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

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,

Actions

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.

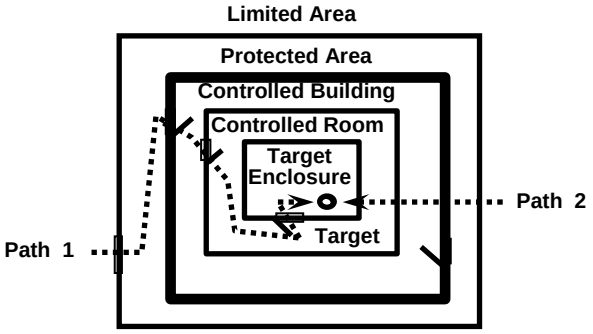


Figure 17-1. Possible Adversary Paths for a Sabotage Threat

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.

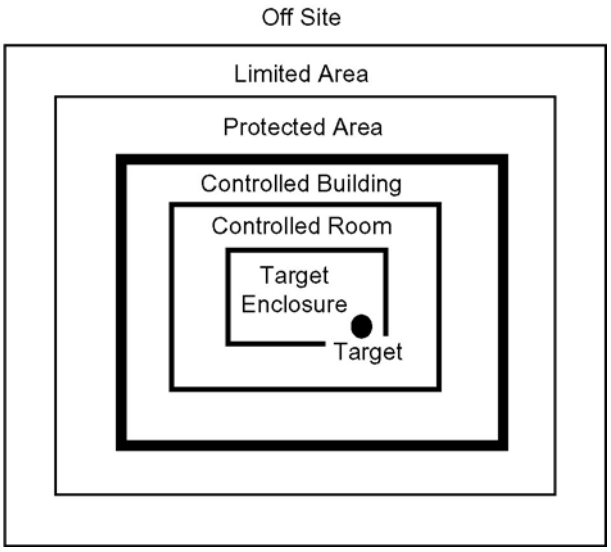


Figure 17-2. Basic Areas At An Example Facility

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.

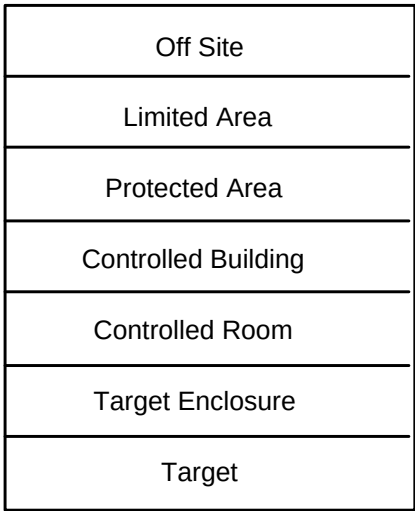


Figure 17-3. Adjacent Physical Areas—Example Facility

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.”

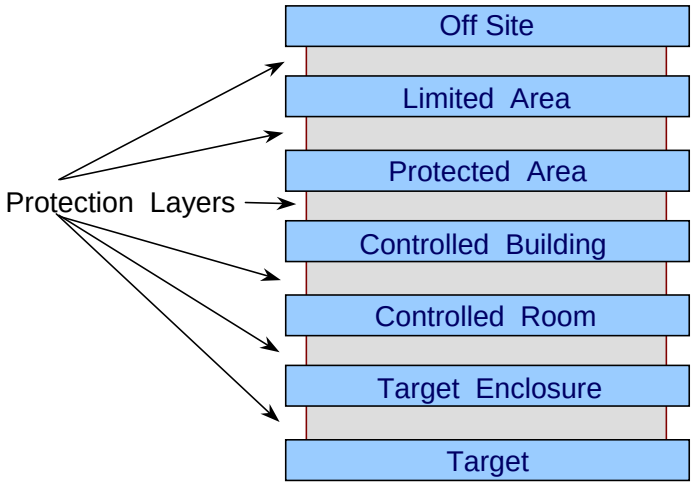


Figure 17-4. Protection Layers Between Adjacent Areas

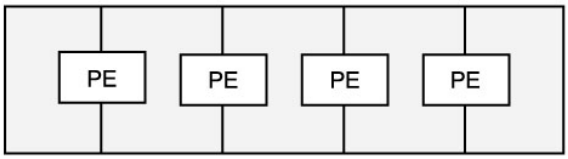


Figure 17-5. Protection Layers Consist of Path Elements

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.

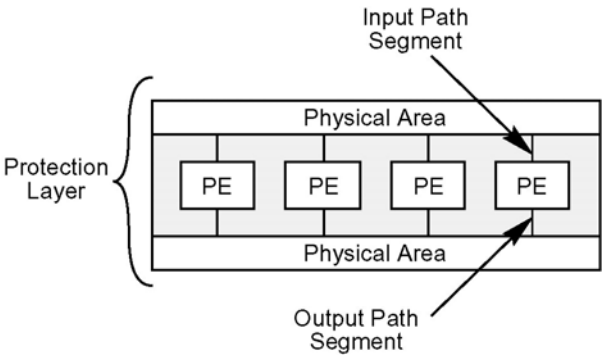


Figure 17-6. Path Element—Input and Output Path Segments

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.

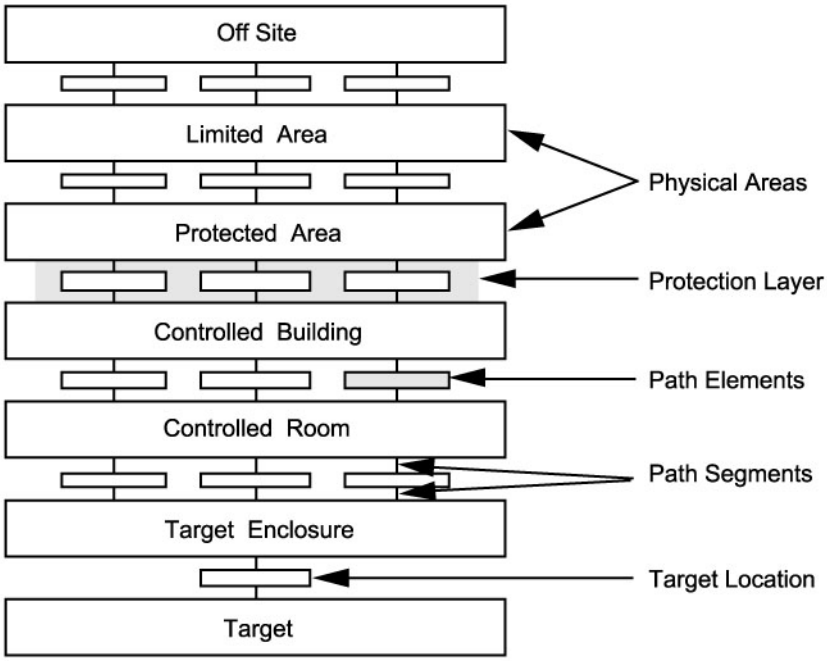


Figure 17-7. ASD Concept

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.

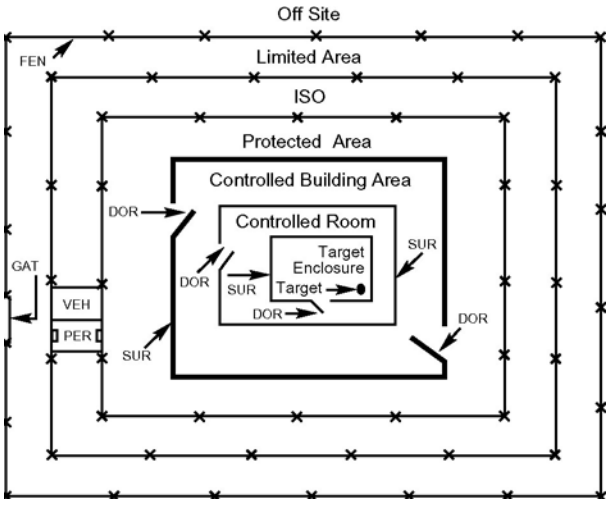


Figure 17-8. Sample Facility

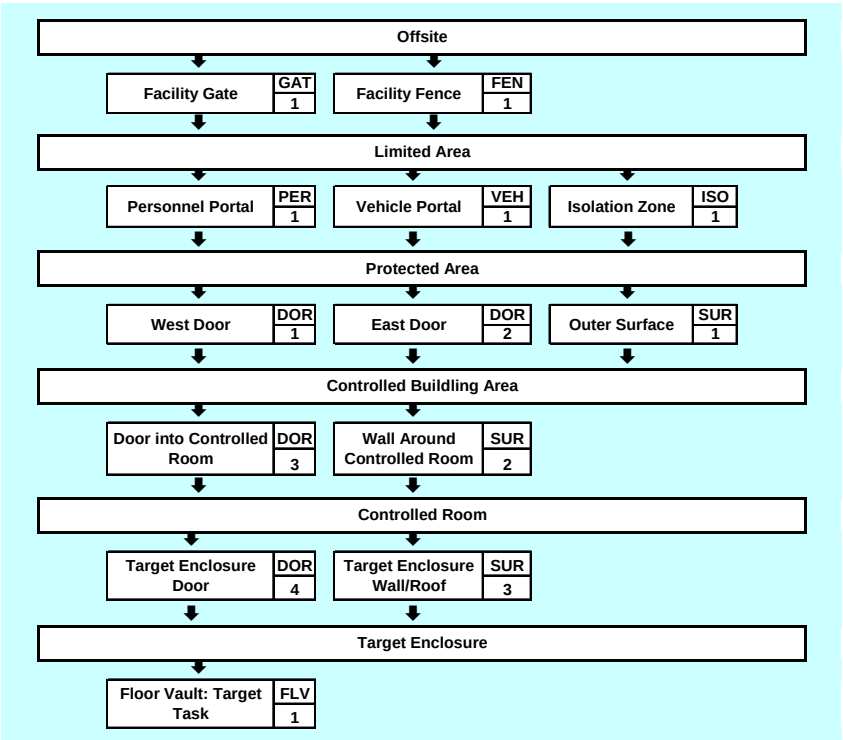


Figure 17-9. Site-Specific ASD for Sample Facility

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.

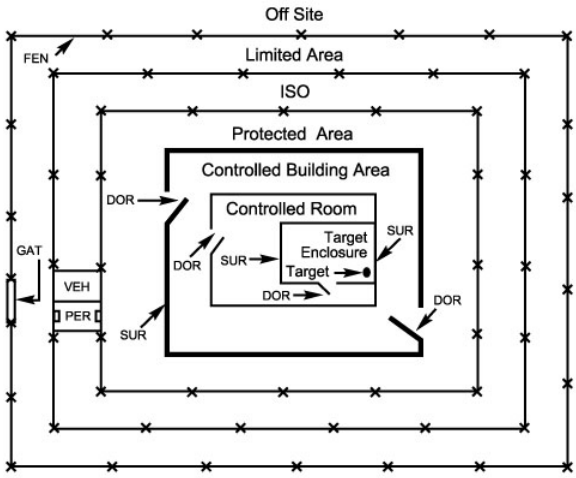


Figure 17-10. Sample Facility with Jump

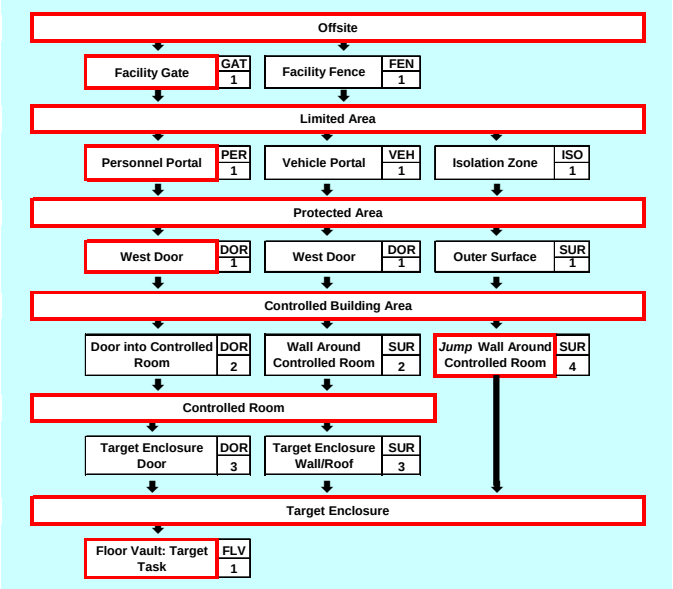


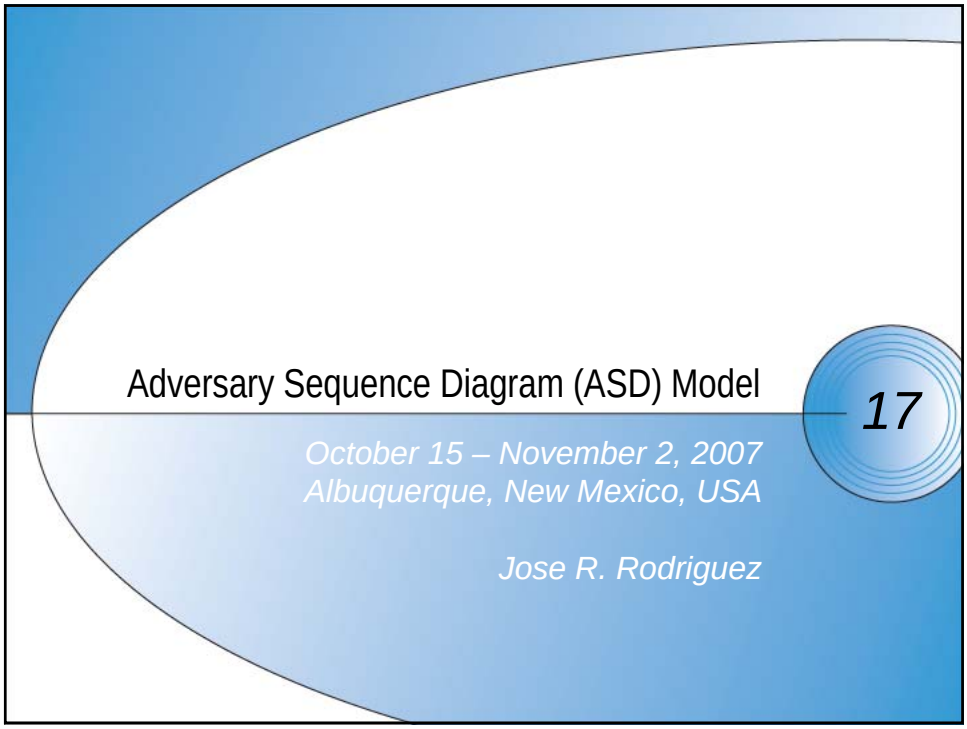
Figure 17-11. Site-Specific ASD for Sample Facility with Jump and Path Indicated in Red

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.

This Page Intentionally Left Blank.



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**

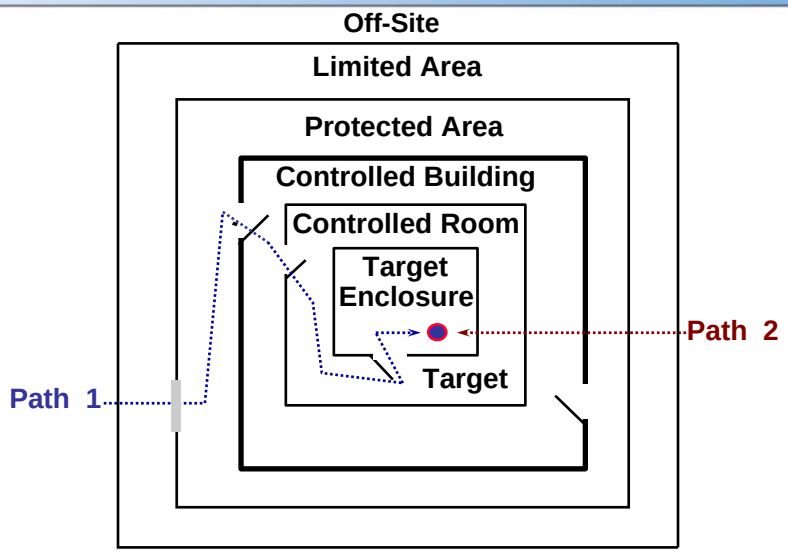
Adversary Sequence Diagram (ASD) Model 2

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



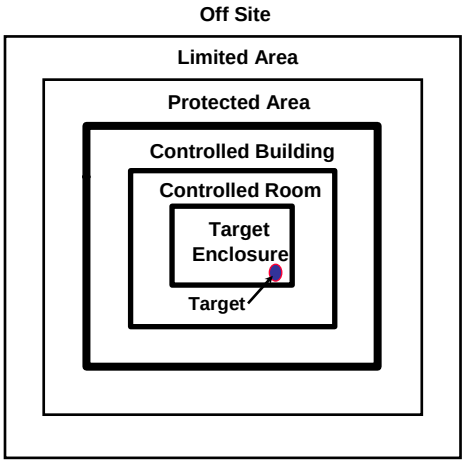
Adversary Sequence Diagram (ASD) Model 4

Six 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
6. **Describe detection and delay components at each element**

Adversary Sequence Diagram (ASD) Model 5

Facility



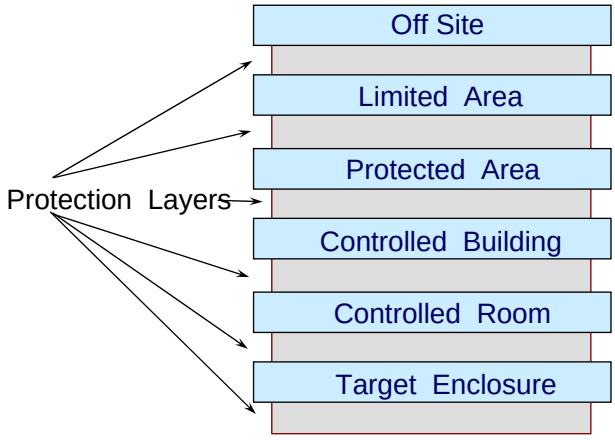
Adversary Sequence Diagram (ASD) Model 6

Step 1: Identify Physical Areas of Facility

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

Adversary Sequence Diagram (ASD) Model 7

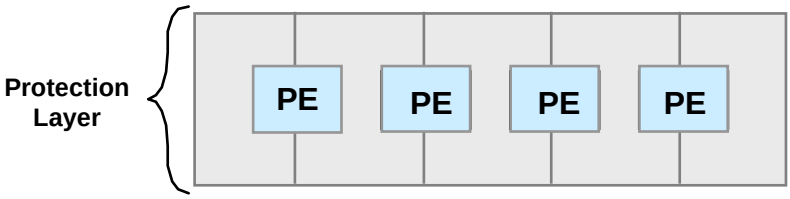
Step 2: Define PPS Layers of Facility



Adversary Sequence Diagram (ASD) Model 8

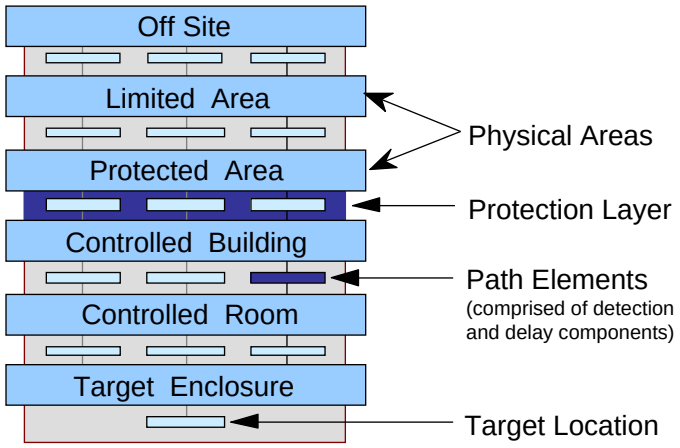
Step 2 (continued): Define Path Elements (PE's)

- **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

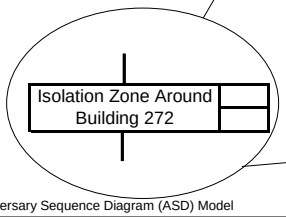
Concept of Adversary Sequence Diagram

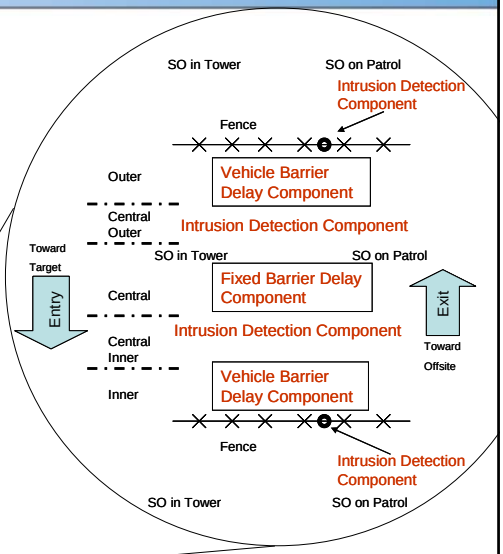


Adversary Sequence Diagram (ASD) Model 10

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):**





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

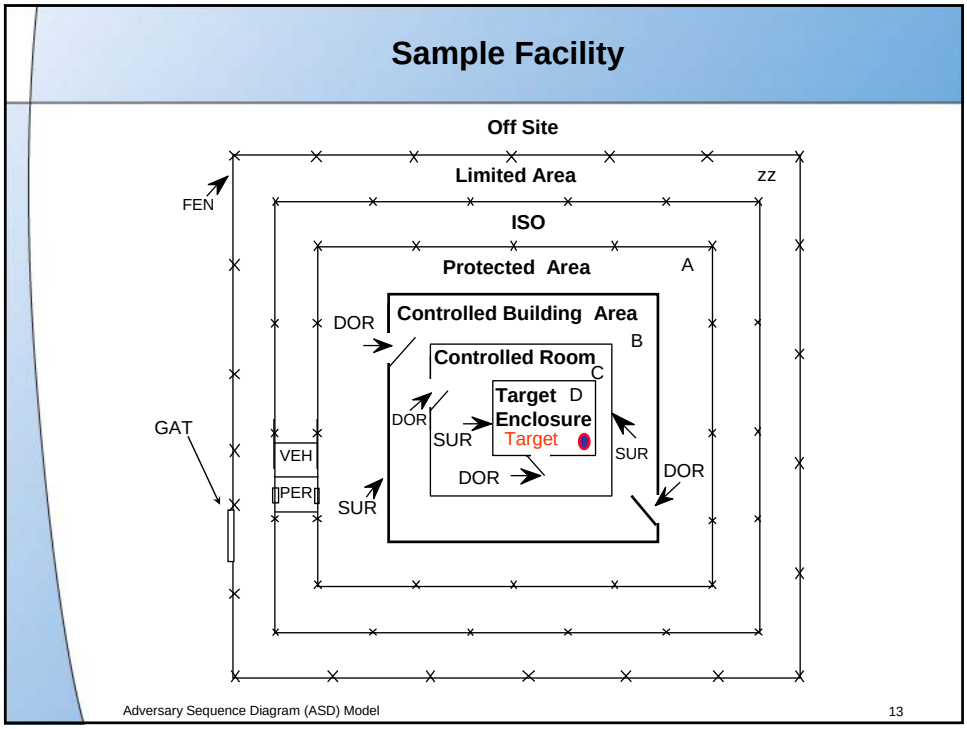
Path Elements (continued):

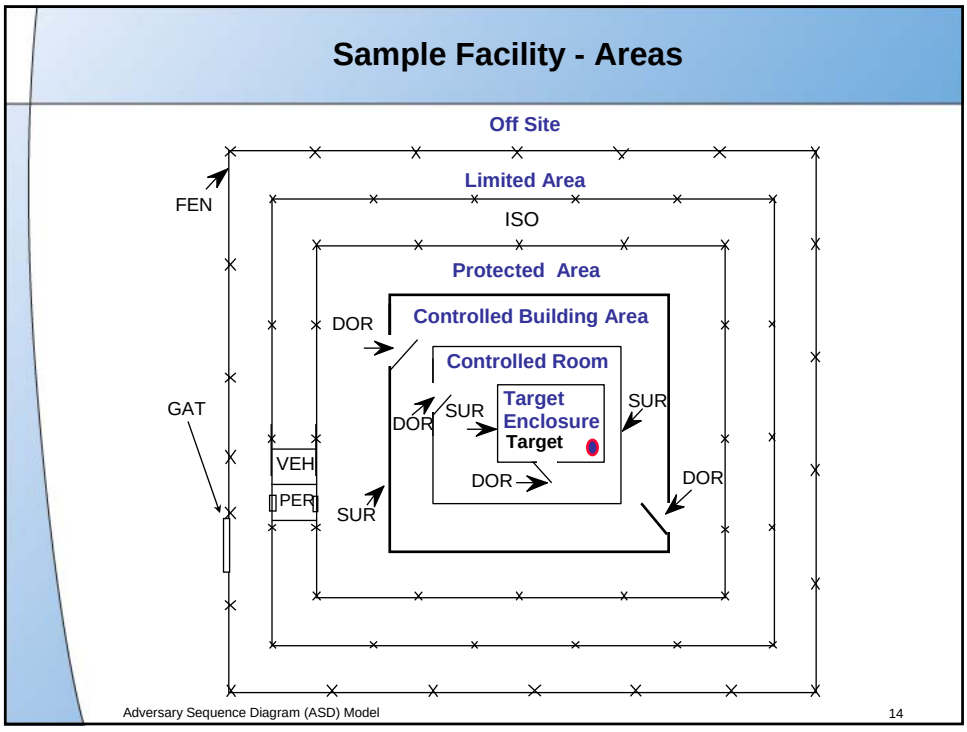
SUR	Surface
TUN	Tunnel
VHD	Vehicle Doorway
VEH	Vehicle Portal
WND	Window

Target Locations:

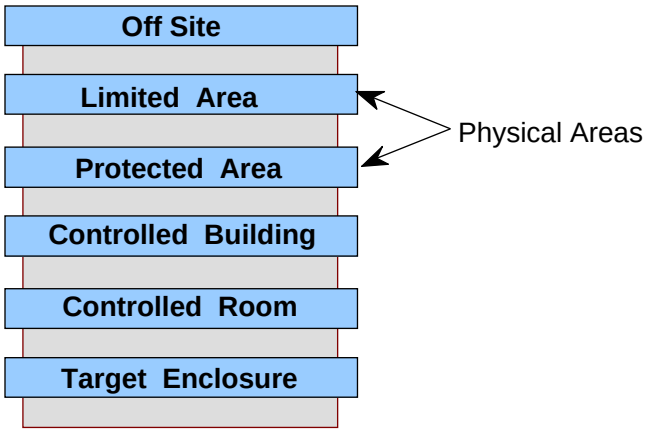
BPL	Bulk Process Line
CGE	Cage
FLV	Floor Vault
GNL	Generic Location
GBX	Glove box
IPL	Item Process Line
OPN	Open Location
TNK	Storage Tank

Refer to Supporting Information for pictorial representations.


Sample Facility
Off Site
Limited Area
zz
FEN
ISO
Protected Area
A
Controlled Building Area
DOR
B
Controlled Room
C
Target
D
Enclosure
Target
DOR
SUR
SUR
DOR
GAT
VEH
PER
SUR
DOR
Adversary Sequence Diagram (ASD) Model
13

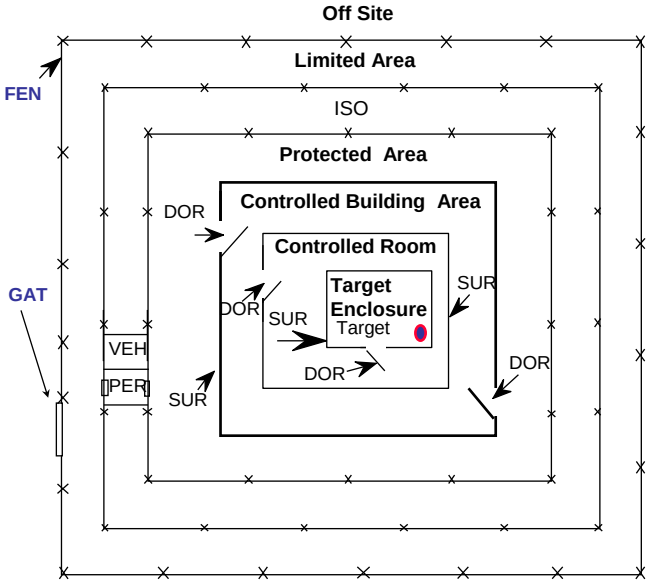

Sample Facility - Areas
Off Site
Limited Area
FEN
ISO
Protected Area
Controlled Building Area
DOR
Controlled Room
Target
Enclosure
Target
SUR
SUR
DOR
DOR
GAT
VEH
PER
SUR
DOR
Adversary Sequence Diagram (ASD) Model
14

Physical Areas in the Sample Facility



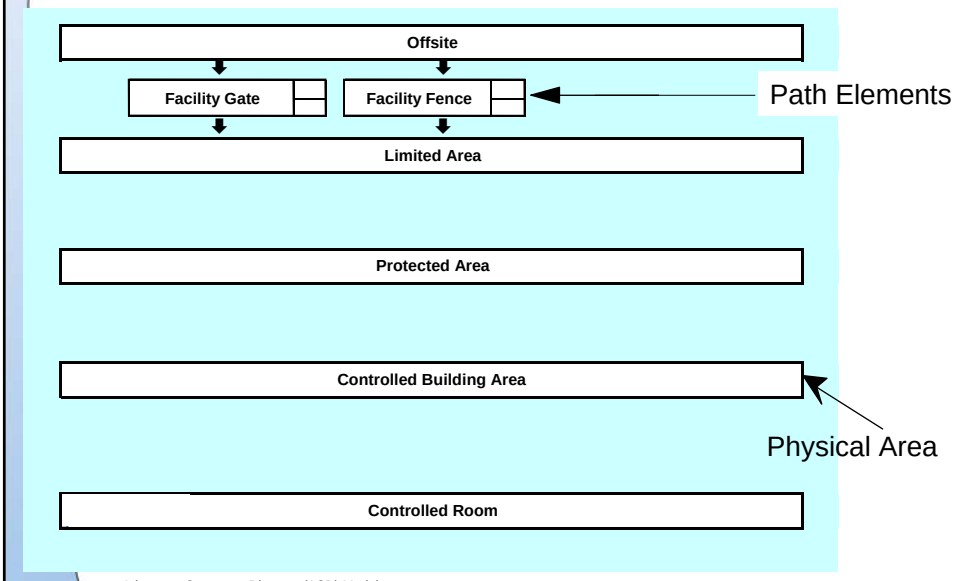
Adversary Sequence Diagram (ASD) Model 15

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



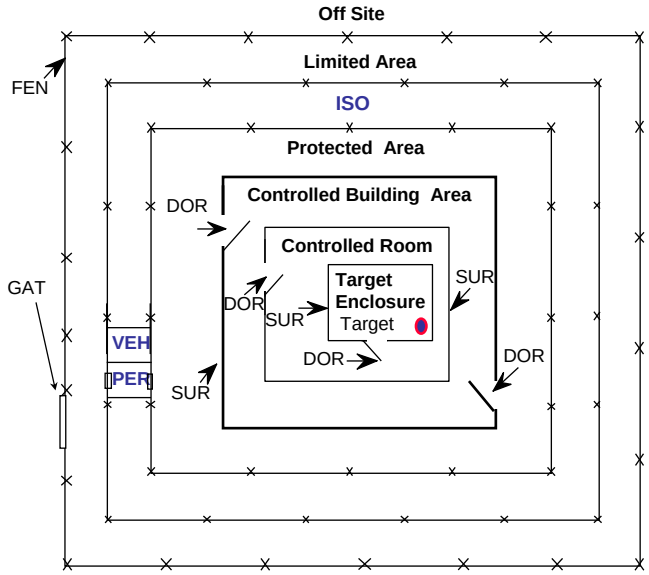
Adversary Sequence Diagram (ASD) Model 16

Protection Layer Between Offsite and Limited Area



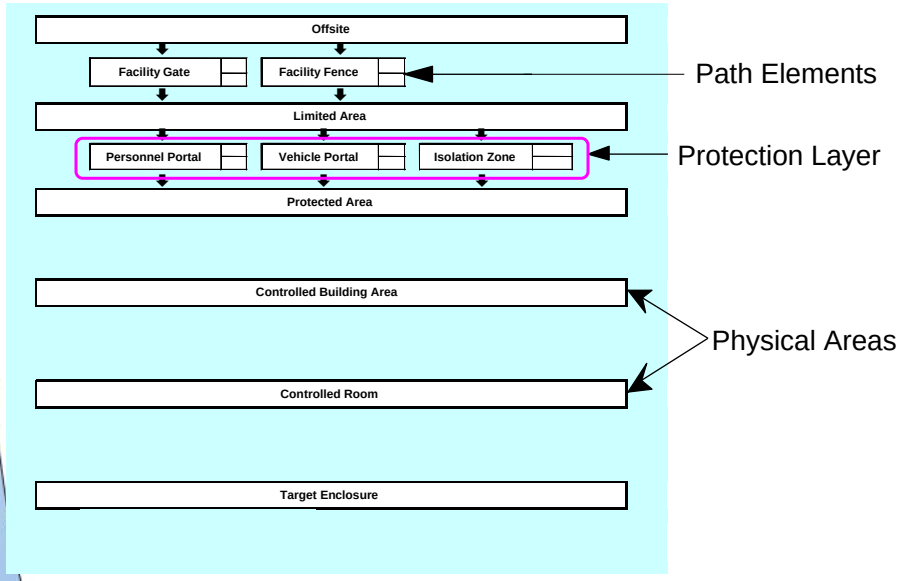
Adversary Sequence Diagram (ASD) Model 17

Second Protection Layer at the Sample Facility



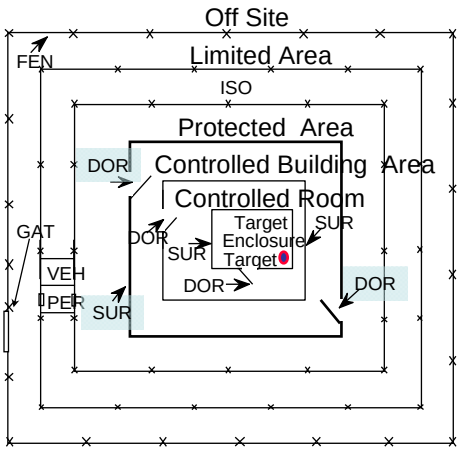
Adversary Sequence Diagram (ASD) Model 18

