

Introduction to Vulnerability Analysis Training Course

Module 1

Vulnerability Analysis Training Course
Date:

Student Learning Objectives

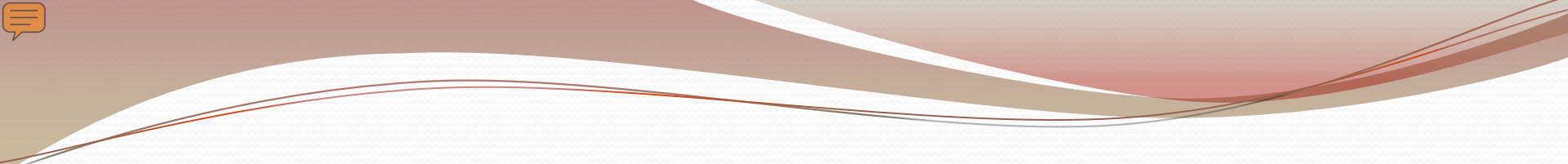
After completing this module, you will be able to:

- Discuss the course goal
- State the prerequisite knowledge
- Discuss training course logistics



Course Goal

Enable participants to conduct a vulnerability assessment (VA) using a systematic approach to quantitatively and/or qualitatively assess the effectiveness of physical protection systems used to protect nuclear and other radioactive materials and nuclear facilities against theft and sabotage.



Prerequisite Knowledge

Participants should:

- Have some experience in the physical protection field
- Have a basic technical background

Participants must:

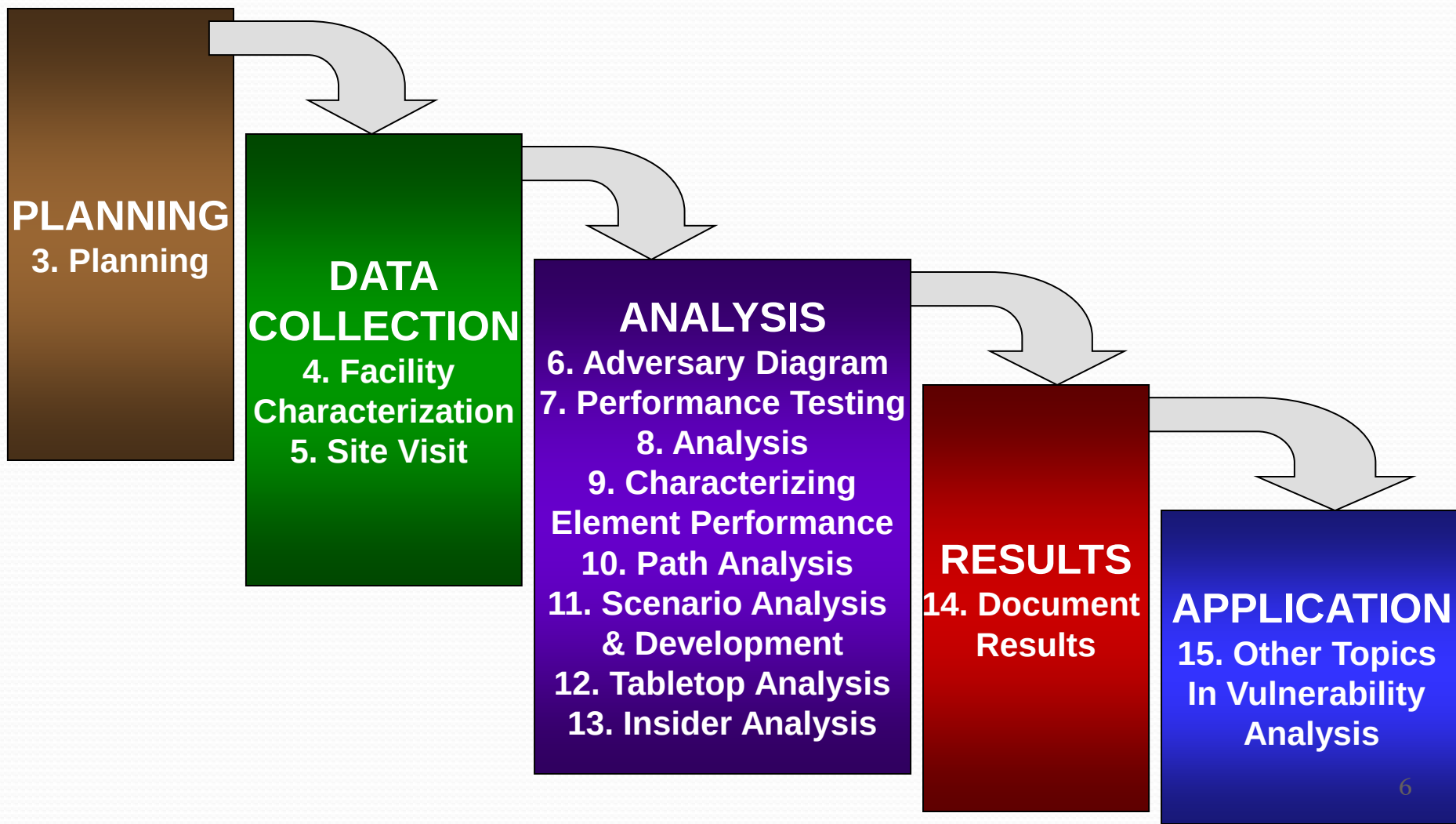
- Have attended the International or Regional Training Course (ITC or RTC) on Physical Protection of Nuclear Materials and Nuclear Facilities
- Be proficient in speaking, understanding, and reading English

This Course Does Not Cover

- How to design or upgrade a Physical Protection System (PPS)
- How to identify theft targets or vital areas for sabotage and how to categorize these targets
- How to perform all aspects of security risk analysis
 - System Risk, $R = P_A * (1 - P_E) * C$ has three components:
 - Probability of Adversary Attack, P_A
 - Probability of PPS Effectiveness (given an attack occurs), P_E
 - Consequence, C (given an attack succeeds)

This course only discusses how to perform a vulnerability analysis to determine P_E against a design basis threat.

Course Structure





Logistical Information

Summary

- **Course Goal:** Enable participants to conduct a VA using a systematic approach to quantitatively and/or qualitatively assess the effectiveness of a PPS.
- Students must have attended an ITC or RTC on Physical Protection of Nuclear Material and Nuclear Facilities.
- This course focuses on nuclear and other radioactive materials and facilities, but the methodology can be applied to other types of facilities.



Overview of Vulnerability Analysis

Module 2

Vulnerability Analysis Training Course
Date:

Student Learning Objectives

After completing this module, you will be able to:

- Discuss the purpose of a vulnerability analysis (VA)
- List the five steps in the VA process
- Describe the VA relationship to the Design and Evaluation Process Outline (DEPO)



Definitions

- ***Physical Protection System (PPS)*** — an integrated system of equipment, personnel, and procedures intended to prevent the completion of a malicious act.
- ***Vulnerability Analysis (VA)*** — A systematic, performance-based process that is used to evaluate the ability of a physical security system to meet performance requirements

Uses of VA

- Determine the relative effectiveness of alternative protective strategies and systems
- Ensure that systems provide balanced protection of assets
- Identify strengths and weaknesses in existing or planned protection systems
- Support cost-effectiveness studies for system design alternatives

Evaluation Requirements in INFCIRC/225/Revision 5

● 3.21

- To ensure that physical protection measures are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection.
- The State's competent authority should ensure that **evaluations based on performance testing are conducted by operators at nuclear facilities and by shippers or carriers for transport.**
- Evaluations should be reviewed by the State's competent authority, and should **include administrative and technical measures, such as testing of detection, assessment and communications systems, and reviews of the implementation of physical protection procedures.**
- When deficiencies are identified, the competent authority should ensure that corrective action is taken by the operator and by the shipper or carrier.



More Guidance on Evaluation

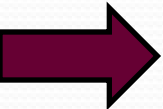
(INFCIRC/225 Revision 5)

- Evaluations include exercises to test integrated system, including training and readiness of guards and response forces
- Operator should develop and implement means and procedures for evaluations, including performance testing and maintenance of the PPS.
- Evaluations should be conducted regularly to determine the reliability and the effectiveness against the threat and to detect any equipment malfunction.
- Establish quality assurance policy and programs to ensure both that the PPS is designed, implemented, operated, and maintained in a condition to effectively respond to the design basis threat and that it meets the State's regulations, including prescriptive and/or performance-based requirements.
- Performance testing a PPS should include exercises to evaluate guards and response force effectiveness and timely response.
- Performance testing of a PPS should be conducted annually.

Analysis Approaches

- ***Expert:*** PPS design and evaluation activities based on personal knowledge and experience
- ***Features Approach:*** PPS design and evaluation based on specification and implementation of a required set of features
- ***Component Criteria Approach:*** PPS design and evaluation based on standards approach that uses performance criteria for some security features
- ***System Performance Approach:*** PPS design and evaluation based on a systems engineering approach specifying and achieving an overall system effectiveness against the Design Basis Threat (DBT) for theft and sabotage

Evaluation Approaches Summary

Approach	Requirement	Metric
Expert	Satisfy expert	Opinion
Features	Include required features	Presence of features
Component Criteria	Include required features that meet specific standard	Presence of feature and performance standard
 System Performance	Prevent theft or sabotage of nuclear material	System effectiveness

INFCIRC/225/Rev. 5 – 3.10 “The State should define requirements...for the physical protection of nuclear material...”



Discussion: 28th Floor Case Study (1 of 4)

There is an external door on the 28th floor of a high-rise building. The building security officer wants to know if the door needs to be locked.

For each of the 4 approaches that have been discussed:

- How do you answer this question?
- How do you validate your answer?



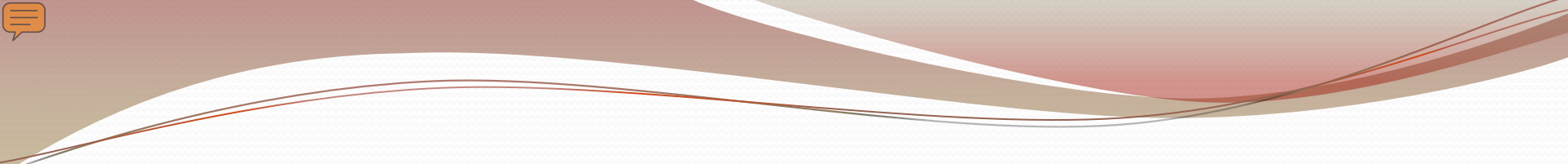
Discussion: 28th Floor Case Study (2 of 4)

- Expert-based approach: a security expert might tell you that it is desirable to lock door, in their opinion.
 - How would you validate that opinion?
- Features-based approach: The company owning the building might require that all external doors below the 20th floor not otherwise identified as entrances for the public to use or emergency exits be locked.
 - How would you then determine if the door should be locked?
 - How would you validate that this requirement will lead to better security?



Discussion: 28th Floor Case Study (3 of 4)

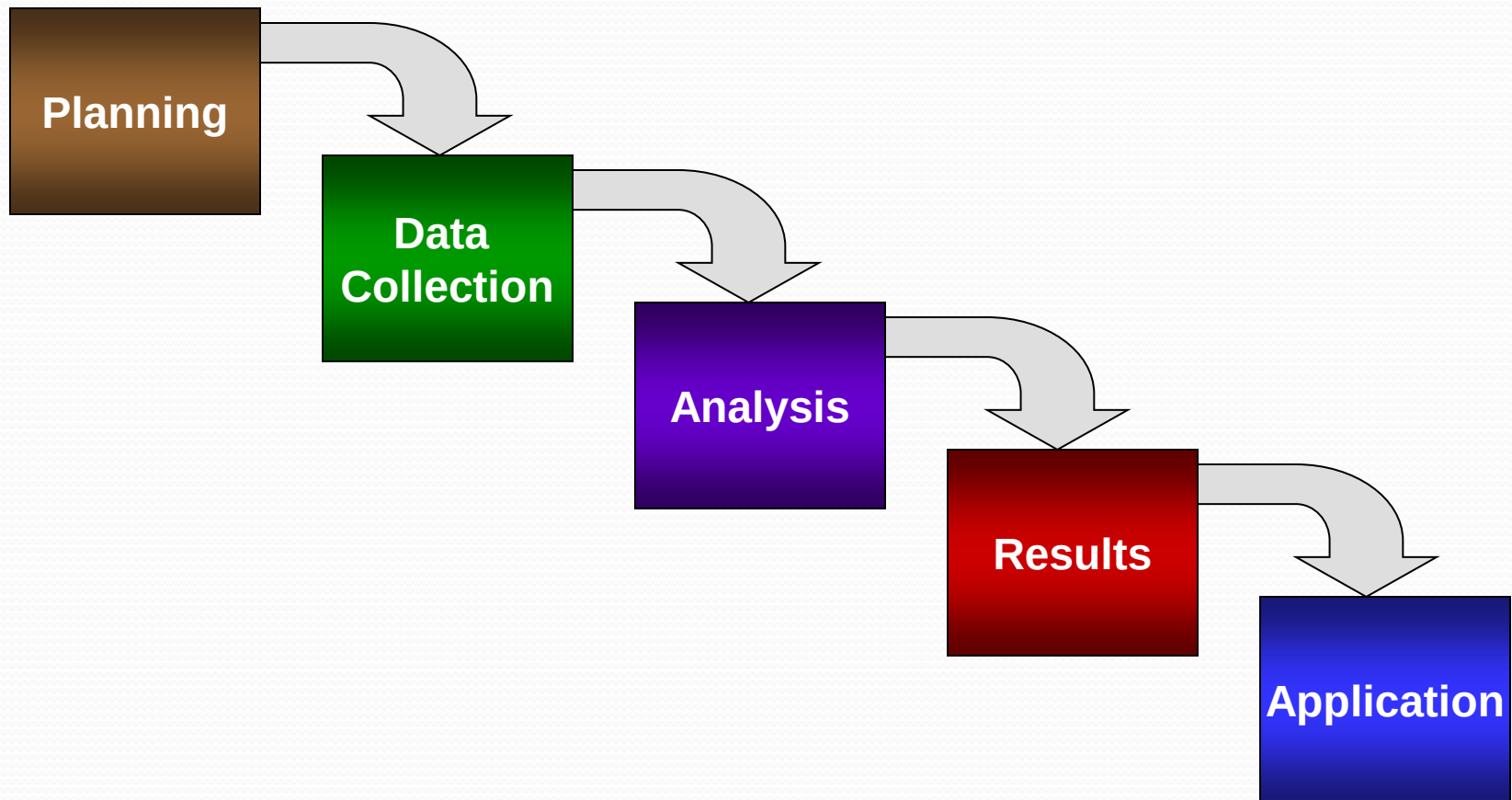
- Component criteria approach: In this approach, there is a requirement to include required features that meet specific performance standards
 - Example: “all external doors below the 20th floor not otherwise identified as entrances for the public to use or emergency exits should be locked and provide at least 3 minutes of delay against an adversary with a hammer and a crow bar.”
 - How would you then determine if the door should be locked?
 - How would you validate that meeting this requirement will lead to better security?



Discussion: 28th Floor Case Study (4 of 4)

- A system performance approach considers several issues in a disciplined approach:
 - Requirements:
 - What assets or items in the building need protecting?
 - Who do these targets need to be protected from?
 - How well do I need to protect the targets?
 - Are there non-security reasons to lock the door or leave it open?
 - Characterizing the PPS
 - Evaluating effectiveness
- How do you answer the “lock or not lock” question?
- How do you validate your answer with the results of the analysis

Phases of Vulnerability Analysis





Planning

Planning

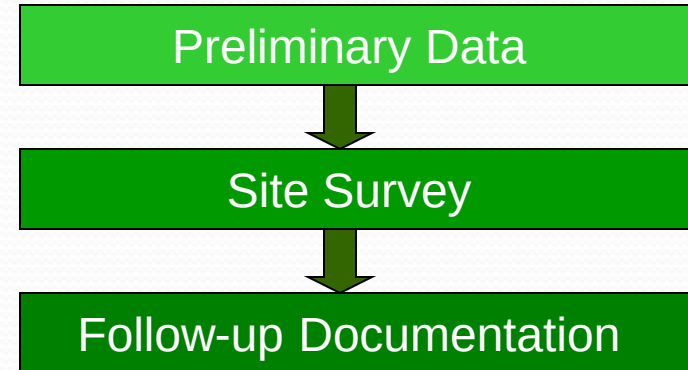
- Question/problem VA is trying to solve
- Determine scope, goals, and requirements
- Type of VA
- Metrics and analysis tools to be applied
- Stakeholders/team composition
- Scheduling and budget
- Access to facility and documentation
- Site visit preparation
- Constraints
- Document control and protection measures

Data Collection

Understanding the requirements for the PPS

**Data
Collection**

- Not conducted just once
- At least three sets
 - Request set of preliminary data to be used in site visit planning
 - Validate preliminary data and collect additional information
 - Request additional information not collected in the previous two steps, but needed for analysis
- Could take several iterations





Site Visit Preparation

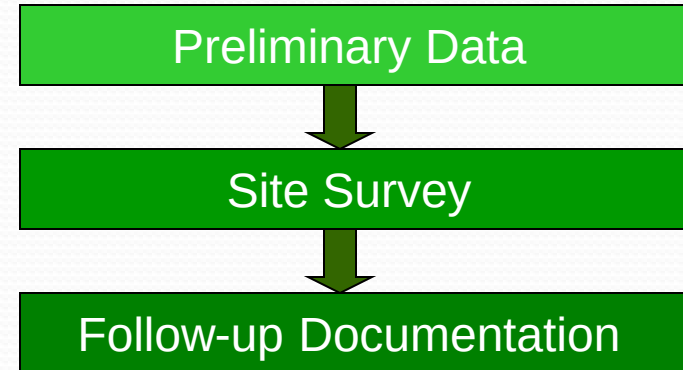
**Data
Collection**

- Review preliminary documentation
 - Site description
 - Facility layouts and relationships
 - Environment/climate information
 - Current DBT
 - Existing Vital Area Analysis
 - Preliminary theft and/or sabotage target list
 - Previous VAs, inspections, audit results
- Identify protection elements
 - Detection
 - Delay
 - Response

Data Collection – Types of Data

Data
Collection

- Facility characterization
 - PPS documentation
 - Open sources
 - Site survey
 - Test data
- Design Basis Threat
 - State
 - Regional or Local
 - Facility
- Target Identification/Consequences
 - Types and characteristics of material
 - Location of material and vulnerable equipment
 - Prioritized theft targets and sabotage vital areas



*May take three phases to
complete the picture*



Site Survey

Filling in the gaps

Data
Collection

- Present a stakeholders/management pre-briefing
 - Basis/assumptions
 - Protection objectives
 - Target set
 - Threat set
 - What we will be doing on site
- Conduct site survey
 - Conduct interviews of facility personnel
 - Validate data
- Present a post-brief
 - Preliminary analysis and results
 - Next steps



