM Detector	Portal SNM Detector	Choice Definitions for SNM Components
A	A	A	Sodium iodide scintillator—uses this type of detector.
B	B	B	Plastic scintillator—uses this type of detector.

Intrusion Detection Components

These are sensors or employees who detect adversaries attempting to perform an unauthorized entry, using force or stealth, through the element.

Comparisons

Exterior versus Interior Sensors

Exterior intrusion sensors are used in open areas and are exposed to different weather conditions and to vehicular and other outside inputs.

Interior intrusion sensors are used in closed-room or building areas.

Single, multiple, or complementary sensor installations

Single-sensor listed—1 sensor (e.g., microwave)—is installed at this location.

Multiple complementary sensors—multiple sensors are present and installed in such a way that one sensor covers another’s weaknesses in terms of detection and provides adequate detection capability under various environmental conditions, such as temperature, rain or snow, vibration, and high wind.

Multiple noncomplementary sensors—multiple sensors are present at a location but do not meet the definition of complementary sensors.

Definitions and Choices

Exterior intrusion sensors

These intrusion sensors are used in open areas and are exposed to different weather conditions and vehicular and other outside inputs (e.g., buried seismic cable sensors).

Interior intrusion sensors

These intrusion sensors are used in closed-room or building areas. There are many sensors that can be used as either exterior or interior applications, but their installation and performance may be different in each area (e.g., ultrasonic sensors).

General Observation

This component is designed to give credit to detection by employees (other than SOs) of any unauthorized act.

Choice Lists for:	
General Observation	Choice Definition for General Observation Components
A	Personnel generally in vicinity—There are occasions when employees are not in the area at which time the adversary can choose to perform an unauthorized act. The Insider module assumes that an insider adversary will choose one of these occasions to perform his act.
B	Personnel always in vicinity—Employees are always there; adversary could not find a time during this element condition in which employees are not present.

Access Delay Components

These components, such as barriers, impede adversary movement through the facility.

Note that locks are considered under Access Control.

Definitions

Infinite Delays

Infinite delays arise in the PANL analysis when the adversary does not possess adequate tools or equipment to defeat the delay component: PANL assigns an infinite delay to that component. If the adversary is on the part of the path where he attempts to defeat such a component, then his progress along that path is terminated. An infinite delay can occur from a physical barrier, a lock that cannot be opened, or an SO that cannot be overcome.

Stage 1 and Stage 2 Delays for High Explosives

When certain types of high-explosive attacks are used on very thick reinforced concrete, there is a long delay after the explosion while the adversary returns to the hole and uses cutting tools to remove any remaining reinforcing bar (rebar) or concrete. This delay after the blast is called the Stage 2 delay.

To determine the explosive attack Stage 1 and Stage 2 delays for user-defined component performance overrides for the outsider threat, assign Stage 1 and Stage 2 delays as follows:

- Stage 1 Delay includes time to set up the explosive package and retreat to a safe range before the device explodes.
- Stage 2 Delay includes wait time after the blast for debris to settle, time to return to the hole, cut through any remaining wall or debris, and crawl through the barrier. If the cut-through time is not significant, as with non-substantial barriers, typically the return time and crawl-through time are lumped into the Stage 1 Delay (leaving a 0-second Stage 2 Delay).

Security Officers (SO) Components

SO is a term for a guard. There are three types of SO-related components that are modeled:

1. SO at Post
2. SO in Tower
3. SO on Patrol

The Facility Module allows the analyst to locate each of the three types of SOs at outer, inner, and central locations on the PEs. Their actual locations at a specific site can thus be properly selected. Care must be taken not to model the same SO more than once.

SOs at posts and in towers are modeled as composite components and are assigned both detection and delay values in the PANL Module. In both cases, the SO's detection capability depends on whether the SO can be incapacitated before he can send an alarm. The detection probability used in the data base is high if the SO has a duress alarm and is protected against the assumed adversary armament, and is zero if he has no duress alarm and is unprotected. The SO's delay capability depends on his protection after the adversary has been detected. There are three levels of protection used—unprotected, inside a small-arms-resistant structure, or inside a LAW-resistant structure.