Path Elements From Limited Area to Protected Area



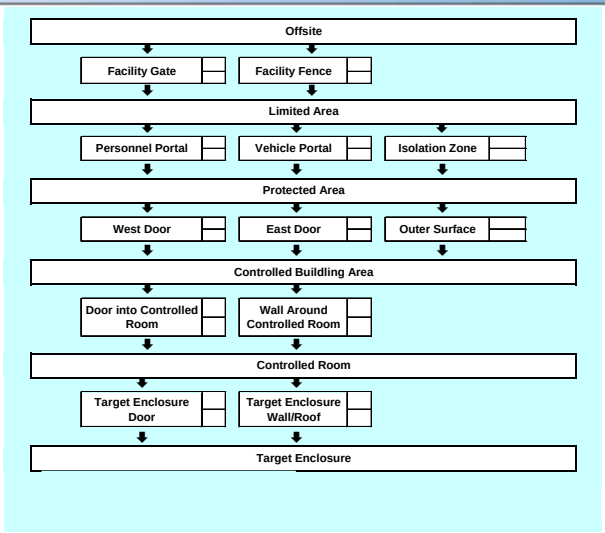
Adversary Sequence Diagram (ASD) Model 19

Third Protection Layer at the Sample Facility



Adversary Sequence Diagram (ASD) Model 20

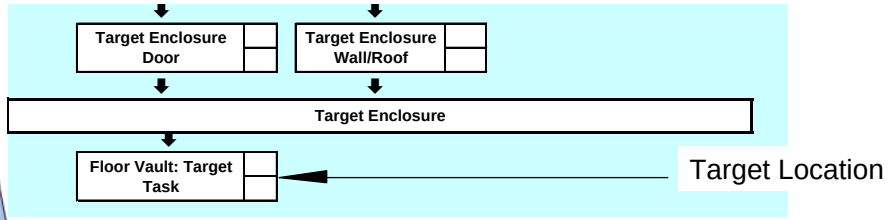
Diagram at the End of Step 2



Adversary Sequence Diagram (ASD) Model 21

Step 3: Add Target Locations

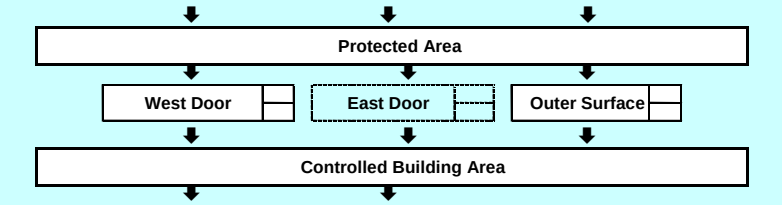
- **Target Locations are added to the last area**
- **Different ASDs may be required for different:**
  - Types of targets with different target locations (glove box versus floor vault)
  - Target enclosures in a building that have different security
  - Buildings at a site if these have different security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



Adversary Sequence Diagram (ASD) Model 22

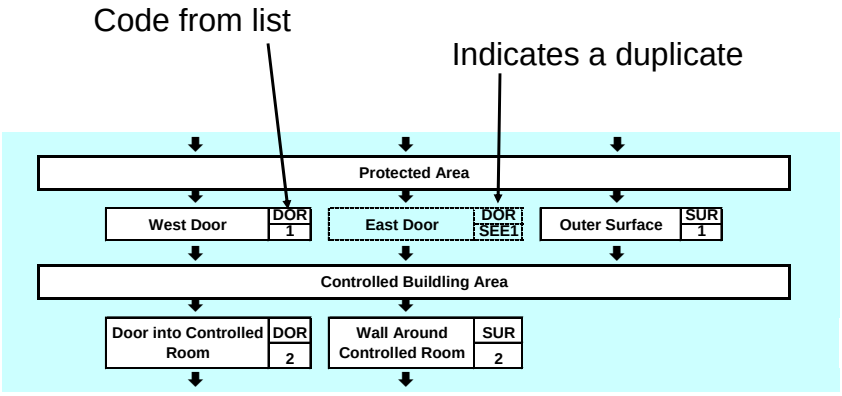
Step 4: Reduce the Size of The ASD, if Possible

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



Adversary Sequence Diagram (ASD) Model 23

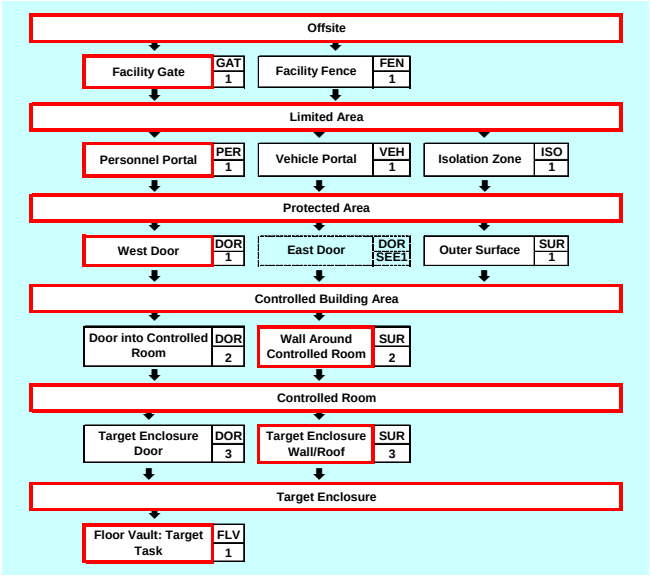
Step 5: Finish Defining Each Element by Assigning A Three Letter Code, A Unique Index, and Segments



Adversary Sequence Diagram (ASD) Model 24

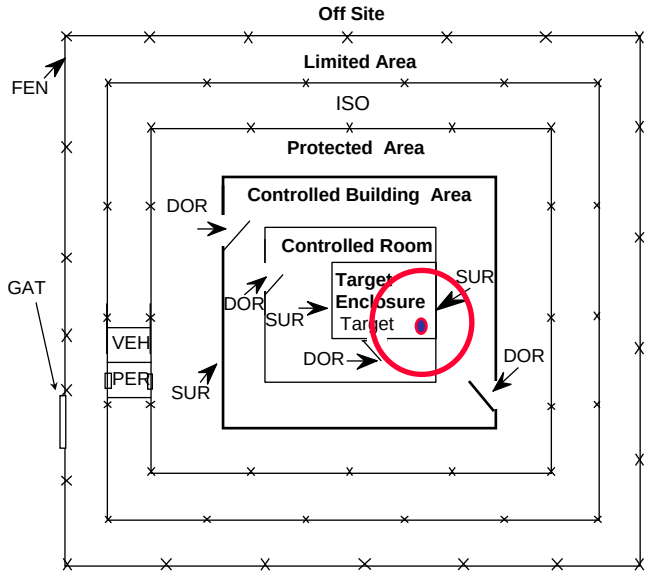
Completed Site-Specific ASD for Sample Facility

Example Path



Adversary Sequence Diagram (ASD) Model 25

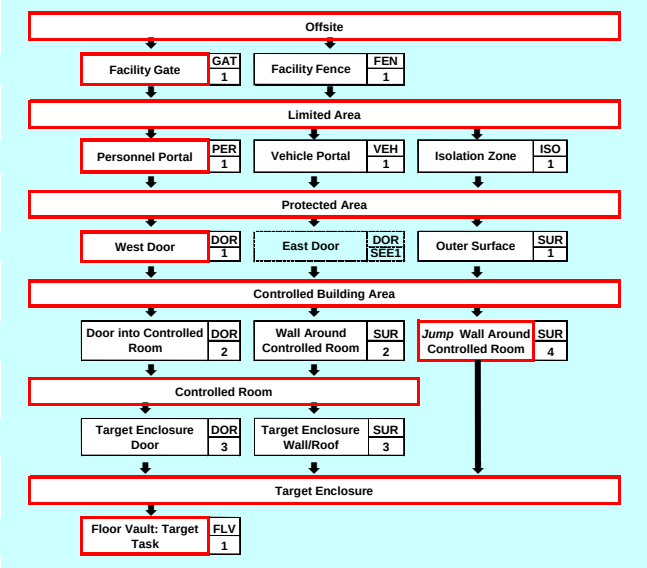
Example of a Jump



Adversary Sequence Diagram (ASD) Model 26

Site-Specific ASD for Sample Facility With A Jump

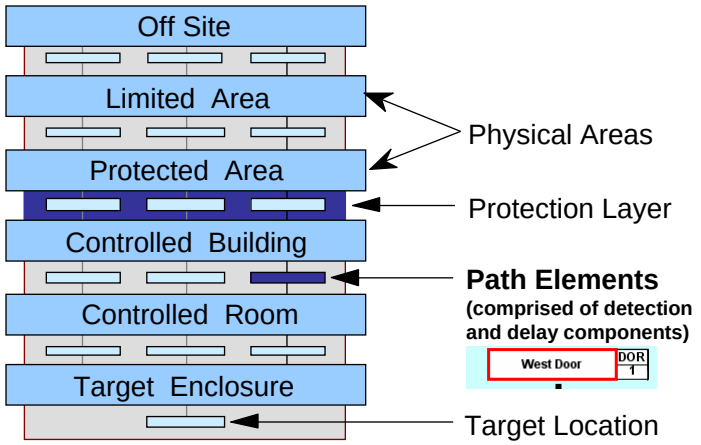
Example Path



Step 6: Define Detection and Delay Components at Each Path Element in the ASD

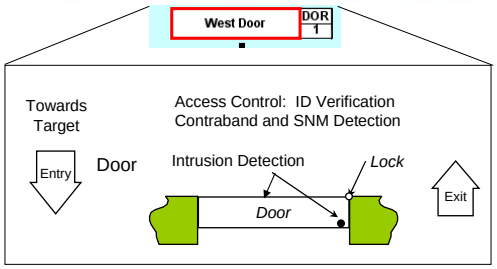
- **Specific components are categorized by *component class*, *component type*, and *component description***
- **Detection component classes (See Facility Data Book, Section 11)**
  - Intrusion Detection
  - Access Control
  - Human Surveillance
  - Contraband and SNM Detection
- **Delay component classes (See Facility Data Book, Section 19 and Access Delay SG)**
  - Barriers
  - Security Officers
  - Locks
  - Tasks
  - Transit Time

Concept of Adversary Sequence Diagram



Adversary Sequence Diagram (ASD) Model 29

As an Example, a Partial Description of Components for the West Door, DOR 1



Detection Components

Component Class	Component Type	Component Description	Part of Element
Intrusion Detection	Position Sensors	Balanced Magnetic Switch	Door
Access Control	ID Verification	Badge Check	Door
Contraband and SNM Detection	Portal Metal Detector	Ferrous materials only	Door

Delay Components

Component Class	Component Type	Component Description	Part of Element
Door	Doors	5 cm wood door	Door
Lock	Locks	High Security Padlock	Door

Adversary Sequence Diagram (ASD) Model 30

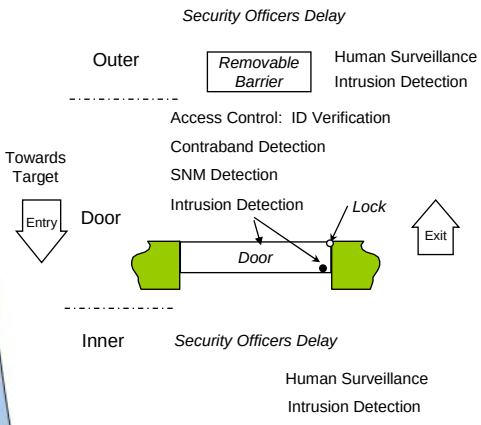
Each Type of Element has a General Structure Within Which Detection and Delay Components Can Be Assigned

PERSONNEL DOORWAY PATH ELEMENT DOR

West Door DOR 1

Element Name: _____

From: _____ To: _____



Detection Components

Component Class	Component Type	Component Description	Part of Element

Delay Components

Component Class	Component Type	Component Description	Part of Element

Adversary Sequence Diagram (ASD) Model 31

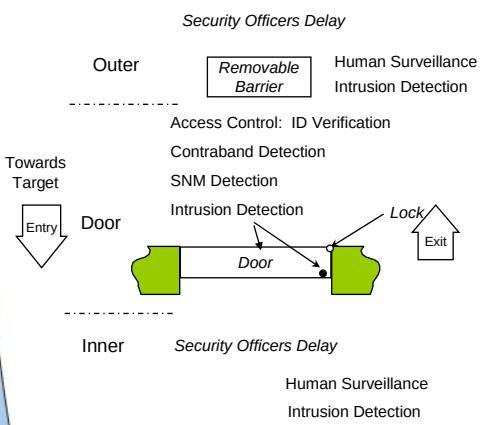
Complete Example of Components for West Door

PERSONNEL DOORWAY PATH ELEMENT DOR

West Door DOR 1

Element Name: _____

From: _____ To: _____



Detection Components

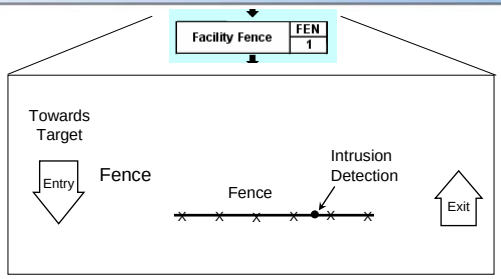
Component Class	Component Type	Component Description	Part of Element
Intrusion Detection	Position Sensors	Balanced Magnetic Switch	Door
Intrusion Detection	Interior Sensor	Microwave	Outer
Intrusion Detection	Barrier Sensors	Vibration	Door
Access Control	ID Verification	Badge Check	Door
Contraband and SNM Detection	Portal Metal Detector	Ferrous materials only	Door
Human Surveillance	SO at Post Observation	Duress, unprotected	Outer

Delay Components

Component Class	Component Type	Component Description	Part of Element
Door	Doors	5 cm wood door	Door
Lock	Locks	High Security Padlock	Door
Security Officers Delay	SO at Post Delay	Unprotected post	Outer

Adversary Sequence Diagram (ASD) Model 32

As Another Example, a Partial Description of Components for the Facility Fence, FEN 1



Detection Components

Component Class	Component Type	Component Description	Part of Element
Intrusion Detection	Fence Sensors	Taut wire	Fence

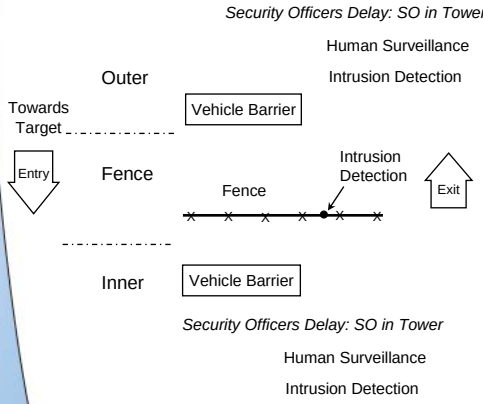
Delay Components

Component Class	Component Type	Component Description	Part of Element
Barrier	Miscellaneous Barriers	2.5 m chain link mesh fence	Fence

Adversary Sequence Diagram (ASD) Model 33

Example of the General Fence Element Model with Site Data

FENCELINE PATH ELEMENT FEN
Element Name: _____
From: _____ To: _____



Detection Components

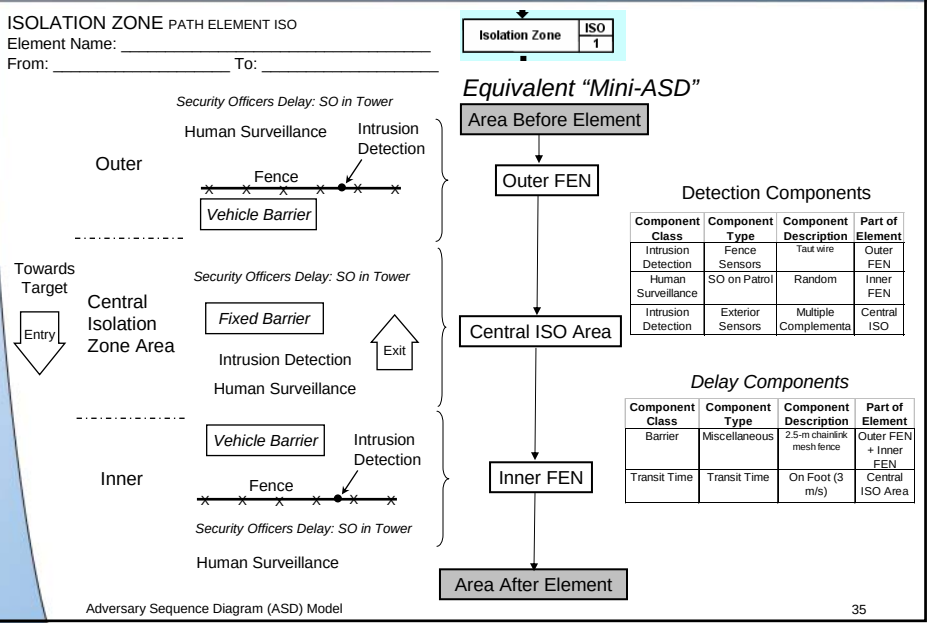
Component Class	Component Type	Component Description	Part of Element
Intrusion Detection	Fence Sensors	Taut wire	Fence
Human Surveillance	SO on Patrol	Random	Outer

Delay Components

Component Class	Component Type	Component Description	Part of Element
Barrier	Miscellaneous Barriers	2.5 m chain link mesh fence	Fence
Security Officers	SO in Tower Delay	Small Arms Resistant	Inner

Adversary Sequence Diagram (ASD) Model 34

Some Elements are Equivalent to "Mini-ASD's" Consisting of Simpler Sub-Elements



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 6 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
  6. Define detection and delay components at each element

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 product vault, beginning with OFFSITE and ending at the TARGET ENCLOSURE. Separate the Institute into 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.

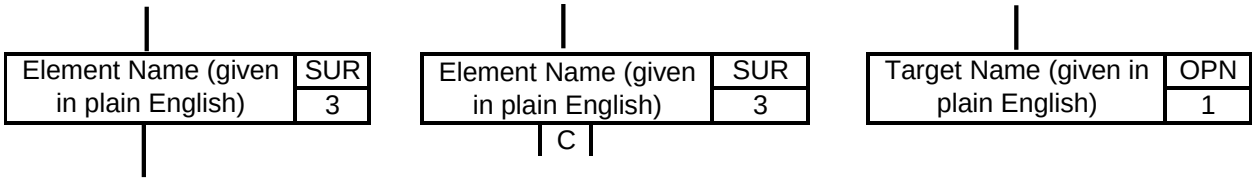
Path Elements:			SHP	-	Shipping/Receiving Portal
DUC	-	Duct	SUR	-	Surface
EMC	-	Emergency Evacuation Corral	TUN	-	Tunnel
EMX	-	Emergency Exit	VHD	-	Vehicle Doorway
EMP	-	Emergency Portal	VEH	-	Vehicle Portal
FEN	-	Fenceline	WND	-	Window
GAT	-	Gateway	**Target Locations:**		
HEL	-	Helicopter Flight Path	BPL	-	Bulk Process Line
ISO	-	Isolation Zone	CGE	-	Cage
PST	-	Material Passthrough	FLV	-	Floor Vault
MAT	-	Material Portal	GNL	-	Generic Location
OVP	-	Overpass	GBX	-	Glovebox
DOR	-	Personnel Doorway	IPL	-	Item Process Line
PER	-	Personnel Portal	OPN	-	Open Location
SHD	-	Shipping/Receiving Doorway	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) to perform the other four steps for creating an ASD.

- Define 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.)*
- Identify 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?*
- Assign 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):*



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 19S, *Multipath Computer Model,* and if time permits, enter it into PANL as an exercise.

PTR ASD for Products Vault

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

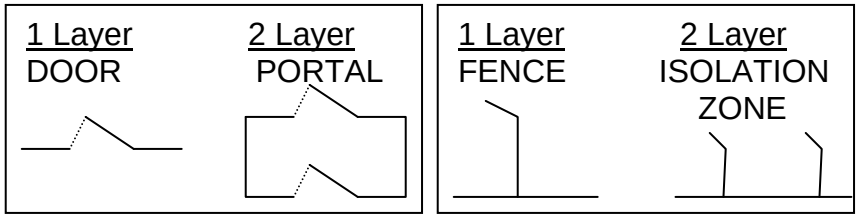
Miscellaneous Elements

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	

Exercise 3 – Define Detection and Delay Components for Two Elements

The purpose of this exercise is to describe all of the detection and delay components that make up two of the elements comprising the PTR Building Perimeter protection layer:

- The Shipping/Receiving Door (SHD); and
- The 20-cm reinforced concrete wall between the Protected Area and the Reactor Building (SUR).

Use the worksheets for SHD and SUR elements found on the next few pages. Assume a normal workday as the operational condition and assume that the adversary is either on foot or in a truck. Review Sections 6, 7, and 12 through 15 in the Exercise Data Book to determine the physical protection element components.

Complete the following steps to fill these sheets out,
1. Label each element with its name, the area it goes from, and the area it goes to.

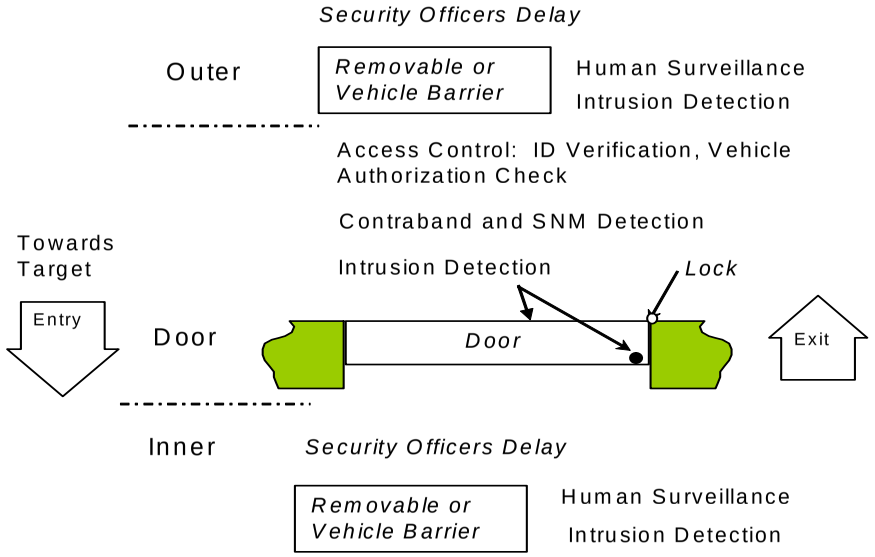
2. For each component, enter the following data in a row in the detection or delay sections (depending upon whether it affords detection or delay) found on the right-hand side of these worksheets:

- 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 what part of the element (e.g., Outer, Door, and Inner for SHD) the component is found at

SHIPPING/RECEIVING DOORWAY PATH ELEMENT SHD

Element Name: _____

From: _____ To: _____



Detection Components

Component Class	Component Type	Component Description	Part of Element

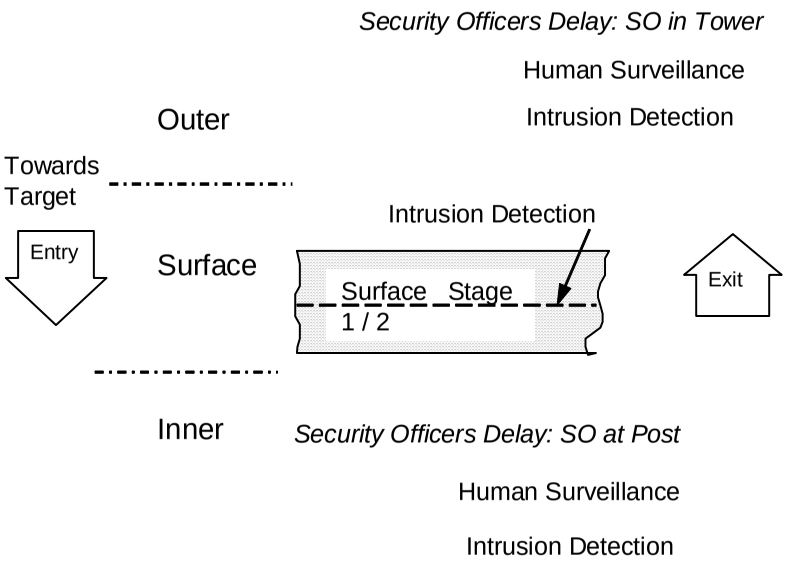
Delay Components

Component Class	Component Type	Component Description	Part of Element

SURFACE PATH ELEMENT SUR

Element Name: _____

From: _____ To: _____



Detection Components

Component Class	Component Type	Component Description	Part of Element

Delay Components

Component Class	Component Type	Component Description	Part of Element

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])

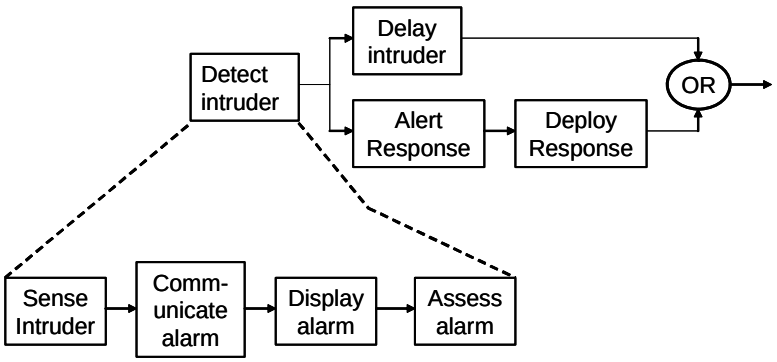


Figure 18-1. PPS Functional Flow Block Diagram Showing Decomposed Detect Function

[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.

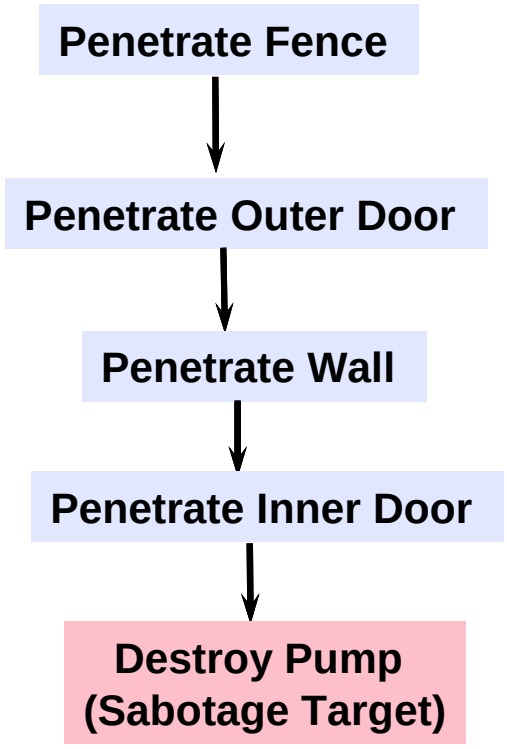


Figure 18-2. An Adversary Path

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.

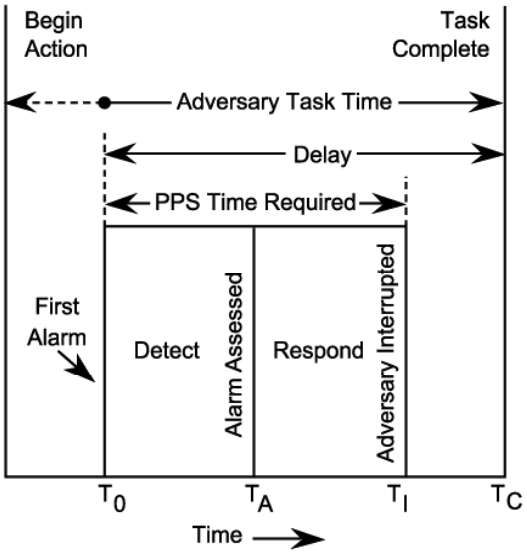


Figure 18-3. PPS Timing Diagram

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

Cumulative Path Delay Deficiency	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 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.

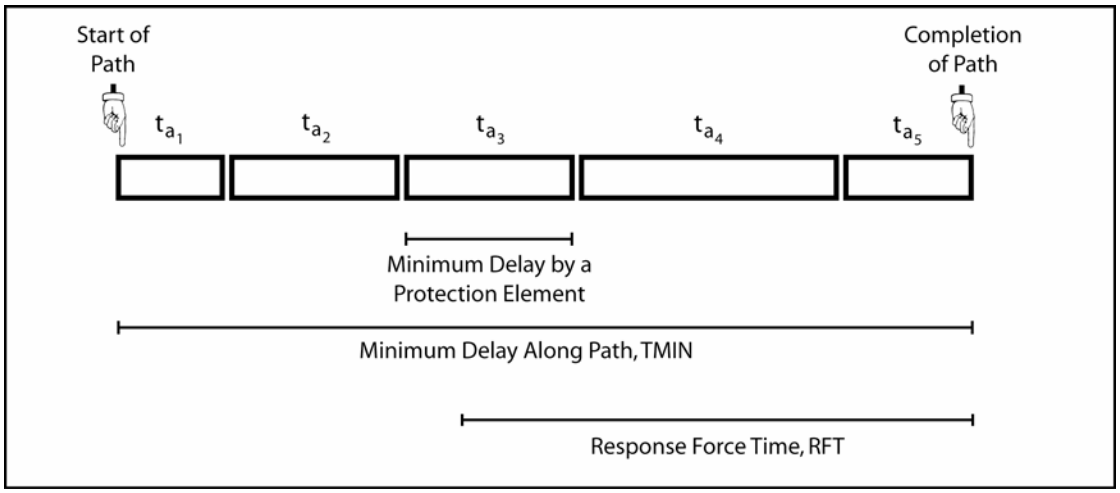


Figure 18.4. Minimum Path Delay as a measure of PPS effectiveness

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: $$T_{\min} = \sum_{i=1}^{m} t_{a_i}$$ 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 ∪ indicates the union (and/or) of two sets, the symbol ∩ 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 <u>non</u>-mutually exclusive events, E_n, states that: $$P(E_1 \cup E_2 \cup \ldots \cup E_n) = 1 - (1 - P(E_1))(1 - P(E_2)) \ldots (1 - P(E_n))$$ 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, $P_{acceptable}$, 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.

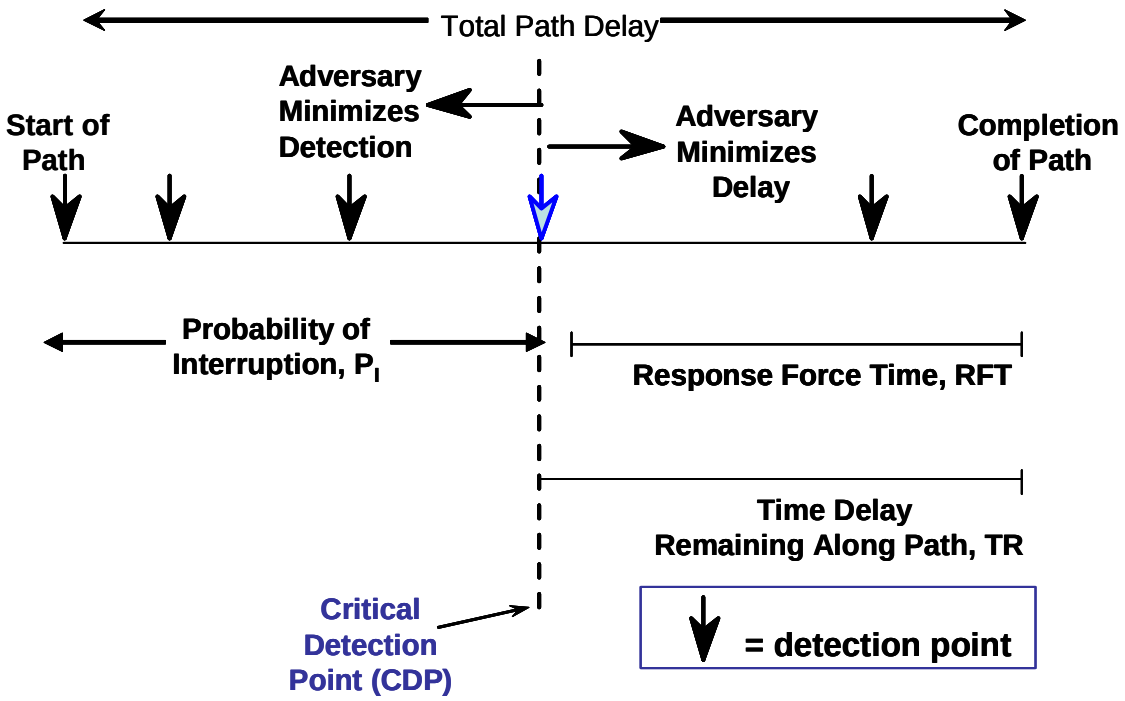


Figure 18-5. *Timely Detection* as a measure of PPS effectiveness

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: $$T_R = \sum_{i=k}^{m} t_{ai}$$
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 i^{th} 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

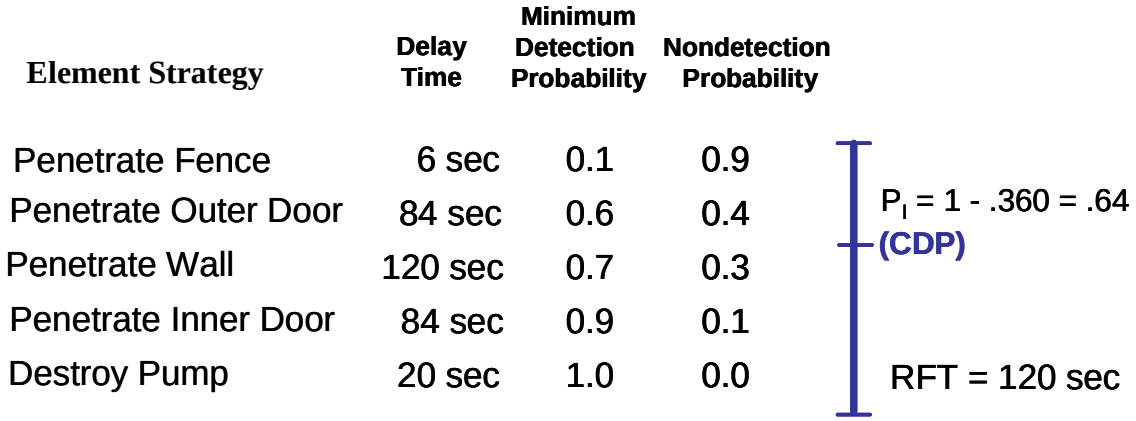


Figure 18-6. Example of Timely Detection

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**	**P_I = 1 - .0027 = .9973**
Penetrate Wall	120 sec	0.7	0.3	
Penetrate Inner Door	84 sec	0.9	0.1	**(CDP)**
Destroy Pump	**50 sec**	1.0	0.0	**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.

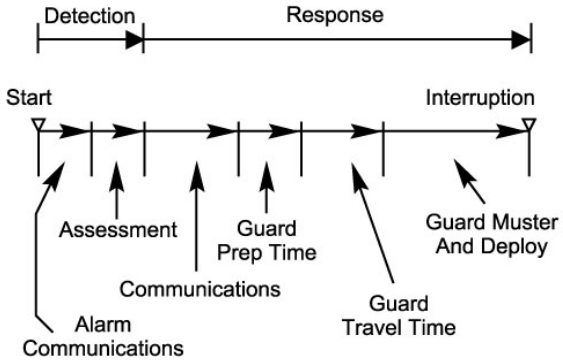


Figure 18-9. Guard Response Time

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.