Analysis

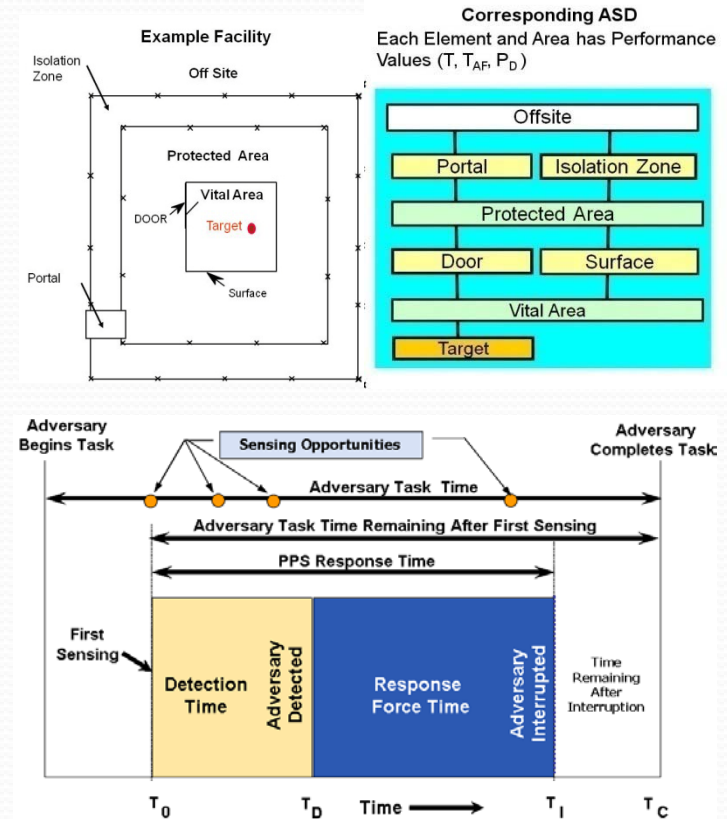
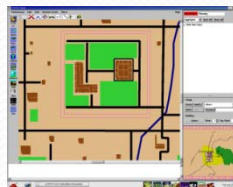
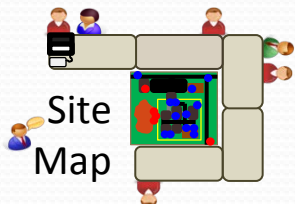
Analysis

- Assign Performance to PPS Elements: Subsystems and Site Features
 - Probability of detection and delay times
 - Response force effectiveness
 - Blast effects on personnel and structures
- Apply Analysis Methods
 - Path Analysis: Search for most-vulnerable paths
 - Scenario Analysis: Look at effectiveness against a range of credible attack scenarios

Some Analysis Tools

Analysis

- Path analysis
 - Adversary Sequence Diagram (ASD)
 - Protection element performance data
 - Adversary and PPS response timelines
 - Most-vulnerable paths
- Scenario analysis
 - Expert judgment
 - Scenario consistency analysis
 - Types of simulations
 - Tabletop analysis
 - Computer simulations
 - Force-on-force exercises





Results

Results

- System effectiveness
- Element performance
- Impact of changes
- Performance against changing threat
- Identification of weaknesses and strengths



Application

Application

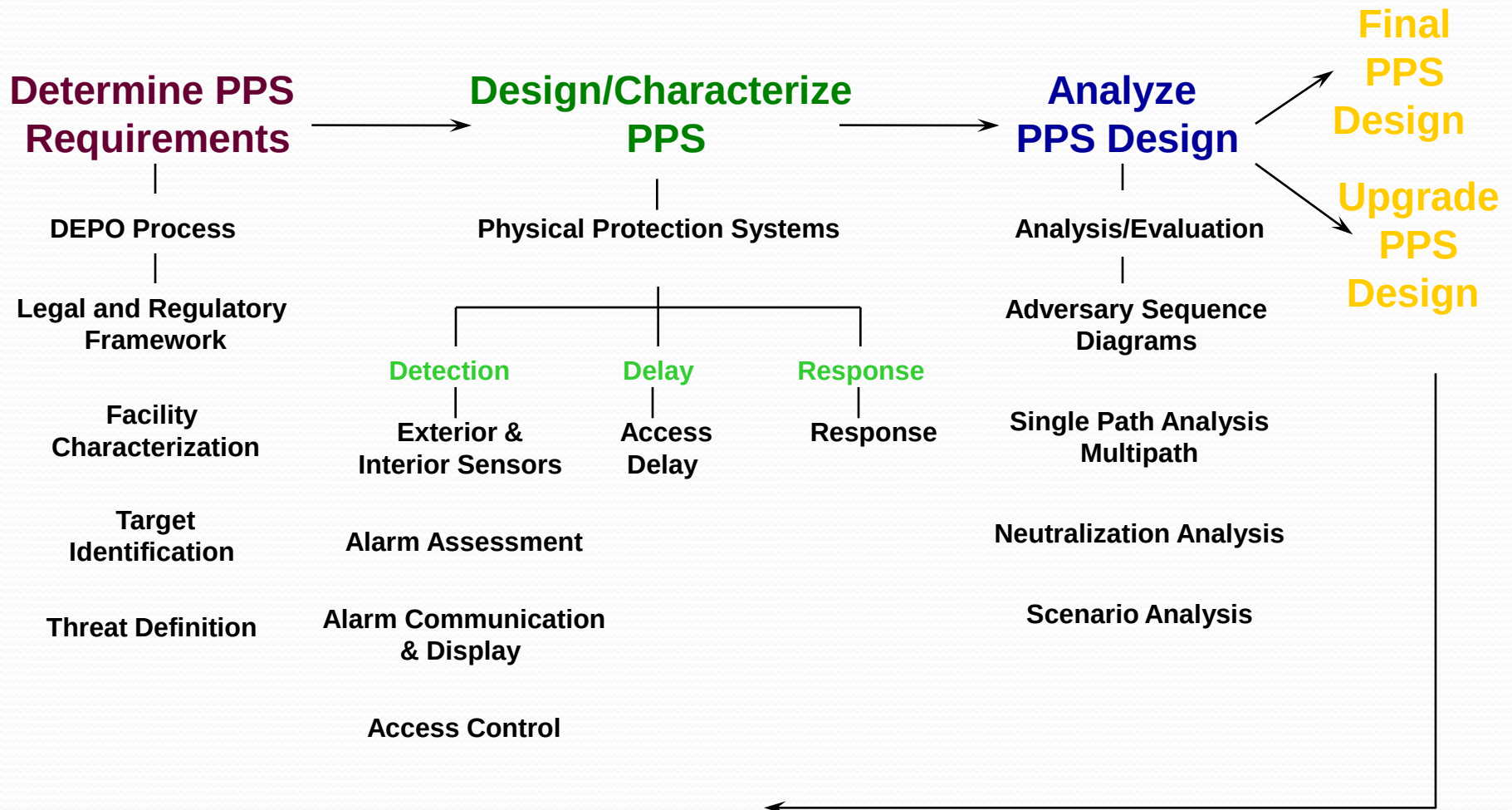
- Assess upgrade alternatives if required to optimize design
 - Policy changes
 - Procedural changes
 - Equipment changes
- Develop conclusions and recommendations
 - Accept existing system
 - Upgrade PPS
 - Eliminate targets
 - Mitigate consequences
- Prepare report

Relationship of VA to Security Risk

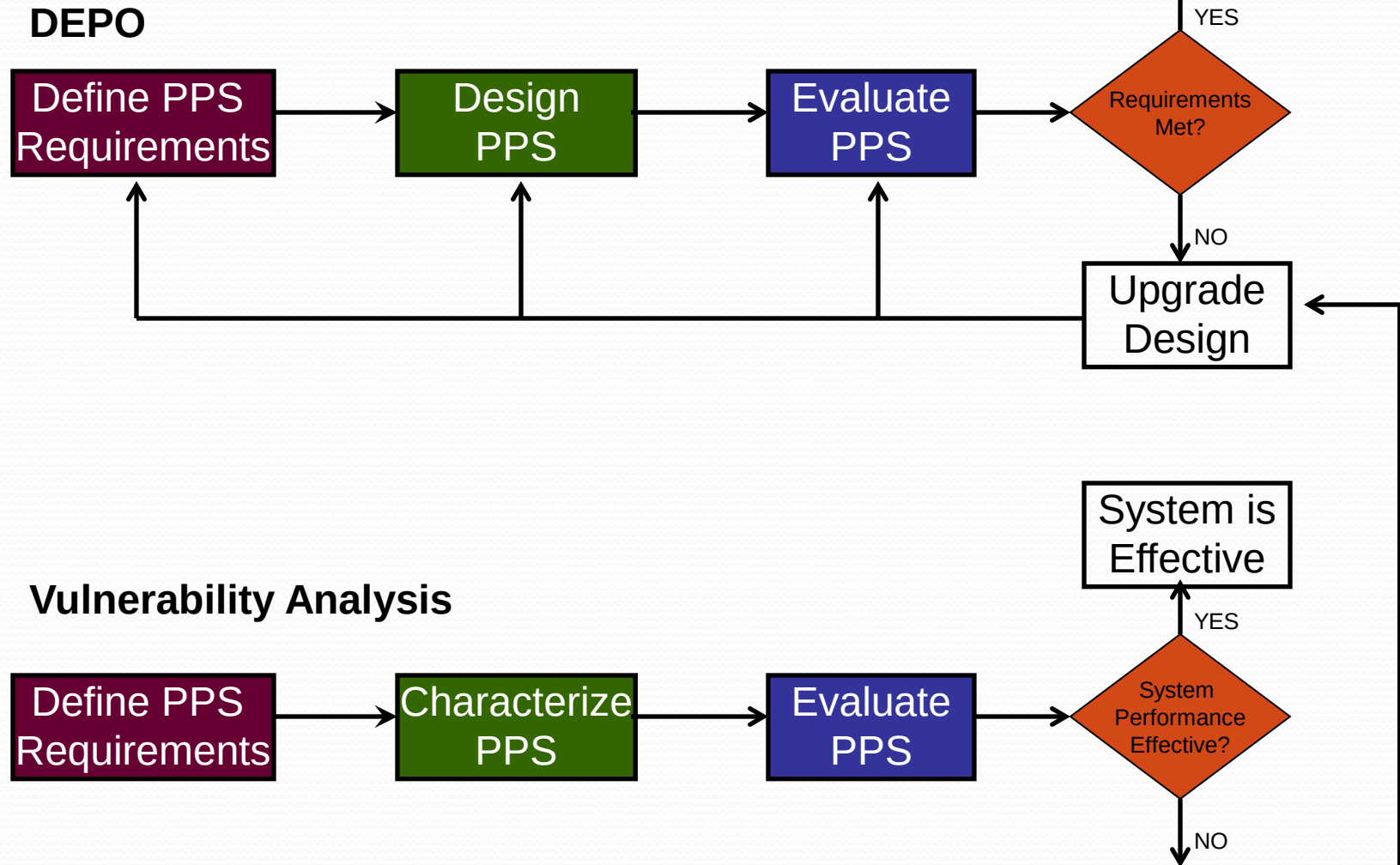
- Security risk is a function of
 - The threat – a measure of the likelihood of success of a malicious action by an adversary
 - The consequences – a measure of harm or loss that will occur if a successful malicious action takes place
 - The performance of the protection system in preventing the success of the malicious act in achieve undesired consequences
- VA can be used to measure the performance of the protection system



Design and Evaluation Process Outline (DEPO)



Relationship to DEPO



Summary

- All nuclear programs are subject to the risk of malicious acts of theft and sabotage.
- Physical protection specialists focus on identifying and implementing a PPS to maintain system effectiveness at an acceptable level.
- Vulnerability analysis is a structured process used to ensure that physical protection systems provide adequate protection.
- The VA process uses many of the concepts that were taught in the DEPO methodology.



Planning a VA

Module 3

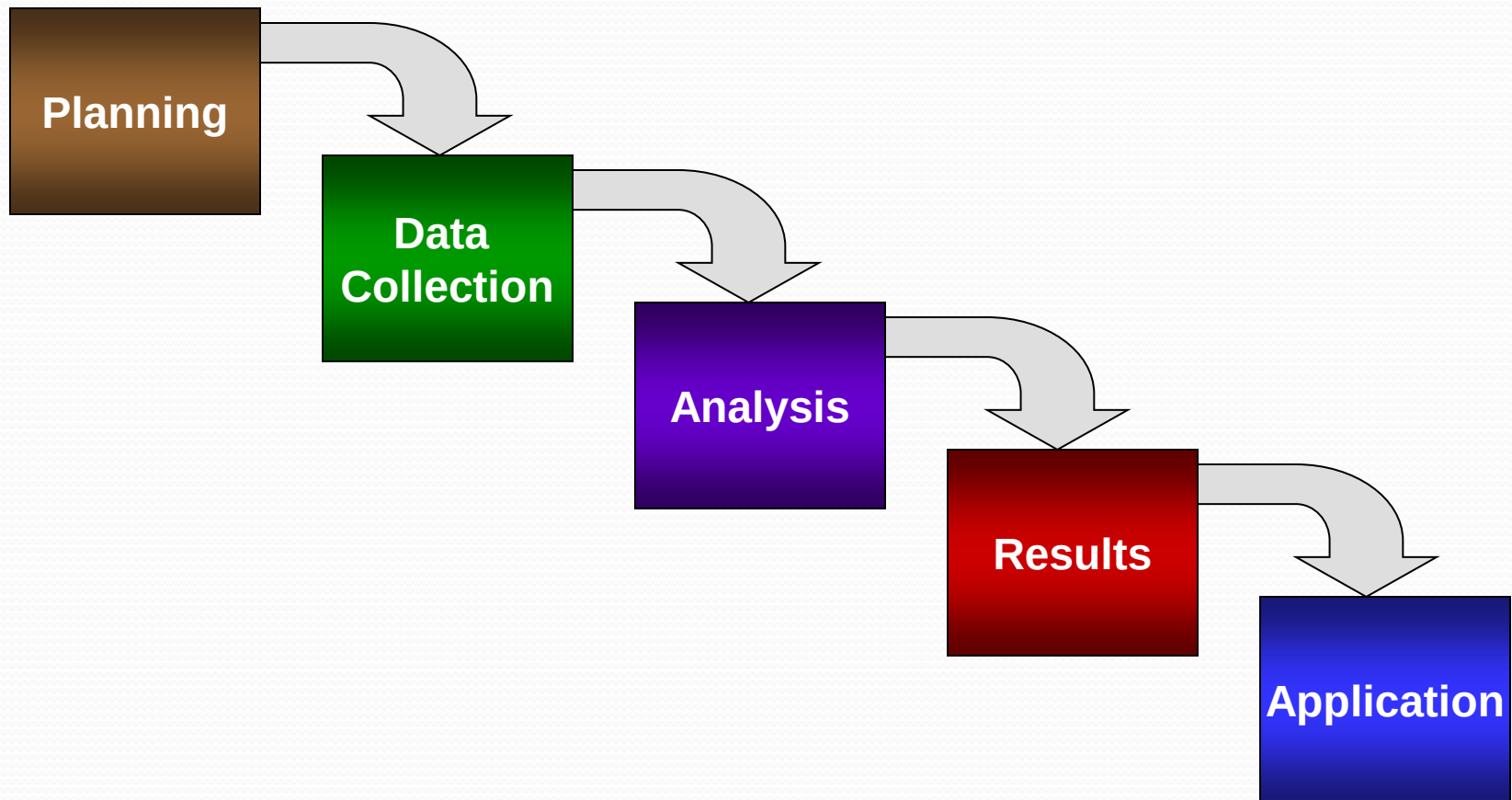
Vulnerability Analysis Training Course
Date:

Student Learning Objectives

At the end of this module, you will be able to:

- Discuss components of planning and managing a VA project
- Discuss the products of the VA planning phase

Phases of Vulnerability Analysis





Planning Considerations

Planning

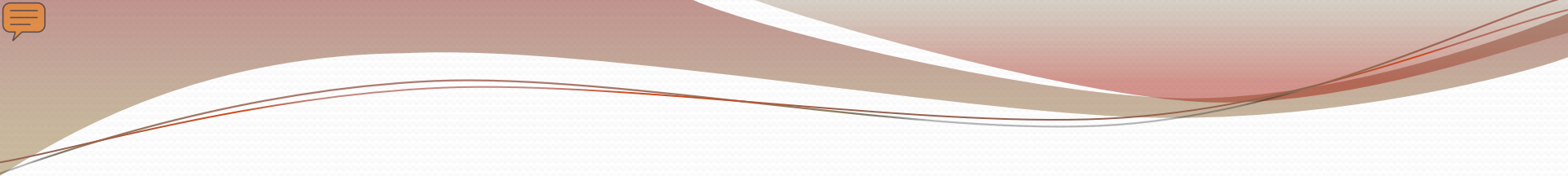
- VA purpose (reason for performing a VA)
- Type of VA
- Metrics and analysis tools to be applied
- Stakeholders/team composition
- Scoping agreement
- Scheduling and budget
- Access to facility and documentation
- Constraints
- Information protection
- Site survey preparation

VA Purpose

- A VA should only be conducted to answer a specific question or address a specific problem, such as:
 - What are the strengths and weaknesses in my PPS?
 - The material or production process at my facility has changed. What are the impacts on the PPS effectiveness?
 - What is the performance of the system against a new threat or revised DBT?
 - The facility has changed; is the PPS still effective?
 - The capabilities of the response force have changed; is the PPS still effective?

Type of VA

- Specified threat or threat spectrum
- System element performance or system performance
- Qualitative or quantitative
- Analysis conducted by an internal vs. external group



Metrics and Analysis Tools

Metrics

- P_I = Probability of interruption
- P_N = Probability of neutralization
- P_E = Probability of physical protection system effectiveness
- Others, such as
 - Probability of Detection
 - PPS Response Time
 - Delay Time

Analysis Tools

- Path analysis
- Scenario analysis
- Table top analysis
- Computer models
- Force-on-force exercises



Stakeholders

Stakeholder: Anyone who can affect the success of a VA.

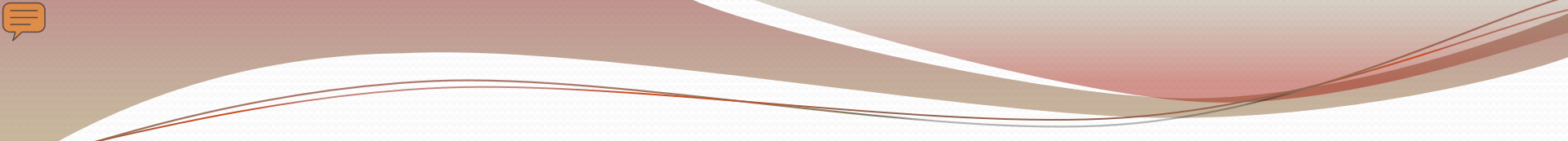
- Competent authority
- Facility operations manager
- Site security manager
- Response force manager
- Guard force manager
- Site safety manager
- Site vulnerability analysts



Obtain Management Commitment

Management responsibilities

- Agree to the schedule
- Obtain necessary funding for the effort
- Concur with initial assumptions
- Participate in status reviews and decision making as necessary
- Support the VA results and negotiate the upgrades



VA Team Members

Example Core Responsibilities

- Team leader (physical protection specialist)
- Security system engineer
- VA analyst
- Operations representative
- Safety representative
- Response expert
- Access delay/explosives expert
- Site representative
- Alarm communication and display engineer
- Administrative support

Example Subject Matter Experts

- Material accountancy and control
- VA software specialist
- Threat specialist
- Safety representative
- Site/region security officer
- Security technicians
- Security force personnel
- Construction/structural engineer
- Information technology administrators
- Locksmith

Diversity is essential!