SO at Post

SO at Post components have delay times and detection probabilities assigned to them in the PANL module. The detection probability depends on whether the SO(s) can send an alarm if attacked. This, in turn, depends on whether the SO has a duress capability and on his protection (i.e., unprotected, small-arms protected, LAW protected) against hostile fire during normal operations before the facility has alerted him that an attack is underway.

The delay value of a post will depend on how it is protected after a facility alert occurs. This may differ from the protection before alert because the alerted SO may be able to take up a more secure position.

Examples:

- No duress, no protection, LAW-protected on alert—This indicates the SO at post does not have a duress switch and that before a site alert, the SO has no protection against small arms. After a site alert, the SO moves to a bunker that is protected against small arms and Light AntiTank weapons (LAWs).
- Duress, small-arms protected—Here, the SO at post does have a duress switch, either at the post or on his radio. Regardless of whether the alert has occurred, the SO remains in a position that is hardened against small arms.

An SO at a post may or may not have a duress alarm. Also, before an alert, he may be located in a visible and vulnerable place under normal facility conditions, but when an alert is given, he may move to a protected position. The list of choices under the SO at Post allows the analyst to choose the conditions that exist at his facility. If the SOs remain in the same place before and after an alert, then only one protection choice is selected. If they move to a harder place after an alarm, the proper protection choice for both detection and delay places is selected. For example, if an SO with duress is normally unprotected, but moves to a LAW-resistant position after an alert, the choices are “Duress, unprotected; LAW protected on alert.”

If more than one SO is stationed at a post, and protection varies among these SOs, then base detection on the best duress-hardening combination for SOs that can observe what is happening at that element. For instance, a portal might include an SO in a hardened station but if he cannot see what is happening outside of the station, do not use this SO for detection.

SO in Tower

SO in Tower components have delay times and detection probabilities assigned to them in the PANL module. The detection probability shown is really the smaller of two probabilities:

- the probability that the tower can detect an adversary sneaking stealthily past the tower
- the probability that the SO(s) can send an alarm if attacked forcefully. This depends, in turn, on whether the SO has a duress capability and on his protection (e.g., small-arms protected or LAW protected) against hostile fire during normal operations before the facility has alerted him that an attack is underway.

The delay value of a tower will depend on how long the SO in the tower can slow down the adversary before either the SO is incapacitated, which depends on his protection (e.g., small-arms protected or LAW protected), or the adversaries cross the field of fire of the tower.

Tower protection from small-arms or LAWs is assumed to be the same before or after a site alert. For example, the SO in the tower cannot move from a small arms-resistant tower to a LAW-resistant tower after a site alert has been sounded.

SO in Tower has both delay and detection, as SO at Post does, but does not require separate hardness answers for detection and delay. In a typical tower, the SO cannot make the tower any harder when he is alerted to an intrusion. For this reason, SO in Tower only displays the detection duress-hardening combinations.

SOs on Patrol

SOs on patrol are given only a detection capability because they are usually insufficiently protected to survive a surprise attack and because of the low probability that they will be at the same location when the adversary is there.

Path Element Types

Comparisons

Ducts Versus Overpasses and Tunnels

These represent ways to cross under (tunnels), over (overpasses), or through (ducts) other path elements.

- Tunnels include drainage pipes, utility, and other access conduits.
- Overpasses are elevated structures, such as a roof, that allow adversaries to cross from one area to another.
- Ducts are located between the ceiling and roof of a building and include HVAC ducts.

NOTE: Ducts and tunnels can be used for passage and diversion of SNM.

Doors Versus Gates and Portals

Door exits, pass-throughs, and gates represent one layer of protection while portals and corrals have two layers of protection within the element.