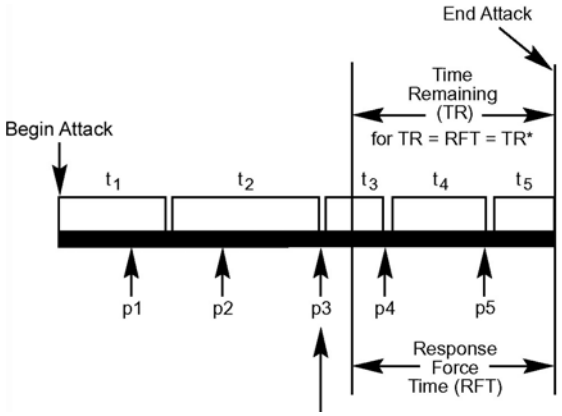


Figure 18-10. Critical Detection Point Indicated on a Path Event Timeline

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).

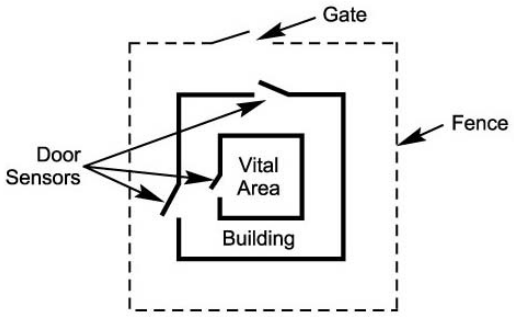


Figure 18-11. Example Facility

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

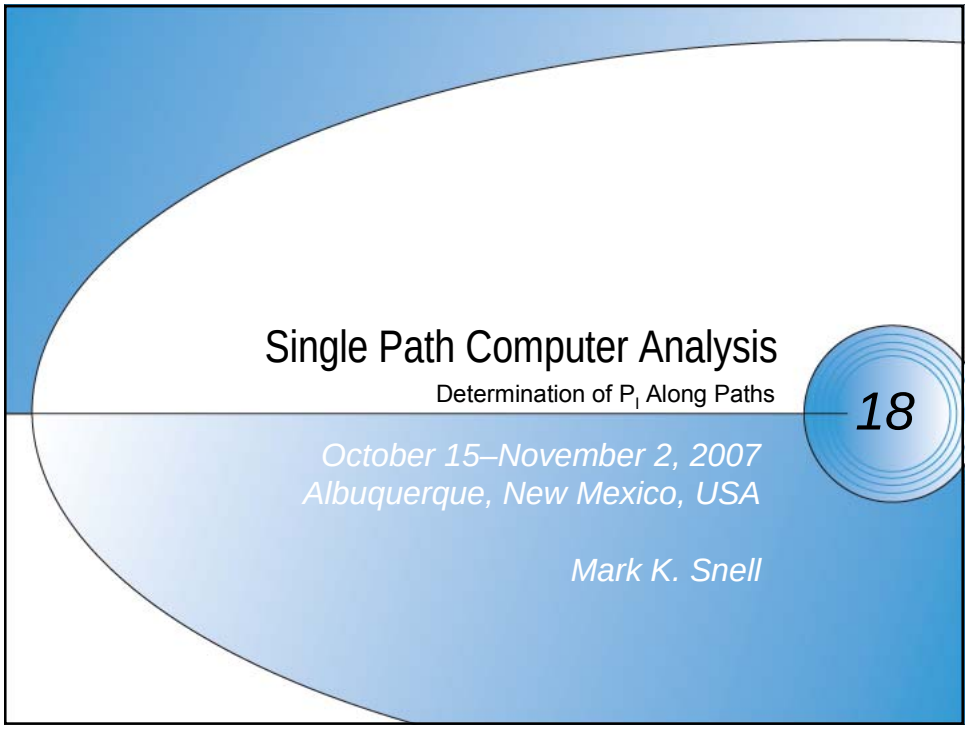
It must be remembered that VEASI only analyzes one specific path, and other paths may have an even lower probability of interruption. Because of this limitation, an exhaustive program, like PANL, is valuable for looking at all possible paths and displaying only the most vulnerable.

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

This Page Intentionally Left Blank.



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**

Single Path Computer Tool 2

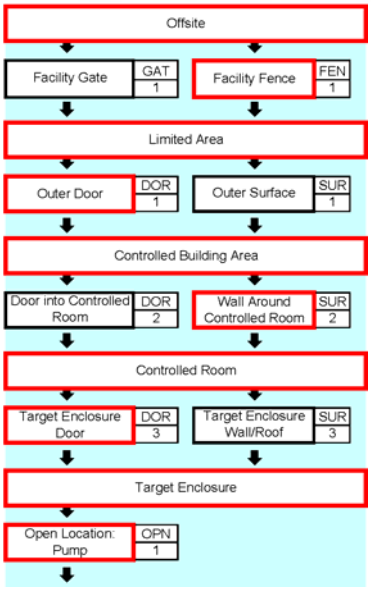
Context for VEASI

- **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**
  - Addresses three basic functions of a physical security system: detection, delay, and response
- **VEASI calculates P_I for a single path and up to five response times**
  - Shows total delay and cumulative probability of detection on the path
  - Determines the CDP

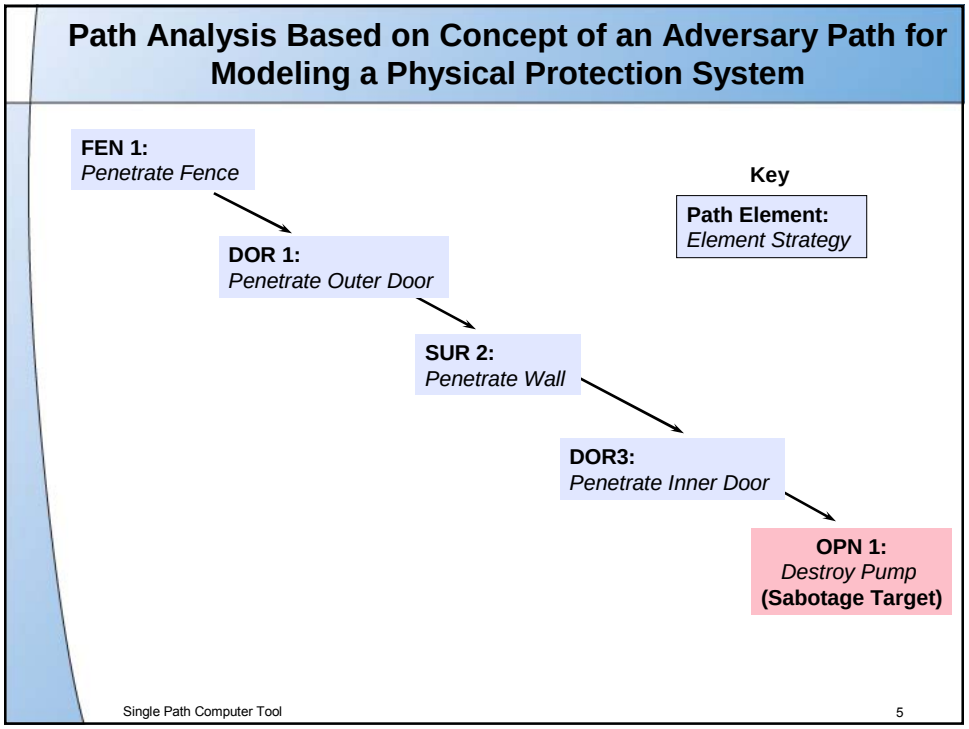
Single Path Computer Tool 3

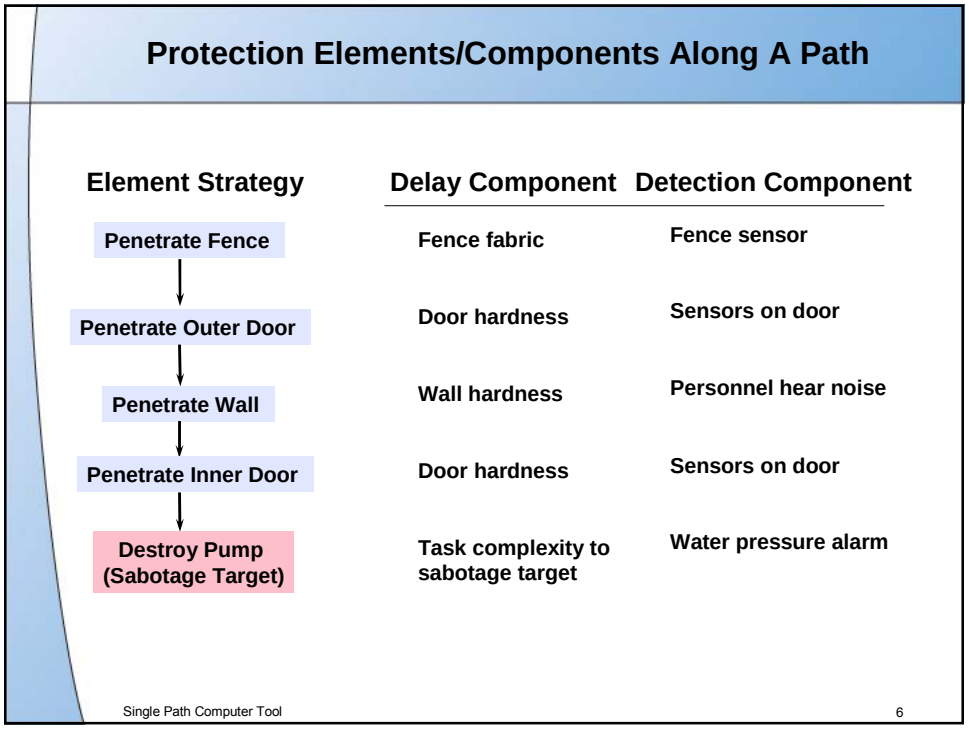
Pump Sabotage Path from Site-Specific ASD

Example Path

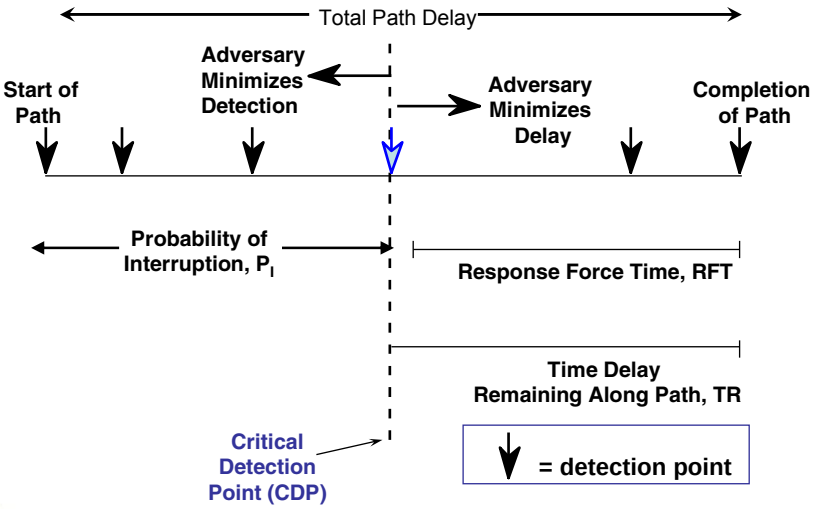


Single Path Computer Tool 4


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



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	P_I = 1 - .36 = .64
Penetrate Wall	120 sec	0.7	0.3	(CDP)
Penetrate Inner Door	84 sec	0.9	0.1	
Destroy Pump	20 sec	1.0	0.0	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

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

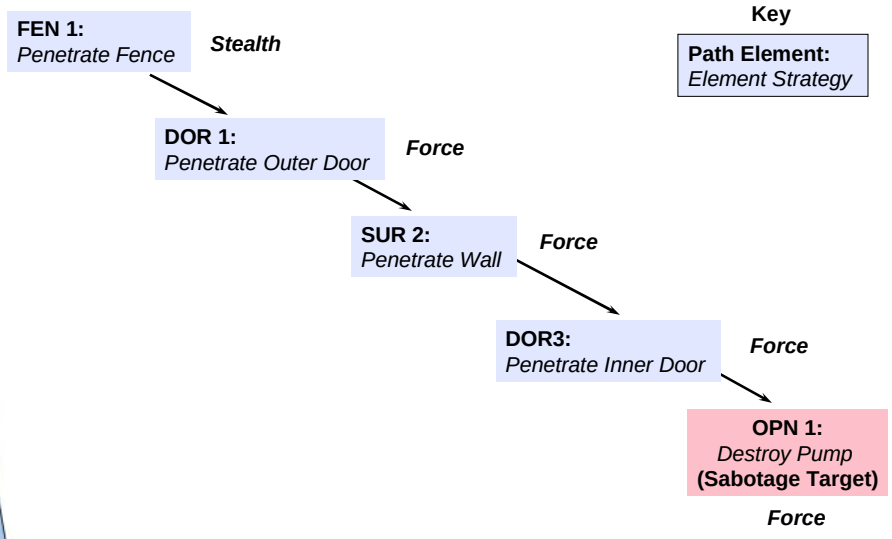
Single Path Computer Tool 8

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**

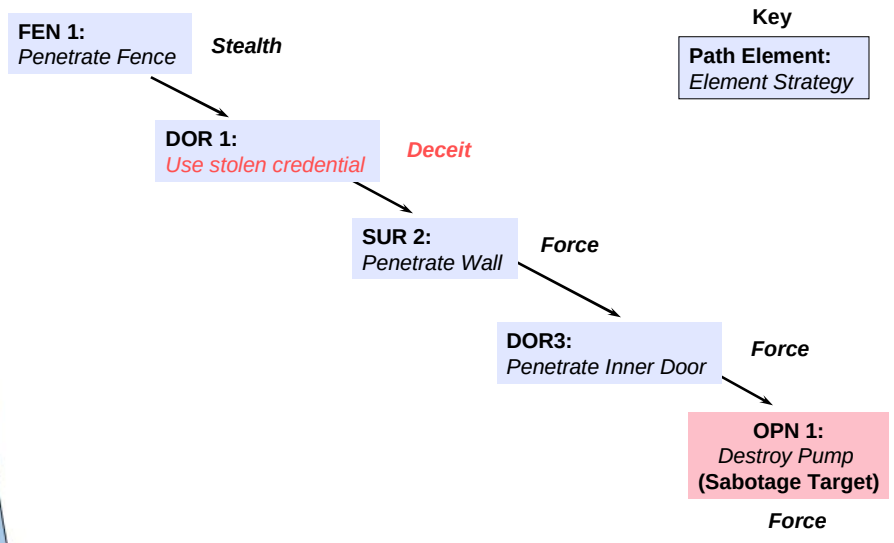
Single Path Computer Tool 9

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



Single Path Computer Tool 10

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



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					

CDP Location

Cumulative PD	1
Cumulative Delay	314

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

RFT Sec	VEASI P(I)
120	0.6400

P_I Value

Single Path Computer Tool 14

VEASI Computer Code

dversary Sequence Interruption) CDP (Critical Detection Point)

	P(Detection)	Location	Delays (Mean:	RFT= 60	RFT= 80	RFT= 100	RFT= 120	RFT= 140
	0.1	E	6					
or	0.6	E	84				*	*
	0.7	E	120	*	*	*		
or	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.

Single Path Computer Tool 15

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

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

Single Path Computer Tool 16

VEASI Computer Code Version of Upgrade

Very EASI
(EASI = Estimate of Adversary Sequence Interruption)

Task	Element Strategy	P(Detection)	Location	Delays (Mean:	RFT= 40	CDP
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						

CDP Location

Cumulative PD	1
Cumulative Delay	344

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

RFT Sec.	VEASI P(I)
40	0.9973

P_I Value

Single Path Computer Tool 17

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

Single Path Computer Tool 18

VEASI Model

- **Advantages of VEASI**
  - Provides analysis of interactions between delay and response
  - 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

Single Path Computer Tool 19

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)

Single Path Computer Tool 20

Detection

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

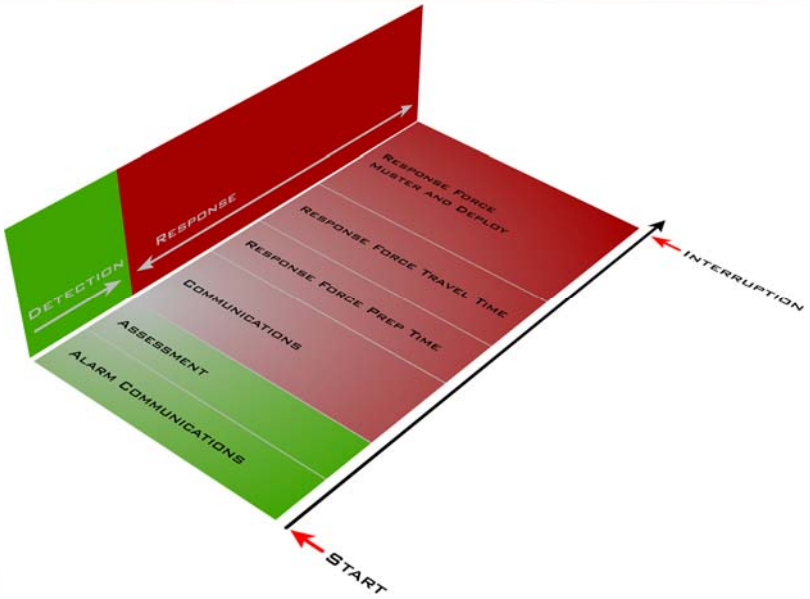
Single Path Computer Tool 21

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**

Single Path Computer Tool 22

Response Force Time



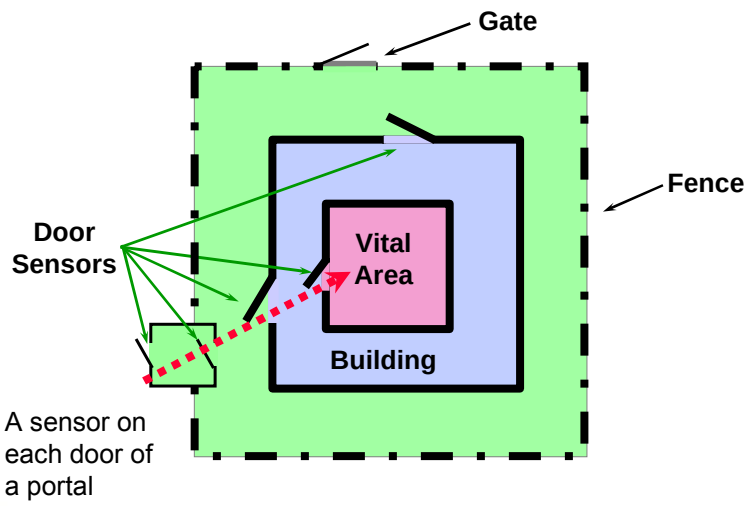
Single Path Computer Tool 23

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

Single Path Computer Tool 24

EASI Example Facility: Modeling More Complex Elements Such as 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 $P_D = 1-\{(1-P_{D1})x\ (1-P_{D2})x\ldots\ x(1-P_{Dm})\}$**
  - Example: .5 sensor on each of two doors
  - $P_D = 1-(1-.5)*(1-.5) = .75$
- **Combined Delay = $Delay_1 + Delay_2 +\ldots+ Delay_m$**
  - 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 $P_D = 1-\{(1-P_{D1})x\ (1-P_{D2})x\ldots\ x(1-P_{Dm})\}$**
  - $P_D = 1-(1-.5)*(1-.5) = .75$
- **Combined Delay = $Delay_1 + Delay_2 +\ldots+ Delay_m$**
  - 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

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

VEASI Summary

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

Single Path Computer Tool 29

This Page Intentionally Left Blank.

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™ version of VEASI.
3. Interpret the results of VEASI.

Exercise 1 – Hand Calculation of P_I for Fence Intrusion

Using the information in the attached data (Table 18S-1) and the Exercise Data Book (Sections 7, 10, 12, 13, 14, 15), develop detection, delay, and location of detection data for the following path, and compute *by hand* the probability of interrupting this sabotage attempt under normal daytime operating conditions at the PTR reactor facility. Draw the path in the diagram on the next page 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

Notes:

- Be sure to use the same unit of time throughout the problem.
- An "ending" (E) location of detection is considered as worse than a "middle" (M) location, which in turn is considered to be worse than a "beginning" (B) location.)

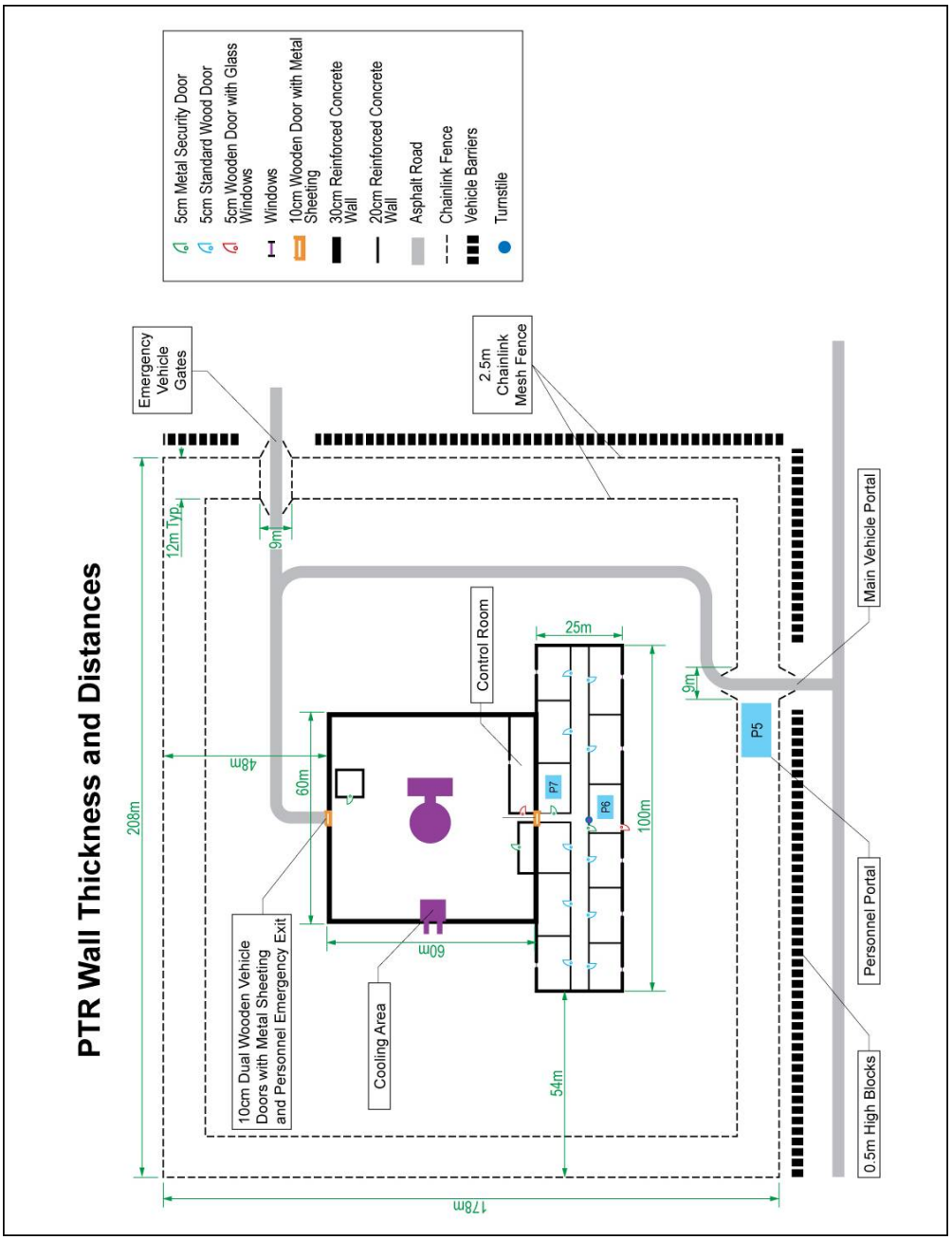
Element Strategy	Probability of Detection	Location	Time Delay (seconds)
1. Penetrate the outer fence			
2. Crosses the isolation zone			
3. Climbs the inner fence			
4. Crosses the protected area			
5. Penetrates the vehicle access doors			
6. Locates the reactor core and sets explosive charges			

To compute the probability of interruption for a path, multiply the probabilities of non-detection from the start of the path to the Critical Detection Point (CDP), and then subtract this product from 1.0 to get P_I. PD = 1-{(1-PD1)x (1-PD2)x… x(1-PDm)}

1) Determine P_I by hand for a response time of 90 seconds (hint: first find the CDP).

P_I = _____

PTR Wall Thicknesses and Distances



Exercise 2 – Determining Minimum Detection and Delay Values for Calculating P_I for Fence Intrusion

The two tables below show detection, delay, and location of detection values for element strategies that minimize P(D) (see the first table) and element strategies that minimize delay (see the second table). (Note that the same elements are being crossed in both tables, only the strategies used at each element differ between the tables.) Fill in the table at the top of the next page using the minimum detection and delay values and worst-case location of detection from among both tables for each element.

Minimize Detection Strategy

Element	Element Strategy	P(D)	Location	Delay
Outer FEN	Climbs outer fence	0	E	10
ISO Central Area	Stealthily cross by using a ladder to get over the active IR at the end	0.5	E	20
Inner FEN	Climbs inner fence	0	E	10
Protected Area	Crosses protected area	0	E	12
Vehicle Access Doors	Stealth entry through vehicle access doors using power tools	0.8	E	120
Target task at core	Locate reactor core and commit sabotage with power tools	0	E	60

Minimize Delay Strategies

Element	Element Strategy	P(D)	Location	Delay
Outer FEN	Breach fence with explosives	0.5	E	8
ISO Central Area	Run across isolation zone right through Active IR beam	0.9	E	3
Inner FEN	Breach fence with explosives	0.5	E	8
Protected Area	Run across protected area	0	E	12
Vehicle Access Doors	Penetrate vehicle access doors using explosives	.99	E	30
Target task at core	Locates reactor core and sets explosive charges	.95	E	45

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			

Exercise 3 – Calculating P_I by Hand and Using VEASI

1) Using the formula

P_I = 1 – (Product of non-detection probabilities from the start to the CDP)

determine P_I by hand for the path described above, given a response time of 90 seconds.

P_I = _____

2) Where is the Critical Detection Point (CDP) along this path?

Load and run the computerized EXCEL™ version of VEASI.

Now enter this data into the VEASI software and answer the following questions using VEASI.

3) What is the probability of interruption given by VEASI for a response time of 90 seconds?

P_I = _____

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

P_I = _____

5) What is the probability of interruption for the response time in question 4 if two minutes of access delay are added at the reactor core?

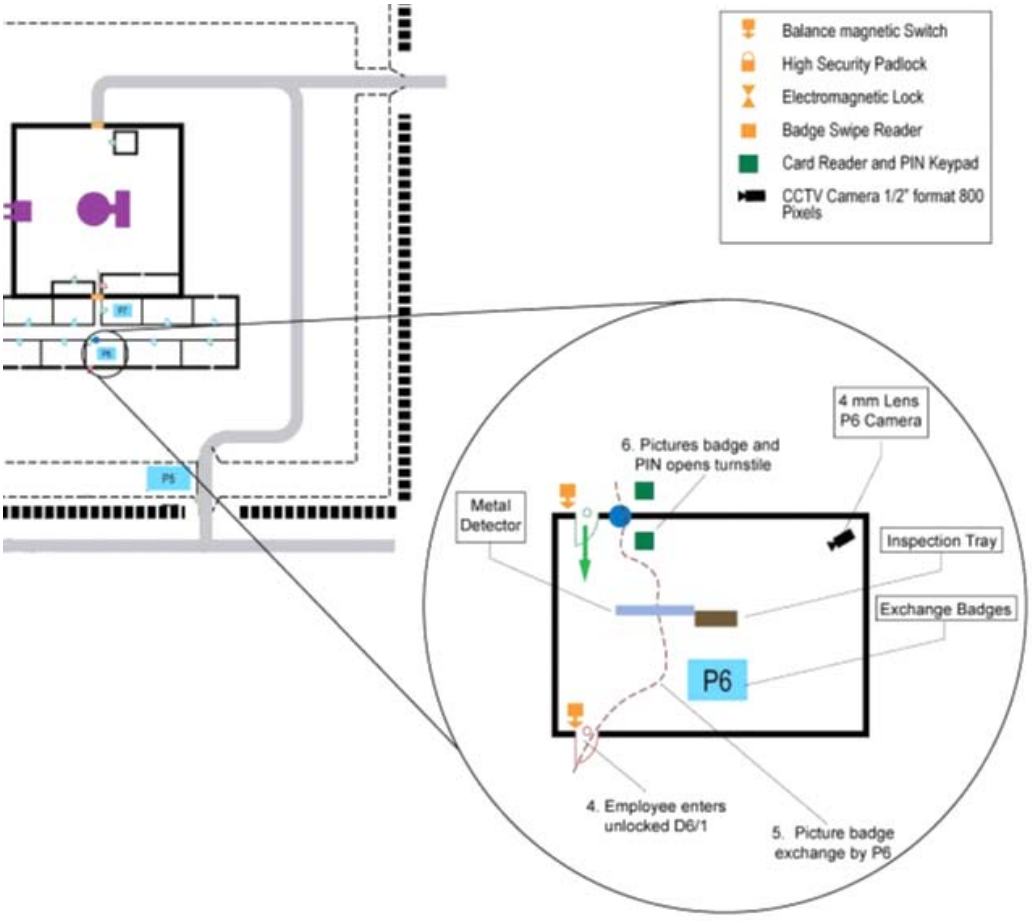
P_I = _____

6) What is the probability of interruption for the case in question 5 if a fence vibration sensor is added at to the inner fence?

P_I = _____

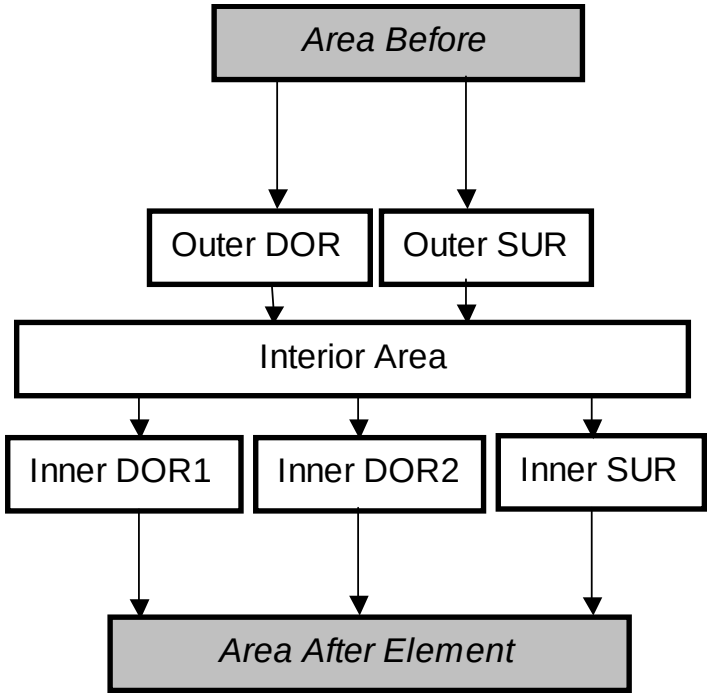
Exercise 4 – Determining Probability of Detection, Delay, and Location of Detection for a Portal Element

In this exercise, you will use the picture below describing P6 (the Building Personnel Portal) and the data in Table 18S-1, determine the probability of detection, delay time, and location of detection for the personnel portal. This will be accomplished in several steps.



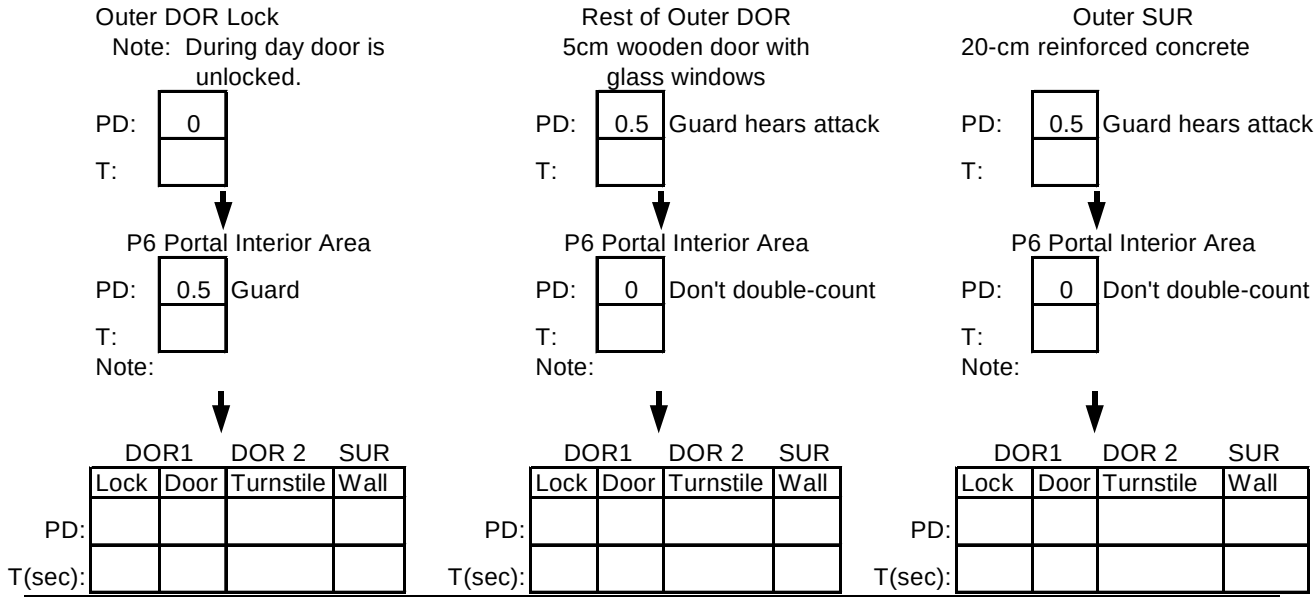
4.1 Record detection and delay values on "mini-ASD" of P6

The diagram to the right is a "mini-ASD" representing the structure of portal P6. For example, the Turnstile is Inner DOR2 while the inner personnel door is Inner DOR1. Using the diagram of P6 and Table 18S-1, record both detection and delay security features of P6 on the diagram (for example, record Security Officer at Post Delay and Observation at the Interior Area while the Outer SUR and Inner SUR consist of 20-cm reinforced concrete).



4.2 Determine minimum force/stealth detection path through P6 and minimum delay path through P6

Based on detection and delay data for components at P6 and on information from P6's "mini-ASD", enter detection and delay values for 9 paths through the mini-ASD" (the 9 are shown on the diagram below) and determine the path(s) through P6 with the lowest detection and delay. Note that we have moved detection due to the guard up on the paths through the Outer DOR and Outer SUR since the guard would hear attackers attempting to penetrate these barriers.