Team Composition

- Commensurate with facility size and complexity
- VA qualified/trained personnel to conduct a VA
- Relevant expertise
- Appropriately sized team with site liaison member

Team Skills

- Communication
- Project management/delegation
- Consequence evaluation
- Data collection
- Understanding of facility operations and critical functions
- Expert threat judgment
- Knowledge of security systems and technologies
- Working knowledge and experience with the analytic process
- Technical writing



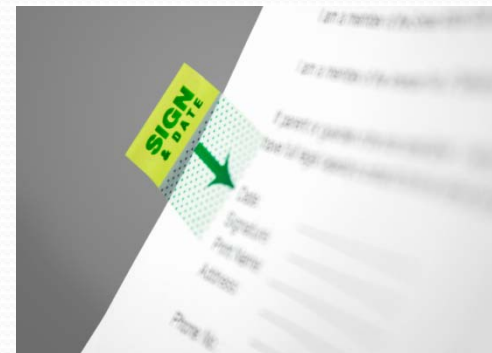


Scoping Agreement

- Is a contract amongst appropriate stakeholders that identifies the parameters of the VA
- Keeps a VA on track to meet the purpose, goals, and objectives and on schedule to meet necessary deliverables
- Maintains checks and balances throughout the VA and prevents scope creep

Scoping Agreement (Cont'd)

- VA goal
 - Should the analysis cover a full system or is the scope limited to portions of the system?
- VA requirements
 - Define resources needed and expected output
- Scope
 - Specifies what the VA will cover and not cover and any limitations on the analysis
- Protection requirements





Scoping Agreement (Cont'd)

- Parameters consist of:
 - Requirements clearly defined
 - DBT statement
 - Facility characterization
 - Target identification (type of targets)
 - Identify credible SMEs for attack planning
 - Types of attack and numbers of scenarios (sabotage/-theft)
 - Identify and agree on assumptions
 - Determine type of Insider (passive/active, etc.)
 - Memorandum of Understanding with government
 - Review security posture
 - Determine picture-in-time
 - Agree on simulation tools and the process for using them



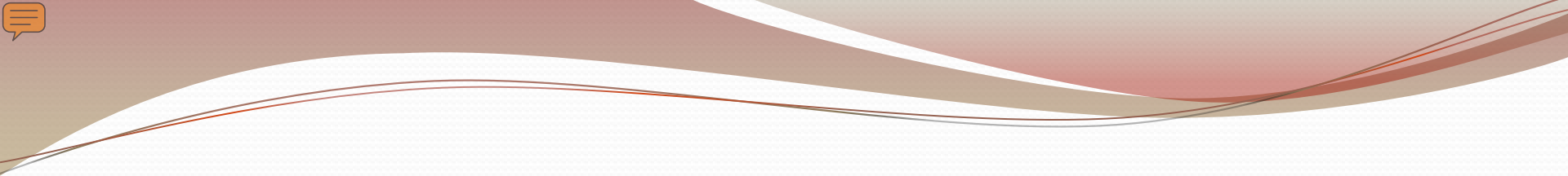
Scheduling and Budget

Scheduling

- Total duration
- Site visits
- Briefings
- Status reporting

Budget

- Planning
- Data review
- Site visits
- Analysis
- Reporting
 - Status reports
 - Final report



Access to Documentation and Facility

Documentation

- PPS design documentation
- PPS performance data
 - Sensor logs
 - On-site testing
 - Maintenance logs
- Contingency and emergency plans
- Previous VA(s)
- Other documentation

Facility Access

- Outside the perimeter
- Badge or visitors office
- Site entrance
- Within the perimeter
- Inside the site
- All buildings within the site

Analysis is only as good as the input received



Constraints

- Limits on threat
- Limits on system
- Limits on access
- Time/budget limits
- Data availability



Information Protection

- Protection of documentation
 - Data received
 - Analysis results
 - Reports
- Classification guidance
 - Protection level required
 - Proper markings on documents, hardcopy, and electronic media
 - Storage requirements
 - Handling and destruction guidelines
- Who can have access?



Planning Products

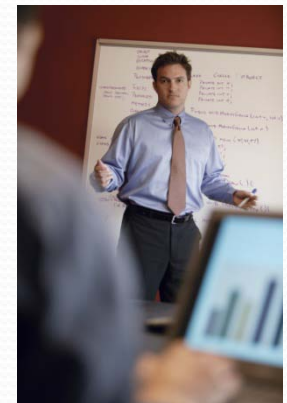
- Scoping agreement between VA team and sponsor
- Site visit kick-off meeting including scoping briefing
 - Purpose is to reach an understanding and general agreement on the scope of the VA and major assumptions
 - Should be presented to all VA stakeholders and customers
 - Ensures that all parties concur with the VA process
- VA team guide
- VA classification guide

Site Survey Preparation

- Review system design and facility documentation
- Identify protection elements
 - Detection
 - Delay
 - Response
- Site survey initial briefing
- Site survey plan

Site Survey Initial Briefing

- Introduction of participants
- Briefing on methodology and expected outcomes
- Briefing on site
 - PPS objectives
 - DBT
 - Materials and targets
 - Possible impact on site
 - Major assumptions
- Review of VA Project Plan
 - Budget and schedule
 - Preliminary data request
 - Status reporting
 - Document information protection control and procedures





Produce VA Team Guide

- Identify and describe the “picture in time” to be used for the evaluation
- Describe the schedule and expected levels of effort
- Identify guiding documents and processes for team use
- Identify critical interfaces and decision points
- Identify how dynamic events will be factored into the evaluation
- Define the process for resolution of questions and issues
- Define team activity documentation methods
- List team members and corresponding site contacts

Summary

- The planning phase provides the
 - VA scoping agreement between VA team and sponsor
 - Schedule and budget
 - VA team guide
 - Information protection guidance
- The planning phase ensures a common understanding of
 - VA objectives and expected outcomes
 - Schedule and budget
 - Site visit requirements



Subgroup Exercise 1:

Planning a VA of the Facility

- After reading the brief description of the facility, develop a plan for the VA team for the analysis on the facility
 - Why is the VA needed?
 - Define the scope
 - List requirements and goals
 - List of team members by expertise
 - Assign general responsibilities to each team member
 - Develop a preliminary schedule
 - Outline a scoping meeting and develop a scoping agreement



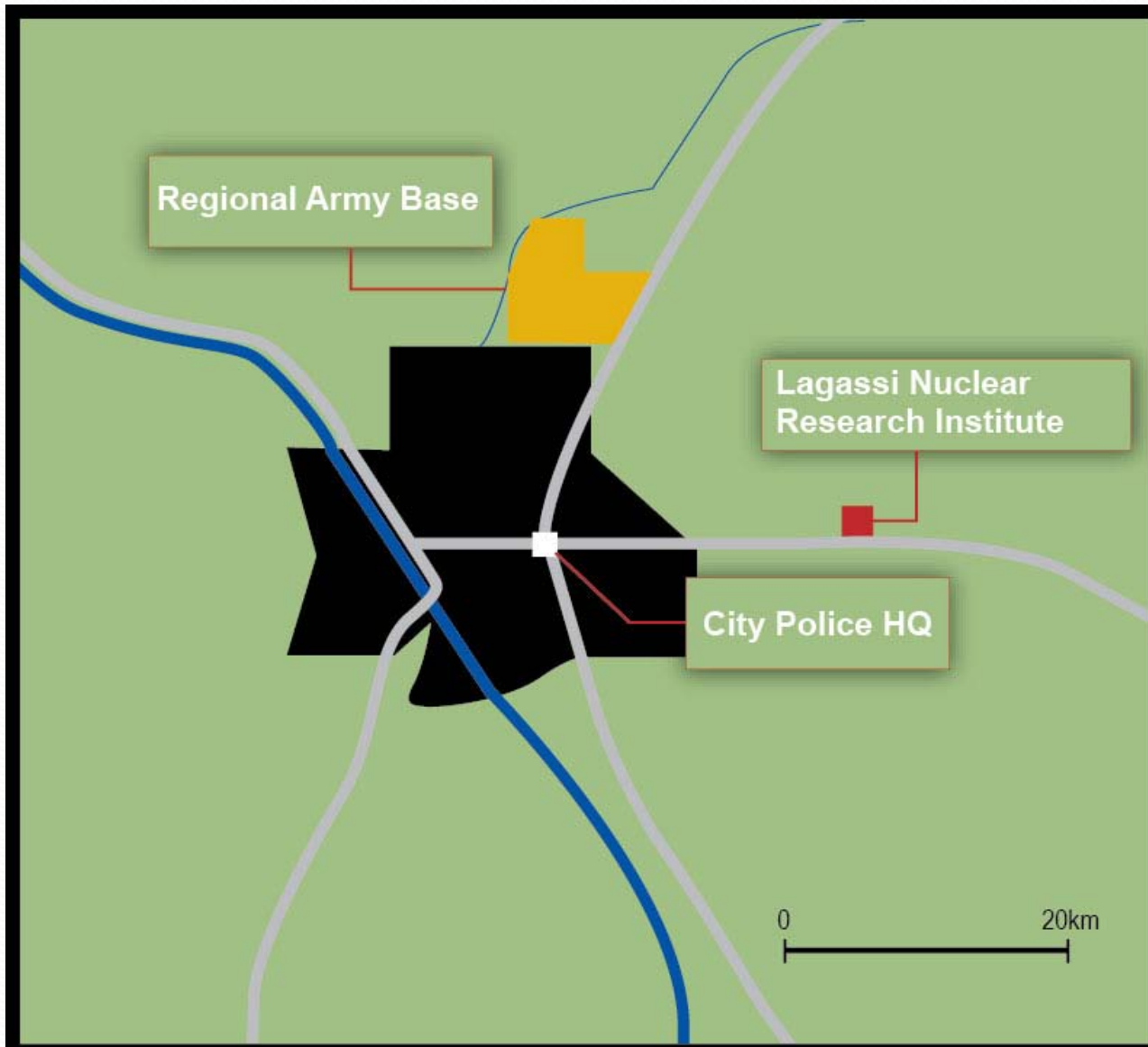
Introduction to the Lagassi Nuclear Research Institute (LNRI)

Module 3

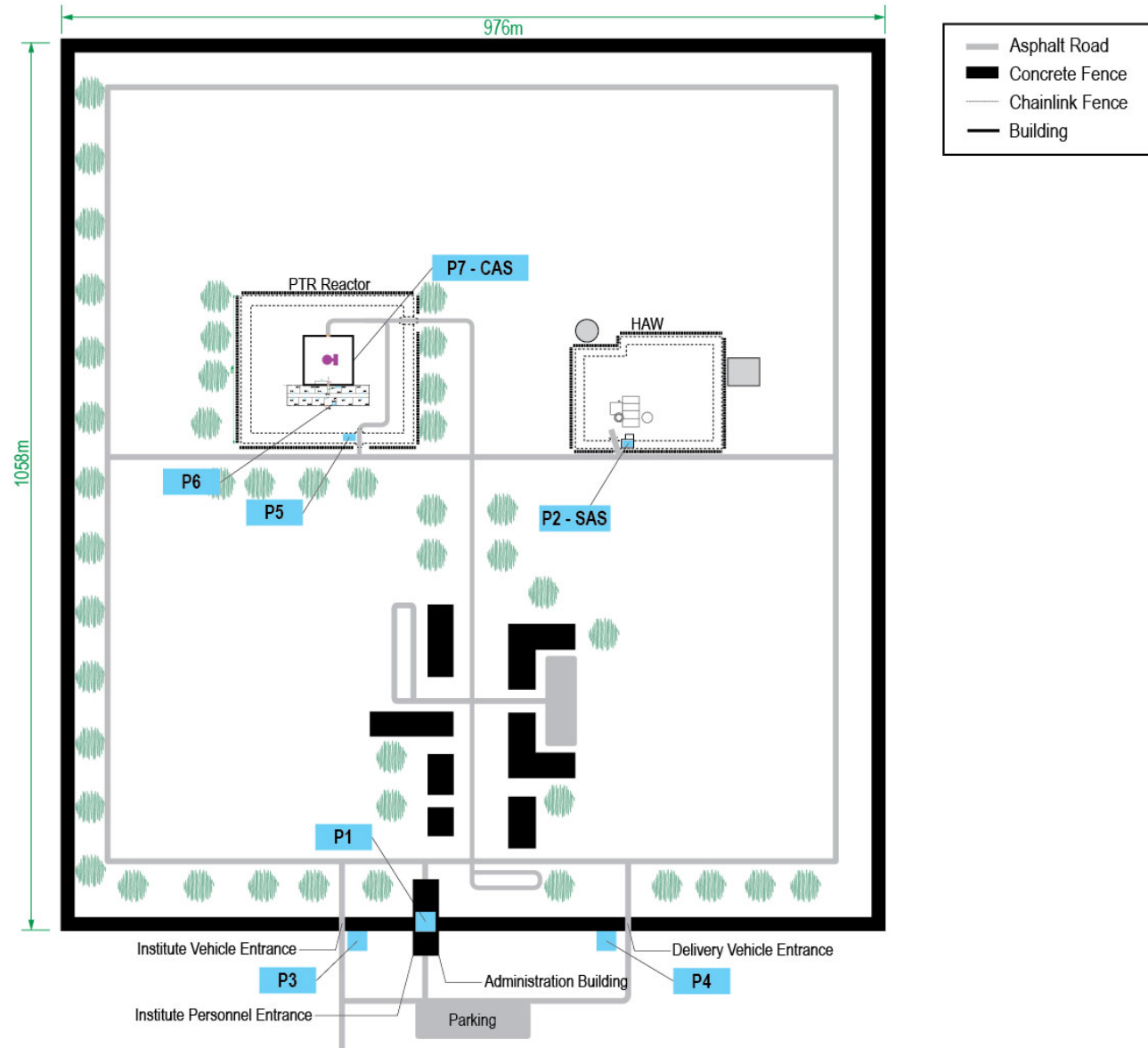
Vulnerability Analysis of Physical Protection Systems

Date:

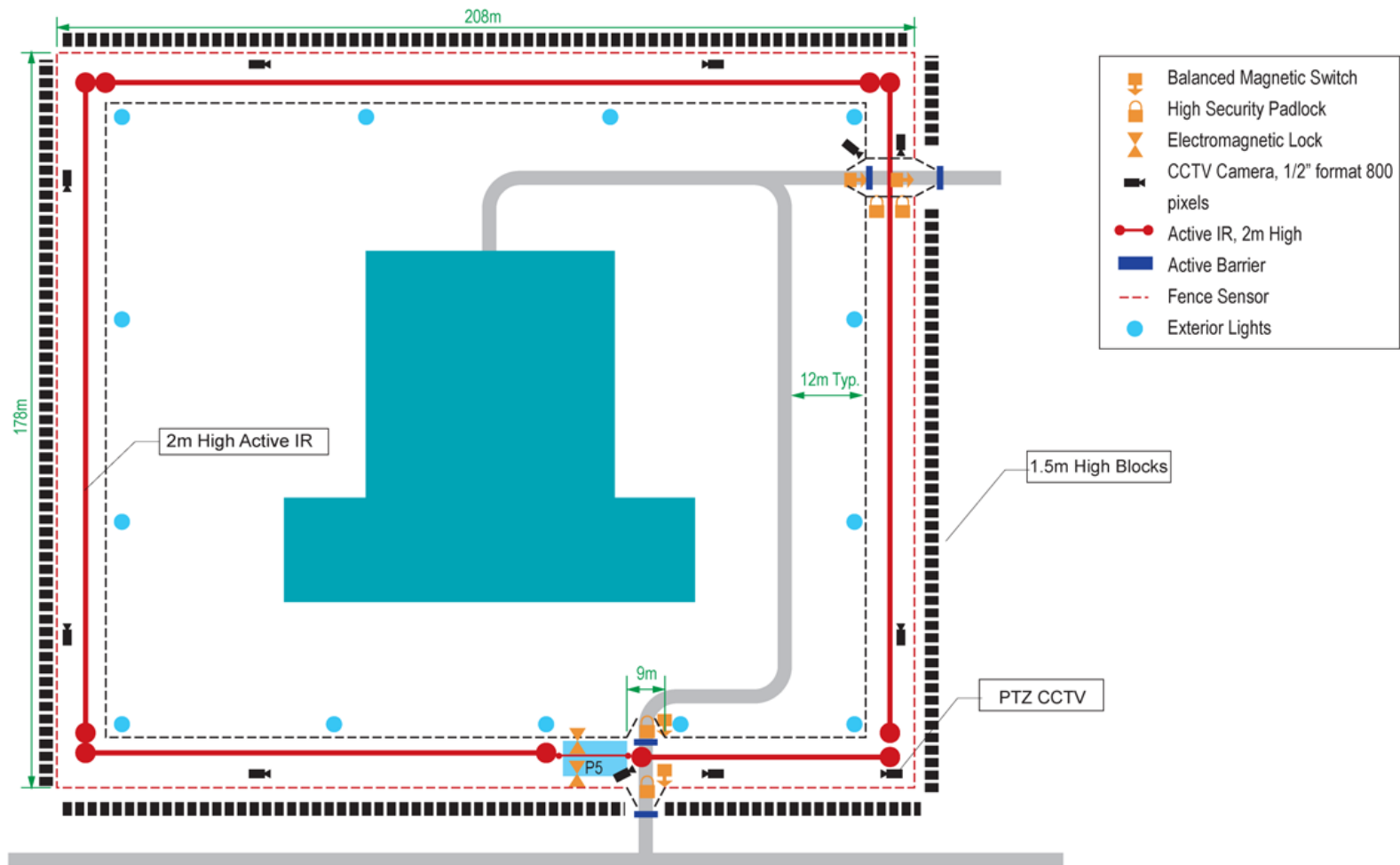
City of Hashbakar



LNRI Site Layout and Response Force Location

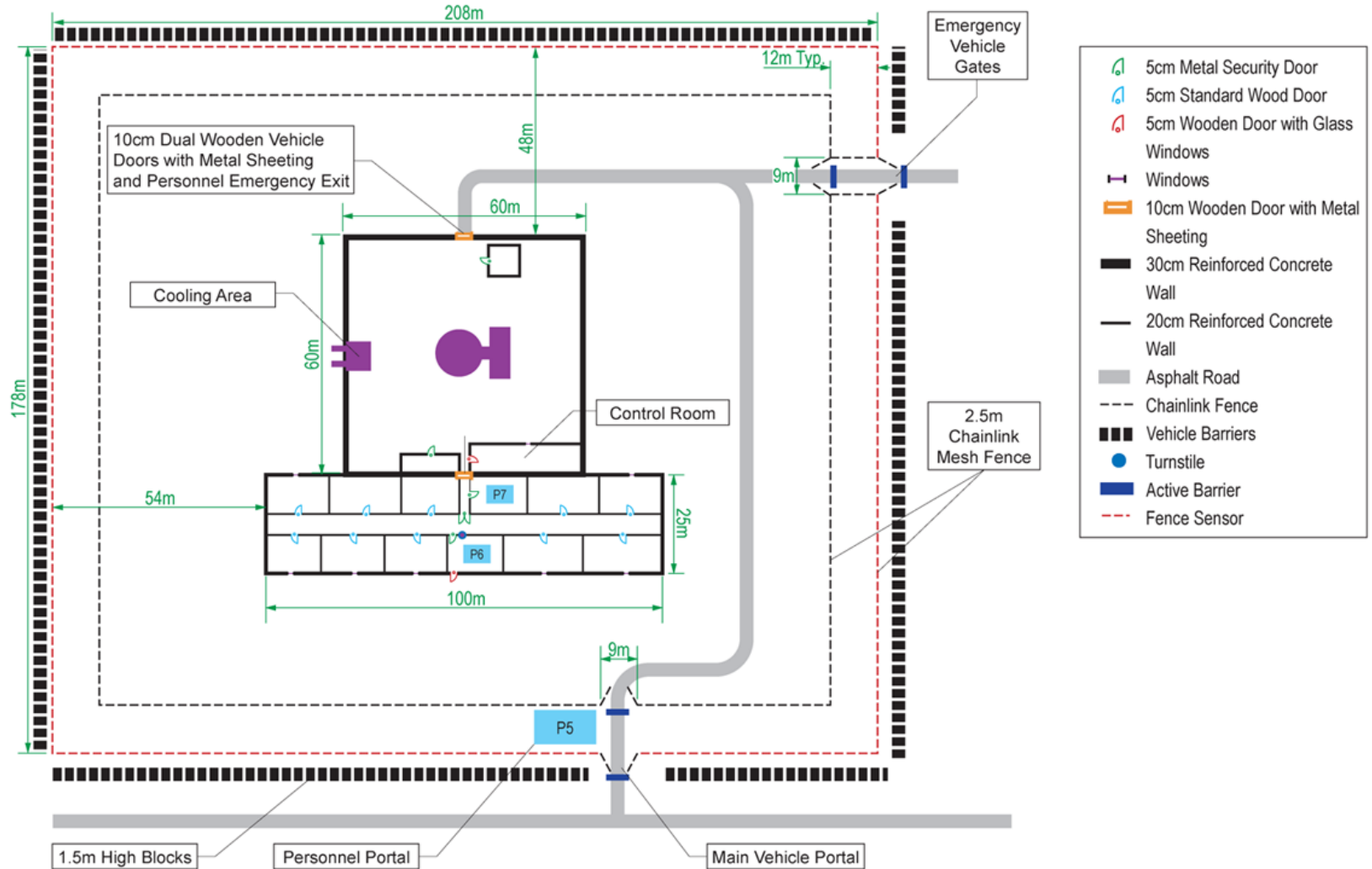


PTR Exterior Physical Protection Elements

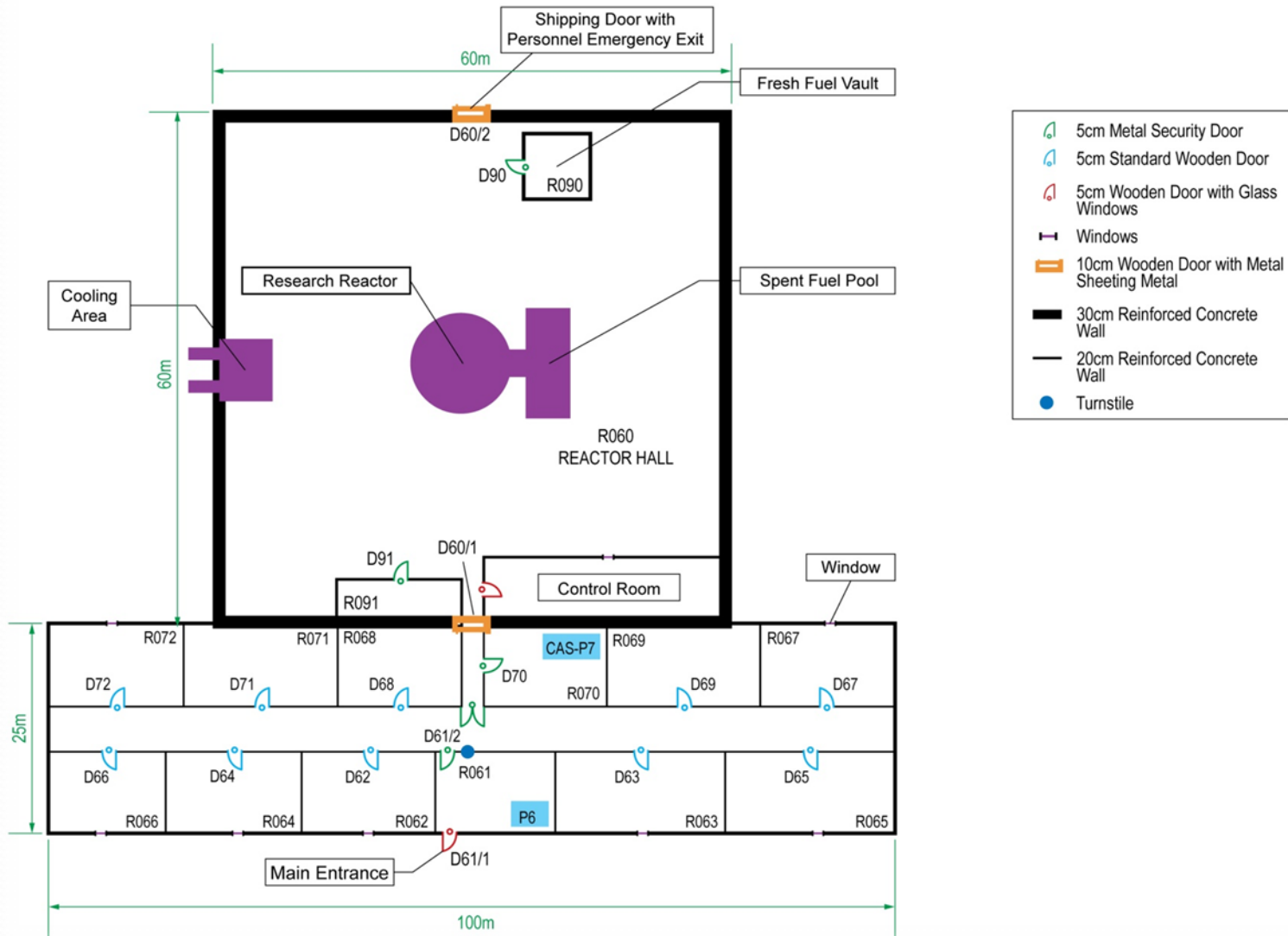


10 fixed exterior CCTV Cameras, 1 PTZ, mounted 4m high on 15cm tubular metal poles, no motion detection, 35mm lenses. There is exterior lighting on poles, 15m high. Lighting was designed to provide at least 10 lux with 6:1 light to dark ratio with the lighting covering at least 70% field of view.

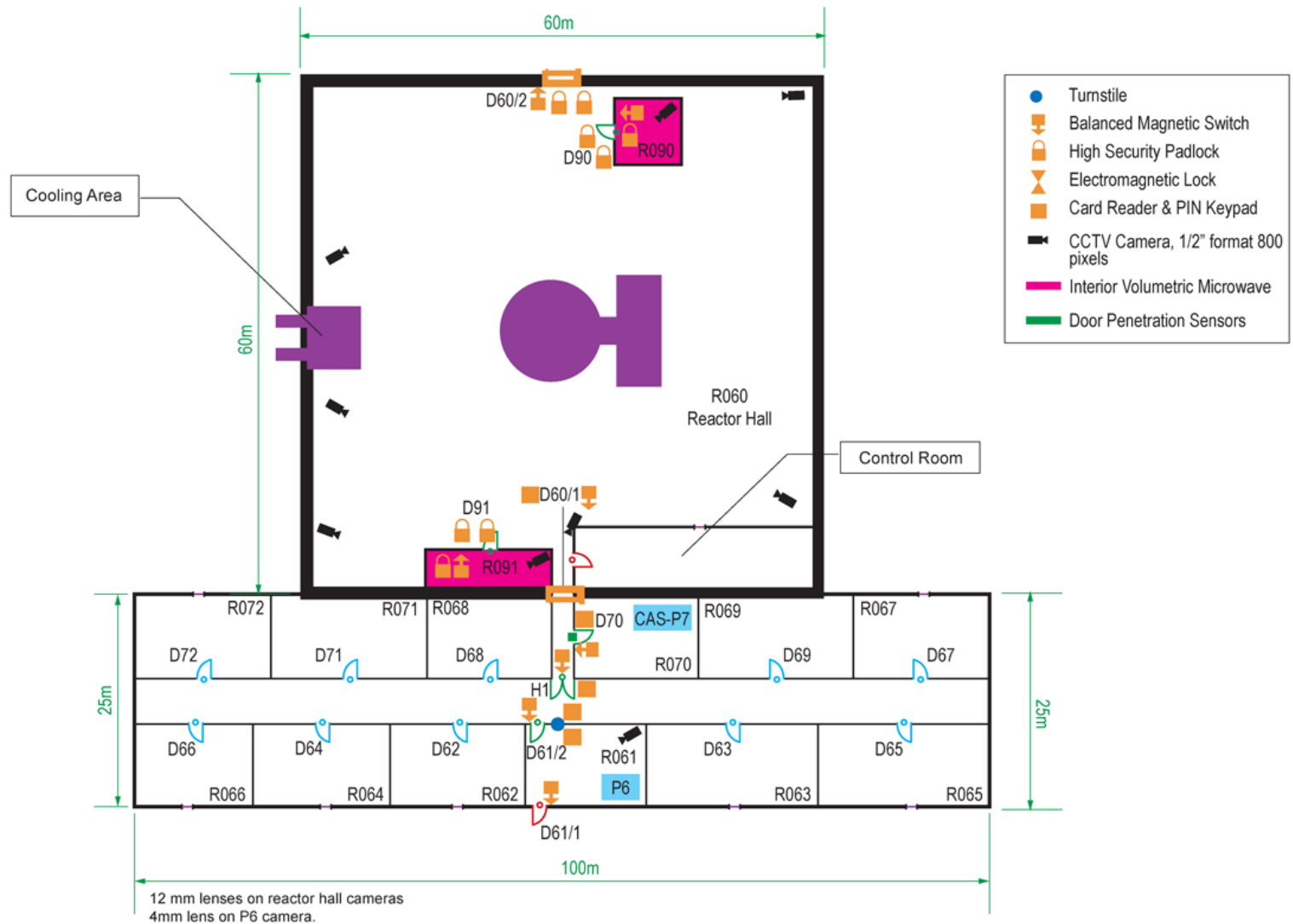
PTR Wall Thickness and Distances



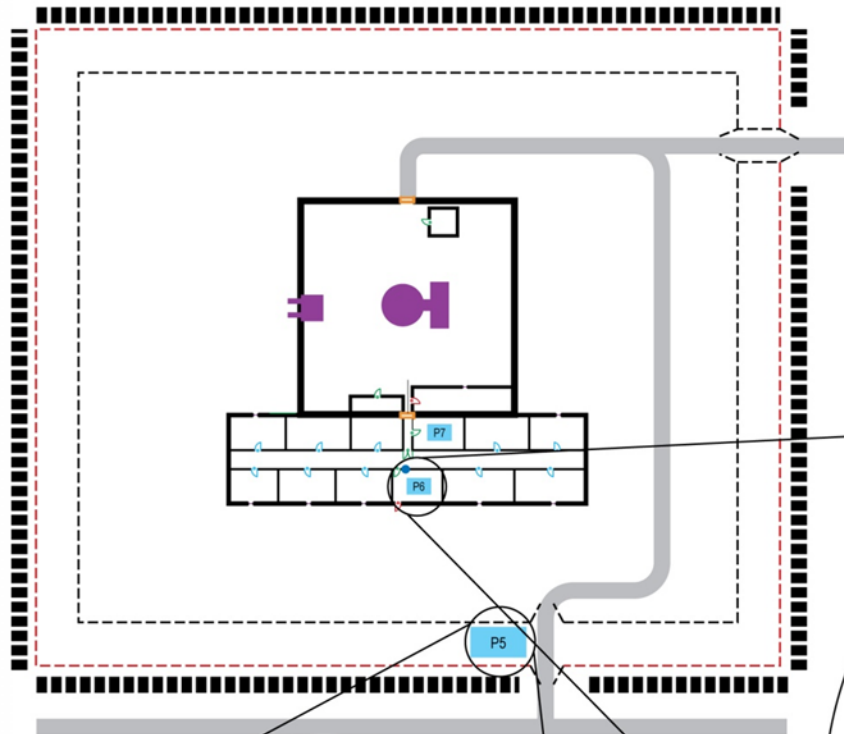
PTR Research Reactor Building Floor Plan



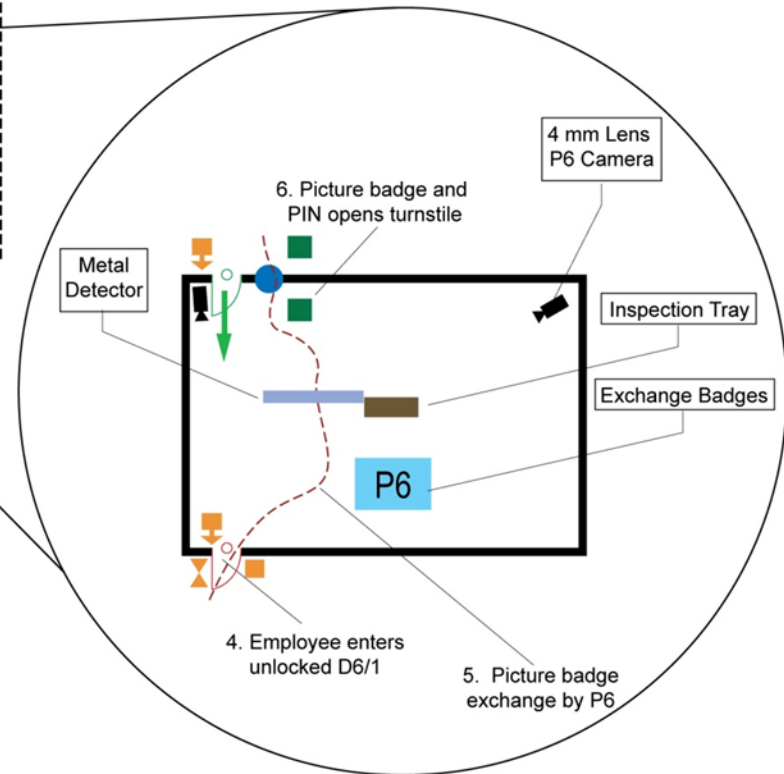
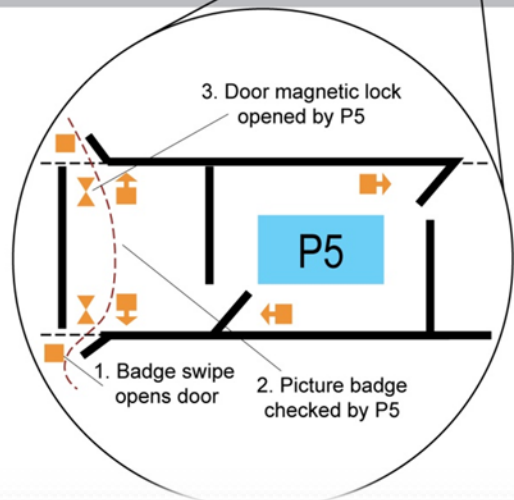
PTR Interior Physical Protection Elements



PTR Access Control Plan



-  Balance magnetic Switch
-  High Security Padlock
-  Electromagnetic Lock
-  Badge Swipe Reader
-  Card Reader and PIN Keypad
-  CCTV Camera 1/2" format 800 Pixels



3. Planning Exercise

Session Objectives

In this session, you will:

1. Decide on several planning variables found in a scoping agreement for a vulnerability analysis (VA) at the hypothetical facility.

Exercise 1 – Decide upon a number of planning variables found in a scoping agreement for a VA at the hypothetical facility.

As discussed in the lecture, a scoping agreement defines several planning aspects, including:

- o VA Sponsor: Who the VA is being conducted for.
- o Reason for Performing the VA: Specific question or problem to be answered by conducting the VA.
- o VA requirements: Defines resources needed and expected output.
- o Scope: Determines what the VA will cover and not cover and any limitations on the analysis.

Background: The Lagassi Nuclear Research Institute (LNRI) recently performed a significant security upgrade, including moving the Central Alarm Station, upgrading the protection features on the Protected Area at the PTR Reactor, and detection and delay features within the PTR Reactor Building.

The Lagassi Atomic Energy Ministry (LAEM) is the competent authority for the Republic of Lagassi. The LAEM has required that LNRI submit a VA. The LNRI, in turn, has contracted with your organization to perform an independent VA for the LNRI to submit to the LAEM.

Other information: The LNRI is structured as a corporation, with 51% of its stock held by the LAEM. Under Republic of Lagassi national regulations, armed response is the responsibility of the police and national military.

Given this background information, answer the following questions:

- o Who is the VA Sponsor?

- o Is this an internal or external analysis as defined in the lecture?

- o Define a list of possible stakeholders for the VA:

- o Discuss some possible procedures that might be used to protect information used and generated during the VA.

- o Brainstorm two possible purposes for conducting the VA?

1)

2)

Choose one of these possible purposes as the “true” purpose for conducting the VA and use it to define the following planning information:

- o Resource Requirements: Given the purpose you have selected, brainstorm team members that you think are necessary for your VA team, determine their areas of expertise, and specify whether they come from your organization or the LNRI. This list need not be complete at this time as you will need more information about the site to finalize this list.

Job Title	Expertise	From LNRI (Yes/No)

- o Brainstorm the scope of the VA, determining what the VA will cover and not cover and any limitations on the analysis.

The VA will cover:

The VA will not cover:

Limitations on the analysis (if any) that you can determine at this time:

- o List some documents that might be reviewed in preparing the VA

Comparing both of the possible purposes you identified for performing the VA, answer the following questions:

- o Discuss how scheduling and budget requirements may differ depending upon which of the two purposes is chosen as the actual purpose for the VA.

- o Discuss how requirements for preliminary documentation may differ depending upon which of the two purposes is chosen as the actual purpose for the VA.

3. Planning Exercise

SOLUTIONS

Session Objectives

In this session, you will:

1. Decide on several planning variables found in a scoping agreement for a vulnerability analysis (VA) at the hypothetical facility.

Exercise 1 – Decide upon a number of planning variables found in a scoping agreement for a VA at the hypothetical facility.

As discussed in the lecture, a scope agreement defines several planning aspects, including:

- o VA Sponsor: Who the VA is being conducted for.
- o Reason for Performing the VA: Specific question or problem to be answered by conducting the VA.
- o VA requirements: Defines resources needed and expected output.
- o Scope: Determines what the VA will cover and not cover and any limitations on the analysis.

Background: The Lagassi Nuclear Research Institute (LNRI) recently performed a significant security upgrade, including moving the Central Alarm Station, upgrading the protection features on the Protected Area at the PTR Reactor, and detection and delay features within the PTR Reactor Building.

The Lagassi Atomic Energy Ministry (LAEM) is the competent authority for the Republic of Lagassi. The LAEM has required that LNRI submit a VA. The LNRI, in turn, has contracted with your organization to perform an independent VA for the LNRI to submit to the LAEM.

Other information: The LNRI is structured as a corporation, with 51% of its stock held by the LAEM. Under Republic of Lagassi national regulations, armed response is the responsibility of the police and national military.

Given this background information, answer the following questions:

- o Who is the VA Sponsor?

Institute (whomever signs the contract to do the assessment)

- o Is this an internal or external analysis as defined in the lecture?

External

- o Define a list of possible stakeholders for the VA:

Institute, Police, military, many others that the students might identify.

- o Discuss some possible procedures that might be used to protect information used and generated during the VA.

Discussions may include: Background checks, policies and procedures for protecting information, information markings and policy and procedures for protection.

- o Brainstorm two possible purposes for conducting the VA?

- 1) Demonstrating the effectiveness of the system after the upgrades (new baseline)

- 2) Comparing the effectiveness of the old system against the upgrade (what was the change in performance between the old and new system)?

These are given as two examples to fill out the rest; students answers may differ.

Choose one of these possible purposes as the “true” purpose for conducting the VA and use it to define the following planning information:

- o Resource Requirements: Given the purpose you have selected, brainstorm team members that you think are necessary for your VA team, determine their expertise, and specify whether they come from your organization or the LNRI. This list need not be complete at this time, as you will need more information about the site to finalize this list.

Job Title	Expertise	From LNRI (Yes/No)
	Depends on purpose	

- o Brainstorm the scope of the VA, determining what the VA will cover and not cover and any limitations on the analysis.

The VA will cover:

Depends on purpose given.

The VA will not cover:

Depends on purpose given.