Comparison of single-layer with their "corresponding" double-layer path elements:

Single Layer	Double Layer
Emergency Exit	Emergency Portal
Material Pass-through	Material Portal
Personnel Doorway	Personnel Portal
Shipping/Receiving	Shipping/Receiving
Doorway	Portal
Vehicle Doorway	Vehicle Portal

The different types of portals allow different passage or are located in different parts of the facility (the corresponding single-layer element has the same passage limitations):

Type of Portal	Passage Limitation
Personnel	Only personnel can pass through from one area to another normally.
Emergency	Personnel are authorized to exit only during an emergency.
Material	Used to pass material only from one area to another; personnel are not allowed passage.
Shipping/Receiving	Used to move vehicles through, usually associated with building boundaries.
Vehicle	Used to move vehicles through, usually located outside buildings.

Fenceline Versus Isolation Zone

Isolation Zones represent “clear-zones” while fencelines represent single fences.

Definitions

Emergency evacuation corrals—These represent safe-haven, enclosed, secured areas where evacuees go during a real or practice evacuation.

Gateway—These are entryways associated with a single layer of fencing on the perimeter of a facility and allowing vehicle traffic.

Helicopter Flight Path—This models the flight that a helicopter or other airborne adversary vehicle would take into the facility from the time that it would first be detected until the time that it arrives at the area it will land in.

Portals—These are airlocks with both doors and surfaces within a single layer of protection.

Surface—These are models walls, roofs, and floors of a building.

Window—These models windows or just big holes in surfaces.

Target Locations

The adversary does not pass through target locations but penetrates them to remove the material so Access control components at target locations serve to allow the target to be opened, not passed through. Only outer and central locations exist at target locations.

Boundary Barrier and Penetration Elements

SUR	Surface	Represents walls, floors, and roofs	
WIN	Window		
DUC	Duct	Represents Penetrations above Grade	Includes HVAC penetrations
TUN	Tunnel	Represents Penetrations below Grade	Includes Drainage Pipes and Conduits

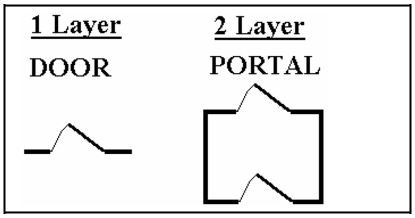
Miscellaneous Elements

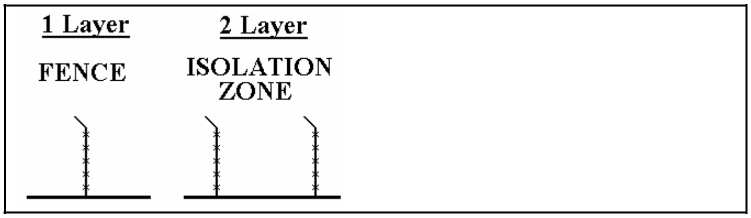
HEL	Helicopter Flight Path	Represents Transit Delay onto Site and Delays Unloading Personnel

Single-Layer/Double-Layer Elements

This category includes element types that occur in pairs:

- One of the pair represents a single-layer barrier;
- the other includes two copies of the same barrier (hence double-layer barriers)





Single-Layer Elements		Double-Layer Elements		Comments
FEN	Fenceline	ISO	Isolation Zone	Surrounds exterior area (e.g., Protected Area)
		OVP	Overpass	Like Isolation Zone but over Buildings
GAT	Gateway			For Human and Vehicle Movement
DOR	Personnel Doorway	PER	Personnel Portal	For Human Movement
MAP	Material Pass-through	MAT	Material Portal	For Material Movement Only
VHD	Vehicle Doorway	VEH	Vehicle Portal	For Vehicle Movement, usually outside
SHD		SHP	Shipping/ Receiving Portal	For Vehicle Movement, restricted to building boundaries (shipping docks)
EMX	Emergency Exit	EMP	Emergency Portal	For Emergency Egress

Types of Path Elements By Groups