P(D) for path with smallest P(D): _____

Time for the path with the smallest P(D): _____

Location of Detection for the path with the smallest P(D): _____

Time for path with smallest time (not necessarily the same as the path with smallest P(D)): _____

P(D) for the path with the smallest time: _____

Location of detection for the path with the smallest time: _____

Note: you now have performance data for two element strategies for defeating the portal, one minimizing detection and the other minimizing delay. These will be used by PANL, which accepts multiple strategies per element. VEASI works best with the worst case performance values over all strategies; these are determined in 4.3 and 4.4 below.

4.3 Determine minimum deceit detection path through P6

Enter the performance values for the components shown on the diagram.

1) Calculate the probability of detector for an adversary entering P6 hiding metal contraband on their person:

P(D): _____

2) Calculate the probability of detector for an adversary entering P6 hiding metal contraband in possessions that they leave on the inspection tray subject to the item search:

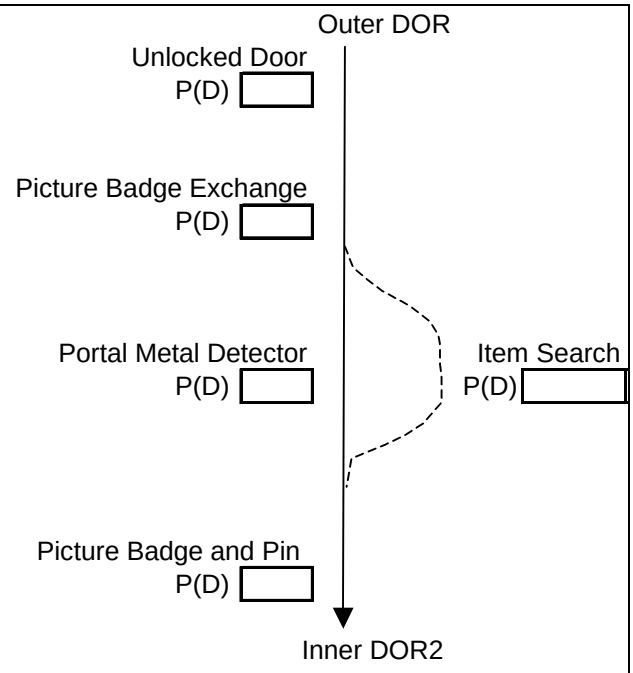
P(D): _____

3) Enter the smaller of these values as the deceit P(D):

P(D): _____

Time (Note: for deceit, use the force delay time, assuming that an adversary detected during deceit will resort to force to defeat the rest of that element.): _____

Location of Detection: _____



4.4 Determine Worst-Case P(D), delay, and location of detection at portal P6 for VEASI:

For P(D), chose the smaller P(D) for questions 4.2 and 4.3: _____

For delay time, T, choose the minimum delay from question 4.2: _____

For location of detection, choose the worst of where force/stealth would cause detection in question 4.2 and where deceit would cause detection in question 4.3: _____

Use these values for P6's data in step 4 of the next exercise.

Exercise 5 - 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.

The adversary will probably use force after detection so assign delay assuming prior detection. Analyze the path for an adversary who:

1) Enters perimeter personnel portal P5 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) Enters P6 through uncontrolled door D61/1, 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 5 - 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			
4. Enters P6 door D61/1, exchange badge with guard, passes ID, IS, and ME checks, enters 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 magnetic-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: (5 cm wood doors with glass panels)	12 second delay per door
Magnetic Locking Door	60 seconds delay
20-cm wall, reinforced concrete:	2 minute delay (using explosives) 14 minute delay (power tools)
Climb fence:	10 second delay (climbing)
Tilt/vibration fence sensor	0.75 probability of detection
Exterior Active IR sensor	0.5 probability of detection
5 cm metal security door	45 seconds delay
10 cm wooden shipping door with metal sheeting	30 seconds delay (using explosives) 120 seconds delay (using power tools)
Visual ID Check (ID):	0.5 probability of detection
Badge Exchange with guard	0.9 probability of detection
Turnstile with PIN	0.9 probability of detection
Steel Turnstile	18 second delay
Metal detector (ME):	0.9 probability of detection
Item Search (IS):	0.1 probability of detection
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
Time to steal material:	2 minutes
Time to sabotage facility (locate reactor core and set explosive charges)	45 seconds
Average guard response time:	90 seconds (NOTE: we are using this value for this exercise only to get results that are more than P_I=0.)

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 VEASI:
   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, within any given task:
   a) detection always follows delay
   b) detection and delay are simultaneous
   c) delay always follows detection
   d) the relationship between 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

This Page Intentionally Left Blank.

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.*

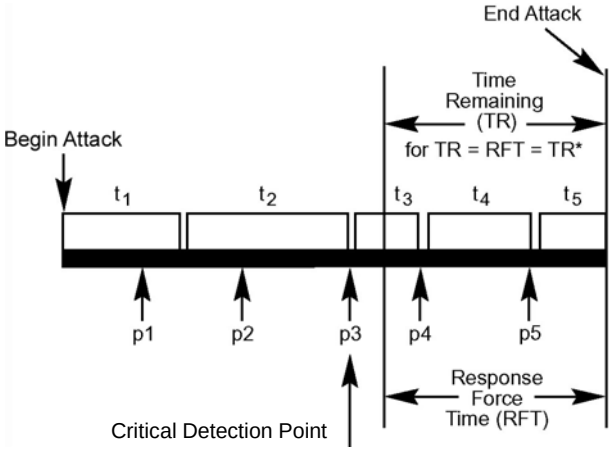


Figure 19-1. Event Time Line

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.

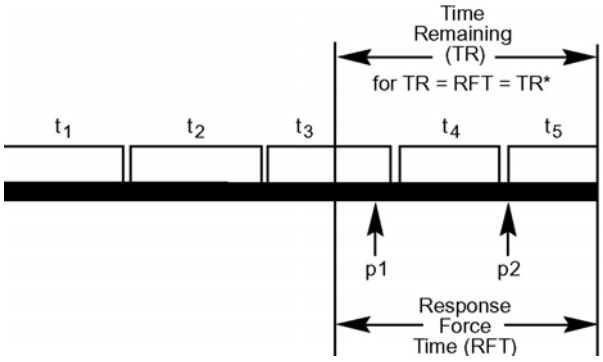


Figure 19-2. No Early Detection

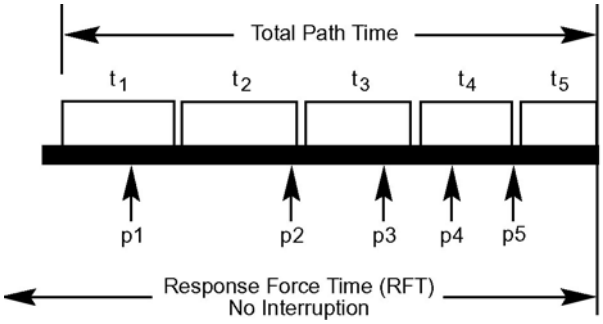


Figure 19-3. Response Time Too Long

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.

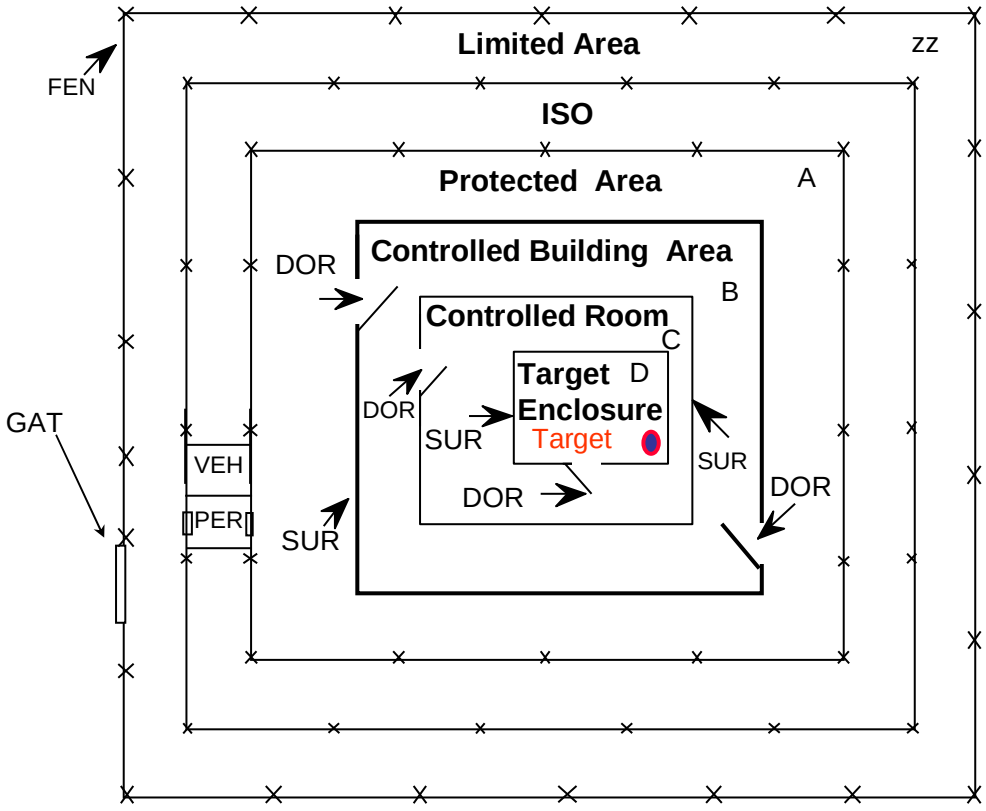


Figure 19-5. Example Facility and PPS Layout

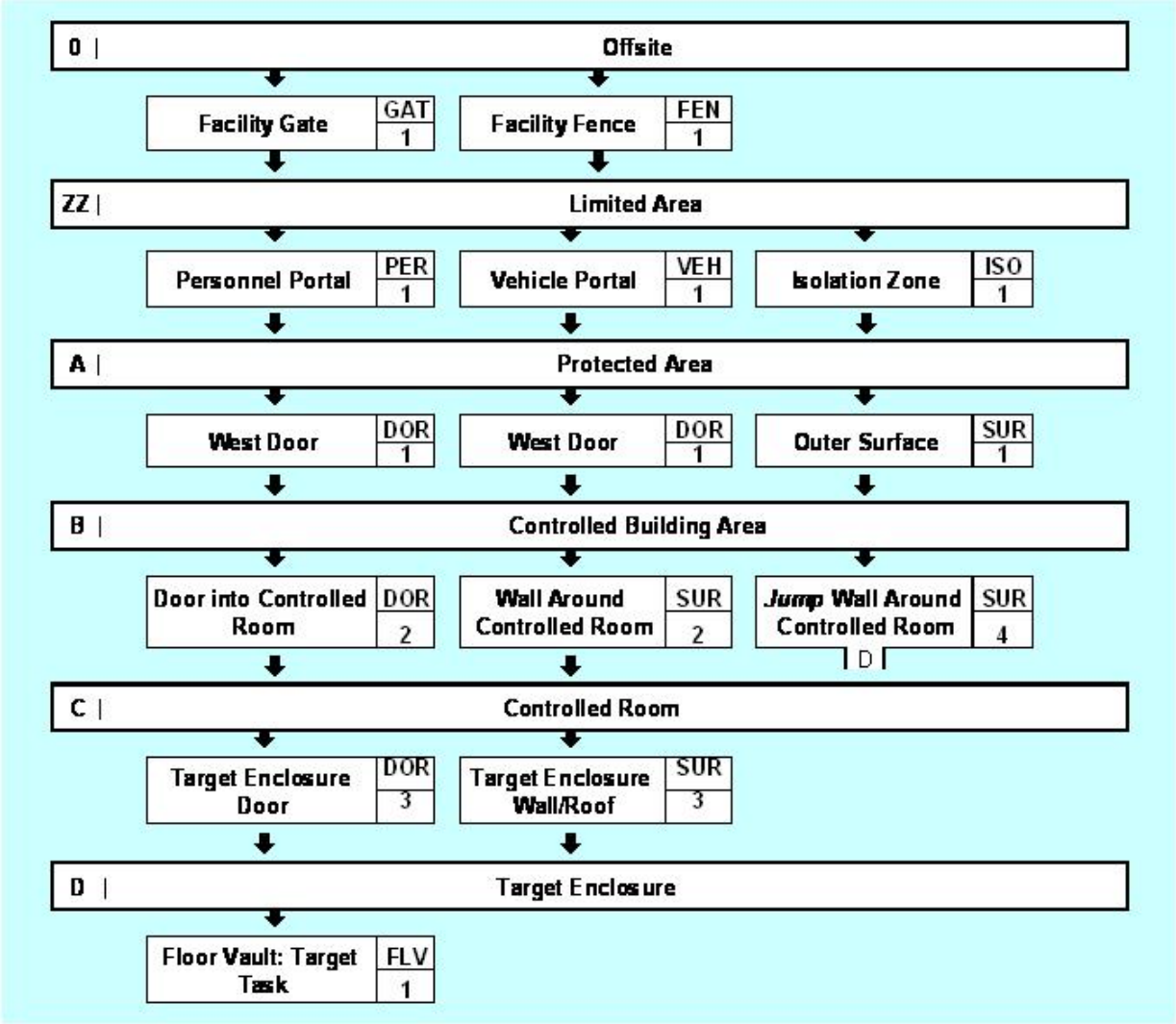


Figure 19-6. Example Facility ASD

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

Element WorkSheet

Element: Personnel Portal, PER

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

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

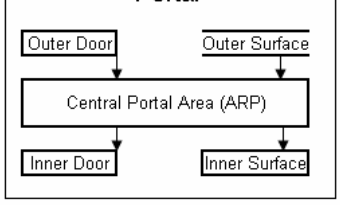


Figure 19-12. Part of the Portal Element Worksheet

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).

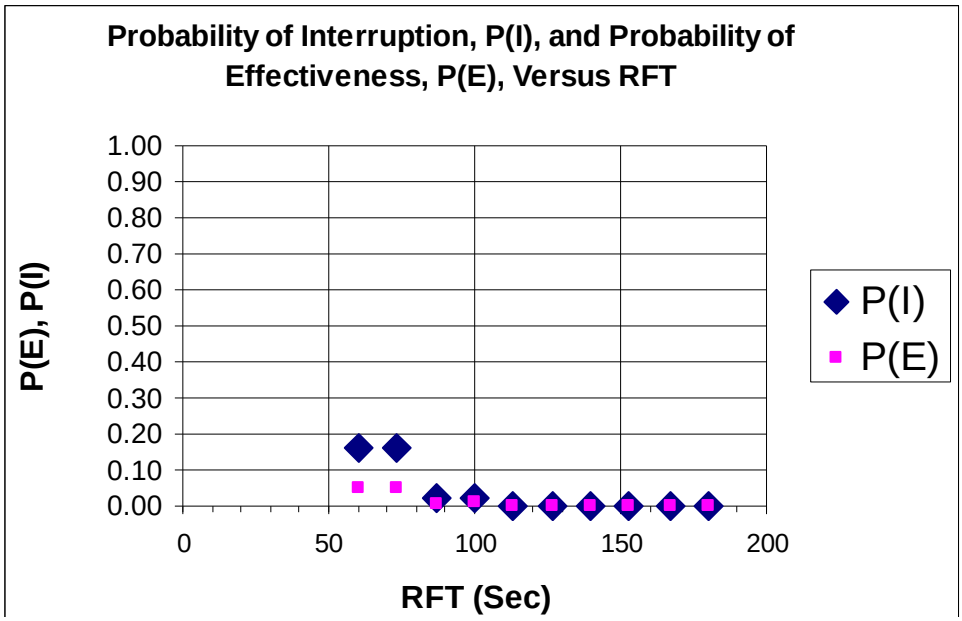


Figure 19-15. Sensitivity Graph of RFT Versus P_I

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 P(I): 0.1622

(Very-Simplified Estimate of Adversary Sequence Interruption) 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.

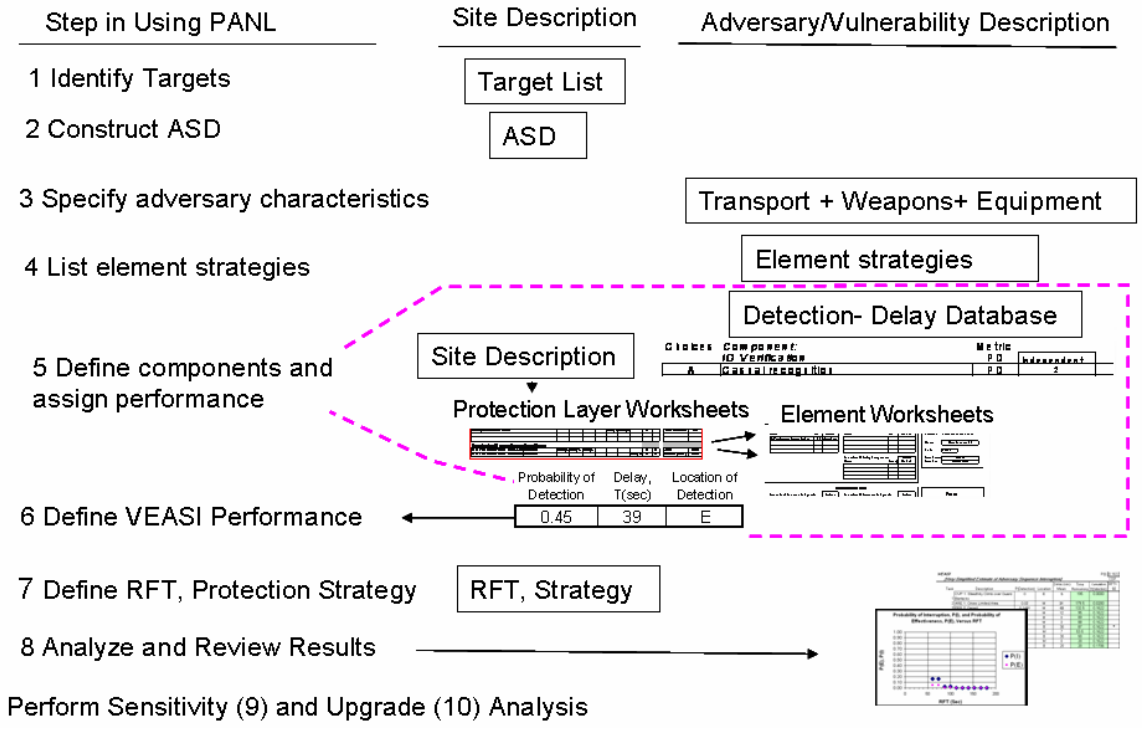
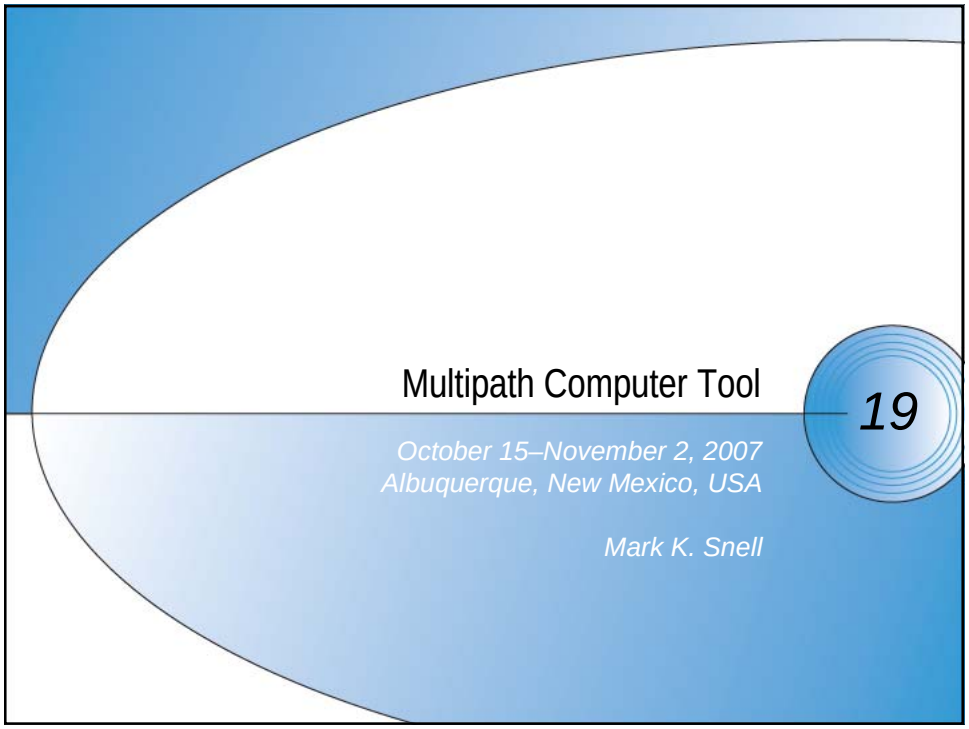


Figure 19-17. PANL-4 Functional Diagram



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

Multipath Computer Tool 3

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**

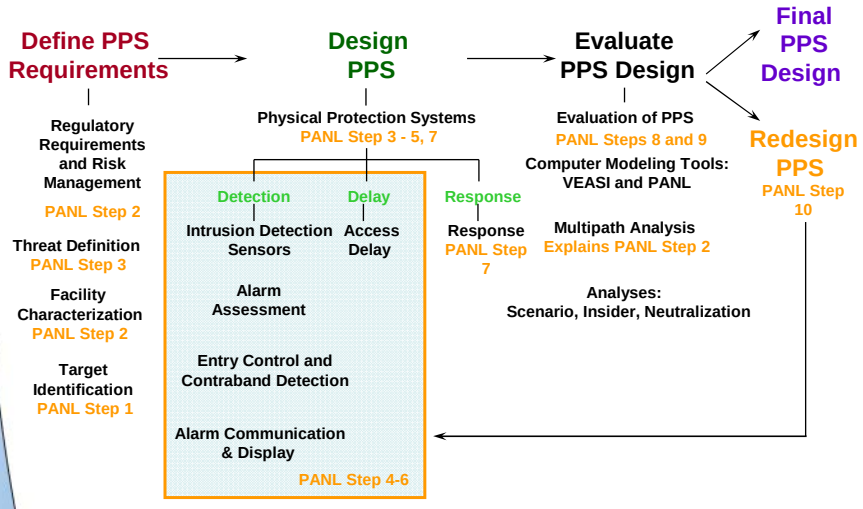
Multipath Computer Tool 4

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**

Multipath Computer Tool 5

DEPO Matched to PANL Steps



Multipath Computer Tool 6

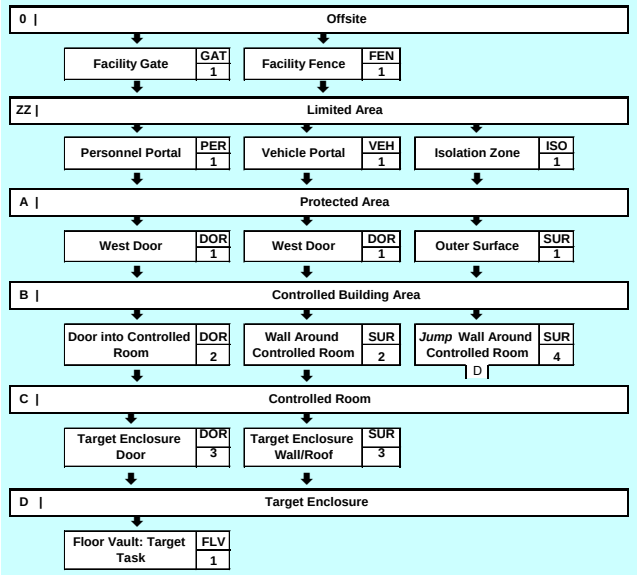
1. Identify Targets

- **Sabotage targets**
- **Theft targets**

Multipath Computer Tool 7

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**



Multipath Computer Tool 8

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	

Multipath Computer Tool 11

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	Transpor-tation
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

Multipath Computer Tool 12

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

Multipath Computer Tool 13

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

Multipath Computer Tool 14

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**

Multipath Computer Tool 15

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

Multipath Computer Tool 16

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	Element List: 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

Multipath Computer Tool 17

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

Component Type	Choice	Entry	Exit	Element List: PER 1	GAT 1	GAT 2	FEN 1	HEL 1	HEL 2	OVP 1	ARE 1
ID Verification	Picture Badge	X	X	Always	Always						
Authorization Check	Authorization Form Check	X	X			Open					
Helicopter Detector	Radar	X	X					Always	Always		
At Post Observation	Duress and Unprotected	X	X	Always	Always	Always					
eral SO Observation	Duress and Unprotected	X	X							Always	

Performance: P(D)/P(S)

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

ited Area Boundary

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

Delay Time, T, in seconds

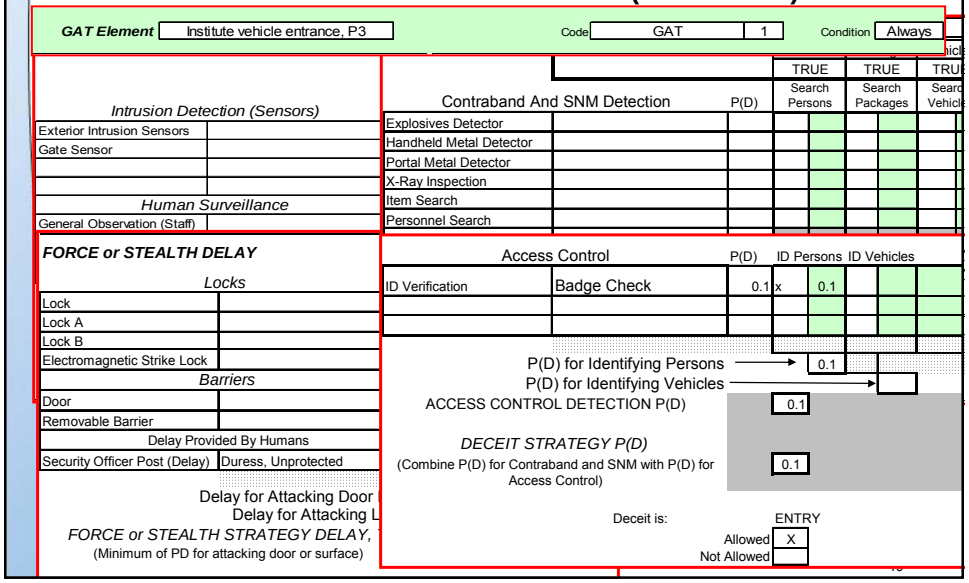
Defeat Method 1	T(sec)	Defeat Method 2	T(sec)
Climb	10	Cut with Tools	8
Climb	10		
Power Tools	60		
Use LAW	0	Use Small Arms	0
Generic Unload	10		
Generic Load	10		
Foot (at 4m/s)	8	Vehicle (at 16m/	1.56
Foot (at 4m/s)	0	Vehicle (at 16m/	0
Helicopter(64 m/s)	16	Vehicle (at 16m/	6
Climb over	12	Vehicle (at 16m/	1
Walking (at 4 m/s)	31	Vehicle (at 16m/	7

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

Multipath Computer Tool 18

5.2 Assign Delay and Detection Values to Each Element Using Worksheets

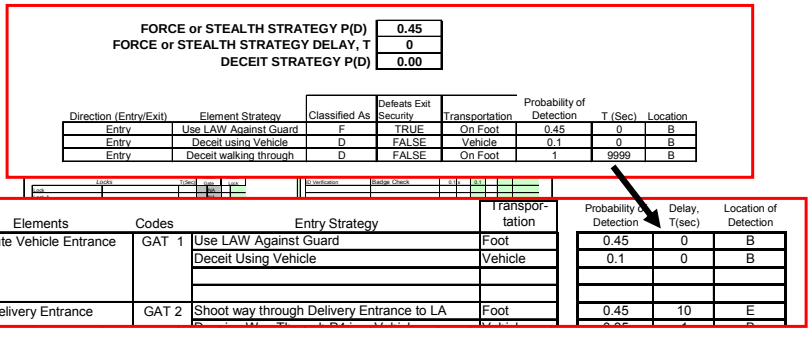
- **5.2.1 Enter element information on sheet (Gate shown)**



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



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

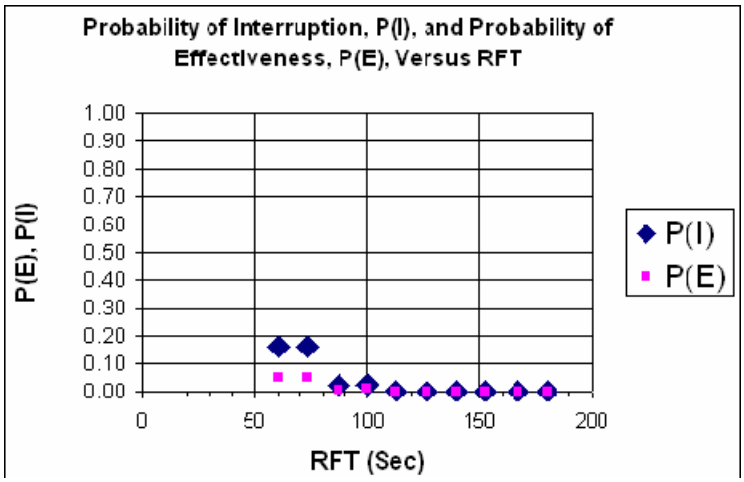
Multipath Computer Tool 21

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



Multipath Computer Tool 23

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

Multipath Computer Tool 24

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

Multipath Computer Tool 25

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

Multipath Computer Tool 26

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

Multipath Computer Tool 27

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**

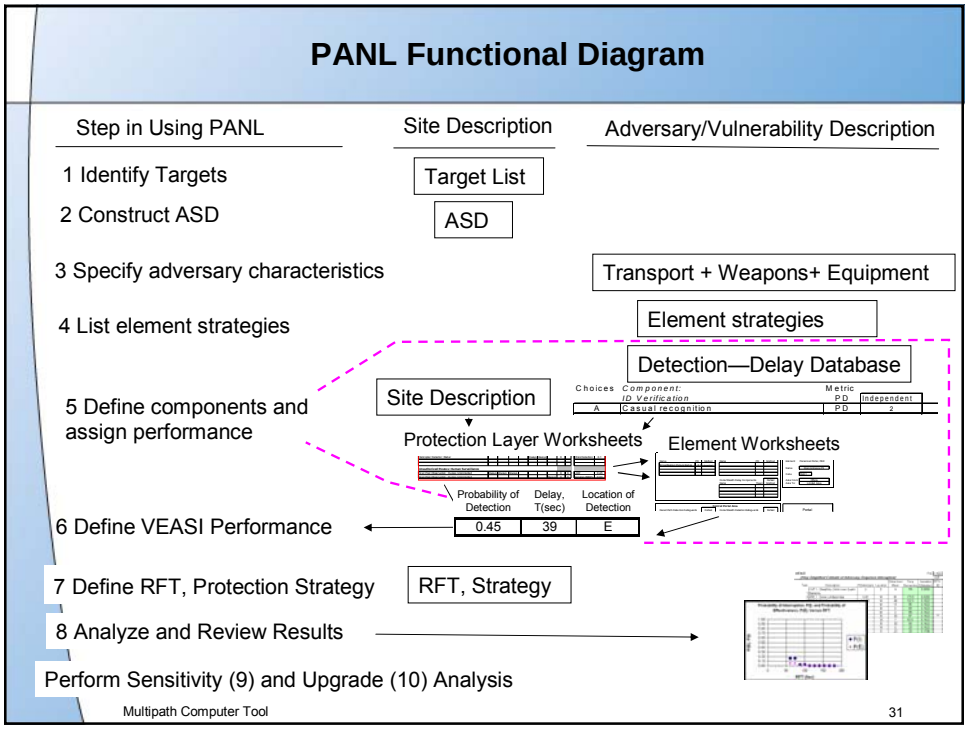
Multipath Computer Tool 28

Demonstration of PANL

Projected Demonstration of PANL

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**


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
Detection—Delay Database
5 Define components and assign performance
Site Description
Choices
Component: ID Verification
Metric
PD
Independent
A
Casual recognition
PD
2
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
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 an 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 directly 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 areas outside buildings, such as the Protected Area, select "Traversable by Vehicle and Foot;" for other areas select "Traversable by Foot Only." Also the dialog displays a "Jump to Area" Code consisting of one or more letters; don't change this, but 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 correct 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," for the element. Click on the okay button.	The name should be a plain-text, non-cryptic 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 indicated by entering an A).	Note: Default codes are automatically assigned to areas. If you change these codes, it is up to you to make sure that the "Jump to Area" Code is correct.
11	Enter the code for the type of element (SUR or PER) in the top right-hand box and enter an index number in the box 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, for example, SUR 1, SUR2, etc.
13	Repeat steps 8-12 until all 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 with the worksheet containing the PTR ASD displayed.

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 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 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 Reactor Building protection layer define two entry element strategies, one minimizing detection and the other minimizing delay, for how the adversary would intrude to the target through: the Shipping/Receiving Door into the Reactor Hall (SHD 1) and the 20-cm walls between the Protected Area and the Reactor Building (SUR 1). Enter these strategies in the column F of the "Element Strat's-Partial Answers" spreadsheet. Also, develop one exit strategy minimizing delay for each of

these two elements and enter them into column G. Merely add rows to enter additional strategies if you want to record 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)? This should categorize your element strategy as Force (F), Stealth (S), Deceit (D), or Force/Stealth (F/S).
- Does using this strategy defeat all element detection and delay components (except transit times) if this element is passed through subsequently? (This is labeled "Defeats Exit Security?" on the spreadsheet.) The assumption for force strategies is to set this variable to TRUE, so that a fence or wall, for example, is does not provide any detection or delay if the adversary passes through the element again. 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. Note: typically, it is assumed that "Defeats Exit Security" is set to FALSE for deceit: at least some components are expected to work subsequent to use of deceit at a portal (e.g., SO's will still be performing their jobs). For stealth, the user needs to decide whether all the components are defeated or not and set this variable to TRUE or FALSE accordingly.
- What transportation is the strategy assuming? Enter "Foot", "Helicopter", or "Vehicle", as appropriate. 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 when 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). Note: Use F/S if you can't decide whether a tactic is F or S.	Enter text as F, S, D, or F/S in column I for entry strategies and column L for exit strategies.
3	Indicate whether the strategy defeats all of the element detection and delay on exit if	Enter TRUE or FALSE in column J for entry strategies and column M for exit

	passed through on entry previously.	entry strategies and column M for exit strategies.
4	Record the type of transportation that the strategy assumes.	Enter "On Foot" or "Vehicle" or "Helicopter" in column K for entry strategies and column N for exit strategies.