Limitations on the analysis (if any) that you can determine at this time:

Depends on purpose given.

- o List some documents that might be reviewed in preparing the VA

DBT, Response Force Plans, Facility Diagrams, etc.

Comparing both of the possible purposes you identified for performing the VA, answer the following questions:

- o Discuss how scheduling and budget requirements may differ depending upon which of the two purposes is chosen as the actual purpose for the VA.

If the VA compares the old and new systems then additional time and budget will be needed to investigate the old system performance through documentation.

- o Discuss how requirements for preliminary documentation may differ depending upon which of the two purposes is chosen as the actual purpose for the VA.

More documentation on the older system's effectiveness would be required if one were comparing old and new system performance.

VA Kick-off Briefing

Team #

Vulnerability Analysis of Physical Protection Systems

Date:

Introduction

VA Team

-
-
-
-
-
-
-

Site Team

-
-
-
-
-
-
-

VA Methodology/Approach

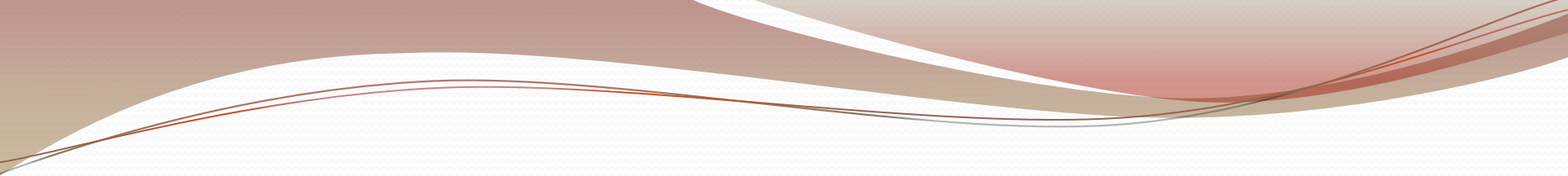
- Describe the approach you will be using to generate the expected outcomes
- Expected outcomes
 - Identify strengths and weaknesses in existing or planned protection systems
 - Ensure that systems provide balanced protection of assets
 - Determine the relative effectiveness of alternative protective strategies and systems
 - Support cost-benefit studies for system design alternatives

Site Briefing (Provided by Site)

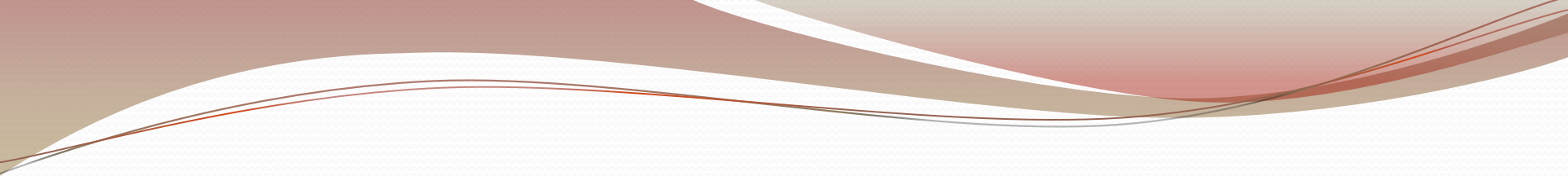
- PPS Objectives
- Design Basis Threat
- Materials and Targets
- Possible Impact to Site
- Major Assumptions

VA Project Plan

- Budget and Schedule
- Preliminary Data Request
- Status Reporting
- Documentation Control and Protection



Requested Documentation



Thank you!



Adversary Sequence Diagram (ASD) Model

Module 4

Vulnerability Analysis of Physical Protection Systems

Date:

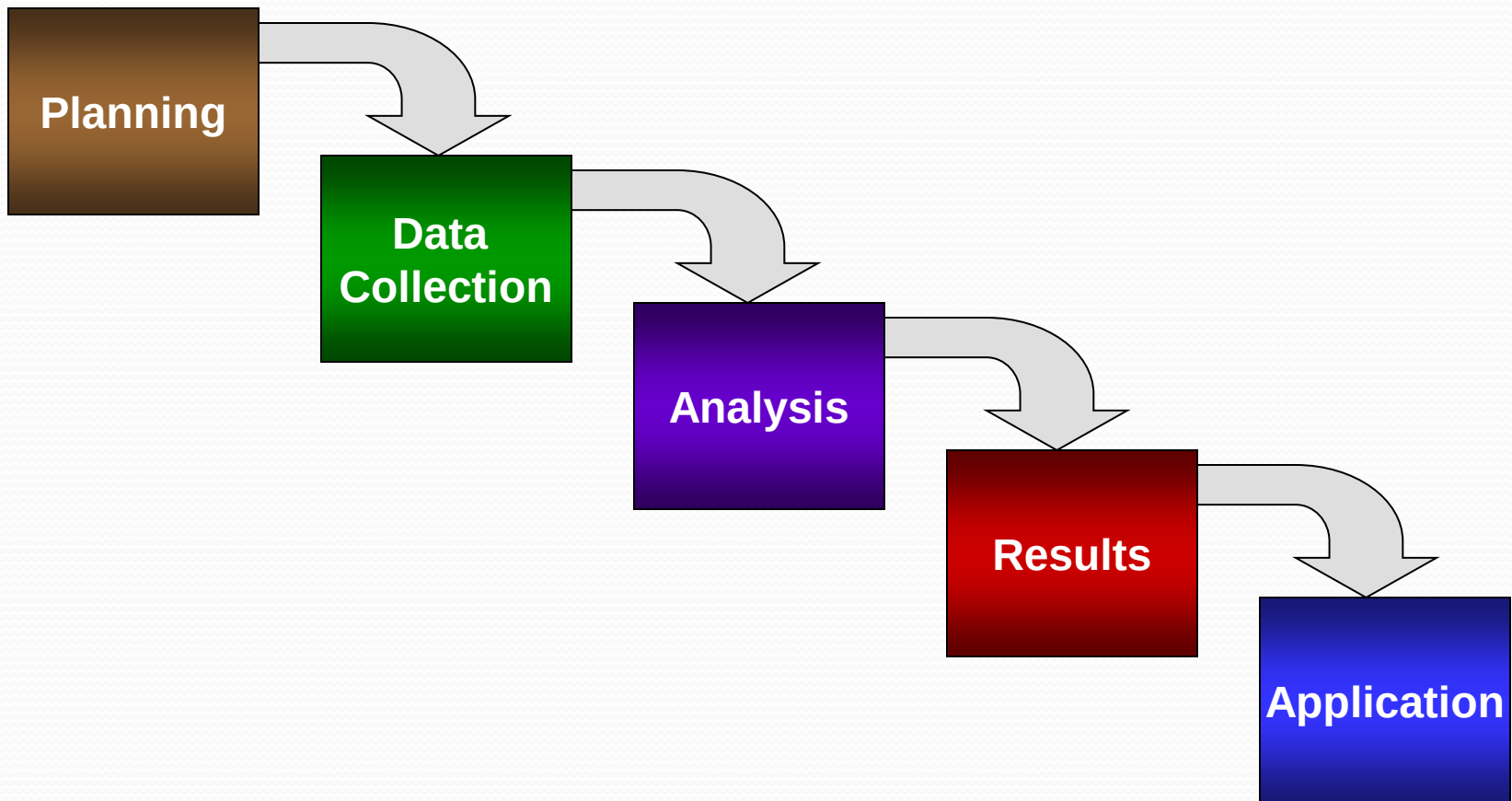


Student Learning Objectives

After completing this module, you should be able to:

- 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 three steps to use when developing an ASD
- Develop an ASD for an example facility

Phases of Vulnerability Analysis

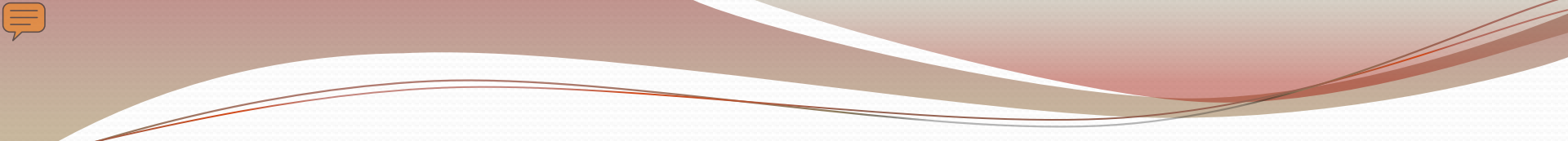




Adversary Sequence Diagram

Adversary Sequence Diagram (ASD): a graphical model used to help evaluate the effectiveness of the PPS at a facility

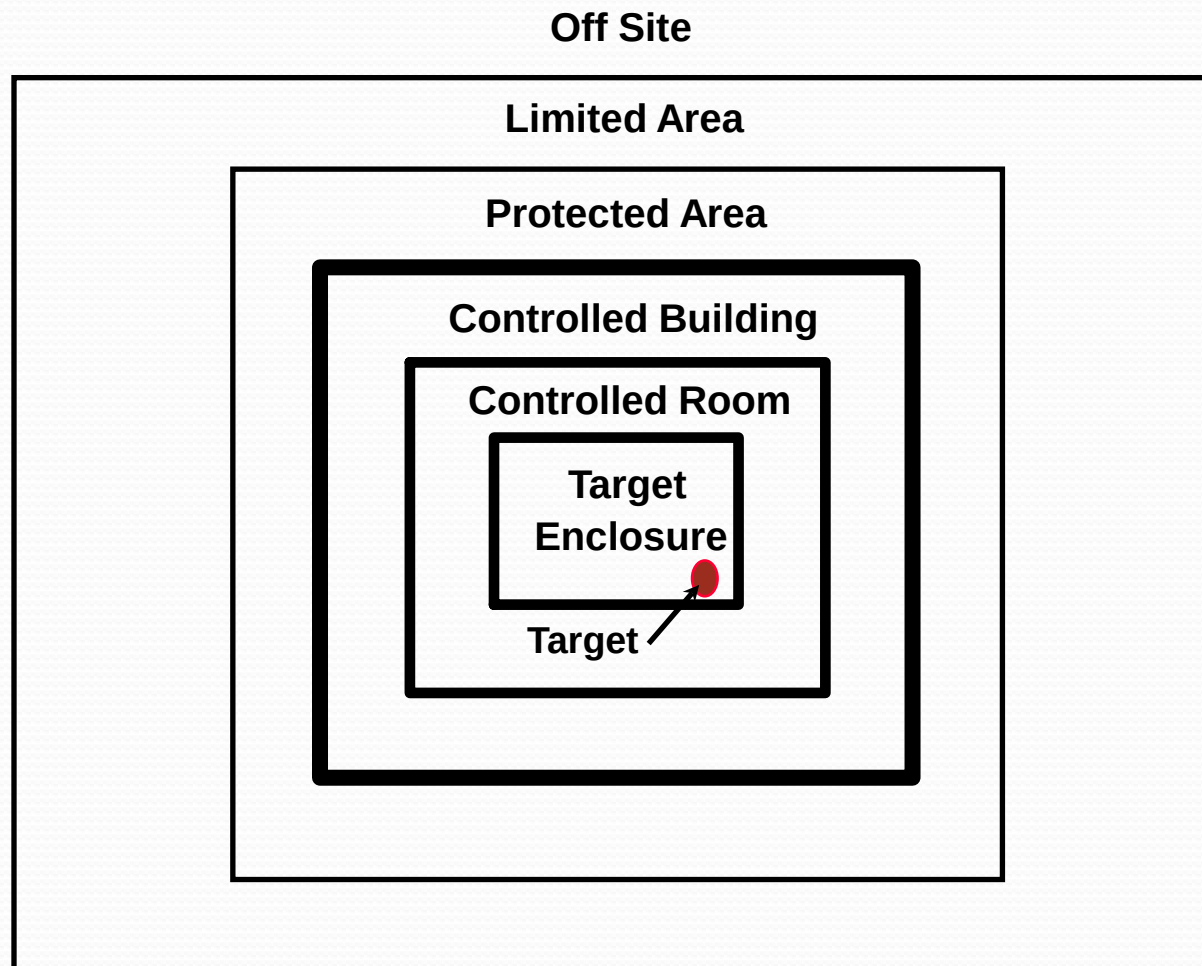
- ASD represents
 - Paths that adversaries can follow to accomplish sabotage or theft
 - PPS elements along paths
- ASD is used to determine the most-vulnerable path for specific PPS and threat



Three Steps to Create an Adversary Sequence Diagram

1. Model the facility by separating it into adjacent physical areas
2. Define protection layers in terms of path elements between areas
3. Assign probability of detection (P_D) and delay time (T) for each path element and physical area

Facility

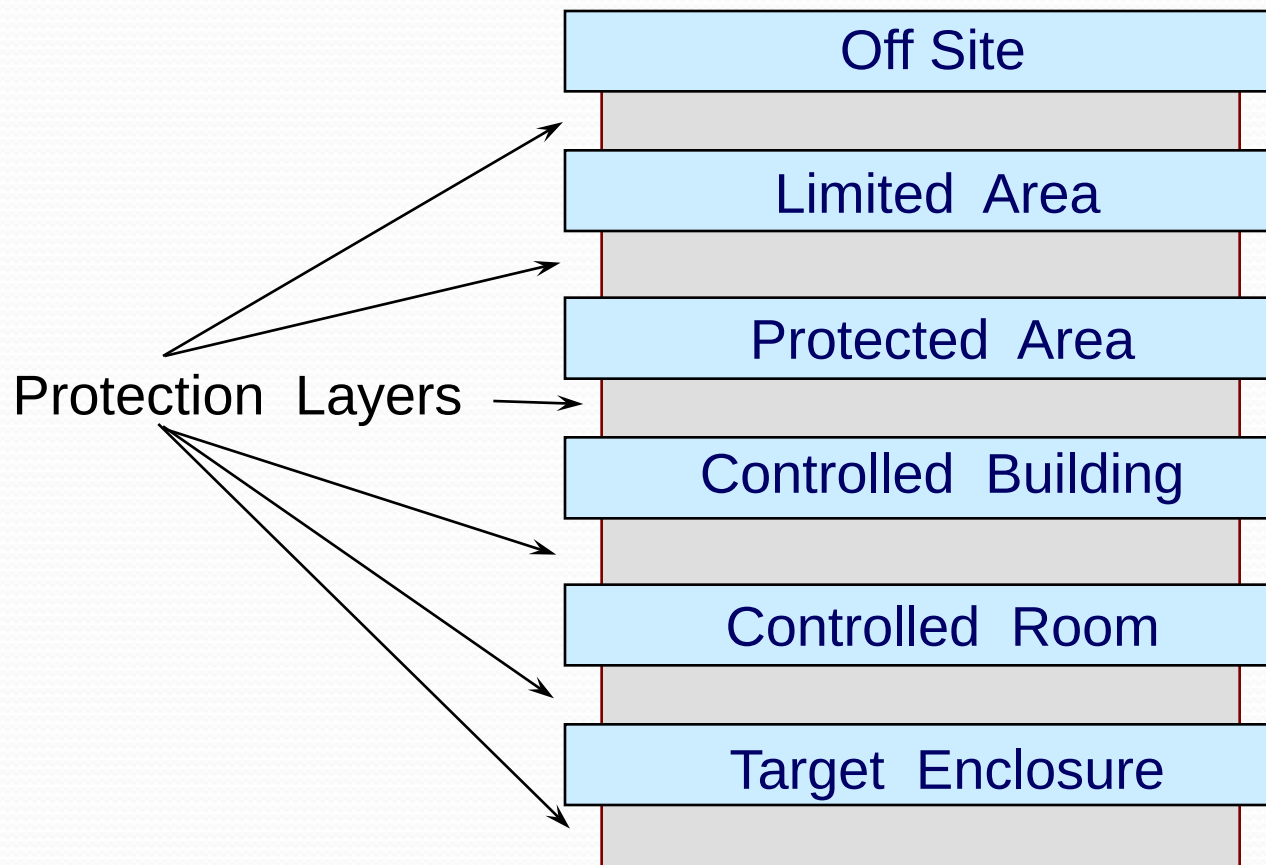




Step 1: Identify Physical Areas of Facility

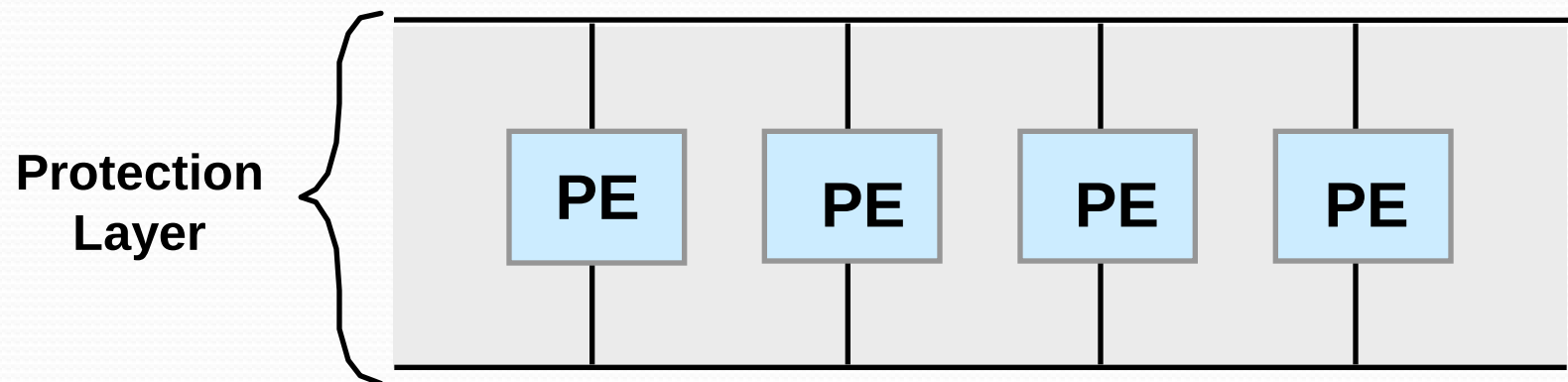
Off Site
Limited Area
Protected Area
Controlled Building
Controlled Room
Target Enclosure

Step 2: Define Protection Layers of Facility

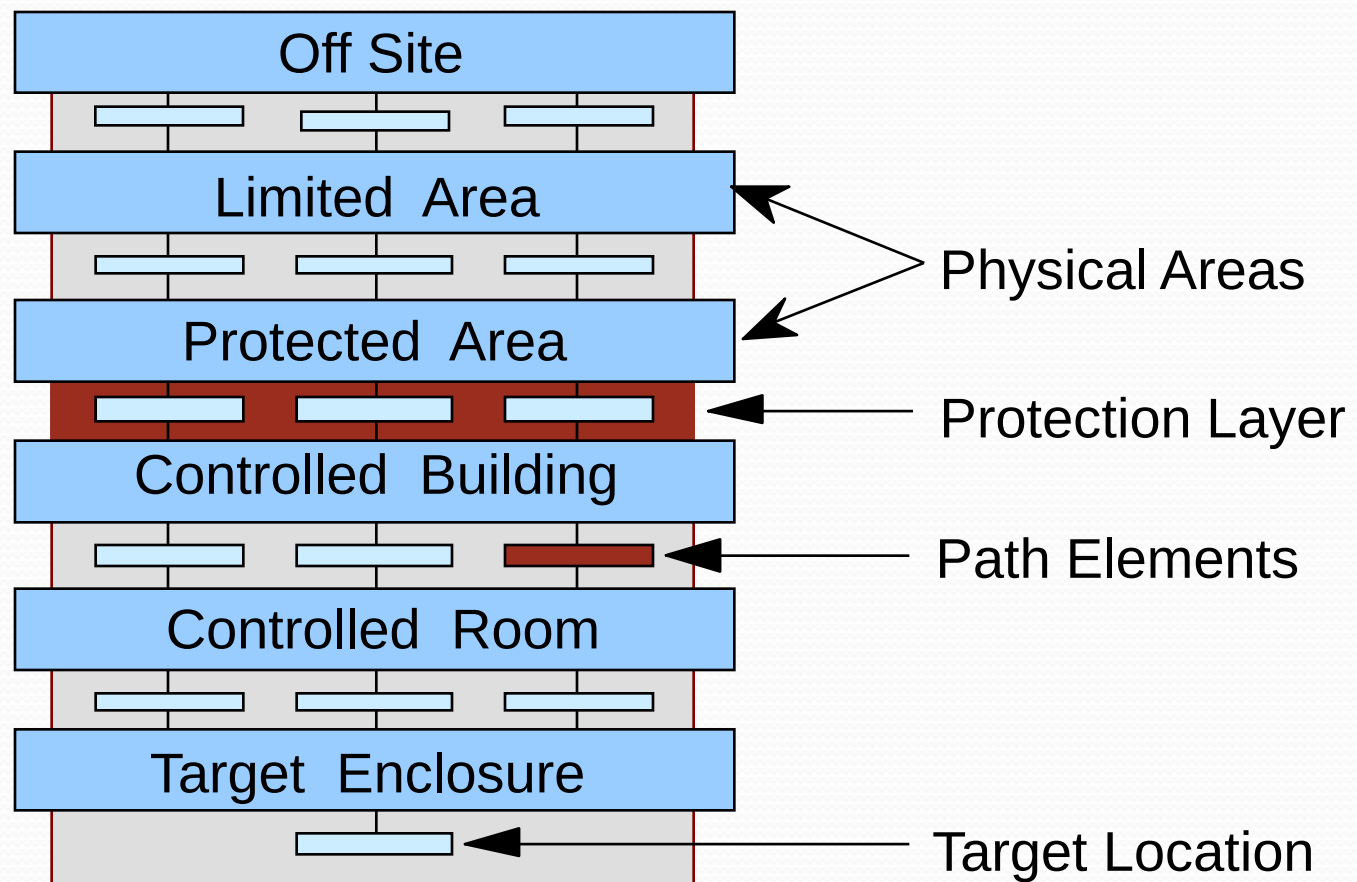


Step 2 (cont'd) : Identify Path Elements

- Each protection layer forms a security barrier that separates two physical areas
- ***Path element(PE)***: any distinct part of the protection layer separating two physical areas
- An adversary must pass over, under, around or through a PE to move between adjacent physical areas