Exercise 3. Define PPS Security Components and Assign Component Performance

This exercise will provide participants practice collecting information about the security components at elements and then assigning appropriate minimum detection and delay values along with worst-case detection locations to element strategies at these elements. Note: performance data for each type of component can be found in 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 5 in Section 11 on page 21*
  - Contraband and SNM detection - providing detection for deceit strategies – *see Table 5 7 in Section 11, page 23*.
  - Intrusion detection (typically by sensors) - providing detection for stealth and force strategies – *see Table 4 in Section 11,page 20*.
  - Human surveillance (by security officers or employees) – providing detection for stealth and force strategies -- *See Table 6 in Section 11, page 22 .*
- Delay components
  - Barriers -- *See Table 8 in Section 19 on page 32*.
  - Locks -- *See Table 8 in Section 19 on page 32*.
  - Target Tasks -- *Typically, user defined*
  - Security Officers – *See Table 9 in Section 19 on page 33.*
  - Transit times -- *Typically, user defined*.

3.1 Determine detection, delay, and location values

In this exercise, we will assign worst-case probabilities of detection and delay times as well as locations of detection values for several elements comprising the PTR Building Perimeter protection layer:

- P6 in Room R061 (PER 3);
- The Shipping/Receiving Door (SHD 1); and
- The 20-cm reinforced concrete wall between the Protected Area and the Reactor Building (SUR 1).

(Note: We have already determined detection, delay, and locations of detection for two strategies at P6 in Exercise 4.2 of Subgroup 18S, Single Path Computer Tool. Following the same process used at P6 earlier, determine probability of detection, delay time, and location of detection for an element strategy of minimizing detection

through SHD1 and SUR1 towards the target; also determine probability of detection, delay time, and location of detection for an element strategy minimizing delay through SHD1 and SUR1 towards the target. Record your results here:

Element	Strategy Name for Strategy minimizing Detection:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SHD1:						TRUE / FALSE	

Element	Strategy Name for Strategy minimizing Delay:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SHD1:						TRUE / FALSE	

Element	Strategy Name for Strategy minimizing Detection:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SUR1:						TRUE / FALSE	

Element	Strategy Name for Strategy minimizing Delay:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SUR1:						TRUE / FALSE	

Use the following rationale for setting the other fields besides P(D) and delay time, T:

- The “Classified as”, “Defeats Exit Security”, and “Transportation” fields should be set as described in exercise 2.2.
- Location: Record the location of detection. As there may be multiple places in an element that provide detection, assign location based on which location provides the largest contribution to P(D). (Example for a portal that consists of an Outer Layer, a Central Area and an Inner Layer: if the Outer Layer provides P(D) = .5 while the Central Area has P(D) = .6, then the element has total P(D) = 1-(1-.5)*(1-.6) = .8. In this case, the Outer Layer provides the largest contribution to P(D) because it adds .5 while the Central Area adds .3. Thus, assume detection occurs at the beginning, “B”)

Note: After such information is determined enter the data into the “Element Strat's-Partial Answers” worksheet in PANL for SHD 1 and SUR 1.

3.2 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 land

vehicle (e.g., a truck). Assume a random patrol by a security officer is conducted 24 hours/day in the Limited Area. (Note: we will only enter the foot rates into PANL.)

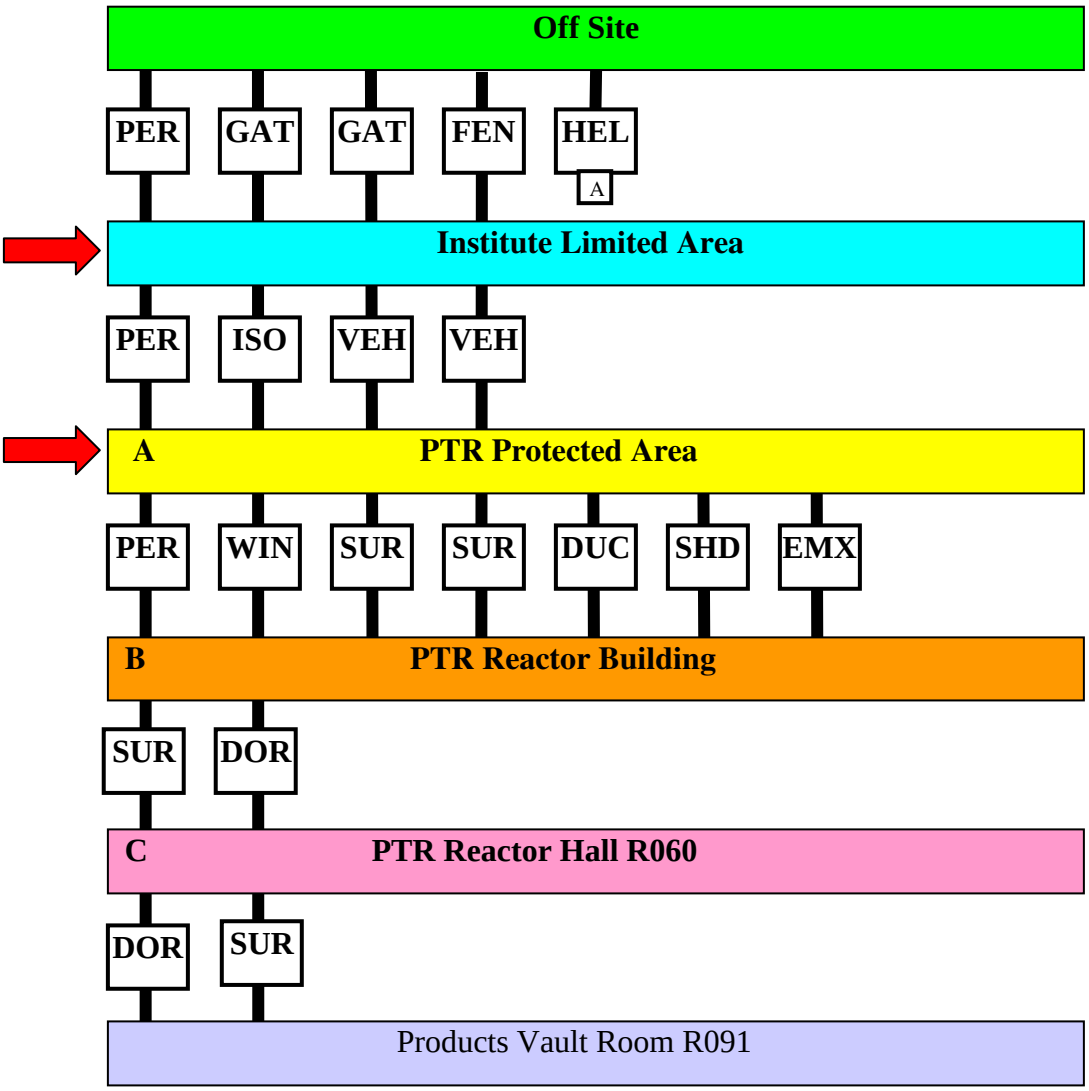


Figure 19.2. ASD for the PTR Research Reactor

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

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

To enter data into PANL, input the data in the appropriate columns (see Figure 19.3) of the Element Strat's-Partial Answers worksheet for the elements and areas and element strategies you worked on in 3.1 and 3.2. When you have completed entering data, save your file.

	What You Do	Comments/Prompts
1	To enter data, move to the "Element Strat's-Partial Answers" worksheet .	To do so, merely select the tab with this name on it
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 Performar		
Codes	Entry Strategy	Exit Strategy	Probability of Detection	Delay, T(sec)	Location of Detection	Probability of Detection	Delay, T(sec)	Loca Det
GAT 1	Deceive Way Through Vehicle Entrance		0.1	0	B			
GAT 2	Shoot way through Delivery Entrance to LA		0.45	10	B		10	
	Deceive Way Through Delivery Entrance		1	10	B			
FEN 1	Climb Outer Walls		0	10	B		10	
HEL 1	Land Helicopter in Limited Area		1	9999	B		9999	

Figure 19.3. 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 denial, to prevent an adversary from removing fresh fuel from 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 Strat's-Correct Answers" worksheet, review each element's strategy and performance value list (the entry values are shown first and then the exit values). Deactivate HEL elements that are associated with helicopter transportation	Enter TRUE to activate and FALSE to deactivate elements in column AB for entry and column AC for exit. Note: using this worksheet allows everyone to have the same data
2	At the top of the Element Strategies worksheet, select "Go to Path Analysis."	This moves to the Analysis 1 worksheet.
3	Then, fill in the response information: For RFT's enter 10 as the number of RFT's and then enter 60, 120, 180, 240, 320, 360, 420, 480, 540, and 600 as values in B7 to B16. Set cells B17 = -1 and B18 =9999.	Enter number of RFTs in cell B5 and the RFT numbers in cells B7 to B16. Note 320 is not evenly spaced among the others.
4	Then click on the "Denial" 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 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 F18.	
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 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 F17	
2	Answer the questions below.	

? What is the Total System Minimum Probability of Detection (P_D) 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 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 Strat's-Correct Answers" worksheet, review each element's strategy and performance value list (the entry values are shown first and then the exit values). Deactivate HEL elements that are associated with helicopter transportation	Enter TRUE to activate and FALSE to deactivate elements in columns AB and AC.
2	At the top of the Element Strategies worksheet, select "Create and Run Path Analysis."	This moves to the Analysis 1 worksheet.
3	Then, fill in the response information: For RFT's enter 10 as the number of RFT's and then enter 60, 120, 180, 240, 320, 360, 420, 480, 540, and 600 as values in B7 to B16. Set cells B17 = -1 and B18 =9999.	Enter number of RFTs in cell B5 and the RFT numbers in cells B7 to B16. (
4	Then click on the "Denial" 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.

Execute the Analyze Command

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.

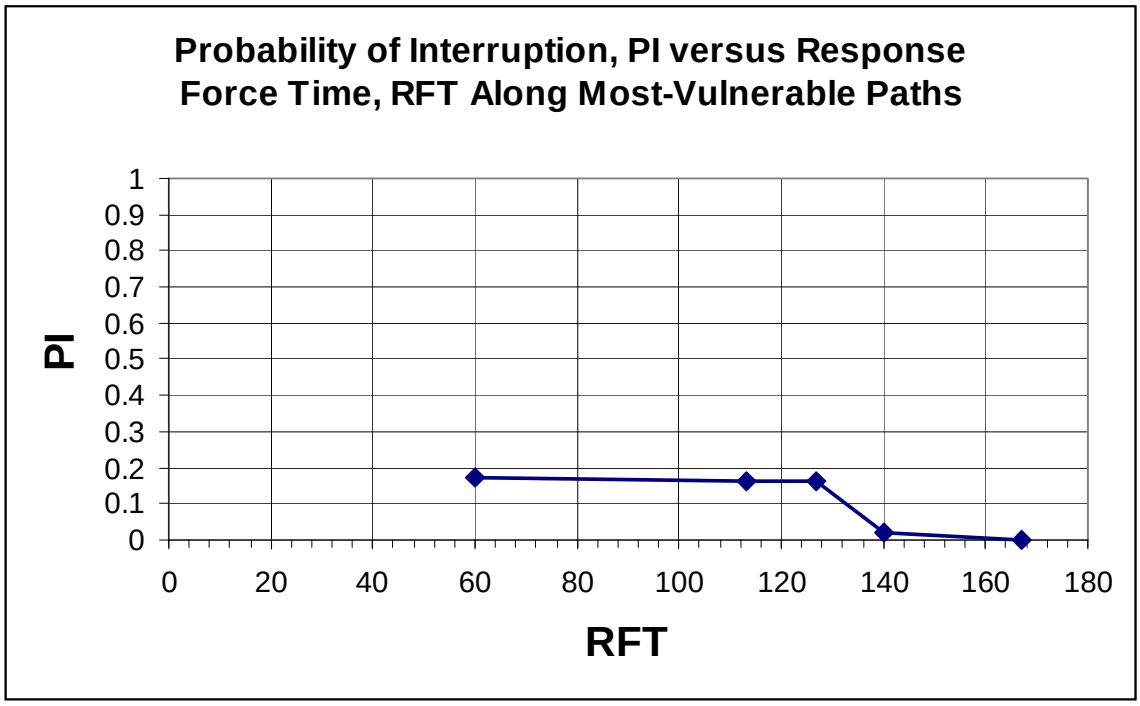


Figure 19.4. Illustration of Sensitivity Graph (Most Vulnerable Path to RFT (from 60 to 180 seconds))

? 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 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 the largest RFT where P_I is greater than 10%?

_____seconds

? 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 Strat's-Correct Answers" 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 Strat's-Correct Answers" worksheet:
  - Minimum probability of detection for each element against forceful or stealthy tactics (e.g., leave out Deceit strategies) on entry;
  - 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).

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

	Protection Path Elements			
	PER 2	**ISO 1**	**VEH 1**	**VEH 2**
Force/Stealth P(D)				
Delay (seconds)				
Element Number	9	10	11	12
Min P_I Through this Element (RFT =60 seconds)				
Min P_I Around this Element (RFT = 60 seconds)				

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 "Element Strat's-Correct Answers**"** worksheet and the Analysis 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 Strat's-Correct Answers" 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) based on RFT = 60 sec; 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) based on RFT = 60 sec.

	Protection Path Elements						
	PER 3	**WND 1**	**SUR 1**	**SUR 2**	**DUC 1**	**SHD 1**	**EMX 1**
Force/Stealth P(D)	0.45		0.0			0.40	
Delay (seconds)	21		120			30	
Element Number	15	16	17	18	19	20	21
Min P_I Through this Element (RFT = 60 sec.)							

Min P_I Around this Element (RFT= 60 sec.)							

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?

_____

5.2.2 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 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 Strat's-Correct Answers 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 "Go to Path Analysis" button.	This should take you to the analysis page. This uses the same analysis settings as found in PANL_EX5.xls
4	Select "Run Path Analysis" to execute the analysis.	Record P_I for RFT = 320 sec. in the following table.
5	Save as PANL_EX6_180.xls	
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 = 320 seconds.
7	Similar to 6, but use 300 sec. at the OPN location. Save as PANL_EX6_300.xls.	Record P_I for RFT = 320 seconds.
8	Repeat 7, but with 360 sec.	Record P_I for RFT = 320 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	Start with PANL_EX5.xls.Study the PANL results in Exercise 5 especially the balance results.	
2	Propose and enter two PPS upgrades for the research reactor on the next page.	Consider improving detection before the critical detection point and delay after the critical detection point.
3	Enter upgrades in performance values on the Element Strat's-Correct Answers worksheet from PANL_EX5.xls	You must determine the effect of each upgrade on element performance by hand.
4	Go to the Path Analysis worksheet, Analysis 1.	Use the ”Go to Path Analysis” button.
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?

This Page Intentionally Left Blank.

Subgroup 19
Multipath Computer Tool

Session Objectives

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

1. Enter an 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 directly 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 areas outside buildings, such as the Protected Area, select "Traversable by Vehicle and Foot;" for other areas select "Traversable by Foot Only." Also the dialog displays a "Jump to Area" Code consisting of one or more letters; don't change this, but 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 correct 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," for the element. Click on the okay button.	The name should be a plain-text, non-cryptic 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 indicated by entering an A).	Note: Default codes are automatically assigned to areas. If you change these codes, it is up to you to make sure that the "Jump to Area" Code is correct.
11	Enter the code for the type of element (SUR or PER) in the top right-hand box and enter an index number in the box 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, for example, SUR 1, SUR2, etc.
13	Repeat steps 8-12 until all 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 with the worksheet containing the PTR ASD displayed.

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 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 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 Reactor Building protection layer define two entry element strategies, one minimizing detection and the other minimizing delay, for how the adversary would intrude to the target through: the Shipping/Receiving Door into the Reactor Hall (SHD 1) and the 20-cm walls between the Protected Area and the Reactor Building (SUR 1). Enter these strategies in the column F of the "Element Strat's-Partial Answers" spreadsheet. Also, develop one exit strategy minimizing delay for each of

these two elements and enter them into column G. Merely add rows to enter additional strategies if you want to record 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)? This should categorize your element strategy as Force (F), Stealth (S), Deceit (D), or Force/Stealth (F/S).
- Does using this strategy defeat all element detection and delay components (except transit times) if this element is passed through subsequently? (This is labeled "Defeats Exit Security?" on the spreadsheet.) The assumption for force strategies is to set this variable to TRUE, so that a fence or wall, for example, is does not provide any detection or delay if the adversary passes through the element again. 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. Note: typically, it is assumed that "Defeats Exit Security" is set to FALSE for deceit: at least some components are expected to work subsequent to use of deceit at a portal (e.g., SO's will still be performing their jobs). For stealth, the user needs to decide whether all the components are defeated or not and set this variable to TRUE or FALSE accordingly.
- What transportation is the strategy assuming? Enter "Foot", "Helicopter", or "Vehicle", as appropriate. 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 when 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). Note: Use F/S if you can't decide whether a tactic is F or S.	Enter text as F, S, D, or F/S in column I for entry strategies and column L for exit strategies.
3	Indicate whether the strategy defeats all of the element detection and delay on exit if	Enter TRUE or FALSE in column J for entry strategies and column M for exit

	passed through on entry previously.	entry strategies and column M for exit strategies.
4	Record the type of transportation that the strategy assumes.	Enter "On Foot" or "Vehicle" or "Helicopter" in column K for entry strategies and column N for exit strategies.

Exercise 3. Define PPS Security Components and Assign Component Performance

This exercise will provide participants practice collecting information about the security components at elements and then assigning appropriate minimum detection and delay values along with worst-case detection locations to element strategies at these elements. Note: performance data for each type of component can be found in 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 5 in Section 11 on page 21*
  - Contraband and SNM detection - providing detection for deceit strategies – *see Table 7 in Section 11, page 23*.
  - Intrusion detection (typically by sensors) - providing detection for stealth and force strategies – *see Table 4 in Section 11,page 20*.
  - Human surveillance (by security officers or employees) – providing detection for stealth and force strategies -- *See Table 6 in Section 11, page 22 .*
- Delay components
  - Barriers -- *See Table 8 in Section 19 on page 32*.
  - Locks -- *See Table 9 in Section 19 on page 33*
  - Target Tasks -- *Typically, user defined*
  - Security Officers – *See Table 10 in Section 19 on page 33.*
  - Transit times -- *Typically, user defined*.

3.1 Determine detection, delay, and location values

In this exercise, we will assign worst-case probabilities of detection and delay times as well as locations of detection values for several elements comprising the PTR Building Perimeter protection layer:

- P6 in Room R061 (PER 3);
- The Shipping/Receiving Door (SHD 1); and
- The 20-cm reinforced concrete wall between the Protected Area and the Reactor Building (SUR 1).

(Note: We have already determined detection, delay, and locations of detection for two strategies at P6 in Exercises 4.2 and 4.3 of Subgroup 18S, Single Path Computer Tool. Following the same process used at P6 earlier, take the information you collected in Exercise 3, subgroup 17S to determine probability of detection,

delay time, and location of detection for an element strategy of minimizing detection through SHD1 and SUR1 towards the target; also determine probability of detection, delay time, and location of detection for an element strategy minimizing delay through SHD1 and SUR1 towards the target. Record your results here:

Element	Strategy Name for Strategy minimizing Detection:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SHD1:						TRUE / FALSE	

Element	Strategy Name for Strategy minimizing Delay:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SHD1:						TRUE / FALSE	

Element	Strategy Name for Strategy minimizing Detection:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SUR1:						TRUE / FALSE	

Element	Strategy Name for Strategy minimizing Delay:	P(D)	T(Sec)	Location	Classified As	Defeats Exit Security?	Transportation
SUR1:						TRUE / FALSE	

Use the following rationale for setting the other fields besides P(D) and delay time, T:

- The “Classified as”, “Defeats Exit Security”, and “Transportation” fields should be set as described in exercise 2.2.
- Location: Record the location of detection. As there may be multiple places in an element that provide detection, assign location based on which location provides the largest contribution to P(D). (Example for a portal that consists of an Outer Layer, a Central Area and an Inner Layer: if the Outer Layer provides P(D) = .5 while the Central Area has P(D) = .6, then the element has total P(D) = 1-(1-.5)*(1-.6) = .8. In this case, the Outer Layer provides the largest contribution to P(D) because it adds .5 while the Central Area adds .3. Thus, assume detection occurs at the beginning, “B”)

Note: After such information is determined enter the data into the “Element Strat's-Partial Answers” worksheet in PANL for SHD 1 and SUR 1.

3.2 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 land vehicle (e.g., a truck). Assume a random patrol by a security officer is conducted 24 hours/day in the Limited Area. (Note: we will only enter the foot rates into PANL.)

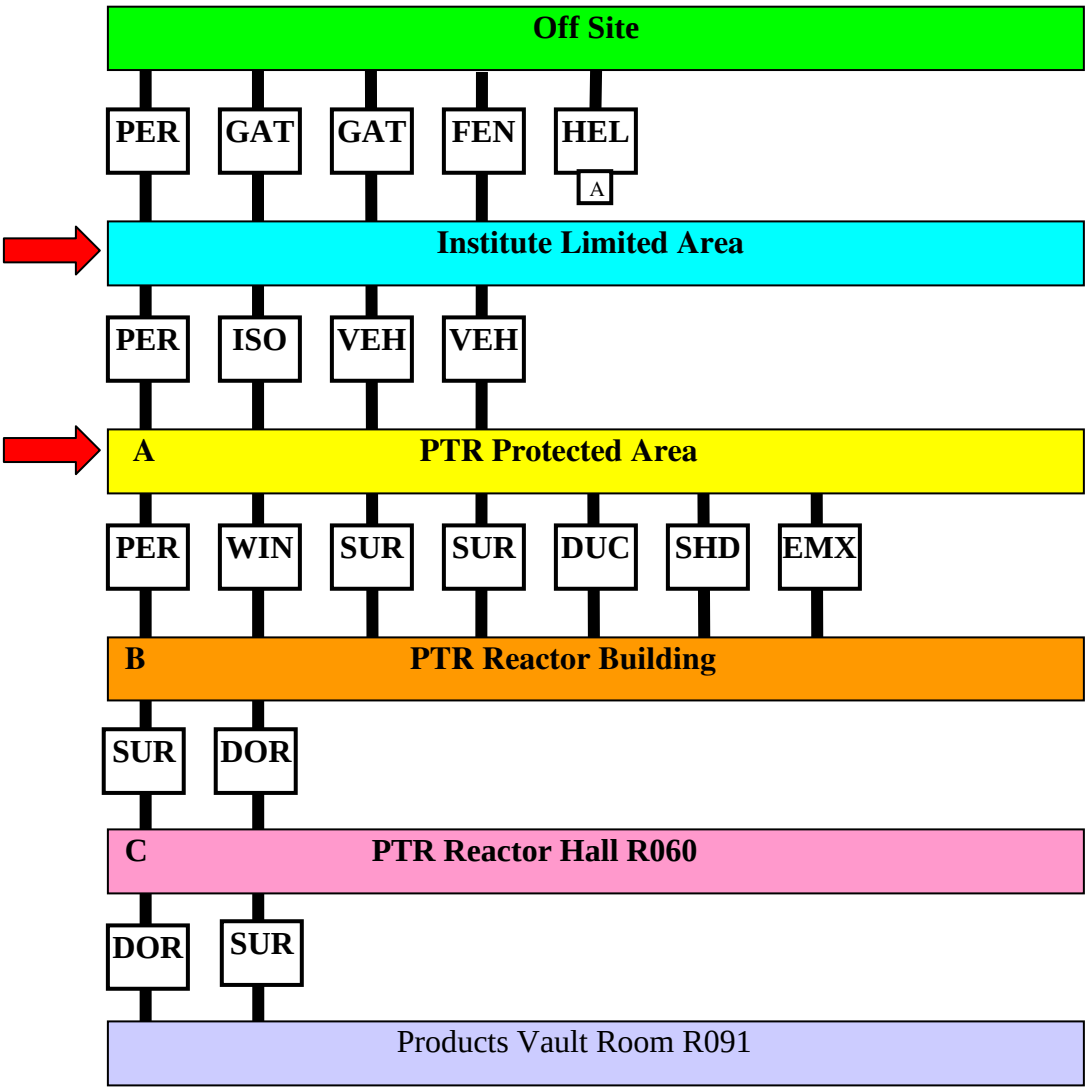


Figure 19.2. ASD for the PTR Research Reactor

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

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

To enter data into PANL, input the data in the appropriate columns (see Figure 19.3) of the Element Strat's-Partial Answers worksheet for the elements and areas and element strategies you worked on in 3.1 and 3.2. When you have completed entering data, save your file.

	What You Do	Comments/Prompts
1	To enter data, move to the "Element Strat's-Partial Answers" worksheet .	To do so, merely select the tab with this name on it
2	Input the performance data – (PD, delay time, and location of detection) for the element and element strategies you worked on.	See Figure 19.3 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.

		Column
	Entry Strategy	F
Entrance Strategy Performance	P(D)	P
	Delay, T(sec)	Q
	Location of Detection	R
Entrance Strategy Data	Classified As	I
	Defeat on Exit	J
	Transportation	K

		Column
	Exit Strategy	G
Exit Strategy Performance	P(D)	T
	Delay, T(sec)	U
	Location of Detection	V
Exit Strategy Data	Classified As	L
	Defeat on Exit	M
	Transportation	N

Figure 19.3. 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 denial, to prevent an adversary from removing fresh fuel from 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 Strat's-Correct Answers" worksheet, review each element's strategy and performance value list (the entry values are shown first and then the exit values). Deactivate HEL elements that are associated with helicopter transportation	Enter TRUE to activate and FALSE to deactivate elements in column AB for entry and column AC for exit. Note: using this worksheet allows everyone to have the same data
2	At the top of the Element Strategies worksheet, select "Go to Path Analysis."	This moves to the Analysis 1 worksheet.
3	Then, fill in the response information: For RFT's enter 10 as the number of RFT's and then enter 60, 120, 180, 240, 320, 360, 420, 480, 540, and 600 as values in B7 to B16. Set cells B17 = -1 and B18 =9999.	Enter number of RFTs in cell B5 and the RFT numbers in cells B7 to B16. Note 320 is not evenly spaced among the others.
4	Then click on the "Denial" 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 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.

	What You Do	Comments/Prompts
1	Examine cell F18.	
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 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 F17	
2	Answer the questions below.	

? What is the Total System Minimum Probability of Detection (P_D) 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 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 Strat's-Correct Answers" worksheet, review each element's strategy and performance value list (the entry values are shown first and then the exit values). Deactivate HEL elements that are associated with helicopter transportation	Enter TRUE to activate and FALSE to deactivate elements in columns AB and AC.
2	At the top of the Element Strategies worksheet, select "Create and Run Path Analysis."	This moves to the Analysis 1 worksheet.
3	Then, fill in the response information: For RFT's enter 10 as the number of RFT's and then enter 60, 120, 180, 240, 320, 360, 420, 480, 540, and 600 as values in B7 to B16. Set cells B17 = -1 and B18 =9999.	Enter number of RFTs in cell B5 and the RFT numbers in cells B7 to B16. (
4	Then click on the "Denial" 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.

Execute the Analyze Command

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.

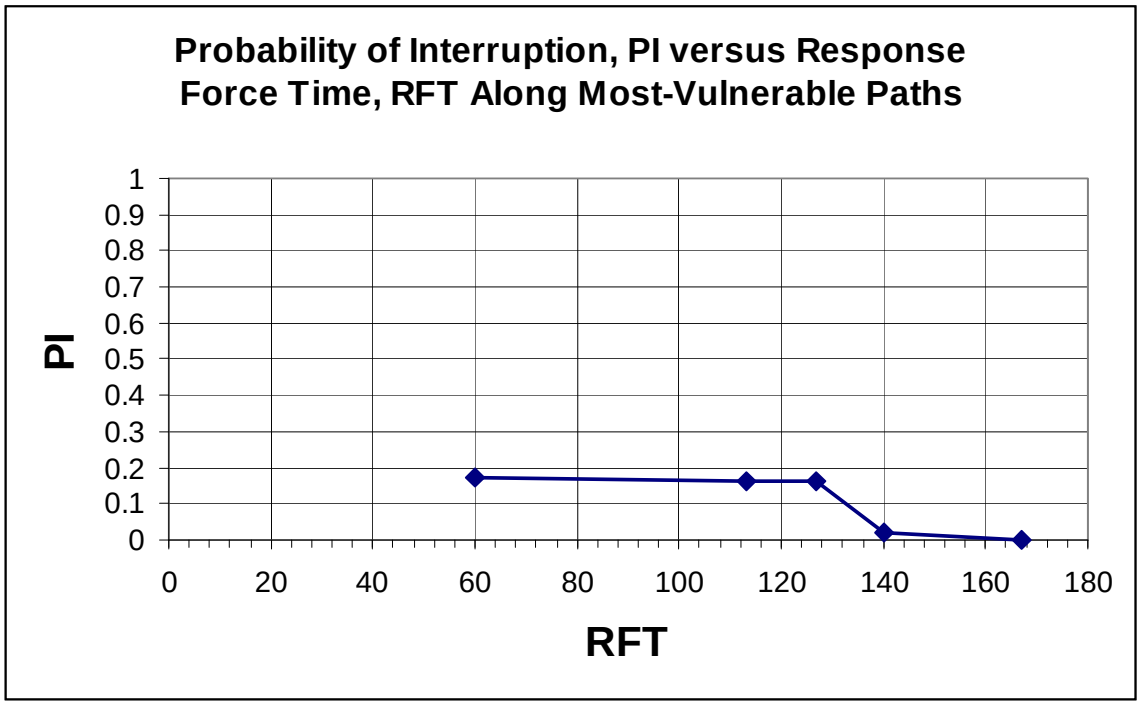


Figure 19.4. Illustration of Sensitivity Graph (Most Vulnerable Path to RFT (from 60 to 180 seconds))

? 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 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 the largest RFT where P_I is greater than 10%?

_____seconds

? 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 Strat's-Correct Answers" 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 Strat's-Correct Answers" worksheet:
  - Minimum probability of detection for each element against forceful or stealthy tactics (e.g., leave out Deceit strategies) on entry;
  - 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).

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

	Protection Path Elements			
	PER 2	**ISO 1**	**VEH 1**	**VEH 2**
Force/Stealth\Deceit P(D)				
Delay (seconds)				
Element Number	9	10	11	12
Min P_I Through this Element (RFT =60 seconds)				
Min P_I Around this Element (RFT = 60 seconds)				

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 "Element Strat's-Correct Answers**"** worksheet and the Analysis 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 Strat's-Correct Answers" 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) based on RFT = 60 sec; 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) based on RFT = 60 sec.

	Protection Path Elements						
	PER 3	**WND 1**	**SUR 1**	**SUR 2**	**DUC 1**	**SHD 1**	**EMX 1**
Force/Stealth/ Deceit P(D)	0.45		0.0			0.40	
Delay (seconds)	51		120			30	
Element Number	15	16	17	18	19	20	21
Min P_I Through this Element (RFT = 60 sec.)							
Min P_I Around this Element (RFT= 60 sec.)							

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?

_____

5.2.2 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 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 Strat's-Correct Answers 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 "Go to Path Analysis" button.	This should take you to the analysis page. This uses the same analysis settings as found in PANL_EX5.xls
4	Select "Run Path Analysis" to execute the analysis.	Record P_I for RFT = 320 sec. in the following table.
5	Save as PANL_EX6_180.xls	
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 = 320 seconds.
7	Similar to 6, but use 300 sec. at the OPN location. Save as PANL_EX6_300.xls.	Record P_I for RFT = 320 seconds.
8	Repeat 7, but with 360 sec.	Record P_I for RFT = 320 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	Start with PANL_EX5.xls.Study the PANL results in Exercise 5 especially the balance results.	
2	Propose and enter two PPS upgrades for the research reactor on the next page.	Consider improving detection before the critical detection point and delay after the critical detection point.
3	Enter upgrades in performance values on the Element Strat's-Correct Answers worksheet from PANL_EX5.xls	You must determine the effect of each upgrade on element performance by hand.
4	Go to the Path Analysis worksheet, Analysis 1.	Use the ”Go to Path Analysis” button.
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). 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 required 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?

22. Tabletop Analysis

Abstract. *This session discusses how tabletop exercises can be performed as part of scenario analysis to qualitatively determine the effectiveness of the security system against adversary attack scenarios. Three phases of a tabletop are presented. The first phase, involves preliminary planning, documentation of assumptions, and formulation of an adversary scenario attack plan. The second phase consists of simulating the attackers interacting with the protective force and security system. During this phase, the simulation starts at time zero, identifies and processes events that occur (e.g., arrivals at locations, detection, and shooting at/hitting/killing targets) at each time, adding new events, and then moving to later events. Information about how a scenario was realized is stored in a timeline describing what each entity is doing at time intervals. The final phase identifies prioritized upgrades and produces documentation. While the results of the tabletop are qualitative, they are lower cost and more easily performed than other combat simulations such as Force-on-Force exercises, and they can be used to plan and structure computer combat simulations that serve to produce quantitative effectiveness results.*

22.1 Introduction

Use of Tabletop Exercises in Scenario Analysis

Tabletop exercises, performed in a fashion similar to the approach described here, are a relatively new U.S. Department of Energy (DOE) process used to perform scenario analysis, where security system effectiveness is evaluated against a scenario based adversary attack when using an agreed upon Threat Statement or Design Basis Threat. While this approach does not produce a quantitative Probability of System Effectiveness, P_E, it still produces a very good qualitative understanding of how the system will perform against adversary scenarios. Where quantitative values are required by the regulatory authority, these same tabletops can be used to plan better combat simulations, such as computer simulations or Force-on-Force exercises, so that the simulations are more realistic and more data can be collected from the process.

Value of Tabletop Exercises

One of the biggest challenges facing all levels of site, facility, and regulatory management is how to establish a baseline to collect accurate data for evaluating security system effectiveness for existing security systems and/or conceptual security system design plans. The tabletop process described here has demonstrated the ability to assist management in achieving such a security system baseline while addressing the critical aspects of achieving balance in the security system and ensuring cost effectiveness reviews are incorporated.

When completed the data collected can assist in providing information to accept the security system in place, or highlight the need for identified enhancement options. As an added value, tabletop exercise can be used to assist in identifying and evaluating the value of those protective elements that cannot be directly linked to security when measured against a given adversary attack scenario.

In all cases, the tabletop process is designed to assist management in improving security system effectiveness and/or assist in providing rationale for risk acceptance.

This section discusses the following aspects of tabletop analyses

- General background on tabletop exercises, including the rigor involved in performing the exercise and the limitations of the methodology;
- Preparatory steps for the tabletop exercise: Scoping meetings, exercise protocols, and "rules of engagement" describing assumptions for the tabletop;
- Adversary attack planning[1] and its relationship with site data collection;
- Execution issues in performing a tabletop including how both formal and informal tabletop exercises are organized and directed; how initial conditions are set up, and how behavioral and random events should be decided.
- How results should be collected and documented.

22.2 Background on Tabletop Exercises

Tabletop Exercises as Collaborative Processes for Assessing System Effectiveness

A tabletop exercise is performed as a collaborative process. It provides insight into the functioning and level of performance of the overall security system under various attack scenarios. Attack scenarios ***may or may not*** be bounded by the established threat statement.