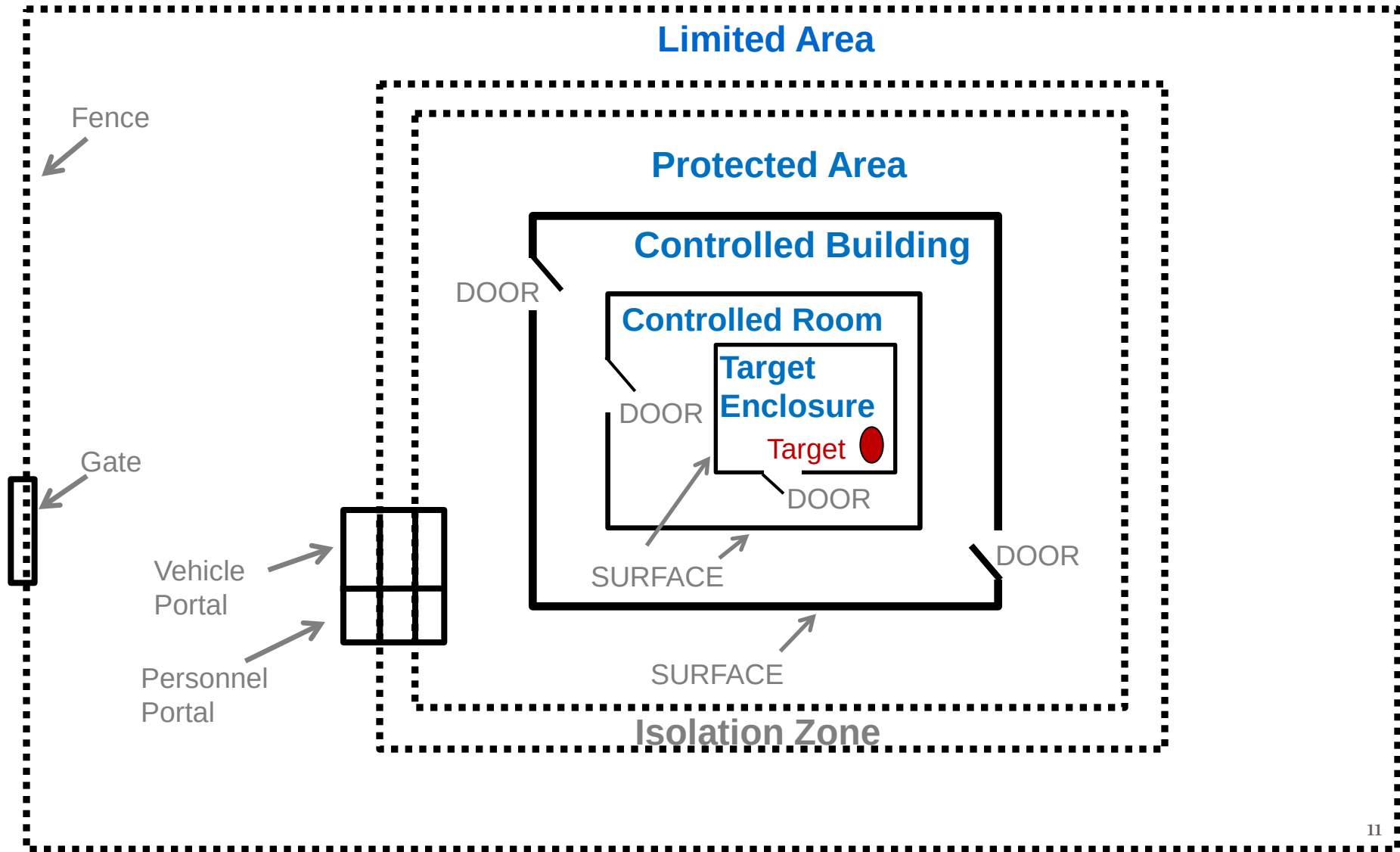


Concept of Adversary Sequence Diagram

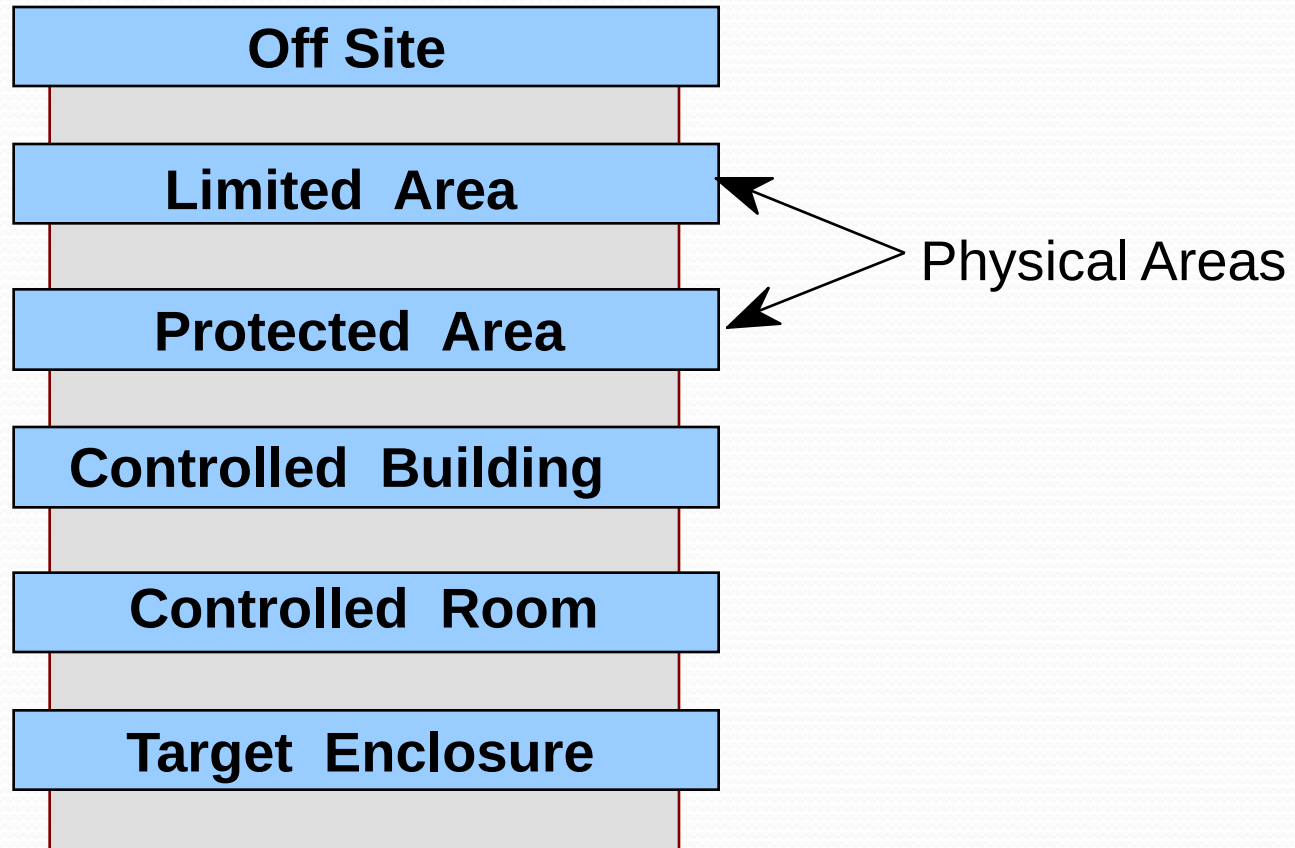


Sample Facility

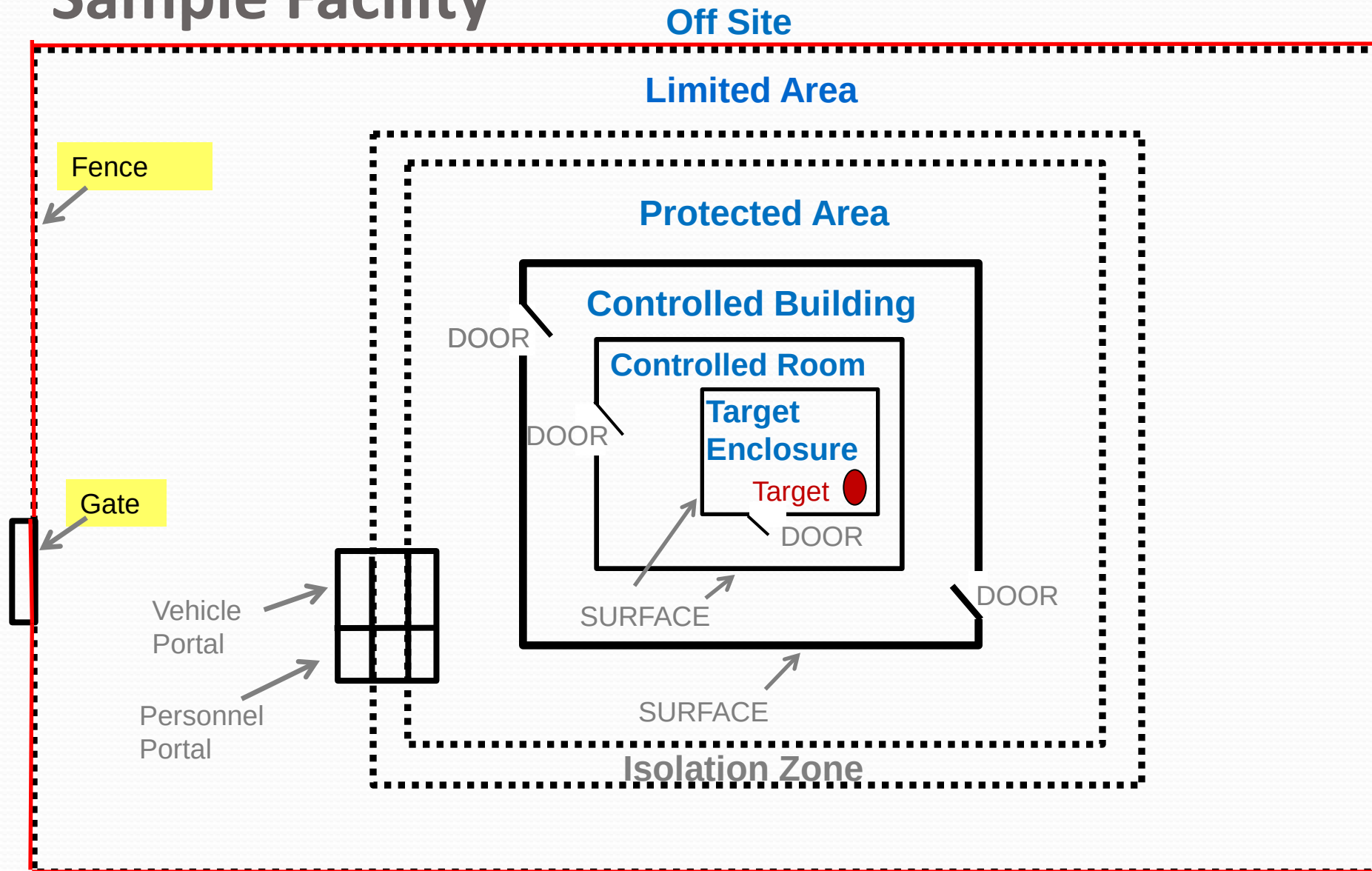
Off Site



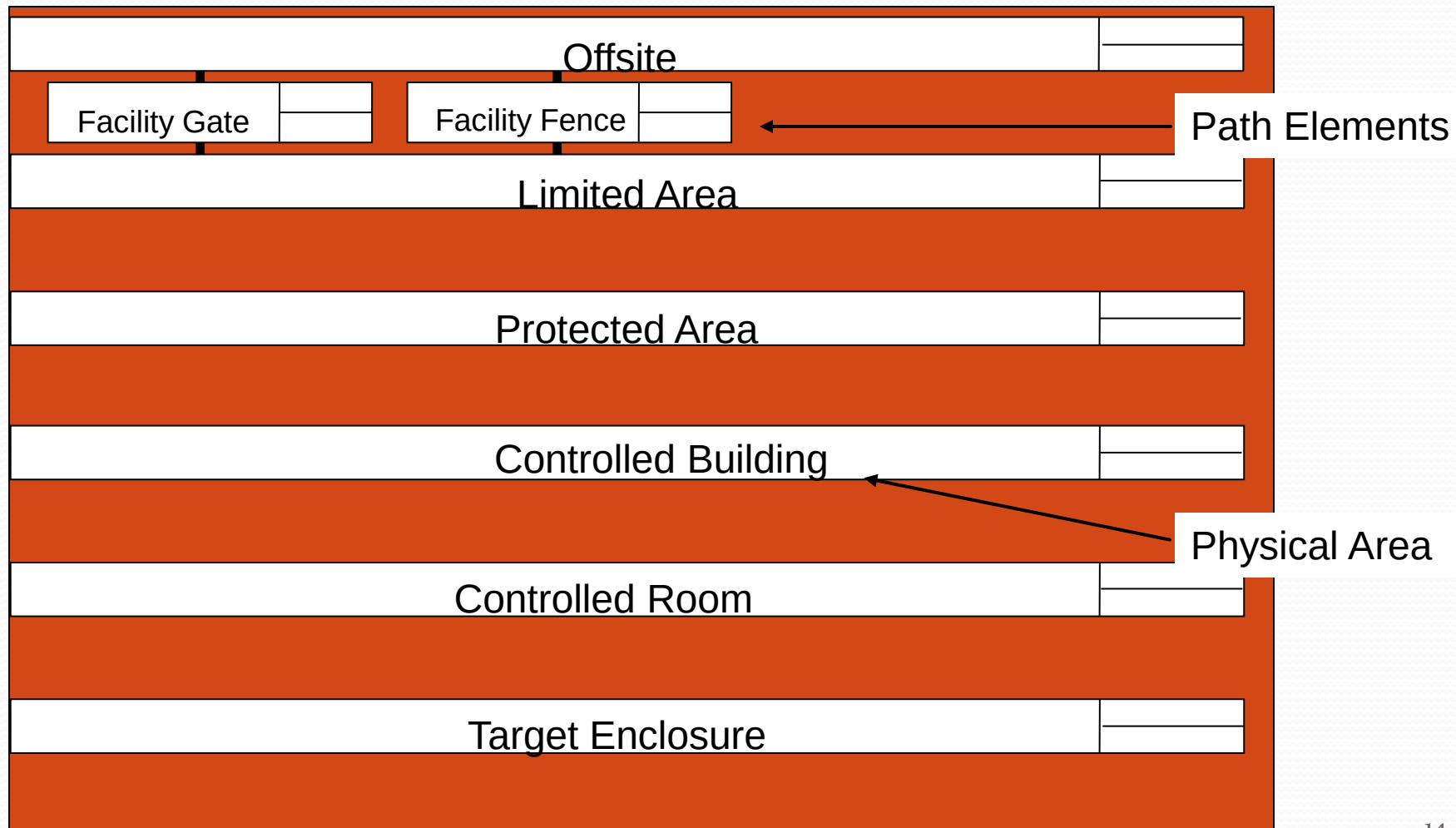
Physical Areas in the Sample Facility



Sample Facility

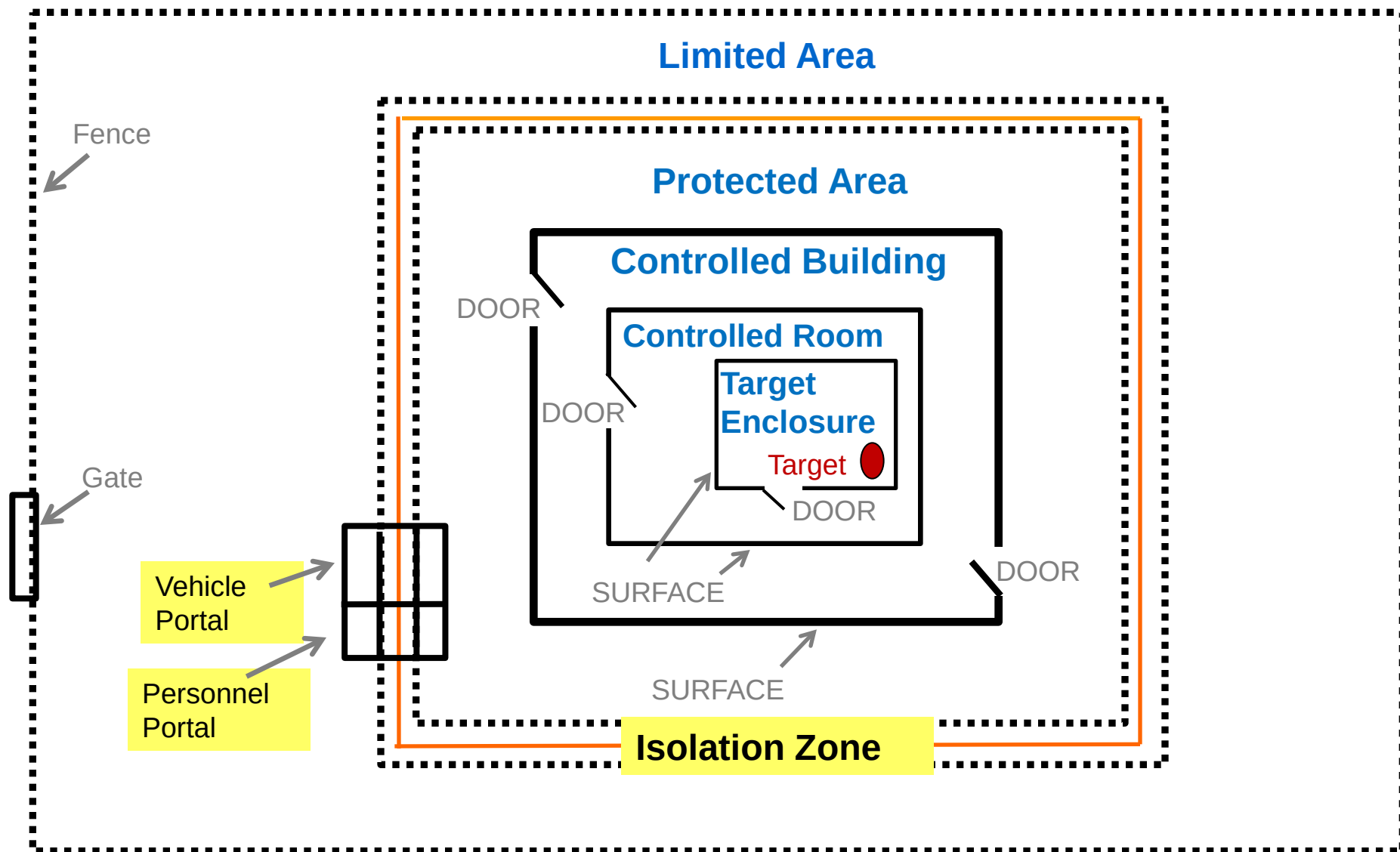


Protection Layer Between Offsite and Limited Area

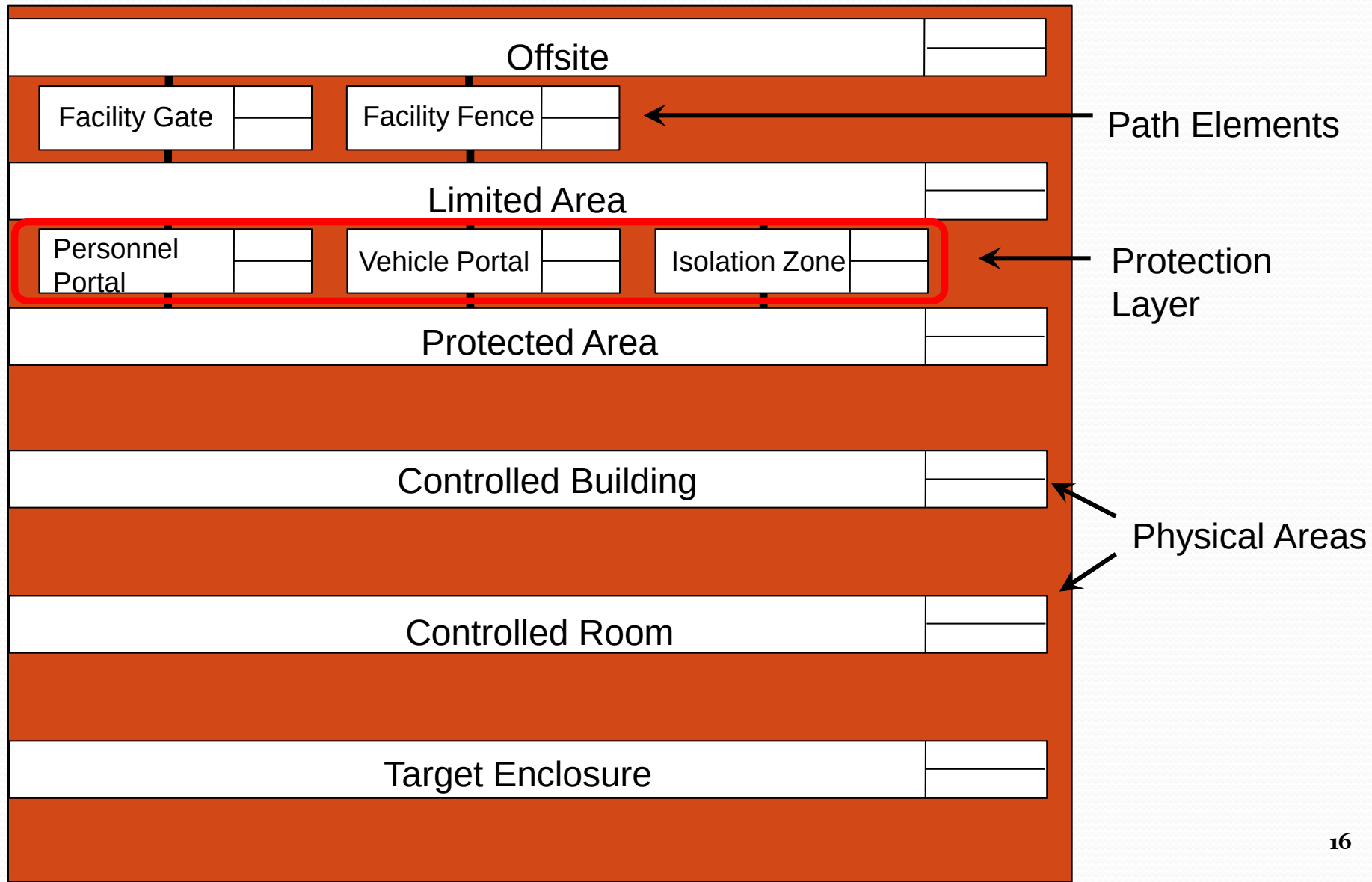


Second Protection Layer at the Sample Facility

Off Site

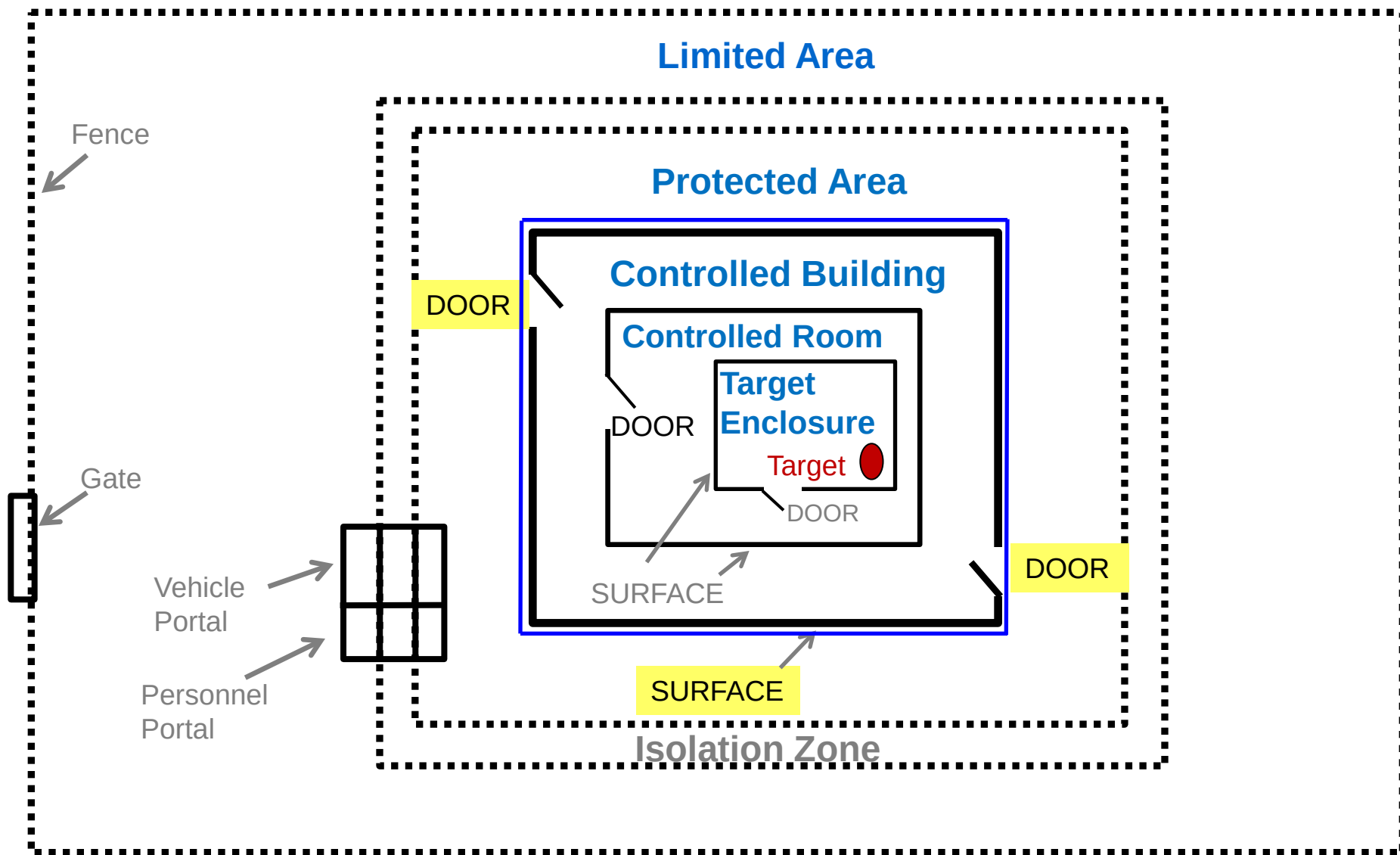


Path Elements From Limited Area to Protected Area



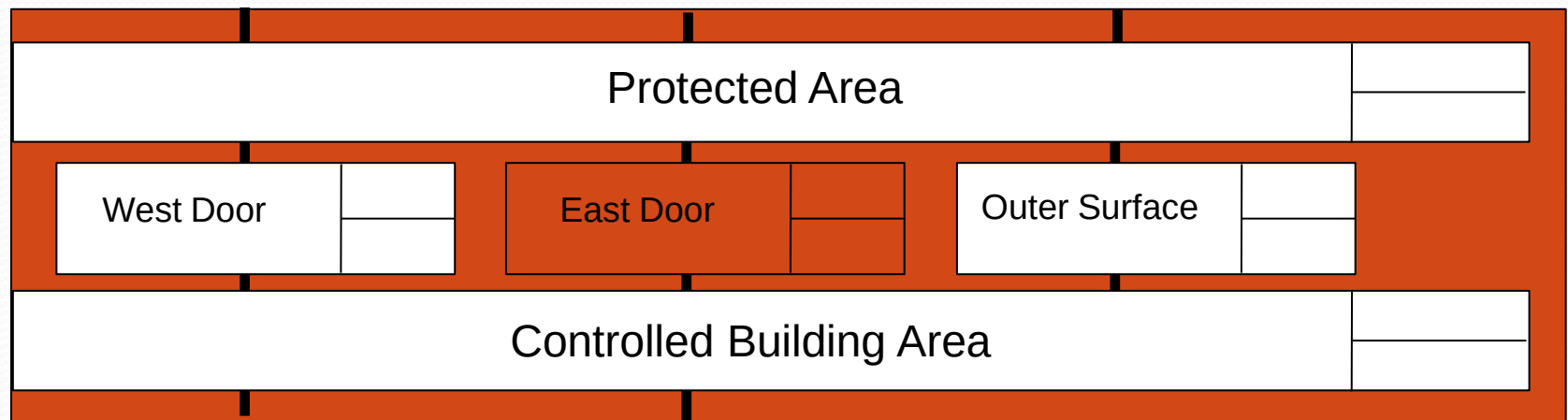
Third Protection Layer at the Sample Facility

Off Site



Path Elements From Protected Area to Controlled Building

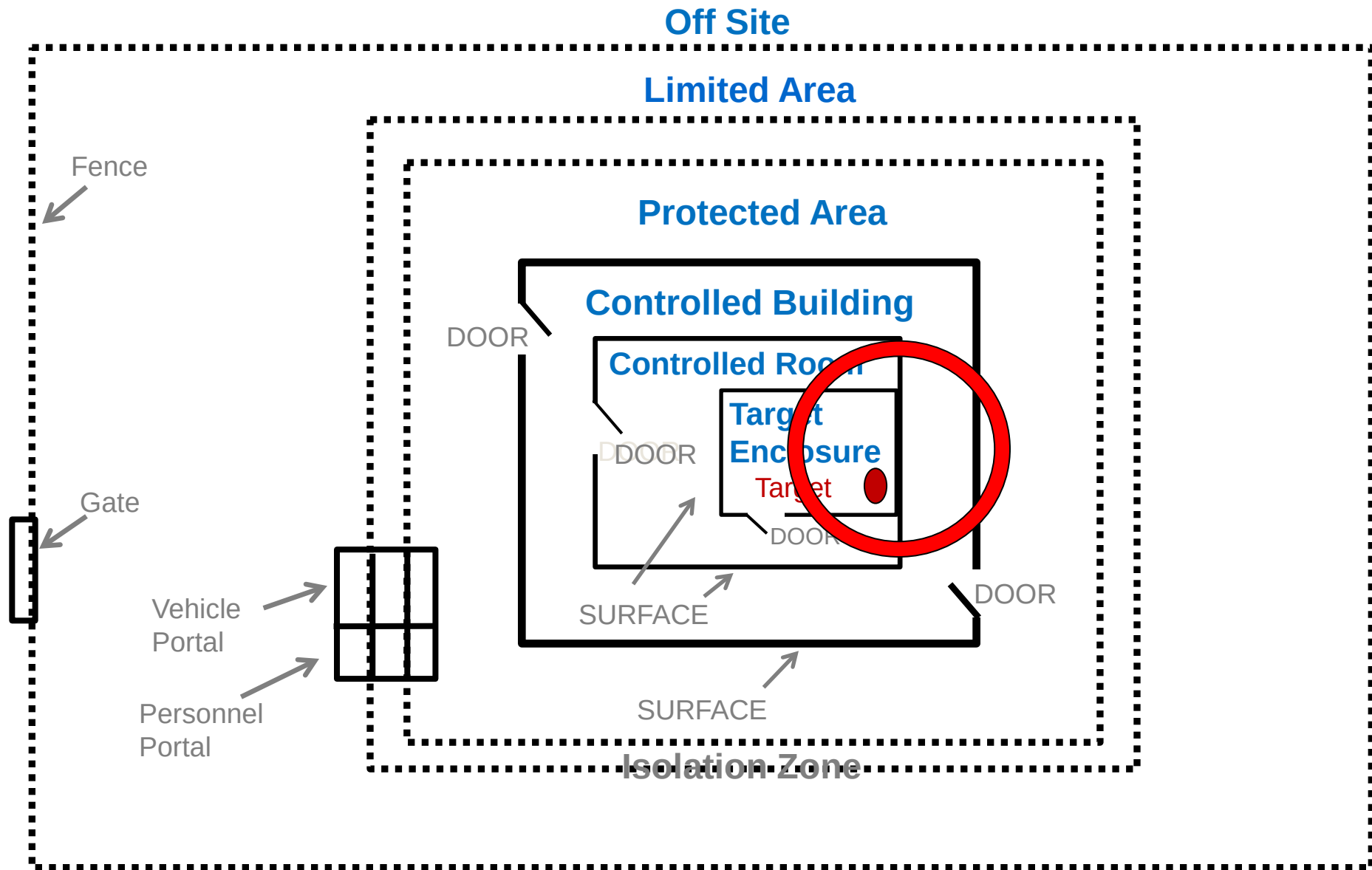
- Include characteristically different path elements in each protection layer
- Multiple path elements with the same characteristics can be represented by a single element



Completed Site-Specific ASD for Sample Facility

Offsite		
Facility Gate		Facility Fence
Limited Area		
Personnel Portal		Vehicle Portal
		Isolation Zone
Protected Area		
West Door		East Door
		Outer Surface
Controlled Building		
Door into Controlled Room		Wall Around Controlled Room
Controlled Room		
Target Enclosure Door		Target Enclosure Wall/Roof
Target Enclosure		
Floor Vault: Target Task		

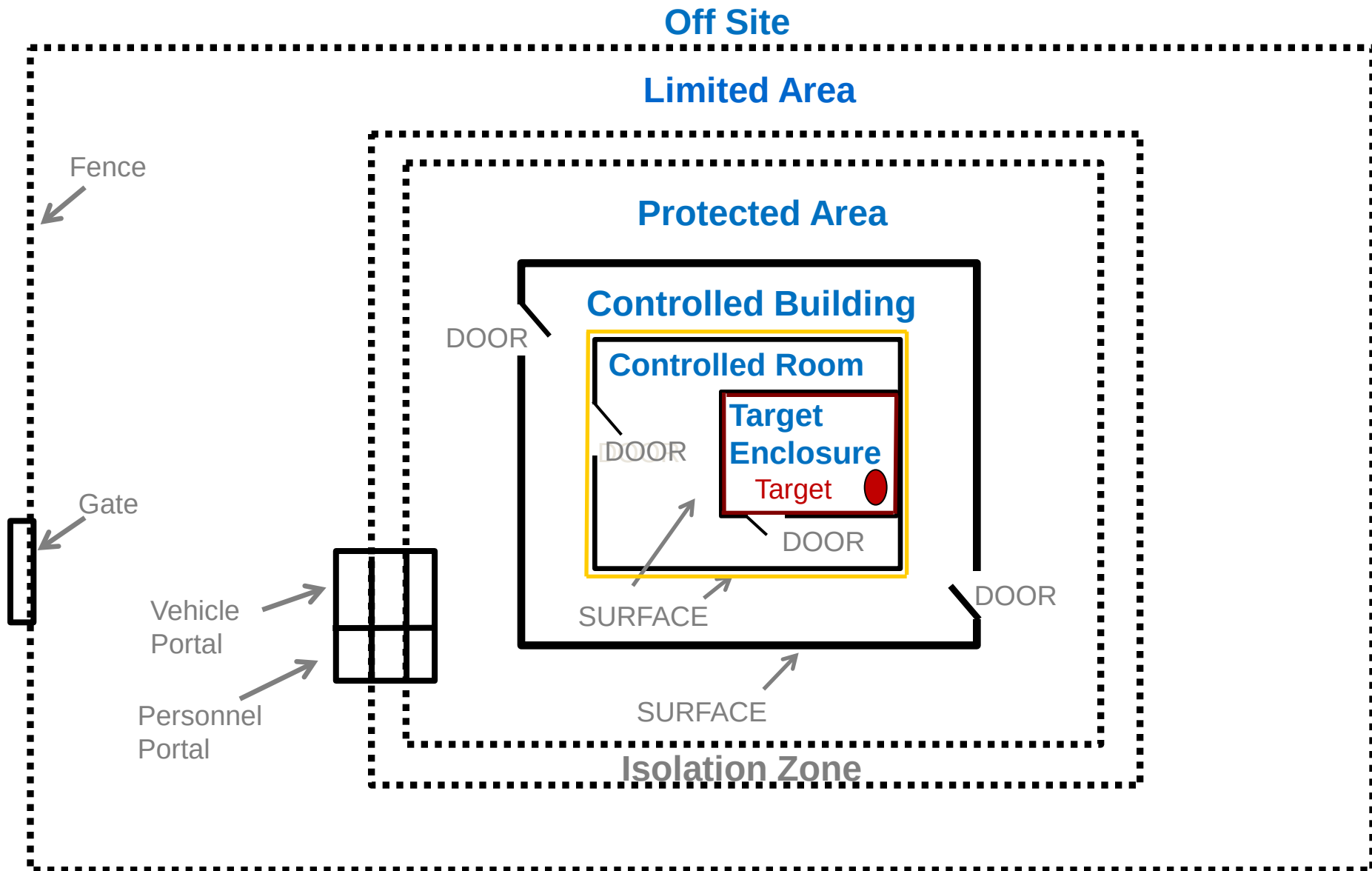
Example of a Jump



Site-Specific ASD for Sample Facility With A Jump

Offsite			
Facility Gate		Facility Fence	
Limited Area			
Personnel Portal		Vehicle Portal	
Isolation Zone			
Protected Area			
West Door		East Door	
Outer Surface			
Controlled Building			
Door into Controlled Room		Wall Around Controlled Room	
Jump Wall Around Controlled Room			
Controlled Room			
Target Enclosure Door		Target Enclosure Wall/Roof	
Target Enclosure			
Floor Vault: Target Task			

Example of a Jump





Multiple ASDs May Be Required

- A different ASD may be required for each unique situation
 - Target
 - Target location (glove box versus floor vault)
 - Facility condition (day, night, normal operation, shutdown, refueling, etc.)
 - Adversary objective (theft or sabotage)
 - Threat characteristics
- The complexity of multiple targets may be reduced by examining “worst-case” or “bounding” situations

Step 3: Assign Detection and Delay Values for Each Path Element and Physical Area

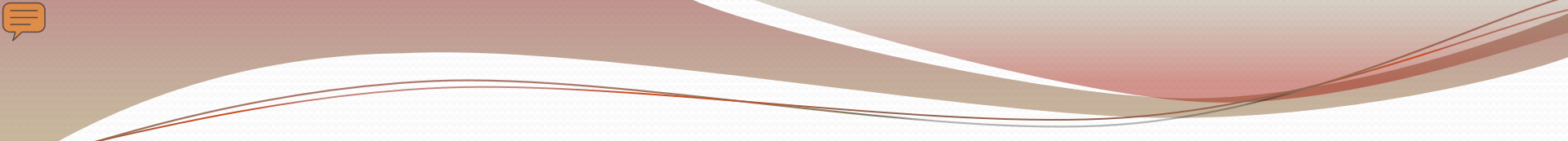
- Path elements
 - Determine minimum P_D
 - Intrusion Detection
 - Access Control
 - Human Surveillance
 - Contraband and Special Nuclear Material (SNM) Detection
 - Determine minimum delay time
 - Barriers
 - Guards
 - Locks
 - Theft or Sabotage Tasks
- Physical areas
 - Determine minimum P_D
 - Intrusion Detection
 - Human Surveillance
 - Determine minimum delay time
 - Guards
 - Transit Time

Data for the detection and delay values can be found in the hypothetical facility data book.