Tabletop exercises produce a deliverable that describes a given facility's security system effectiveness. Also, it provides a recommended list of prioritized system upgrades that, when implemented, should enhance security system effectiveness. Expected outcome of the collective tabletop exercises is an assessment of the potential vulnerability to a range of threats. Tabletop exercise data reviews and analysis are intended to ensure the security system is sufficiently formidable to perform well against the current Threat Statement.

In some cases the tabletop exercise can accommodate reasonable increases in adversary numbers, capabilities, or changes in tactics. Ideally, the security system should not be such that slight increases in adversary actions cause catastrophic failure instead of a preferred ***gradual*** degradation of system effectiveness. This will ensure that protection of attractive materials will only degrade slowly when stressed to failure instead of degrading rapidly with only a small increase in adversary tactics and capabilities.

Need for Rigor and Discipline

When conducted carefully, with high level of rigor and discipline, information from tabletop exercises can be beneficial in conducting subsequent performance testing, force-on-force exercises, and modeling simulations.

[1] For the purpose of this section, "attack plans" and "scenario descriptions" or even "scenario plans" will be considered equivalent terms as they refer to the same thing. "Attack plan" is the term used originally in the tabletop exercise methodology described here while "scenario description" matches the terminology used in this specific course.

Alternatively tabletop exercises may lose their credibility and value if a high level of rigor and honesty is not maintained throughout the entire tabletop process.

Tabletop Exercise Limitations

It is important to not only know what a security effectiveness tool does well, but just as important understand what it does not do. Without an understanding of the associated limitations, it is unlikely that the value of tabletop exercises will ever be understood and/or appreciated. Limitations for tabletop exercises include:

- Tabletop exercises are interactive from a discussion point of view only and do not attempt to be real-time simulations.
- It is typically difficult to obtain a credible and experienced individual to represent the adversary force planner. This limitation can reduce the quality and credibility of attack scenarios, resulting in inaccurate portrayals of system effectiveness.
- The quality of the tabletop depends upon both the professional judgment of those that participate, and upon Subject Matter Experts (SMEs) in a variety of fields.
- Lastly, there is presently no official published protocol document to describe rigor and utilization.

Types of Tabletop Exercises:

Figure 22-1 describes 8 types of tabletop exercises, dependent upon who is conducting the tabletop (whether it is being run by the site management or by an external authority), whether the protection system under evaluation is conceptual or existing, and whether the design basis threat under consideration is the existing official Design Basis Threat (DBT) or some conceptual threat which might be above or below the official DBT. of
Internal tabletops typically need less formal structure than externally directed ones, although both demand the same high standards of rigor.

Four types of tabletops will be mentioned here as a commonly applied subset of the 8 possible tabletops. The first is an internal site tabletop exercise to determine security system effectiveness against an existing protection strategy. The second type of tabletop exercise is also a site review to determine effectiveness and up-grade options when a conceptual security strategy is measured against a postulated threat increase. The third is an external directed tabletop exercise to determine security system effectiveness against a site's existing protection strategy. The fourth type of a tabletop exercise is also an external review to determine effectiveness and up-grade options when a site's conceptual security strategy is measured against a postulated threat increase.

#	Conducting Authority	Protection System	Threat	Primary Purpose
1	External	Existing	Existing	Establishing a baseline, oversight-approved
2	External	Existing	Conceptual	Sensitivity/Degradation, oversight-approved
3	External	Conceptual	Existing	Downgrades and/or new technologies, oversight-approved
4	External	Conceptual	Conceptual	Upgrades and/or new technologies, oversight-approved
5	Internal	Existing	Existing	Establishing a baseline, internal analysis only
6	Internal	Existing	Conceptual	Sensitivity/Degradation, internal analysis only
7	Internal	Conceptual	Existing	Downgrades and/or new technologies, internal analysis only
8	Internal	Conceptual	Conceptual	Upgrades and/or new technologies, internal analysis only

Figure 22-1. Types of Tabletop Exercises That might be Performed

Tabletop Exercise Challenges

Experience has demonstrated, as with other security effectiveness tools, that given the lack of a tabletop exercise culture and/or experience site bias associated with business unit interests quickly creep into the process. Another problem is a misunderstanding concerning resource and time requirements, which is a result of a failure to conduct adequate scoping meetings. Scoping meetings lay the foundation and prevents the tendency not to develop exercise protocol and/or rules of engagement documents, which prevents a natural tendency to game and/or intentionally mislead.

How to Address Tabletop Challenges

As guiding principles Fairness, Tactical and Technical Reality and High Degree of Integrity of the exercise process is considered to be a critical element in gathering usable data and assisting in site security system and protective force improvements. These three essential principle ingredients are rooted in conducting proper scoping meetings.

Phases and steps of a Tabletop Exercise

Tabletop exercises, as described here, consist of three phases, with several steps making up each of these phases:

- Phase I
  - Step 1. Identify and assign team leaders to those teams (adversary team, site protective force team, etc.) applicable for the tabletop.
  - Step 2. Team leaders meet with target facility security management to scope the tabletop and to work out protocols and rules of engagement.
- Phase II
  - Step 3. Adversary team collects information, possibly using an insider, and completes initial mission planning.
- Phase III

Step 4. Team members arrive at facility where the tabletop will be held, the exercise is set up, and any practice/dry runs required are performed
Step 5. Tabletop simulations of each attack scenario are performed.
Step 6. Each security component and critical adversary action is graded for Probabilities of Detection, Assessment, Interruption, and Neutralization after each scenario.
Step 7. Potential changes to the security system, if any, are identified after each scenario is completed.

- Phase IV

Step 8. All teams meet to prioritize upgrades to determine which are most effective.
Step 9. Tabletop team leaders brief site and, depending upon whether the tabletop is internal or externally conducted, national authority management.
Step 10. A final set of tabletop documents are provided to management, along with briefings.

Section 22.3 discusses steps 1 and 2 while 22.4 covers step 3. Section 22.5 covers steps 4 and 5 and steps 6 and 7 are covered in 22.6. Phase IV (steps 8-10) are described in section 22.7. These discussions are not intended to instruct you about each topic or step completely – that would require a detailed manual – but merely to provide a familiarization of what activities are performed.

22.3 Tabletop Exercise Preparation: Scoping Meetings, Exercise Protocols, and Rules of Engagement

Organizational Commitment to the Tabletop

Once a decision to conduct a tabletop exercise has been made, someone has to take the lead in organizing the event. Remember tabletop exercises as described here require detailed planning and preparation to be valuable. Because of the rigor required, without a *management* commitment to an agreed upon process it is unlikely that a site can conduct a worthwhile tabletop exercise.

Scoping Meetings, Exercise Protocols, and Rules of Engagement

One of the first steps in organizing a tabletop exercise is the initial scoping meeting. This means someone has to write the scoping document. All stakeholders and/or their representative should attend the scoping meeting. However, the final agreements should be between two representatives. It is during the scoping meetings that exercise protocols and rules of engagements are agreed upon, schedules are made and resources are dedicated. The author of the scoping meeting document should send advanced copies to participants before meeting. When conducting the scoping meeting, the atmosphere should be serious and take on the appearance of a legal process.

Scoping Meeting Organization

A scoping meeting typically involves the following participants:

- Adversary Team Representative
- Protective Force Representative
- Documentation Team
- Site Vulnerability Analyst Representatives
- Appropriate Site Management and Supervisors
- Safety and Operations Representatives

So as to not contaminate the process all scoping meeting participants are considered "Trusted Agents" who will not release information to their "side" participating in the tabletop.

Topics to Be Addressed in the Scoping Meeting

The scoping meeting should cover a number of topics that need agreement eventually among all participants in the scoping meeting:

- Assumptions about what protection system information is to be provided to the Adversary Team Representative
- How information will be otherwise be collected based on simulated reconnaissance and use of a simulated insider.
- How actual Protective Force (response) positions and status will be recorded as "Snap-shots in time" for use as starting positions in the tabletop.
- Performance assumptions for adversary and defender weaponry as well as detection probabilities and delay times of barriers.

Adversary Data Collection Considerations

When discussing information to be provided to the adversary planner, the tabletop exercise scoping representatives should consider that mirroring reality as much as possible is the most desirable. During information gathering efforts how the adversary will attempt to avoid detection given the sites' on-going counter-intelligence operations and reliance on employee security programs will be a major concern. Attacks, especially armed assaults, do not occur in a vacuum, and they must painstakingly put together the attack one activity at a time.

How the information will be gathered, and subsequently relayed, within the adversary group are very delicate operations and represent real concerns of being detected that are unacceptable at this stage. Remember a major aspect of planning and conduct of the actual attack is ensuring the adversary controls both the point of detection and time of engagement. This is the only way to get inside the site's decision making process. During the attack if not perfectly synchronized and coordinated there will be a high probability of 100% mission failure.

This creates the problem of creating more than a casual cover for action and cover for status. An adversary's success will be contingent on conducting their data collection activities in a low visibility or clandestine manner. This requires that the adversary conduct a detailed review of all critical pre-attack preparation in order to make a judgment as to the probability for detection and probability of attack success in relationship to information gathering.

Information

This critical activity is time consuming and lays the foundation for realistic

Collection and Rules of Engagement

attack scenario development and determines the true value of the exercise process. Protocols and rules of engagement should be determined before the exercise begins, and only after careful negotiation with representative management, adversary, protective forces and exercise oversight personnel.

Protective Force Positions

Critical to conduct of the tabletop exercise is a fair method for determining Protective Force positions to be used at the beginning of the Tabletop. Experience has shown that the fairest way is to saturate the Protective Force with a series of unannounced "Snap Shots in Time" for which folders representing normal workday, night shift, and weekend/holiday protective force security conditions are developed. These records are sampled to determine starting conditions for each exercise.

Information to be collected as Part of "Snapshots in Time"

"Snap Shots in Time" or "Pictures-in-Time" (PITs) shall include the minimum following documentation:

- Date and time snap shot in time was taken
- Crew or "shift" that participated in the snap shot in time (within the Department of Energy there are typically three crews:" "day shift" in the morning to afternoon, "swing shift" in the afternoon to early evening, and "grave yard" shift in the evening and early morning)
- Location of each post and patrol
- Configuration of each individual protective force such as where their weapon, radio, cellular telephone, pager, gas mask, and armored vest were located.
- Whether weapons are locked (such as a locked rack at a post or in a vehicle) or unlocked and the configuration of weapon, i.e. empty, half load or full load configuration.
- Whether protective force personnel were eating at the cafeteria, participating in physical fitness, etc. and where their equipment was located.
- Patrol vehicles windows being up or down, headlights on or off and direction of travel.
- Direction of view for the CCTV monitors that are present within the Central Alarm Station (CAS) at the point the snap shot in time was taken.
- Weather conditions during the snap shot in time, i.e. temperature, wind, precipitation, etc.

All of these factors are recorded because they may influence the progression of the tabletop.

Selection and Utilization of an Insider to Pass Information

Judgments in this section are based upon the premise that an adversary will develop a plan with supporting tasks that has the greatest advantages in eluding law enforcement and intelligence agency efforts. Attack plans will be selected and based on what provides the most technical and tactical advantages over the site's Protective Force and security system to achieve the highest probability of success. Success will depend on identifying and recruiting the right insider to pass information or to actively collude during the attack. A decision will need to be made of whether or not the insider needs to be a technical or tactical. A well pre-prepared adversary would

assume that the operation would be detected at some point—only it should not be allowed to occur during information gathering.

The challenges associated with successfully identifying and subsequently recruiting an appropriate site insider will require perfection of all tasks associated with agent handling, and the difficulties should not be under estimated. Insiders are either coerced or blackmailed, or become an insider for financial or ideological reasons. The insider's reasons can make a difference in the quality of information and willingness to take risk. In addition, the insider's employment position, technical or tactical, will have an impact on obtaining sufficient information to plan an attack. Lastly, the concern and difficulty to the adversary of recruiting an insider is compounded if the insider was to also become violent.

Bottom line, the site is responsible (due diligence) to evaluate all insider threats (passive, active non-violent, active violent) as it relates to colluding with an outsider adversary force regardless of whether or not an adversary force would or would not use a particular category of insider.

Examples of Rules of Engagements

Rule of engagements agreed to in the scoping meeting lay the foundation for the tabletop process. Early in the process it is agreed as to the quantity and quality of information to be provided to the adversary team. This information is key to planning and is referred to as Phase-One. Given the importance of information below are some examples of information ROEs that may be considered.

- Determine who will have access to tabletop exercise data, i.e. all exercise information is the sole property of the site and will not be shared will any outside sources.
- Determine legal bounding of safeguarding tabletop information, i.e. all exercise participants will sign non-disclosure agreements.
- Determine who will gather information, i.e. personnel not from site will be used for Phase-I information gathering.

Note: Information gathers cannot use their issued badge to acquire information.

- Determine period of time represented by the information gathering effort, i.e. information gathering simulates at least two years of post September 11, 2001 preparation and planning.
- Determine level of dedication of adversary attack force, i.e. terrorist group is willing to commit suicide and/or die during the attack.
- Determine collection methods that information can be gathered, i.e. information gathering efforts will utilize concepts and principles associated with clandestine operations and agent handling—avoiding pre-incident detection will be a guiding principle.
- Determine control methods for information collection, i.e. adversary information-gathering will be coordinated with and approved by appropriate officials before conducting the activity(s).
- Determine methods for safeguarding information, i.e. all

information gathered will be handled as classified data, unless it is determined to be sensitive matter.

- Determine methods for reviewing data from insider meetings, i.e. for documentation and attack planning purposes all insider interviews will be taped recorded.
- Determine method for storing insider information, i.e. all information obtained and documented from the insider source will be stored at the site.
- Determine sources of information gathering, i.e. open-source information can be gathered from the Internet, DOE reading rooms, general public, contractors, subcontractors, city, county, state and federal government agencies, site tours, etc.
- Determine external site information gathering methods, i.e. external pre-attack surveillance will be approved and coordinated by site that will provide a digital camera for taking external pictures of the site during both day and nighttime conditions at locations to be negotiated.
- Determine method for identifying external picture taking, i.e. the location of where the pictures are to be taken represents covert surveillance and a low probability of detection, and may be different for day and night.
- Determine how aggressive surveillance/picture taking can be, i.e. external information gathering activities that have a reasonable possibility of being detected or compromised will not be conducted.
- Determine who will accompany information gather conducting surveillance/picture taking, i.e. appropriate site representatives will accompany all information gathering and picture taking efforts that are conducted external of site locations.
- Determine motivation of insider, i.e. insider is providing information for the purpose of financial gain.
- Determine insider's access and knowledge base, i.e. insider will have access, authority and be knowledgeable of Security and Protective Force operations.
- Determine who will be candidates for insider selection, i.e. site will provide a list of five attractive insiders that are proportional to the number of site-specific positions such as SRT Lieutenants, VA Analysts, PF Officer in Tactical Command, etc.
- Determine insider capabilities, i.e. a single "passive" insider, who passes information only, will be selected.
- Determine method for pre-insider information review, i.e. before each insider interview the site management and/or their designated representative will review and approve the questions to be asked.
- Determine method for post insider information review, i.e. after each insider interview, the appropriate management, or their designated representative can debrief the insider for purpose of ensuring the insider is not intentionally being deceptive.
- Determine method for making changes to the process if required, i.e. before initiating modifications to any agreed upon insider activities, the concern will first be highlighted by the person/ representative who desires the change.

- Determine method for decision making, i.e. during the information gathering process no unilateral decisions will be made.
    - If a question arises the Adversary and Protective Force representatives, to include Site representative, will first attempt to resolve the issue.
    - Once concurrence on the issue being highlighted has been reached it becomes the rule of engagement and will be documented.
    - In event above persons cannot come to an agreement than the individual making and/or desiring the change(s) has the responsibility to notify appropriate management.
    - Information gathered that is deemed inappropriate will be removed before being reviewed by the Adversary.
- Determine amount of information insider can provide, i.e. when requested the insider will provide and gather information on all areas they have knowledge, access, or authorities, such as vulnerability assessments, the SSSP, special security studies, threat statements, after action survey reports, pictures, other unwitting individuals, etc.
- Determine degree of insider assistance, i.e. when gathering information the insider can ask one other site source for information if there is a reasonable belief of not being detected and the new source is not asked to be an additional insider

Other Rules of Engagement

Examples of other Rules of Engagement are:

- Insider information assistance will not be requested from an individual who has no access.
- Activities that have a reasonable possibility of being detected or compromised will not be conducted.

Modifications to Information Gathering

Depending upon the purposes and the formality of the tabletop the information gathering assumptions can be modified to be:

- Site provides all available information for adversary attack planning.
- Site allows for unrestricted external and internal surveillance and walk through.

Conclusions About the Scoping Meeting

A major key to successful tabletop exercises is the scoping meeting(s). Using the above information you should be able to frame the issue so the effort contributes to better security system design and subsequent useful effectiveness data.

22.4 Adversary Attack Planning and Its Relationship with Site Data Collection

Planning Scenarios

Several activities are performed by the Adversary team planners to generate

an attack plan:

- Data collection: adversary data collection about the site is simulated, within the limits of the scoping agreement. Such data collection must be performed without detection, possibly with the use of a simulated insider if that has been agreed upon in the scoping agreement.
- Data analysis: the adversary team planners review all available information regarding the Site facilities, geography and climate, Physical Protection System, and Targets.
- Target selection: the planners decide on the most advantageous target in terms of probability of success, using the least resources or the shortest time;
- Select tactical and technical options: tactics will be reviewed to determine what is the most favorable attack approach using the least amount of personnel to accomplish the mission (Possible capabilities and technologies will be evaluated for 1) the ease of equipment/capability acquisition without detection, 2) the complexity of the tactic or technology, and 3) the level of training required to use it);
- Scenario Generation: The Adversary team uses analysis to generate various scenarios within Mission Parameters (defined within Scoping Agreement) and these scenarios are documented in formal, structured attack plans.

Not all of these steps should be attempted during informal tabletop exercises that lack expert planners as site personnel typically do not have the required competence.

Adversary Data Collection Compared

Adversary data collection will typically differ from data collection by the Vulnerability Assessment team as the former do not have access to a full set of site data. Much of the information may be similar but adversaries may lack key pieces of planning information or misinterpret the data they have.

Review of Tactical and Technical Options

An initial adversary planning activity will be to conduct an extensive review of all tactical and technical options available. Within this planning phase, tactics are reviewed to determine what is the most favorable attack approach using the least amount of personnel to accomplish the mission.

Considerations in Selecting Tactical and Technical Options

Capabilities and technologies are evaluated for the ease of acquisition without compromise, and the complexity of the tactic or technology. Extensive technical equipment or weapons drive complex training and requires continuous practice to maintain the level of expertise necessary to be successful in an attack.

In the end, attack plans will be selected and based on what provides the most technical and tactical advantages over the site's Protective Force and security system to achieve the highest probability of success.

Pre-Attack Detection

In formal tabletops, a planner serving to create the adversary attack plan should, where competent, conduct a detailed review of all critical pre-attack preparation and attack activities in order to make a judgment as to the

Considerations

probability for detection in relationship to the attack plan.

These judgments should be evaluated in a Post- September 11 operating environment where suspicious activities are investigated more vigorously than they were previously.

A general guide is each activity will have a probability rating (High-75%-100%, Moderate-50%-74%, or Low-0%-49%) of success.

It should be kept in mind that detection and success ratings for attack activities most likely have not been performance tested, and are taken in a vacuum. Clearly estimates of pre-attack probabilities of detection at best are broad qualitative judgments and should not be attempted without the assistance of national intelligence authorities.

Also, they do not represent the difficulties of having to complete all of the tasks in the plan collectively where suspicion and probability of adversary detection would be increased.

Such estimates are not used directly in determining system effectiveness (as the tabletop and further simulations serve this purpose) but help to capture the planner's perspective on the plan.

Identification of Security System Limitations

Adversary team planners also identify the site and security system limitations which are security system characteristics that reduce adversary probability of success. Each limiting characteristic will be assigned a value based upon the impact to the adversary and the amount of effort needed to overcome the limitation based on the number of "work arounds" or countermeasures required

.

Criteria ratings are based on the sequence of activities making up the adversary attack plan. This attack sequence starts at the last offsite staging area, where the adversaries would start their assault, and would end either at the completion of a sabotage task (for sabotage attacks) or at the adversary leaving the site (for theft attacks).

Limitation Rating Criteria Explanation

Limitation ratings are assigned based on information about the site as well as information about the adversary outlined in the Threat Statement.

Ratings are as follows:

- High (H) – This category represents the most significant impediments to adversary action.
- Moderate (M) – This category represents impediments that could have an impact on adversary operations.
- Low (L)– This category represents minor impediments that may have a minor degree of impact on mission success; however, several easily implemented mitigation measures are usually available.

Definition of Attack Plan Credibility

In all cases the goal is to present information and/or to develop an attack plan that is considered credible by all participants and stakeholders. Absent this the security system will most likely never achieve the objective of balance and cost-effectiveness

To get insight into what it means for an attack plan to be credible, we describe some of the attributes of what makes an attack plan credible versus fictitious:

- Credible: Information and/or the plan presented:
  - Have sufficient detail, and
  - Are consistent with technical and tactical capabilities, and
  - Provide a distinct tactical advantage with a "Reasonable Likelihood of Success"

- Fictitious: Information and/or the plan presented:
  - Is fake, phony, represents gaming, or an attempt to mislead, or
  - Requires suspension of reality to be achievable.

In our experience, very few set out to create a fictitious attack plan but this can happen with the best of intentions by using inexperienced "experts," leaving detail out of attack plans, and not checking for consistency between the steps in the attack plan versus reality.

Attack Plan Content

The scenario or attack plan is formatted to the outline shown in Figure 22-2.

Scenario documentation should also mention which factors were used for selecting a target to be attacked, for example, the asset/target:

1) Provided the highest probability of success;
2) Allowed using the least resources; and/or
3) Took the least amount of time to complete.

Besides the details of the attack itself, the attack plan contains adversary planning assumptions about the site and national capabilities, procedures, and policies.

Format for Sections in Attack Plan

1) SITUATION:
   A. Target Information:
      - Geographical Setting:
      - Weather and Light Data:
      - Target:
      - Target Location:
      - Target Description:
   B. Site Protection Information:
      - Protection Goal:
      - Protection Objectives:
      - Protective Force Locations:
      - Supplemental Positions:
      - Barriers and Delays:
      - Protective Force Weapons and Ammunitions:
      - Other Site Security Equipment:
      - Other Protective and/or Security Directives

2) MISSION: (Who, What, When and Where)

3) EXECUTION:

4) Concept of Operation:
   A. Pre-Attack Activities:
   B. Attack Activities:

5) IV. COMMAND and CONTROL
   A. Command:
   B. Communications:
      - Adversary's Communication Frequencies
      - Site Security Communication Frequencies

Figure 22-2 Format for Sections in Attack Plan

22.5 Performing Formal and Informal Tabletop Exercises

Performing Tabletop Exercises

The following areas should be considered when planning and conducting a tabletop exercises:

- How the tabletop exercise itself is organized
- The schedule for the tabletop
- Tabletop protocols and procedures

Organization of the tabletop exercise

Depending upon whether the conducting authority is external or internal and upon the desired formality and desired rigor of the tabletop exercise the tabletop may be organized differently. For this discussion, the adversary

team is referred to as the Red Team, the team representing the site is the Blue Team, and the vulnerability analyst and data recording team is the Green Team. These titles are used even if the team consists of one person as in smaller informal tabletops.

Room Layout

At the high end of formality, an externally-conducted tabletop may involve dozens of people (see Figure 22-3). In this case, not only are there specialized Red, Blue, and Green teams, there are teams of Blue Team response force members and Red Team adversary planners that are sequestered in isolation rooms. These isolated members are used to answer specific questions during the tabletop and are not used again to represent other protective force members because their previous knowledge would taint their later answers.

Figure 22-4 depicts a much more informal tabletop, probably conducted internally. This group still has an exercise director (although the responsibility of the director is much more demanding), red, blue, and green team. If necessary the tabletop could be made simpler than this.

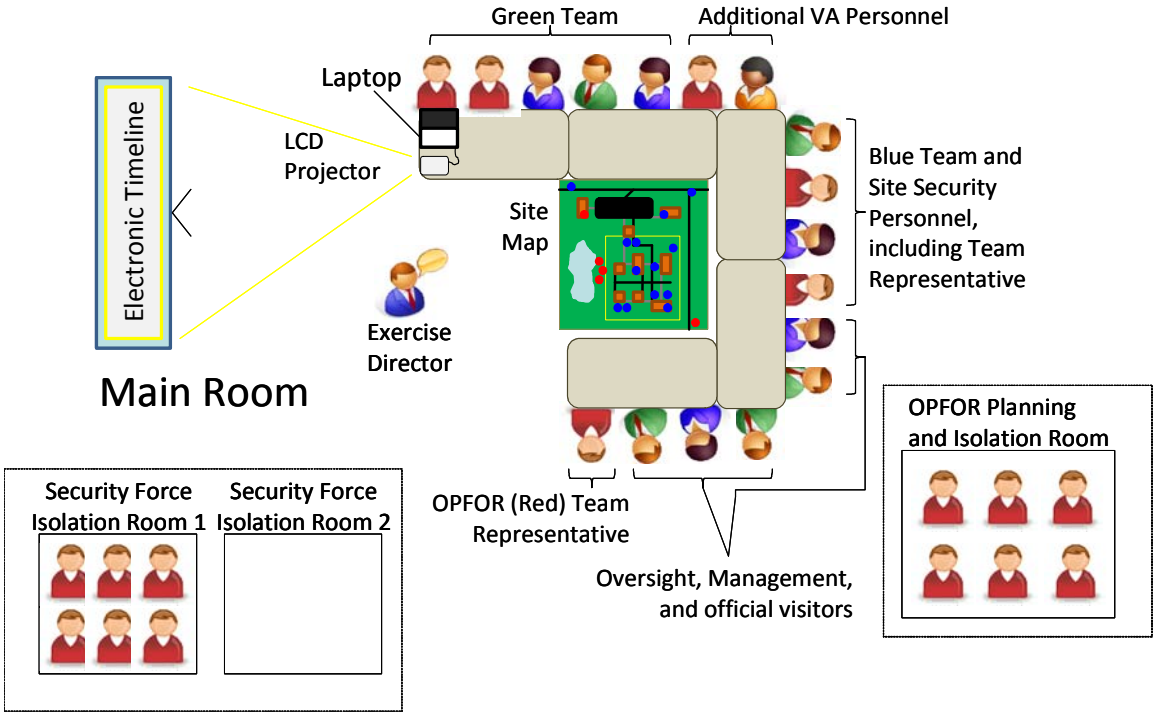


Figure 22-3: Highly Formal Tabletop Exercise

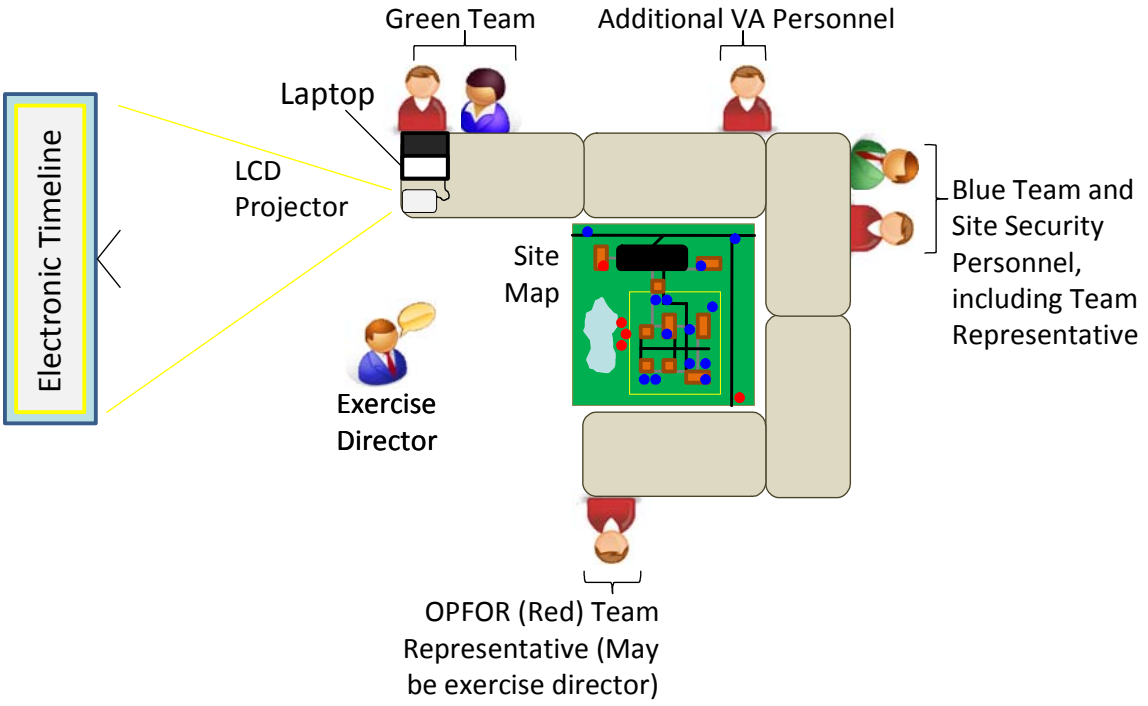


Figure 22-4: Highly Formal Tabletop Exercise

The Tabletop Schedule for Each Day

The length of the tabletop exercise depends upon the complexity of the scenario and the tabletop organization. Historically, exercises have required one day of tabletop exercise per scenario. The schedule for a day typically looks like the following:

- Preliminary Presentations
  - Adversary Scenario Presentation
  - Review of the Scenario Plan and Timeline
  - Discussion of Security Force Posture, Including Snapshot in Time
- Tabletop Simulation
- Data Collection and Scoring Based on the Scenario Outcome

Simulation Protocols and Details

- Decisional Outcomes
- Outcome Weighting
- Arbitration and Judgment
- Additional Data Collection
- Decision Recording
- Timeline Recording

Attack Resolution

Adversary Scenario Review and Presentation

In a formal tabletop as described in Figure 22-3, the day begins with the Red Team submitting the attack plan and its timeline to representatives of the other teams for review. Once the timeline has been reviewed for accuracy of timing as well as process, the Red Team will be presented with questions from these teams if they have identified conflicts and/or process

that may not be accurate. All questions and conflicts will be resolved prior to the Red Team timeline briefing. The attack plan is formatted and presented by the Red Team in a military "five-paragraph operation order" manner (see Figure 22-2 above) and includes timelines for each planned task. Questions from the representatives from the other teams are held until after the Red Team completes its briefing. Once questions are answered adequately, the Red team planner that sits in the isolation room departs the table-top briefing area, returning to their designated planning area to begin preparation of the attack plan for the next scenario.

Development of the Red Timeline Based on the Attack Plan

The Green Team, using the Red Team attack plan, develops the Red Timeline with all critical elements identified by the Red Team noted on the timeline. The scenario is typically subdivided into 5-second slices-in-time and plots all identified adversary tasks for each adversary along a time axis horizontally (see Figure 22-5).

The Green Team will also document the expected Blue Team reactions to these Red Team tasks on the lower part of the Timeline. The Blue Team reaction tasks will be supported by valid VA documentation.

The reason for the sequential approach is to avoid the potential for unintentional distortion of how the existing security forces/system would respond to the attack scenario. The slices-in-time presentation will provide information about how effective the system is at various points along the attack scenario and more accurately reflects how the site would experience an attack. Also, this process may provide insight into measures that could be added along the timeline path to foil the adversary, had they been in place during the event.

When the Timeline is complete, the Green Team Leader briefs the Red Timeline to all present in the exercise room.

The Red Team Leader will ensure that all attack scenarios are completely documented and that no salient or critical attack elements are omitted. This documentation will be combined with documentation provided by the Green Team Leader that describes in detail the results of each attack, rationale for decisions made, and/or any technical disagreements between Red/Blue teams and the results of those disagreements rendered by the Green Team.

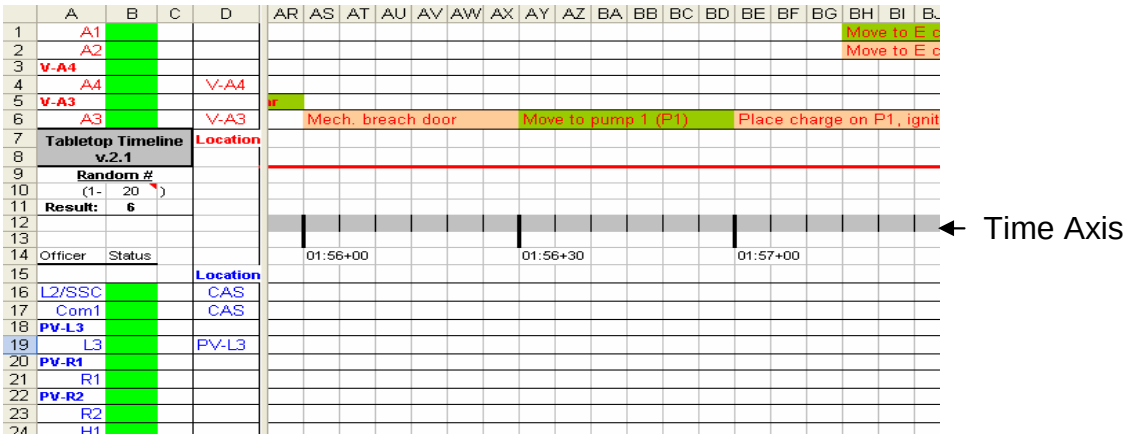


Figure 22-5: Timeline Depiction

Setting Up Initial Response Units Based on the Snapshot in Time

The Blue Team will, while the Green Team is formulating the Red Timeline, determine the location of Blue Team responders and response weapons deployed, special vehicles, etc., during the snapshot-in-time consistent with the timing of the Red attack plan. This information is normally captured during performance tests. The presentation of the scenario plan as well as the tabletop itself will require the best available site maps, aerial photographs, building drawings, and information regarding detection, assessment, delay, and response contained in vulnerability assessment documentation.

The Response Strategy Briefing

After the Red timeline is briefed, the Blue Team presents a response strategy briefing that covers, but is not limited to: Command, control, and communications operations, where responders are located during the "snapshot-in-time," response weapons deployed, special vehicles, etc. As each element is presented, the appropriate Protective Force (PF) tactical leader is asked how his/her response element would respond, or in the case of the Central Alarm Station (CAS) leader, how the security system would respond and response force timelines are plotted accordingly. The Blue Team Leader must be thoroughly impartial in providing the Protective Force picture, as well as knowledgeable of all security system elements, response force plans and tactics, response force times, and PF communication procedures.

Detailed Tabletop Simulation Protocols

Simulation protocols should be documented and followed concerning:

- Behavior-based decisional outcomes: Where a human being simulated has a choice (e.g., who to shoot at or where to go), how that choice is made consistent with site plans and procedures?
- Chance-based decisional outcomes: If an event during the simulation is based on a random outcome (e.g., does the sensor alarm or does the shot hit its target), how is the outcome determined (dice, random numbers, etc.)?
- Outcome Weighting: What factors will be included in determining

what events occur and how the effects of those events will be affected? (As an example, fog coming in can be a weather related events that subsequently is a factor affecting who can see whom.)

- Decision and Timeline Recording: The initial Timeline depicted in Figure 22-5 is subsequently modified to reflect behavior-based and chance-based decisional outcomes and the resulting events during the scenario. The timeline should store events about adversary activities, response force activities, and alarm communications and display system activities.
- Attack Resolution: The timeline can also be used to record the outcomes of battles between security and adversary entities.

At the end of the scenario, the Timeline should show the list of all events and their outcomes for all adversaries, defenders, and for relevant security subsystems.

Tabletop Simulation

Each scenario is played out, starting at time zero and at each time, processing all events whether they involve movement, shooting, or decision making) that occur at that time. Once all activities are completed at a certain time, the clock is advanced by 5 seconds (or until the next event).

The Green Team validates, as necessary, Blue Team response force times and detection parameters using retrievable PF performance testing data. Timelines from the adversary attack plan are compared to response force timelines. Green Team validates player locations based on slices-in-time data.

Should unresolved technical or security-related issues arise between Red and Blue Team Leaders, the Green Team will provide subject matter expertise in order to resolve them and will be the final authority for technical or security-related issues. The tabletop process encourages these issues to be resolved at the lowest level possible, which is between the Red and Blue Team Leaders.

The scenarios are "played through" until there is a consensus between the Red, Blue, and Green Team Leaders that either the Red adversary actions have been effectively neutralized or the Blue security system has failed.

22.6 Collecting and Documenting Scenario Results

Documentation Activities After Each Scenario

After each scenario is completed, the security system components and critical adversary actions are graded for effectiveness and potential upgrades are identified against that scenario.

Scenario Ratings for Components

For each task identified on the scenario timeline that correlates with a security system component or series of components (e.g., random patrol, PIDAS, combination of target delays), a rating will be documented for the performance of the component(s) against the following criteria:
P_D – the security element detects a potential malevolent act: the sensor

activated, employee reports unspecified activity with no specific threat

P_A – command and control elements assess the detection as having hostile intent

P_I – adversary engaged by protective force in manner to delay progress

P_N – adversary mission failure/neutralization: adversary attrition to insufficient numbers to achieve mission success or adversary capabilities deteriorated to point of failure (e.g., needed equipment destroyed, unanticipated barriers encountered, equipment failure)

Also included in P_N determination is the judgment of how many SPOs and what kinds of weapons are engaged against how many adversaries at this security element, and the number surviving the engagement.

At each of these points, the evaluation should also consider the status of the mission - Is the adversary still able to continue with the mission or have they failed at this element?

Other relevant documentation and comments should be captured while the simulation is fresh in everyone's mind.

The decisions and scores will either be based upon the values established in already existing vulnerability assessment data or from the consensus of expert opinion from the Green Team Leader. The experts' names, the decision scale, and their decisions will be documented so as to be a part of the overall documentation of the tabletop exercise.

Potential Upgrade Identification

A list of potential upgrades should be identified after each scenario for that scenario alone. The next, final phase of the tabletop will sort out the upgrade options.

22.7 Post-Tabletop Upgrades, Briefings, and Documentation

Collecting and Documenting Exercise Results

After all scenarios have been simulated as part of the tabletop exercise, the results need to be collected, suggested upgrade packages defined, and briefings and reports completed.

Collaborative Upgrades Analysis

A set of prioritized overall system upgrades for the facility will be developed based upon results of the tabletop scenarios. This step of the process is finalized only after all the scenarios have been completed, graded, and documented. All tabletop exercise teams, along with the facility management involved in the tabletop, participate in this collaborative "upgrades analysis" meeting wherein the combined upgrades list (derived from each scenario "run") is prioritized to determine which would be most effective in deterring an attack.

This collaborative "upgrades analysis" is a critical step of the tabletop exercise. The set of upgrades is prioritized in a manner that identifies which

upgrades would most likely negate the adversary's chance of mission success. In an externally-conducted tabletop exercise this is the first time that Red and Blue "Outside" Team members isolated in their respective rooms interact directly.

After-Action Review Briefing for Management

Briefings may be necessary for management who were not involved in the tabletop exercise. For such audiences an After Action Review briefing may be held. The outline for such a briefing are shown below:

I. Title

II. Review of Exercise Objectives

III. Targets Tested and Lessons Learned

A. Target 1
- Summary of actions
- Lessons learned

B. Targets 2 – n, etc.

IV. Upgrades Analysis Results

V. Other Recommendations

Documentation

The final set of documents developed by the analysts involved in the tabletop are:

- General Discussion/Issues/Decisions Rendered;
- Overall Upgrade Analysis Matrix; and
- For each scenario: the Timelines, an Upgrades list, and effectiveness scores for site detection, assessment, interruption, and neutralization.

Such documentation should be provided to the facility management for review and future use.

Effectiveness Criteria

The intent is to translate a probability number from PANL data to a qualitative score on a rating scale from Very Low to Very High. The Effectiveness Criteria Definitions (discussed in the subgroup exercise) are intended to be used as conversion criteria to provide consistency when PANL data is used to establish rating criteria.

The Effectiveness Criteria Definitions are intended for use during the tabletop exercises, to serve a general guide to focus the Green Team in grading security-system elements during scenario interactions between Blue and Red Teams.. It must be emphasized that all ratings are scenario, protective force, and adversary interdependent. Additionally, the vulnerability analysts setting the ratings must use their best professional judgment and must have analysis experience with solid security backgrounds, preferably in multiple security disciplines.

22.7 Summary

Use of Tabletop Exercises

Tabletop exercises are used to perform scenario analysis where security system effectiveness is evaluated against a scenario-based adversary attack consistent with the Design Basis Threat. While this approach does not produce a quantitative Probability of System Effectiveness, P_E, it still produces a very good qualitative understanding of how the system will perform against adversary scenarios. Where quantitative values are required by the regulatory authority, these same tabletops can be used to plan better combat simulations, such as computer simulations or Force-on-Force exercises, so that the simulations are more realistic and more data can be collected from the process.

Discussed in This Section

This section has described a three-phase approach for performing tabletop exercises of varying complexity that have been able to achieve a high degree of rigor if performed honestly, without bias for protective forces or adversaries.

An approach for creating and documenting adversary attack plans was described, that can use varying degrees of insider information about the site. Technical details about how to perform the tabletop exercise itself and how to document results were also discussed.

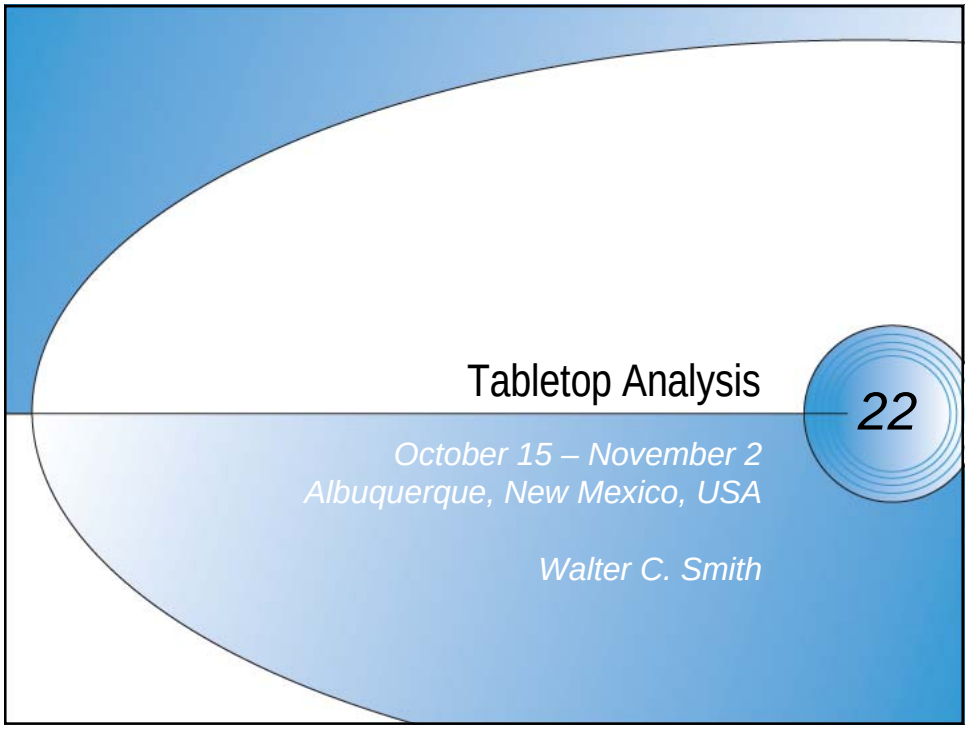
Limitations and Potential of Tabletop Exercises

Tabletop exercises have several limitations. Tabletop exercises produce qualitative system effectiveness results. They are interactive from a discussion point of view only and do not attempt to be real-time simulations.

The quality of the tabletop depends upon both the professional judgment of those that participate, and upon Subject Matter Experts (SMEs) in a variety of fields. Further, it is typically difficult to obtain a credible and experienced individual to represent the adversary force planner. This limitation can reduce the quality and credibility of attack scenarios, resulting in inaccurate portrayals of system effectiveness.

Lastly, it is difficult to control the quality of the tabletop. Part of this is that there is presently no official published protocol document to describe how to perform tabletops uniformly and consistently. As a result, it can be difficult to replicate results.

On the other hand, tabletop exercises have several potential strengths. They can be performed for real and conceptual sites without requiring Force-on-Force simulations to be performed that are complex logistical activities. Tabletops, compared to Force-on-Force and computer combat simulations, arguably give the most balanced, complete view of scenario events and behavioral decisions. And finally, they can be used to identify issues to be controlled and analyzed quantitatively during computer combat simulations.



Learning Objectives

At the end of this session, participants should be able to:

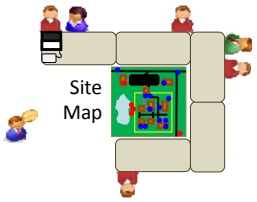
- Describe a tabletop exercise
- Discuss the role of tabletop exercises in helping to determine security system effectiveness
- Describe the tabletop exercise planning and execution process
- Describe the use and integration of tabletop exercise results with other system analysis tools
- State the general benefits, capabilities, limitations and tabletop exercise obstacles

Tabletop Analysis 2

Description

- **A Tabletop exercise is a method of simulating a Physical Protection System under attack by an adversary force**

- **Tabletop Properties**
  - Maps, photographs, or "sand tables" are used to display the site, attackers, and defenders
  - Moderated forum
  - Collaborative input, with assigned roles
  - Simulation functions are performed by people
  - Chance-based outcomes are decided openly, in view of all
  - Yields QUALITATIVE data that can stand alone or be used in other simulations



Tabletop Analysis 3

Description

Additional Attributes

- **Designed to be conducted with**
  - extensive collaborative input
  - a very high degree of rigor, planning, and detail

- **Subject-Matter Experts (SME) are utilized extensively**
  - fosters technical and tactical accuracy

- **Useful in a wide range of situations**
  - current and proposed protection systems
  - current and increased (postulated) threats

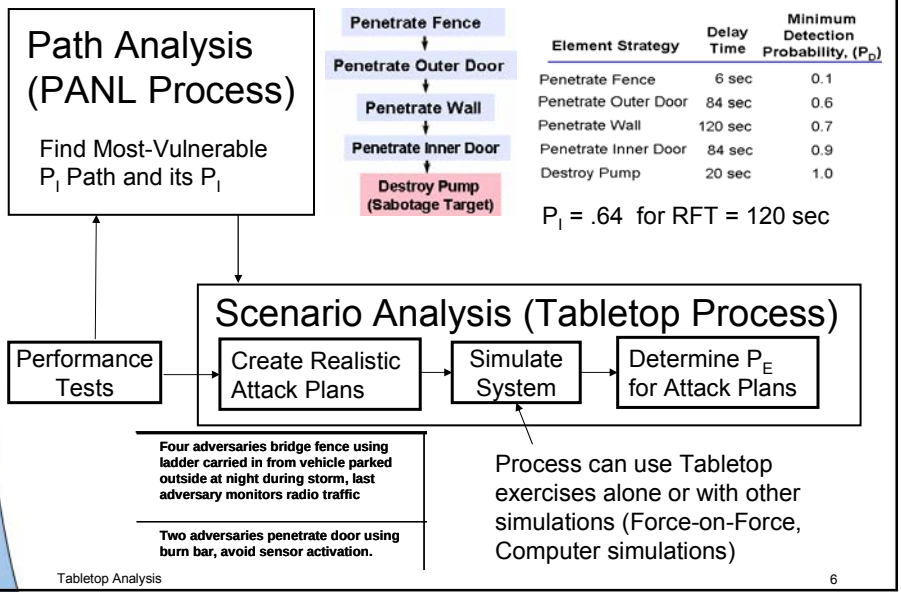
Tabletop Analysis 4

Purposes

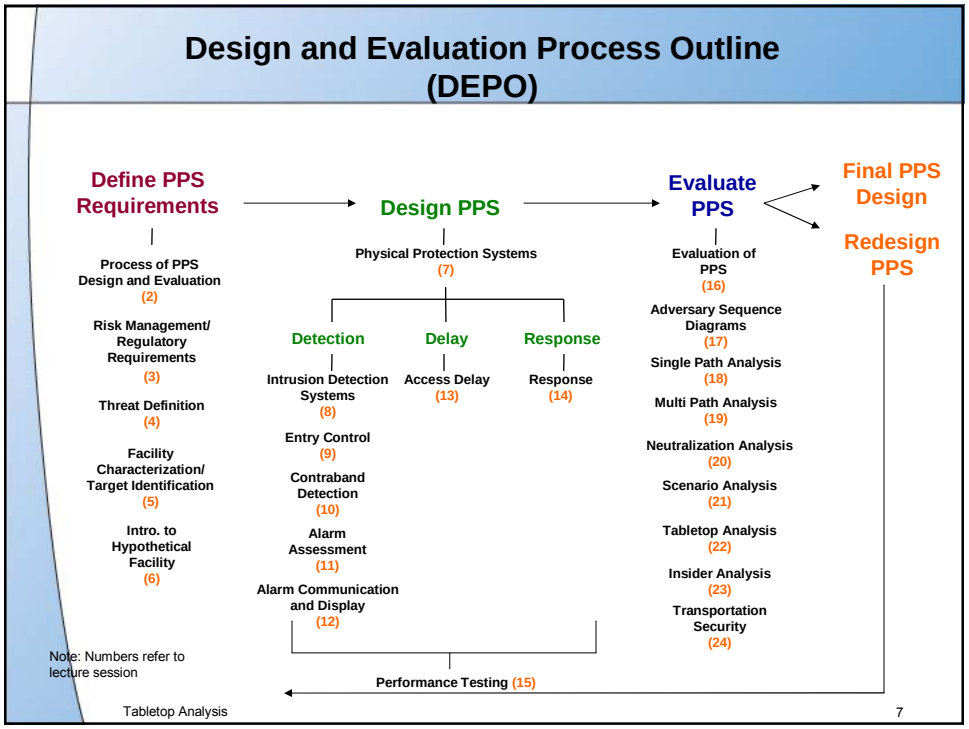
- **Overall**
  - Helps Management improve security system effectiveness
  - Establishes rationale for risk-acceptance
- **Specific**
  - Establishing a protection system "baseline"
  - Sensitivity analyses
    - Gradual degradation instead of rapid
  - Upgrades/downgrades analysis
  - Threat change analysis
  - Validating results from other tools
  - Incorporating attack or protection elements that are difficult to accurately model/simulate using other tools

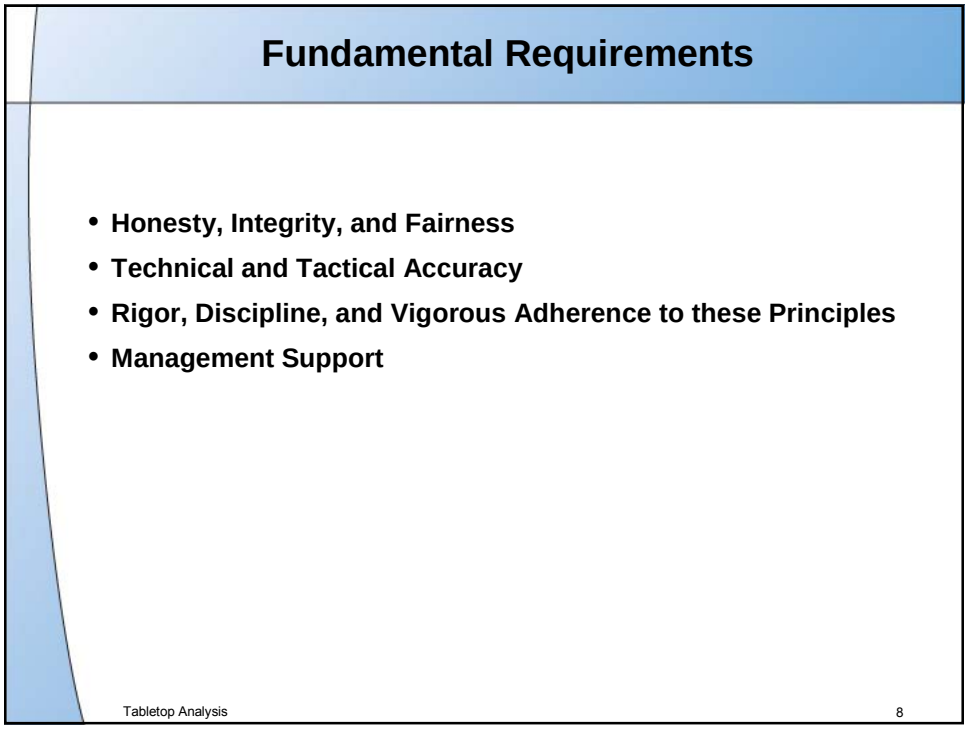
Tabletop Analysis 5

Sequence For Performing Path and Scenario Analysis



Tabletop Analysis 6


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/ Target Identification (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)
Evaluate PPS
Evaluation of PPS (16)
Adversary Sequence Diagrams (17)
Single Path Analysis (18)
Multi Path Analysis (19)
Neutralization Analysis (20)
Scenario Analysis (21)
Tabletop Analysis (22)
Insider Analysis (23)
Transportation Security (24)
Final PPS Design
Redesign PPS
Performance Testing (15)
Note: Numbers refer to lecture session
Tabletop Analysis
7


Fundamental Requirements
• Honesty, Integrity, and Fairness
• Technical and Tactical Accuracy
• Rigor, Discipline, and Vigorous Adherence to these Principles
• Management Support
Tabletop Analysis
8

4 Phases of Tabletop Exercise Process

1. **Planning**
   - Background
   - Scoping and Assumptions
   - Participant Selection and Vetting
2. **Adversary Data Collection, Analysis, and Attack Planning**
   - Data Collection
   - Data Analysis
   - Attack Planning Considerations and Process
   - Attack Plan Credibility
3. **Execution**
   - Typical Room Layout
   - Attack Plan Presentation and Timeline Review
   - Simulation Protocols and Details
4. **Results**
   - Collective meeting
   - Documentation and Integration

Tabletop Analysis 9

Planning Background

- **Scenario analysis historically has been hampered by**
  - Unchecked or undocumented assumptions
  - Failure to check feasibility of scenario requirements
  - Incomplete descriptions of adversary tasks
  - Optimistic expectations about team coordination
  - Unwarranted assumptions about adversary knowledge
  - Lack of scenario credibility with respect to element strategies
  - Systematic conservatism in favor of the adversary
- **Most of the time, the net effect of these limitations is to make the facility look less protected than it actually is**

Tabletop Analysis 10

Scoping and Assumptions

- Schedules for Adversary Force arrival and phases
- Resources including personnel, rooms, and funding
- Threat Statement upper limits and use of jamming
- Information collection (Rules of Engagement)
- Site target facilities and materials
- Assumptions: weapons effects/task times
- Exercise
  - **Types and number**
  - **Protocols**
  - **Information**
- Security Force details
  - Numbers
  - Locations
  - Equipment/Armament/ Ammunition
  - Response Plans
  - Hit Probability in all-weather conditions
  - Pictures-in-Time
  - Training
  - Rules-of-Engagement
  - Communications

Tabletop Analysis 11

Participant Selection and Vetting

- **Quality of tabletop results is dependent upon quality of experts**
- **While you may not be in a position to decide who is selected as an expert, you should ask about their qualifications**
- **Weight their answers by your view of their credibility as an expert**

Tabletop Analysis 12

4 Phases of Tabletop Exercise Process

1. **Planning**
   - Background
   - Scoping and Assumptions
   - Participant Selection and Vetting
2. **Adversary Data Collection, Analysis, and Attack Planning**
   - Data Collection
   - Data Analysis
   - Attack Planning Considerations and Process
   - Attack Plan Credibility
3. **Execution**
   - Typical Room Layout
   - Attack Plan Presentation and Timeline Review
   - Simulation Protocols and Details
4. **Results**
   - Collective meeting
   - Documentation and Integration

Tabletop Analysis 13

Adversary Team Data Collection

Armed attacks require rigorous efforts in:

- Target Selection
- Surveillance
- Team selection and weapons configuration
- Procurement and transport logistics
- Maintaining operations security (OPSEC) during all pre-attack activities (including rehearsal)

- **For Tabletop exercises, this is performed as accurately as possible (within Scoping Agreement limitations)**
- **Larger forces, more complex tasks and attacks, and multiple objectives all greatly increase OPSEC risks, complexity, costs, and overall signature**

Tabletop Analysis 14

Adversary Data Analysis

- **Adversary Team Personnel review all available information regarding the Site facilities, geography and climate, Physical Protection System, and Targets**
- **Primary Target Selection Factors are:**
  - Highest probability of success
  - Utilizing the least resources for mission success
  - Taking the least amount of time for mission success
- **During initial planning, the Adversary Team reviews tactical and technical options available**
  - Determine what is the most favorable attack approach using the least amount of personnel to accomplish the mission
  - Evaluate capabilities and technologies for ease of acquisition and complexity

Tabletop Analysis 15

Attack Planning Considerations

- **Attack plans should stress the site's physical protection system instead of focusing on wins/losses.**
- **Unrealistic advantages/disadvantages are not allowed**
- **Adversary Team uses analysis to generate various scenarios within Mission Parameters (defined within Scoping Agreement)**

Tabletop Analysis 16

Attack Planning Process

- **Team focuses on most favorable scenarios and develops them to a draft state**
  - Attack Plan Considerations
    - Logic and Layout
    - Creation of timelines
    - Relationship of final plan to list of Critical Activities
- **Adversary Team Representative reviews the scenario drafts for credibility and mandates adjustments accordingly**
- **Team produces final versions of credible attack plans, checks them for errors, and submits them for final review**
- **Adversary Team Representative performs final review and correction on the scenarios**
- **Adversary Team Representative notifies Exercise Director that Adversary Team is ready**
- **Exercise Director reviews plan as a validation step**

Tabletop Analysis 17

Attack Plan Credibility

- **In all cases the goal is to present information and/or to develop an attack plan that is considered credible by all participants and stakeholders**
- **Absent this the security system will most likely never achieve the objective of balance and cost-effectiveness**
- **Planning definitions compared:**
  - **Credible:**
    - Information and/or the plan presented
      - have sufficient detail
      - are consistent with technical and tactical capabilities
      - provide a distinct tactical advantage with a "Reasonable Likelihood of Success"
  - **Fictitious:**
    - Information and/or the plan presented
      - is fake, phony, represents gaming, or an attempt to mislead
      - requires suspension of reality

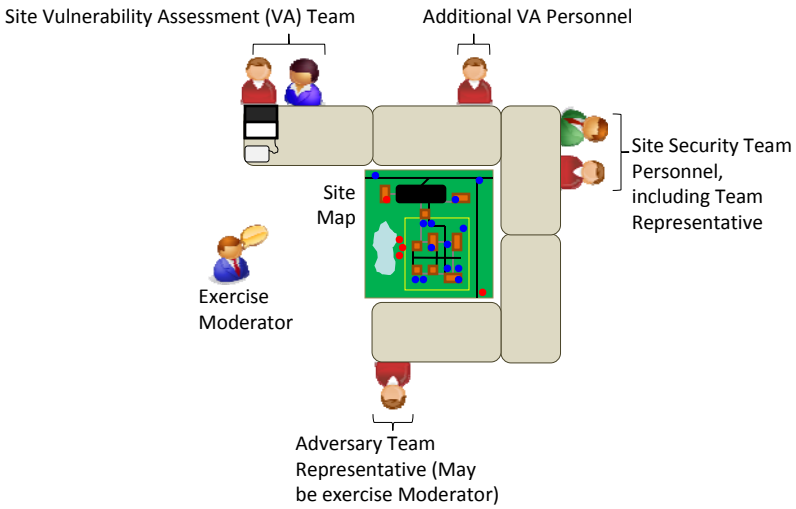
Tabletop Analysis 18

4 Phases of Tabletop Exercise Process

1. **Planning**
   - Background
   - Scoping and Assumptions
   - Participant Selection and Vetting
2. **Adversary Data Collection, Analysis, and Attack Planning**
   - Data Collection
   - Data Analysis
   - Attack Planning Considerations and Process
   - Attack Plan Credibility
3. **Execution**
   - Typical Room Layout
   - Attack Plan Presentation and Timeline Review
   - Simulation Protocols and Details
4. **Results**
   - Collective meeting
   - Documentation and Integration

Tabletop Analysis 19

Typical Room Layout



Tabletop Analysis 20

Attack Plan Presentation and Timeline Review

- **Adversary team briefs attack plan to collected participants**
- **A review is conducted to check the accuracy of assumptions, timing, process and timeline/plan consistency**

Tabletop Analysis 21

Simulation Protocols and Details –Topics

- **Security Force Picture-in-Time (PIT)**
- **Simulation Progression**
- **Decisional Outcomes**
- **Outcome Weighting**
- **Arbitration and Judgment**
- **Additional Data Collection**
- **Timeline and Decisional Recording**
- **Attack Resolution**

Tabletop Analysis 22

Security Force Picture-in-Time (PIT)

- **The Site Security Force Representative:**
  - receives instruction from the Vulnerability Assessment team Representative regarding which PIT to use for the attack
  - Sets up markers, figures, etc. on the playing surface to represent his Force in the specified PIT
  - Briefs the collective participants regarding
    - Force mission
    - Post and Patrol
      - Call signs
      - Locations
      - Routine Patrol Responsibilities
      - Equipment
      - Emergency Response Responsibilities
  - At the conclusion of this presentation, participants can ask questions about the Site Security Team (PIT, Response, etc.)
  - After questions, the Exercise Moderator begins the simulation

Tabletop Analysis 23

Simulation Progression

- **The Exercise Moderator begins at the start of the timeline, before the initial point of detection or engagement**
- **The timeline is stepped through until the first point that detection, contact, or engagement may occur**
  - The Adversary timeline and Security Force PIT are overlaid and any potential detection, contact, or engagement are played through
- **Upon recognition of a situation with a decisional outcome, the factors contributing to the outcome event are considered.**
- **The event (and effect) are assessed and recorded.**
- **The timeline and participant status is adjusted and the Exercise Moderator moves forward to the next step in time.**
- **Simulation continues to the next point of decisional outcome…**

Tabletop Analysis 24

Decisional Outcomes

- **If a person has reasonable behavior options, ask whomever is playing the individual**
- **To decide chance-based outcomes (with random number generator, dice, pull numbers out of a hat, etc.):**
  - Determine different event possibilities and odds
    - (example: 25% hit, 75% miss)
  - Determine event outcome (hit or miss)
- **If event outcome results in an effect:**
  - Determine different effect possibilities and odds
    - (example: 33% death, 33% combat-ineffective, 33% suppressed for 10s)
  - Determine effect outcome (death, combat-ineffective, suppressed)

Tabletop Analysis 25

Decisional Weighting

- **Weighting is a change from baseline probability**
- **With increased rigor comes increased decisional weighting**
- **Low rigor example**
- **Higher rigor example**

Tabletop Analysis 26

Arbitration and Judgment

- Heated disputes WILL arise
- Exercise Moderator must remain emotionally detached and neutral
- If the participants believe the Exercise Moderator is biased or emotionally-invested in a certain outcome, the exercise will be worthless
- Often, the Vulnerability Assessment Team Representative must collect additional information before a decision can be made

Tabletop Analysis 27

Additional Performance Testing Data Collection

- The Vulnerability Assessment Team Representative delegates additional collection tasks
- The Team Representatives and Exercise Moderator may need to participate in or witness critical data collection
- Exercise timelines can be significantly affected by additional data collection

Tabletop Analysis 28

Timeline and Decisional Recording

- **Common recording methods:**
  - Electronic Visual Timeline
  - Written Narrative (Notes)
  - Flip-chart or Manual Whiteboard Visual Timeline
- **For narrative logging, capture details not easily written into the timeline**
- **Simulate small time steps of an engagement**
  - Seconds (usually 5 seconds…too small for "Project" software)
  - Balance small time intervals with technology and simulation limitations
  - "Empty" space can be skipped, advancing to next decision-point

Tabletop Analysis 29

Timeline and Decisional Recording

- **Determine if there are any comments or disagreements about the results**
  - Record and adjust results, where necessary
- **Record who was suppressed, injured, or killed and when**
- **Try to capture anything that could be of use later**
- **Recursively adjust events that are affected by the outcome**
  - Go back in time
- **Be aware that all notes, documents, tapes will likely become controlled/classified.**
  - Collection, control, daily re-distribution issues must be addressed

Tabletop Analysis 30

4 Phases of Tabletop Exercise Process

1. **Planning**
   - Background
   - Scoping and Assumptions
   - Participant Selection and Vetting
2. **Adversary Data Collection, Analysis, and Attack Planning**
   - Data Collection
   - Data Analysis
   - Attack Planning Considerations and Process
   - Attack Plan Credibility
3. **Execution**
   - Typical Room Layout
   - Attack Plan Presentation and Timeline Review
   - Simulation Protocols and Details
4. **Results**
   - Collective meeting
   - Documentation and Integration

Tabletop Analysis 31

Collective Meeting

- **After execution phase, a collective, round-table meeting is held between all active participants**
- **Adversary Team discusses key attack points, other scenarios considered but not used, etc**
- **Adversary Team and Exercise Moderator suggest system changes that would have affected the attack scenarios**
- **Group discusses and propose upgrades, acceptance, and downgrades options**
- **Scribe (or two) captures as much detail as possible, including video or audio recording for accurate transcription**

Tabletop Analysis 32

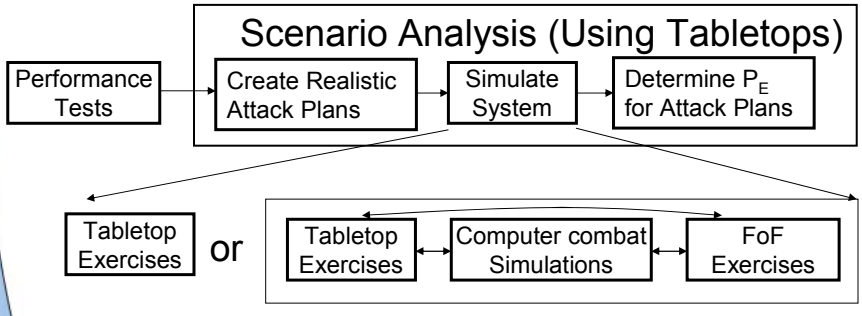
Documentation and Integration

- **Exercise Moderator and Adversary Team Representative remain onsite after execution phase**
- **Vulnerability Assessment (VA) and Site Security Team Representatives meet with and assist Exercise Moderator and Adversary Team Representative.**
  - Review and discuss notes, timelines, narratives, and system-change options
- **System-change recommendations compiled and prioritized**
- **Documents compiled, written, and turned over to VA Team Representative**

Tabletop Analysis 33

Documentation and Integration

- **Scenarios and recommendations incorporated into other tools:**
  - When conducted with the same rigor and discipline other tools validate tabletop exercise results
  - If used up front, tabletop exercises can serve as a baseline for determining security system effectiveness
  - Assist in identifying cost effective upgrades



Tabletop Analysis 34

Additional Considerations About Tabletop Process as a Tool

- **Benefits**
- **Limitations**
- **Obstacles to Common Use**

Tabletop Analysis 35

Benefits

- **Particularly useful at sites that do not have large technology, financial, or labor resources**
- **Participants learn things that are not revealed by most simulation tools**
- **When properly performed, the greatest effort is spent on scenarios that are most attractive to adversaries.**
  - Incredible, relatively risky, and unproductive adversary strategies are weeded out by experienced Adversary Team and Exercise Moderator
- **Produces results that stand-alone or can be used with other tools**
- **Readily handles difficult-to-simulate technologies and tactics**
- **Small system changes can be analyzed more effectively**
  - No time spent rebuilding computer models or resetting people
  - No Protective Force or Adversary "learning" or "leaning forward"

Tabletop Analysis 36

Limitations

- **Extensive, time consuming discussion**
- **Visible decision-making process makes the process <u>appear</u> more dependant upon professional judgment than other tools**
- **Will NOT yield a numerical value for P_N**
- **Limitations that apply to ALL High-Rigor simulation tools:**
  - Difficult to replicate scenario results
  - Creditable and experienced personnel required
  - Subject Matter Experts (SMEs) required from a variety of fields

Tabletop Analysis 37

Obstacles to Common Use

- **No published protocol**
- **No tabletop cultural or experience**
- **Resource/time requirements fallacy**
- **Failure to do satisfactory scoping**
  - Failure to develop rigorous exercise protocol and/or rules of engagement documents.
- **Potential for introduction of site bias**

Tabletop Analysis 38

Summary

- **Tabletop exercises:**
  - simulate protection system performance when exposed to credible, realistic adversary tactics and tools
  - reveal areas of weakness and teach you things about your system that no other commonly-used tool can
  - require extensive scoping and planning, careful participant selection, and rigorous conduct
  - perform well at sites that have little technology, funding, or spare labor resources
  - yield results that are useful alone or with other tools

Tabletop Analysis 39

Hypothetical Facility Attack Plan

The Lagassi Institute of Medicine and Physics (LIMP)

Purpose:

- Goal of these tabletop discussions is to develop attack plans that will test the ability of the Lagassi Institute of Medicine and Physics (LIMP) Site's security systems to prevent successful adversary action.
- The emphasis is on presenting a formidable force in order to validate and document security system effectiveness against a fictitious Design Basis Threat (DBT).
- Once analyzed the information gathered will serve as a baseline for subsequent computer combat simulation, Limited-Scope Performance Testing, and Force-on-Force exercises.
- After above tools have been utilized, the site will analyze information to determine tactical and technical requirements in order to address an integrated system that meets Lagassi security system effectiveness objectives.

Assumptions:

1) National-Level Assumptions:

- ***Assumption:***

1) T-Cell has the financing as well as the technical and tactical competence to plan, organize, and establish the clandestine mechanism necessary to support such an adversary attack in Lagassi.

2) Even with improvements in international detection and investigation capabilities, T-Cell competencies include eluding all foreign and domestic law enforcement and intelligence resources while coordinating the operation without being detected.

3) This assumption excludes potential pre-incident detection capabilities and results in a probability of **0.0%** that the adversary's operation will be compromised before the initiation of any attack action.

- ***Assumption:***

1) T-Cell was able to recruit insider assistance to obtain specific public, sensitive, and/or classified information necessary.

2) The information T-Cell was able to obtain is similar to information developed by the site's cleared vulnerability analysis personnel, who have knowledge and authorized access to classified information and to other subject matter experts.

3) This extensive information is to be obtained with **0%** probability of being detected during the recruitment or information gathering process.

2) Site Assumptions (Rules of Engagement):

- ***Assumption:*** T-Cell was able to conduct external surveillance with a probability of **0.0%** that the operation would be compromised.
- ***Assumption:*** T-Cell was able to establish Mission Support Sites (MSS) with a probability of **0.0%** that the operation would be compromised.
- ***Assumption:*** T-Cell was able to establish pre-position hide-sites outside of protective force security sweep area with a probability of **0.0%** that the operation would be compromised before attack initiation.
- ***Assumption:*** T-Cell was able to control both the point of detection and time of weapons and explosives engagement.

I. SITUATION:

A. Target:

- **Geographical Setting:**

1) Site is located in a semi-arid, high desert climate.
2) The site is located about 30km East of the city of Hashbakar.
3) There are a limited number of small communities within 100km radius of the site.
4) The city is less than 100km away from the borders of two neighboring countries.
5) Terrain is flat with little or no deviation in elevation around target area.
6) Vegetation consists mainly of prairie grasses, sagebrush and shrubbery, and is approximately two-feet high.
7) Dead vegetation and debris are commonly blown about by the wind in the spring.
8) Low-flying aircraft and heavy nearby passenger vehicle traffic are common.
9) Occasional earthquakes in the region.
10) Small varmint and predatory animals and various bird species inhabit the LIMP area.

- **Weather and Light Data:**

1) *Sunset*: 1813 Hours
2) *Sun Rise*: 0628 Hours
3) *Moon Rise*: 1918 Hours
4) *Moon Set*: 0846 Hours
5) *Moon Phase*: 0%--Illumination
6) *Winds:*
   - Average: 2-5 Km/h
   - Gusting: 50 Km/h
   - From North-North East to South-South West
7) *Temperature*: Day: 18° Celsius. Night: 3° Celsius.
8) *Visibility*: 16 Km, daytime
9) *Cloud*-Cover: Minimal to partly-cloudy

- **Target Areas**

1) PTR Reactor
2) NBR Reactor
3) Radioactive Waste Site

- **Target Selection**

Primary Target, Theft Operation (Mission would be a success upon the successful removal of <u>either or both</u> of these target-sets from the Site)

1) Target: Mixed Oxide Fuel Rods/PU Experiment Cylinders (PU239)
   a. Location: PTR Reactor Facility/R091 Product Vault (SSW in main reactor room)
   b. Size (Length): unknown, assumed man- and vehicle-portable
   c. Weight: 30kg per rod assembly, 2kg PU239 per rod assembly
   d. Number: 4 total cylinder units (8kg total PU239)
   e. Configuration: cylindrical rod
   f. Portability: assumed man- and vehicle-portable.

2) Target: HEU Metal
   a. Location: PTR Reactor Facility/R091 Product Vault (SSW in main reactor room)
   b. Size (Length): unknown, assumed man- and vehicle-portable
   c. Weight: 23kg, containing 22kg U235.
   d. Number: Assumed to be one block or a group of smaller, subdivided pieces
   e. Configuration: Assumed to be a single lumped-mass
   f. Portability: assumed man- and vehicle-portable.

B. Site Security Systems:

- **Protection Goal**: Prevent adversary attack success

- **Protection Objectives:**

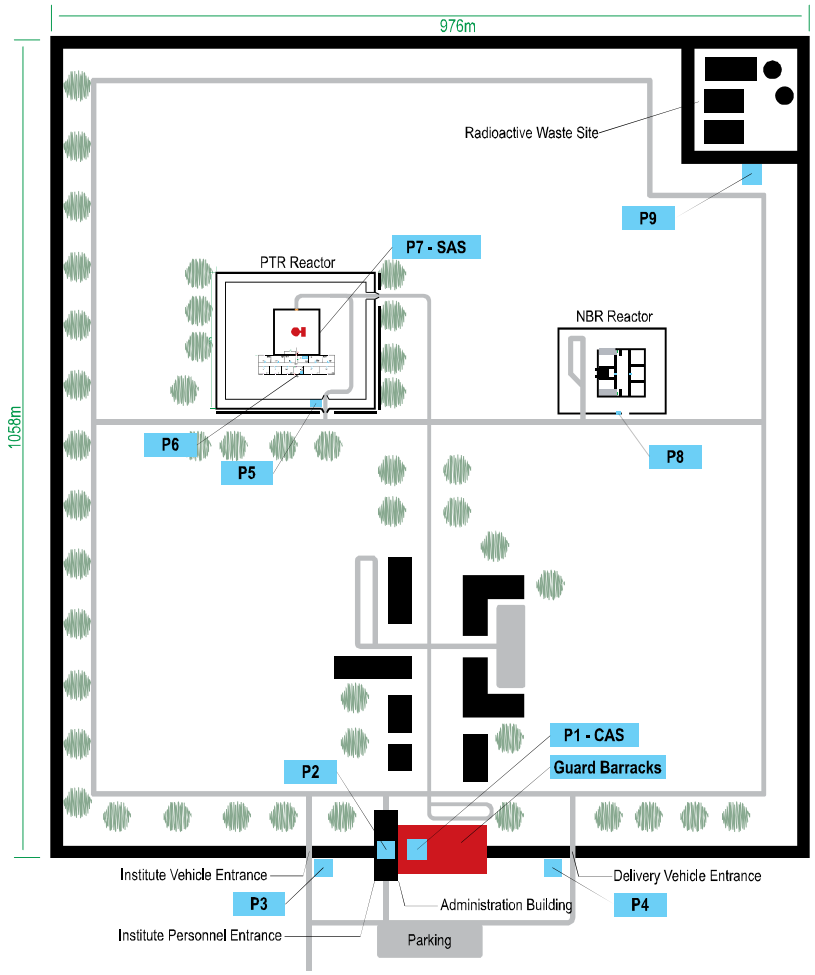
1) Detect adversary before attack initiation
2) Deny adversary most suitable attack positions
3) Delay adversary movement into target area
4) Prevent adversary access to general target area
5) Prevent adversary access to immediate target areas
6) Deny adversary task completion
7) Prevent adversary from escaping with target (if appropriate)

- **Protective Force Armament and Equipment:**

Equipment: Armed Guards	All **armed guards** are equipped with: • A Makarov pistol with a fully loaded magazine, but the pistol does not have a round in the chamber • two spare magazines of ammunition • a straight baton • one set of handcuffs • a small flashlight • a handheld radio
Equipment: Tactical Response Team	The **tactical response** team members are equipped with • a Makarov pistol with a fully loaded magazine but without a round in the chamber and • a Kalishnikov assault rifle. with a fully loaded magazine but without a round in the chamber (locked in the armory) • two spare magazines of ammunition for each weapon. Both weapons are carried with a fully loaded magazine but without a round in the chamber. • a straight baton • handcuffs • flashlight • handheld radio • body armor is readily available in the response force building

- **Protective Force Organization and Locations:**

Post No.	Description	Security Personnel (non-operational hours)	
S-1	Response Force Commander	Captain	1
S-2	Guard Commander	Lieutenant	1
P-1	Response Force Headquarters	Tactical Teams	10
P-1	Central Alarm Station	Guard	1
P-2	Institute Personnel Entrance	Guard	1
P-3	Institute Vehicle Gate	Guard	1
P-5	PTR Personnel/ Vehicle Portal	Guard	1
P-7	Secondary Alarm Station	Guard	1
P-8	NBR Personnel Portal	Guard	1
P-9	Waste Storage Facility	Guard	1
P-10	Random two-man patrol of Institute	Guard	2
		Totals	**21**



C. T-Cell Organization and Primary Responsibility:

***TV-1* Element:**

1) Tango-One (***T-1***) - Assaulter
2) Tango-Two (***T-2***) - Element Leader/Assaulter/Breacher

***TV-2* Element:**

3) Tango-Three (***T-3***) - Assaulter
4) Tango-Four (***T-4***) - T-Cell Leader/Element Leader/Assaulter/Breacher

***TV-3* Element:**

1) Tango-Five (***T-5***) – Driver/Element Leader

D. T-Cell Weapons, Ammunition, and Equipment:

1) Individual-issue Uniform, Weapons and Equipment:

a. Cell Members *T-1, T-2, T-3,* and *T-4*

Item:	**Weight:**
1) BDU (Desert)	01.36 Kg
2) Assault Boots (Desert)	01.36 Kg
3) Load Bearing Vest (Desert)	01.36 Kg
4) Hand-held Radio w/ spare battery	00.45 Kg
5) Head Lamp	00.45 Kg
6) Leatherman Knife	00.45 Kg
7) Head-mounted NVGs w/ IR	02.00 Kg
8) Assault back-pack	00.91 Kg
9) Elbow and Knee Pads	00.45 Kg
10) Flightline Nomex/Leather gloves	00.25 Kg
11) Sure Fire 6P Tactical light	00.45 Kg
12) AK47 w/30-round magazine, ball ammo, select-fire	03.86 Kg
13) Red-Dot Sighting System, night-vision compatible	00.91 Kg
14) 30-round magazine (x4)	03.64 Kg
15) Firing Device Shocktube (4x)	00.45 Kg
16) Explosive Priming System (300 feet)	04.77 Kg
17) 0.5kg TNT equivalent plastic explosive, pre-fused	00.50 Kg
18) Mini-portable Welding Torch	03.64 Kg
19) Welding Rods, ½Kg	00.50 Kg
	Total: 27.30 Kg

b. Cell Member *T-5*

Item:	**Weight:**
1) Commercial service technician uniform, complete with shoes _____	03.00 Kg
2) Hand-held Radio w/ spare battery _____	00.45 Kg
3) Leatherman Knife _____	00.45 Kg
4) Head-mounted NVGs w/ IR _____	02.00 Kg
5) Sure Fire 6P Tactical light _____	00.45 Kg
6) Suppressed Ruger .22-caliber pistol and spare 15-round magazine ___	00.90 Kg
	Total: 07.25 Kg

2) Vehicles and vehicle-based equipment

Note: Chevy Suburban/crew-cab truck or similar (each must have four doors and an ample rear storage or bed area; Land Rovers, Toyota Land Runners, Jeep Cherokees, any crew-cab pickup, commercial delivery vehicles, etc. would suffice). Four trucks are needed; one for the VB/IED, two for assault, and one spare. Could be well-used, but must be reasonably reliable. Source from the regional market to better blend into the indigenous population.

Vehicle One (TV-1) – Lead Assault Vehicle

Item:	**Weight:**
1) Vehicle _____	????? Kg
2) Fuel _____	127.00 Kg
3) Fabricated Push-Bar front-grille assembly _____	150.00 Kg
4) 55 kg TNT Bulk Breaching Charge w/ dolly_____	70.00 Kg
5) Tie-Down kit for explosive dolly _____	03.00 Kg
6) Hand-held GPS receiver _____	00.45 Kg
7) ***T-1*** and individual Gear _____	111.39 Kg
8) Nylon Tow Strap, low-visibility, 3m _____	07.00 Kg
9) Towing Eyelet (Rear) _____	02.00 Kg
10) Tire Slime (sealant for minor leaks, 1 KG in each tire) _____	04.00 Kg
11) Bottled water, (8 x 12oz ea) _____	07.00 Kg
	Total: 481.84 Kg
	(plus vehicle weight)

Vehicle Two (TV-2) – Second Assault Vehicle

Item:	**Weight:**
1) Vehicle _____	????? Kg
2) Fuel _____	127.00 Kg
3) Fabricated Push-Bar front-grille assembly _____	150.00 Kg
4) 55kg TNT Bulk Breaching Charge w /dolly_____	70.00 Kg
5) Tie-Down kit for explosive dolly _____	03.00 Kg
6) Hand-held GPS receiver _____	00.45 Kg
7) ***T-3*** and individual Gear _____	111.39 Kg
8) ***T-4*** and individual Gear _____	111.39 Kg
9) Nylon Tow Strap, low-visibility, 3m _____	07.00 Kg
10) Towing Eyelet (Rear)_____	02.00 Kg
11) Tire Slime (sealant for minor leaks, 1 KG in each tire) _____	04.00 Kg
12) Bottled water, (8 x 12oz ea) _____	07.00 Kg
Total:	**593.23 Kg**
(plus vehicle weight)	

Vehicle Three (TV-3) – Vehicle Bomb/Improvised Explosive Device Vehicle

Item:	**Weight:**
1) Vehicle _____	????? Kg
2) Fuel _____	127.00 Kg
3) 900Kg ANFO Improvised Explosive Device _____	900.00 Kg
4) Triggering mechanism for IED _____	04.00 Kg
5) Suspension reinforcement for additional load-capability _____	100.00 Kg
6) Hand-held GPS receiver _____	00.45 Kg
7) ***T-5*** and individual Gear _____	91.34 Kg
8) Nylon Tow Strap, low-visibility, 3m _____	07.00 Kg
9) Towing Hook (Front) _____	02.00 Kg
10) Tire Slime (sealant for minor leaks, 1 KG in each tire) _____	04.00 Kg
11) Bottled water, (2 x 12oz ea) _____	01.75 Kg
Total:	**1,237.54 Kg**
(plus vehicle weight)	

Vehicle Four (Spare) – Spare Vehicle

Item:	**Weight:**
1) Vehicle	????? Kg
2) Fuel	127.00 Kg
3) Fabricated Push-Bar front-grille assembly	150.00 Kg
4) 55kg TNT Bulk Breaching Charge w/dolly	70.00 Kg
5) Tie-Down kit for explosive dolly	03.00 Kg
6) Hand-held GPS receiver	00.45 Kg
7) ***T-2*** and individual Gear	111.39 Kg
8) Nylon Tow Strap, low-visibility, 3m	07.00 Kg
9) Towing Eyelet (Rear)	02.00 Kg
10) Spare Fuel (3 x 23 Kg Jerry Cans with 19L fuel/can)	69.00 Kg
11) Spare Coolant (3 x 25 Kg Jerry Cans with 19L coolant/can)	75.00 Kg
12) Spare Engine Oil (3.8L Oil)	04.00 Kg
13) Spare Wheel and Tire for ***TV-3***	34.00 Kg
14) Jack and Lug wrench set for ***TV-3***	12.00 Kg
15) Tire Slime (sealant for minor leaks, 1 KG in each tire)	04.00 Kg
16) Truck tire-patch kit	01.00 Kg
17) Tire inflator can	02.00 Kg
18) Bottled water, (8 x 12oz ea)	07.00 Kg
	Total: 678.84 Kg
	(plus vehicle weight)

II. MISSION:

T-Cell Conducts an armed attack at ***the PTR Reactor Facility at the LIMP Institute*** on 22 August 2007 at *0200 Hours local time*, to initiate theft of target material.

III. EXECUTION:

Concept of Operation:

A. Pre-Attack Activities:

- The Mission Support Site (MSS) has been established approximately one hour's drive east of the LIMP site. The site is a small number of tents in a similar style and arrangement to that of indigenous people of the region.
- The Cell's three mission trucks are concealed inside the tents. A fourth is outside the tents and serves to answer camp-occupant transportation questions for any passers-by. The fourth truck also serves as a mission spare, in case of failure of one of the designated mission vehicles.
- The MSS was established approximately two and a half days before the attack, and the three mission trucks arrived approximately one half day later (in the middle of the night) and were concealed upon arrival.
- The MSS is occupied by the entire T-Cell upon the arrival of the mission-trucks, and the Cell-members remain concealed during daylight hours.
- All four trucks are similar in capability, but are not so externally similar as to draw undue attention en-route target.

B. Attack Activities:

- Attack plan consists of successfully employing two elements: 1) vehicle bomb element and 2) target assault/breaching element.

First Element:

- ***00:30:00 hours*** ***TV-3*** departs MSS en-route LIMP in convoy with the other Cell vehicles, west-bound on unnamed east-west road that runs directly next to the LIMP Site.
- ***01:15:00 hours*** Upon command from ***T-4***, ***TV-3*** holds approximately 15 minutes away from the LIMP south parking area, blacked-out (including disabling brake-lights) and outside of visual range of personnel at LIMP (in reality, this distance from LIMP would be fine-tuned to reflect actual terrain visibility-limitations). ***T-5*** drives and navigates by Night-Vision Devices from this point on.
- ***01:45:00 hours*** ***TV-3*** rolls to LIMP in the middle, of the three-truck convoy.
- ***01:58:00 hours***, ***T-4*** calls for final status-check (pops and clicks). ***T-5*** responds. ***T-4*** issues code-sound for Attack engagement.

- ***01:59:30 hours*** ***TV-3*** continues to roll to target, even as ***TV-1*** and ***TV-2*** drop out of line.
- ***01:59:45 hours*** While ***TV-3*** continues to target, ***T-5*** keys and holds radio microphone button.
- ***01:59:55 hours*** Approximately five seconds before detonating ***TV-3***, ***T-5*** shouts into microphone.
- ***02:00:00 hours*** ***T-5*** detonates ***TV-3***.

Second Element:

- ***00:30:00 hours*** ***TV-1***, ***TV-2***, and the spare truck depart MSS en-route LIMP with ***TV-3***, west-bound on unnamed east-west road that runs directly next to the LIMP Site.
- ***01:15:00 hours*** Upon command from ***T-4***, vehicles hold approximately 15 minutes away from the LIMP south parking area, blacked-out (including disabling brake-lights) and outside of visual range of personnel at LIMP (in reality, this distance from LIMP would be fine-tuned to reflect actual terrain visibility-limitations). Cell members drive and navigate by Night-Vision Devices from this point on. Spare truck is parked on the side of the road. Driver (***T-2***) dismounts and mounts ***TV-1*** passenger seat.
- ***01:45:00 hours*** Three assault vehicles roll to LIMP, with ***TV-2*** leading, ***TV-3*** in the middle, and ***TV-1*** in the rear.
- ***01:58:00 hours***, ***T-4*** calls for final status-check (pops and clicks). Upon receipt of proper signal from ***T-5***, ***T-1***, and ***T-3***, ***T-4*** issues code-sound for Attack engagement.
- ***01:59:30 hours*** ***TV-2*** and ***TV-1*** hold 400m short of the LIMP south parking lot.
- ***01:59:55 hours*** Upon hearing ***T-5*** shout over the radio, the other team members close their eyes until after the blast-flash subsides.
- ***02:00:00 hours*** ***TV-1*** and ***TV-2*** roll to target and after the ***TV-3*** blast-flash, all open their eyes to begin the actual attack.

IV. COMMAND and CONTROL:

A. Command:

Tango-Four (***T-4***): T-Cell Leader
Tango-Two (***T-2***): 2nd T-Cell Leader

B. Communications:

Hand-held Radio, 2.4GHz, lithium-ion with a spare battery, and simple privacy/encryption system.

T-CELL ATTACK EVENT TIMELINE

21 October 2007

Initial Expected Engagement--***02:00:00 Hours***

Event	Activity(ies)	Start Time	Event Time	Total Time
1	***TV-1*, *TV-2*, *TV-3*, Spare** depart MSS en-route **LIMP**	0:30:00	45:00.0	0:45:00
2	Blacked-out ***TV-1*, *TV-2*, *TV-3*, Spare** hold per ***T-4***. All don NVGs. **Spare** truck is left on the side of the road, ***T-2*** dismounts, and mounts ***TV-1*** passenger seat	1:15:00	30:00.0	1:15:00
3	Convoy rolls to **LIMP** per ***T-4***. Order: ***TV-1*, *TV-3*, *TV-2***	1:45:00	13:00.0	1:28:00
4	***T-4*** calls for final status, gets responses, issues attack order.	1:58:00	00:20.0	1:28:20
5	Convoy continues to roll to **LIMP**	1:58:20	01:10.0	1:29:30
6	***TV-1*, *TV-2*** peel out of convoy and hold 400m from **LIMP** south parking lot	1:59:30	00:05.0	1:29:35
7	***TV-3*** continues to roll on to **LIMP** south parking lot	1:59:35	00:10.0	1:29:45
8	***T-5*** keys and holds microphone open	1:59:45	00:10.0	1:29:55
9	***T-5*** shouts loudly into radio. **All Cell members** other than ***T-5*** hear the shout and close their eyes until they sense the blast flash. ***T-5*** detonates ***TV-3*** next to the south wall of the Site building where **P2** is stationed.	1:59:55	00:05.0	1:30:00
10	***TV-1*, *TV-2*** roll towards **LIMP Institute Vehicle Entrance** gate (***BP-1***) and open their eyes. On approach, ***T-2*** rolls down the window, raises his AK, and covers **P3**'s post area. Likewise, ***T-4*** rolls down his window and covers the **P2** post area	2:00:00	00:40.0	1:30:40
11	***T-2*** and ***T-4*** dismount and advance to ***BP-1***. ***T-2*** leads, establishing front security while ***T-4*** removes ***BC-1*** from his tactical vest.	2:00:40	00:20.0	1:31:00
12	***T-4*** places ***BC-1*** and signals ***T-2*. *T-2*** and ***T-4*** retreat behind ***TV-1*** while ***T-1*** ducks behind the dash. ***T-4*** detonates ***BC-1***	2:01:00	00:15.0	1:31:15
13	***T-4*** covers front and moves to ***BP-1*. *T-2*** moves up and mounts ***TV-1*,** covering right. ***T-4*** pushes the gate open and ***TV-1*** drives through en-route ***BP-2***	2:01:15	00:20.0	1:31:35
14	***TV-2*** advances to ***BP-1*** and ***T-4*** mounts. ***TV-2*** moves through ***BP-1*** en-route ***BP-2***	2:01:35	00:15.0	1:31:50

15	***TV-1*** moves to ***BP-2*** as ***T-2*** rolls up window and buckles his seat belt **(*T-1*** had already buckled-up). ***TV-1*** hits ***BP-2*** and moves through towards ***BP-3***	2:01:50	01:00.0	1:32:50
16	***TV-1*** moves N of **PTR** Facility and stops about 30m NNE of ***BP-3*****.** ***T-2*** dismounts, removes the ***BC-1*** dolly from the bed of the truck, and dismounts the truck bed. ***TV-2*** arrives, moves through ***BP-2*****,** and stops about 30m ENE of ***BP-3*** **(*TV-2*** arrives at task time = 15 sec). ***T-1*** removes NVGs.	2:02:50	00:30.0	1:33:20
17	***TV-1*** rams ***BP-3*****.** ***T-2*** begins moving to **BP-3** with ***BC-2***	2:03:20	00:05.0	1:33:25
18	***TV-2*** advances to a cover position (with rear tailgate towards BP-3) about 10m E of ***BP-3*****.** ***T-4*** begins assessing the breach. ***T-2*** continues moving to ***BP-3*** with ***BC-2***	2:03:25	00:10.0	1:33:35
19	***T-2*** finishes moving up to ***BP-3*** with ***BC-2*****.** ***T-3*** and ***T-4*** dismount ***TV-2*** and enter ***BP-3*** to clear the Reactor Hall	2:03:35	00:15.0	1:33:50
20	***T-3*** and ***T-4*** finish clearing the Reactor Hall. ***T-2*** enters the Hall with the ***BC-2*** and begins moving towards ***BP-4*****.**	2:03:50	00:30.0	1:34:20
21	***T-3*** and ***T-4*** shoot the surveillance cameras in the Reactor Hall. ***T-2*** continues moving towards ***BP-4*** with ***BC-2***	2:04:20	00:10.0	1:34:30
22	***T-2*** continues moving towards ***BP-4*** with **BC-2.** ***T-4*** moves to assist ***T-2*****.** ***T-3*** removes mini torch and welding rod from load-bearing vest and lights torch while moving to **D60/1**	2:04:30	00:20.0	1:34:50
23	***T-2*** and ***T-4*** deliver and set ***BC-2*****,** then ***T-4*** moves towards ***TV-1*** and ***T-2*** moves towards ***BP-3*****.** ***T-3*** finishes tack-welding **D60** shut.	2:04:50	00:30.0	1:35:20
24	***T-2*** moves to ***BP-3*** to establish security. ***T-4*** begins helping ***T-1*** get out of ***TV-1*****.** ***T-3*** moves to assist ***T-4*** with ***T-1***	2:05:20	00:20.0	1:35:40
25	***T-2*** clears area around ***BP-3*** exterior and holds security. ***T-3*** and ***T-4*** help ***T-1*** move away from ***TV-1*** towards ***BP-3*****.** ***T-2*** and ***T-3*** exit through ***BP-3*** and establish exterior security.	2:05:40	00:30.0	1:36:10
26	***T-4*** and ***T-1*** move outside ***BP-3*** and take cover. ***T-2*** and ***T-3*** hold security. ***T-4*** accounts for the team.	2:06:10	00:10.0	1:36:20
27	***T-4*** detonates ***BC-2***	2:06:20	00:05.0	1:36:25
28	***T-3*****,** ***T-4*****,** ***T-1*****,** and ***T-2*** enter Reactor Hall through ***BP-3*****.** ***T-2*** resumes rear security through ***BP-3*****.** ***T-3*****,** ***T-4*****,** and ***T-1*** move to ***BP-4*****.**	2:06:25	00:20.0	1:36:45

29	***T-3*, *T-4*,** and ***T-1*** move to **R091** and enter vault through ***BP-4*.**	2:06:45	00:15.0	1:37:00
30	***T-4*** loads a MOX rod assembly into the backpack of ***T-3*. *T-3*** exits ***BP-4*** en-route ***BP-3***	2:07:00	00:30.0	1:37:30
31	***T-4*** Loads a MOX rod assembly into the backpack of ***T-1*. *T-1*** loads the 23kg HEU slug into ***T-4*'s** backpack. ***T-1*** exits ***BP-4*** en-route ***BP-3*.** ***T-3*** calls coming out, moves to ***BP-3*,** exits ***BP-3*,** then replaces ***T-2*** on security detail. ***T-4*** tosses the third MOX rod out ***BP-4*.**	2:07:30 **2:07:30**	00:55.0 00:45.0	1:38:25 **1:38:15**
32	***T-2*** enters through ***BP-3*,** then proceeds to ***BP-4*.**	2:08:15	00:30.0	1:38:45
33	***T-1*** calls coming out, exits ***BP-3*.**	2:08:25	00:10.0	**1:38:35**
34	***T-1*** moves to ***TV-2*,** establishes security	2:08:35	00:10.0	1:38:45
35	***T-2*** reaches ***BP-4*,** then calls to ***T-4*. *T-4*** hands ***T-2*** the last MOX rod.	2:08:45	00:15.0	**1:39:00**
36	***T-2*** moves to ***BP-3*** ***T-4*** exits **R091** through ***BP-4***	2:09:00 **2:09:00**	00:40.0 00:10.0	1:39:40 **1:39:10**
37	***T-4*** kneels, picks up last MOX rod assembly, stands, and moves to ***BP-3***	2:09:10	01:00.0	1:40:10
38	***T-2*** calls coming out, exits ***BP-3*.**	**2:09:40**	00:10.0	**1:39:50**
39	***T-2*** moves to ***TV-2*** and places the MOX rod into bed/rear area.	2:09:50	00:15.0	1:40:05
40	***T-2*** moves up to ***TV-2*** driver's area and starts the vehicle from outside	2:10:05	00:10.0	1:40:15
41	***T-4*** calls coming out, exits ***BP-3*.**	**2:10:10**	00:15.0	**1:40:25**
42	***T-4*** moves to ***TV-2*** and places the MOX rod next to the existing rod. ***T-2*** moves to ***T-4***, removes the HEU plug from ***T-4*'s** backpack, and places it next to the MOX rods.	2:10:25	00:20.0	1:40:45
43	***T-2*** remounts front left (driver's) seat and calls ***T-3*** in. ***T-4*** mounts front right seat and calls ***T-1*** in. ***T-4*** assumes right side security, shifting to front-right once **V*T-2*** is in motion.	2:10:45	00:10.0	1:40:55
44	***T-3*** mounts rear left seat. ***T-1*** mounts rear right seat. They turn sideways to assume appropriate door-gunner responsibilities during exfiltration.	2:10:55	00:15.0	1:41:10
45	***T-2*** begins driving for exfiltration. Within five seconds of motion, all three gunners have their windows down and their weapons in full-automatic mode. The vehicle will attempt to leave blacked out and all of T-Cell still have their NVGs on and active.	2:11:10	01:20.0	1:42:30
	Mission Complete	**2:12:30**		**1:42:30**

Subgroup 22S
Tabletop Exercise

Session Objectives

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

1. Recognize issues that need to be addressed in the scoping stage of tabletop exercises.

2. During Post Execution Discussion the participant will differentiate between attack descriptions resulting from path analysis and scenario analysis,

3. Describe After-Action Activities by identifying what LAGASSI PPS elements were exploited and describe what mitigation measures can be implemented to address each limitation.

Exercise 1 – Scoping Agreement and Appropriate Stakeholders

Your instructor will cover topics addressed in a typical scoping agreement.

Exercise 2 – Post Execution Discussion Comparison with Path Analysis

The threat description developed during Subgroup 4 was used in determining a most-vulnerable P_I path and during neutralization analysis. Now consider the equipment assigned to the adversaries in the attack plan and compare it to your threat description from Subgroup 4. Describe below any equipment used in the attack plan that is not described in your threat description (These additional threat assumptions needed for a tabletop would be worked out in conjunction with the competent authority with regulatory responsibility for the threat.)

Compare your theft path developed during Exercise 5 of the Subgroup 18S, Single Path Tool to the attack plan. Compare the following:

Start and end of the path:

Details about equipment types and weights:

Details about what each adversary is doing as a function of time:

Exercise 3 – After-Action Activities

An after action review is conducted with all participants and observers to discuss the simulation and capture lessons learned. This is an opportunity for all involved to analyze the battle and provide different perspectives on what worked, what didn't work, and offer ideas on how to improve the overall effectiveness of the security system. This is also an opportunity to discuss potential upgrades that should be modeled in subsequent tabletop analyses.

Based on the tabletop exercise you witnessed, answer the following questions.

Determine System Effectiveness Qualitatively

Can you identify any specific vulnerabilities?

Scenario analysis will often show vulnerabilities in how the response forces are normally deployed and used. The two 5-man tactical teams currently found in P-1 seem to be vulnerable to this scenario. Against this scenario, record the relative merits of dispersing these teams in smaller 2-man teams in small vehicle patrol units versus stationing all tactical team elements in a hardened response force center constructed within the Lagassi Limited Area but outside the PTR and NBR perimeters.

Dispersal of units (Pro):

Hardened Response Force Center Constructed Within the LIMP Limited Area (Pro):

How could further tabletop exercises be used to compare the effectiveness of these options?

What types of mitigation measures are recommended for each vulnerability described above?

Application Considerations

1. In what ways could this exercise help you plan for a Force-on-Force at your site?

2. In some countries the response is provided by organizations other than the organization operating the reactor or performing the research. In such a case, what issues need to be addressed in order to perform a high quality tabletop exercise?

3. It can be difficult to get Probability of Hit/Probability of Kill data about weapons so that some might attempt to collect it themselves. What are some of the safety issues involved in trying to do so? What are tests that might be safely performed by the site? What are others best performed by outside organizations?

Effectiveness Criteria Definitions

General Criteria for Each Critical Attack Element Under Evaluation

[Critical Attack Elements may include initial attack actions, breaching target, accessing material, exiting target area, etc. Other elements may be included depending upon the scenario.]

Rating Criteria	Detection	Assessment	Interruption
Very High	Detection is nearly perfect; there are at least two nearly simultaneous methods of detection, such as PIDAS, Pro-force, personnel etc. Or a single detection method that is very robust and is accompanied with a high degree of performance testing data.	Assessment is most likely to happen and in a positive, well-communicated way. Jamming would be difficult or there are good alternative communications. The assessment is relayed to ground forces effectively. C3 is very effective.	Pro-forces are in the immediate vicinity and can interrupt adversary actions by bringing effective fire. Pro-forces are within the target area in superior numbers and have good fighting positions and effective weaponry. Pro-forces are effectively positioned between the adversary and their target.

Rating Criteria	Detection	Assessment	Interruption
High	Detection is most likely to take place. There may be some doubt with some elements of the system but adversary would have to be able to surreptitiously compromise the system, or have a way to fool or spoof the system during the attack.	Assessment occurs but there are few backups for jamming, still effective in getting information to the ground forces. Jamming causes some confusion and could delay assessment for a short time. C3 is still effective.	Pro-forces are in vicinity. A significant number can bring fire on the adversary to interrupt actions. Pro-forces have good weaponry to combat the approaching threat. Some of the pro-forces have good fighting positions. Pro-forces are near the target intercepting the adversary.
Moderate	Detection has a good chance of occurring, the system(s) are in place and functioning. The reliability may be in some question, may be some intermittent dead spots. Probability of detection from sources other than systems (such as pro-forces, or other personnel) detecting is not good.	Assessment will likely occur. If jamming occurs Assessment may be delayed to the point of effecting response. Ground forces will have to have pre-determined response places to remain effective. Independent collaboration from ground forces is harried and can give erroneous information. C3 is negatively affected.	Pro-forces are within effective weapons range of adversaries. Only a few can bring effective fire on adversaries, which intermittently interrupt their actions. Only a few PF have fighting positions. PF personnel are taking casualties.
Low	Detection could take place, likely it will not, only one method for detection, or others	Assessment may not occur, especially in a timely fashion, may know there are	Few pro-force are in vicinity of the target. A few can engage with some ineffective fire.

Rating Criteria	Detection	Assessment	Interruption
	are unlikely. Systems are not reliable. Numerous methods to spoof or interfere with alarm could occur.	people in the area but not have ability to know if they are hostile. High susceptibility to jamming or other deceit methods to avoid assessment. C3 is not effective.	Adversaries have a direct inbound line to the target, and can achieve numerically superior firepower, with effective weaponry. Pro-forces are taking higher casualties than above.
Very Low	Detection likely will not take place. No systems, or very low reliability. Pro-force is not in place to detect except by happen-stance.	Assessment likely will not occur, ability to overcome jamming and other ruses is poor. Very susceptible to diversion. No ground forces near to get a visual on adversary. C3 is absent.	No pro-force in target vicinity to engage effectively. Adversaries continue unimpeded to target. Pro-force does not have sufficient weaponry to counter or interrupt the progress of the adversary. Pro-forces are taking significant casualties.

This page intentionally left blank