Minimum Performance Values

- Minimum performance data are used for each path element and physical area to provide a conservative estimate of system performance
- Review data for each path element and select the minimum performance value that is within the DBT capabilities
- P_D and delay time values do not have to be for the same tool set within the DBT



Path Element Example

- DOOR₁ Characteristics
 - 10-cm wood door with metal sheeting
 - Balanced magnetic switch position sensor
 - Vibration sensor
- DBT Capabilities
 - Traveling on foot
 - Hand tools
 - Power tools
 - Explosives

Path Element Data

- Door penetration time: 30 sec

Component Type	Component Description	No Equipment	Hand Tools (sec)	Power Tools (sec)	Explosives (sec)		Land Vehicle (sec)
					Stage 1	Stage 2	
Doors	10-cm wood door with metal sheeting	Infinite	300	180	30	0	5 for large vehicle door

- Probability of detection: 0.4

Component Type	Component Description	No Equipment P(D)	Hand Tools P(D)	Power Tools P(D)	High Explosives P(D)	Land Vehicle P(D)
Position Sensors	Position Switch	0.5	0.2	0.2	0.2	N/A
	Balanced Magnetic Switch	0.8	0.8	0.8	0.8	N/A
Barrier Sensors	Vibration	0.9	0.4	0.4	0.9	N/A
	Glass Breakage	0.9	0.6	0.6	0.9	N/A



Physical Area Example

- Protected Area Characteristics
 - 30 meters minimum distance from isolation zone to building
 - Random patrol by guards
- DBT Capabilities
 - Traveling on foot
 - Hand tools
 - Power tools
 - Explosives

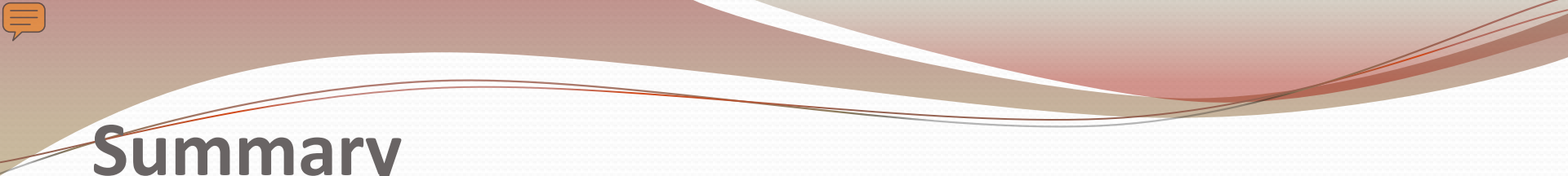
Physical Area Data

- Transit time: 6 sec (Data book, Table 20, Running Rates; running with tools)
- Probability of detection: 0.02 (Guard on random patrol)

Component Type	Component Description	No Equipment P(D)	Small Arms P(D)	Light Antitank Weapons (LAW) P(D)	Independent of Threat Attribute P(D)
Guard on Patrol	Random				.02
	Scheduled				.01

ASD with Example Data Added

Offsite		PD=
		T=
Facility Gate	PD=	
	T=	
Facility Fence	PD=	
	T=	
Limited Area		PD=
		T=
Personnel Portal	PD=	
	T=	
Vehicle Portal	PD=	
	T=	
Isolation Zone	PD=	
	T=	
Protected Area		PD= 0.02
		T= 6Sec
West Door	PD= 0.4	
	T= 30Sec	
East Door		
Outer Surface	PD=	
	T=	
Controlled Building		PD=
		T=
Door into Controlled Room	PD=	
	T=	
Wall Around Controlled Room	PD=	
	T=	
Controlled Room		PD=
		T=
Target Enclosure Door	PD=	
	T=	
Target Enclosure Wall/Roof	PD=	
	T=	
Target Enclosure		PD=
		T=
Floor Vault: Target Task	PD=	
	T=	



Summary

- An ASD represents paths that adversaries can follow to accomplish sabotage or theft and the PPS elements along those paths
- ASD is used to determine the most vulnerable path for specific PPS and threat
- The 3 steps used to create an ASD are:
 - Model the facility by separating it into adjacent physical areas
 - Define protection layers in terms of path elements between areas
 - Assign probability of detection (P_D) and delay time (T) for each path element and physical area

4. Adversary Sequence Diagram Model

Session Objectives

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

1. Construct a site-specific and target-specific Adversary Sequence Diagram (ASD).
2. Demonstrate that the ASD represents credible paths that adversaries can follow to accomplish sabotage or theft and the path elements along the path.
3. Assign delay times and probabilities of detection to elements within the ASD.

Exercise 1 - Identify Adjacent Physical Areas

The purpose of this subgroup session is to construct an ASD. Using the Exercise Data Book (Sections 4-5 and 10 -14) for the Lagassi Institute of 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.

- Use colored markers to indicate the boundaries between the physical areas and name the physical areas.

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 and 10 through 13) to define the path elements for your ASD.

Begin your ASD at the Offsite area and end at the Target Enclosure. The result of this exercise is an ASD for the PTR reactor.

Below is a list of abbreviations for reference, you may use them, but there is no requirement to do so.

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 - Fence line		WND - Window
GAT - Gateway		Target Locations:
HEL - Helicopter Flight Path		BPL - Bulk Process Line
ISO - Isolation Zone		CGE - Cage
PST - Material Pass through		FLV - Floor Vault
MAT - Material Portal		GNL - Generic Location
OVP - Overpass		GBX - Glove box
DOR - Personnel Doorway		IPL - Item Process Line
PER - Personnel Portal		OPN - Open Location
SHD - Shipping/Receiving Doorway		TNK - Storage Tank

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

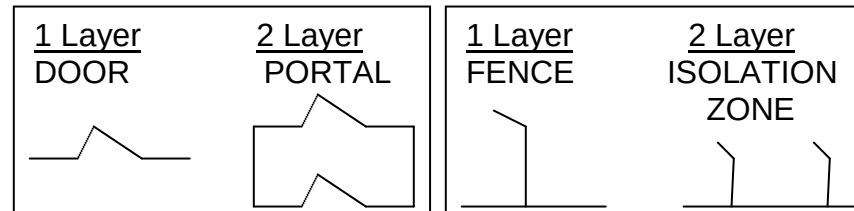
Miscellaneous Elements

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 2copies of the same barrier (hence double-layer barriers)



<u>Single Layer Elements</u>		<u>Double Layer Elements</u>		<u>Comments</u>
FEN	Fence line	ISO	Isolation Zone	Surrounds exterior area- e.g.: Protected Area
		OVP	Overpass	Like Isolation Zone but over Buildings
GAT	Gateway			For Human and Vehicle Movement
DOR	Personnel Doorway	PER	Personnel Portal	For Human Movement
MAP	Material Pass-Through	MAT	Material Portal	For Material Movement <u>Only</u>
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

The purpose of this exercise is to assign probability of detection and delay time data to each physical area and each path element in the ASD developed in the previous two exercises.

Use the hypothetical facility data book (sections 27 and 28) to get values for each physical area and each path element. Use the worksheets on the following pages to record the data. You should also record the data on your ASD. This information will be used in later exercises.

For this exercise assume normal shift workday conditions for the analysis and that the adversary is traveling on foot. Assume the adversary can travel 4 m/s on foot and 16 m/s in a vehicle. Assume a random patrol by a security officer is conducted 24 hours/day in the Limited Area.

Descriptions of components:

Detection components:

- Access control - providing detection for deceit strategies – *See table 5 in Section 27*
- Contraband and SNM detection - providing detection for deceit strategies – *see Table 7 in Section 27*
- Intrusion detection (typically by sensors) - providing detection for stealth and force strategies – *see Table 4 in Section 27*
- Human surveillance (by security officers or employees) – providing detection for stealth and force strategies -- *See Table 6 in Section 27*

Delay components

- Barriers -- *See Table 8 in Section 28*
- Locks -- *See Table 8 in Section 28*
- Target Tasks -- *Typically, user defined*
- Security Officers – *See Table 9 in Section 28*
- Transit times -- *Typically, user defined.*

NOTE: When you identify elements that are portals, leave the data blank, this will be determined in a later exercise.

Fill in the appropriate information for each physical area.

[illegible]

Fill in the information for each path element.

Protection Layer Between _____ and _____

[illegible]

Protection Layer Between _____ and _____

[illegible]

Protection Layer Between _____ and _____						
Path Element Code	Path Element Description	Delay Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate
Protection Layer Between _____ and _____						
Path Element Code	Path Element Description	Delay Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate
Protection Layer Between _____ and _____						

Path Element Code	Path Element Description	Delay Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate

Protection Layer Between _____ and _____

Path Element Code	Path Element Description	Delay Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate

Application Considerations

1. Are there any facilities that an ASD cannot be constructed for?
2. Is an ASD the best way to determine most-vulnerable paths?
3. In addition to identifying possible paths, an ASD can also help you determine shortest delay pathways, delay balance between areas, and delay protection in depth. How can this information benefit your facility?

4. Adversary Sequence Diagram Solutions

Session Objectives

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

1. Construct a site-specific Adversary Sequence Diagram (ASD).
2. Demonstrate that the 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 (20 minutes)

The purpose of this subgroup session is to construct an ASD. Using the Exercise Data Book (Sections 4-5 and 10 -14), for the Lagassi Institute of 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.	OFFSITE
2.	Institute Limited Area
3. A	PTR Protected Area
4. B	Reactor Building
5. C	PTR Reactor Hall R060
6. D	TARGET AREA- Products Vault R091

Exercise 2 – Define Protection Layers, Path Elements, Target Locations, and Path Segments (40 minutes)

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.

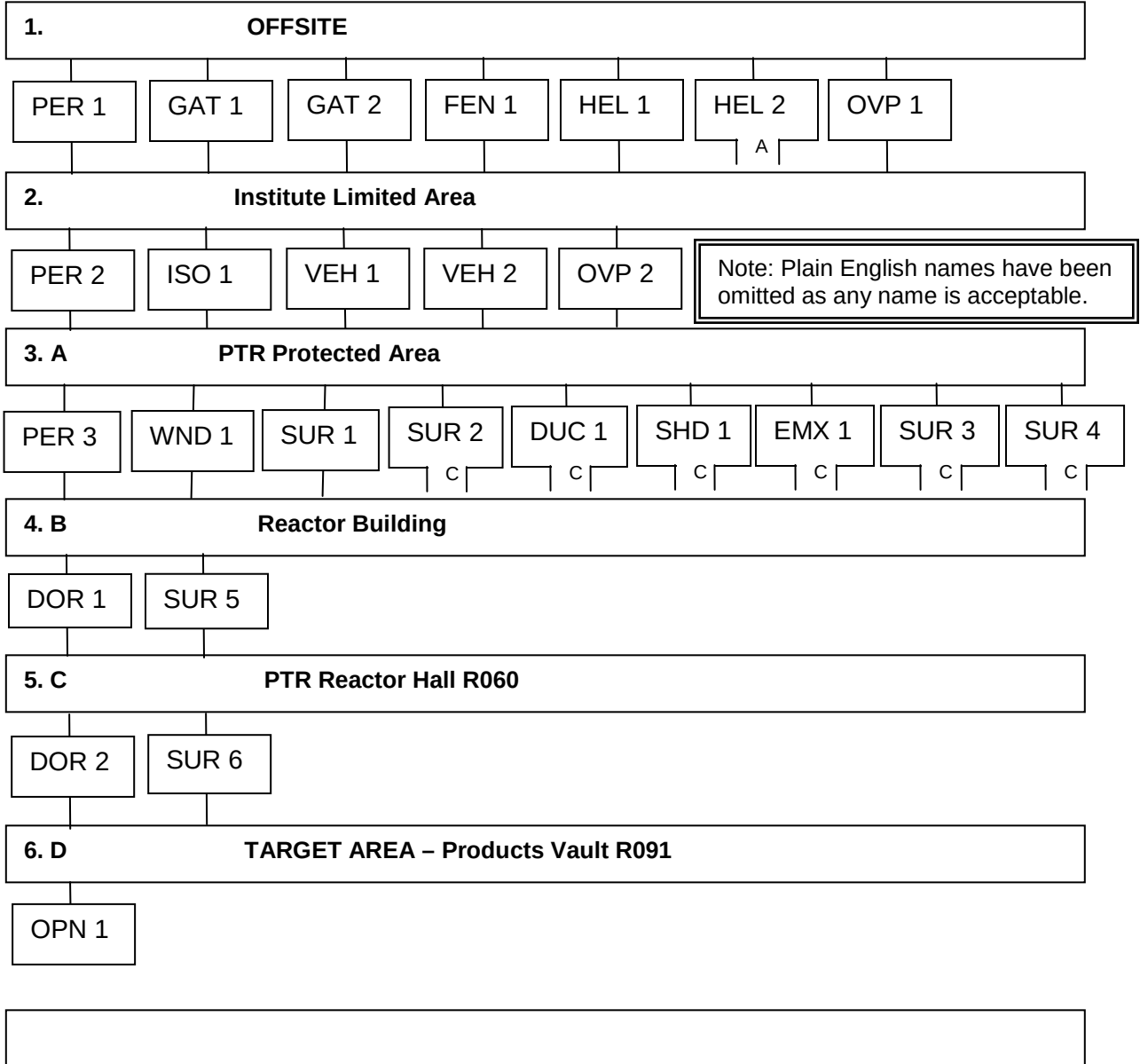
Use information about the PTR reactor (Exercise Data Book, Sections 7 and 10 through 13) to perform the other four steps for creating an ASD.

- 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 the characteristically different 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.)*
- Give each element an abbreviated name for use with later tools. *(Examples are provided below.)*

During your construction, begin your ASD at the Offsite area and end at the Target Enclosure. The result of this exercise is an ASD for the PTR reactor. This ASD will be analyzed in Subgroup 19S.

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 - Fence line	WND - Window
GAT - Gateway	Target Locations:
HEL - Helicopter Flight Path	BPL - Bulk Process Line
ISO - Isolation Zone	CGE - Cage
PST - Material Pass-Through	FLV - Floor Vault
MAT - Material Portal	GNL - Generic Location
OVP - Overpass	GBX - Glove Box
DOR - Personnel Doorway	IPL - Item Process Line
PER - Personnel Portal	OPN - Open Location
SHD - Shipping/Receiving Doorway	TNK - Storage Tank

PTR ASD for Products Vault



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

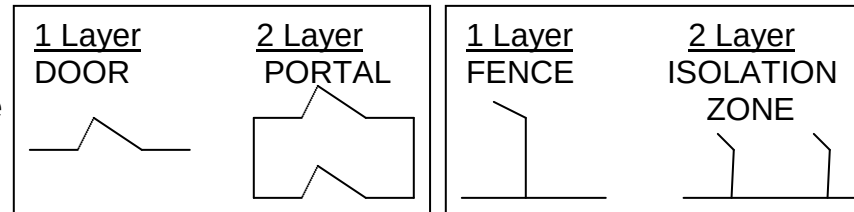
Miscellaneous Elements

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)



<u>Single Layer Elements</u>		<u>Double Layer Elements</u>		<u>Comments</u>
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 <u>Only</u>
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 (60 minutes)

The purpose of this exercise is to assign probability of detection and delay time data to each physical area and each path element in the ASD developed in the previous two exercises.

Use the hypothetical facility data book (sections 27 and 28) to get values for each physical area and each path element. Use the worksheets on the following pages to record the data. You should also record the data on your ASD. This information will be used in later exercises.

For this exercise assume normal shift workday conditions for the analysis and that the adversary is traveling on foot. Assume the adversary can travel 4 m/s on foot and 16 m/s in a vehicle. Assume a random patrol by a security officer is conducted 24 hours/day in the Limited Area.

Descriptions of components:

Detection components

- Access control - providing detection for deceit strategies – *See table 5 in Section 27*
- Contraband and SNM detection - providing detection for deceit strategies – *see Table 7 in Section 27*
- Intrusion detection (typically by sensors) - providing detection for stealth and force strategies – *see Table 4 in Section 27*
- Human surveillance (by security officers or employees) – providing detection for stealth and force strategies -- *See Table 6 in Section 27*

Delay components

- Barriers -- *See Table 8 in Section 28*
- Locks -- *See Table 8 in Section 28*
- Target Tasks -- *Typically, user defined*
- Security Officers – *See Table 9 in Section 28*
- Transit times -- *Typically, user defined.*

NOTE: When you identify elements that are portals, leave the data blank. This will be determined in a later exercise.

Fill in the appropriate information for each physical area.

Instructor Note: Ensure groups don't get engrossed in details, help them move along, it is possible to run out of time on this exercise.

After they fill out these charts, have them enter the data into their ASD.

Physical Area	Distance Across	Transit Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate
Offsite	Unknown	Unknown	Not possible to know.	None	0	People are free to roam; no detection elements.
Limited Area	120 m.	7.5 seconds	120 m. /16m/s= 7.5 seconds (adv. In vehicle)	Roving Patrol (presence in areas)	0	If roving patrol is not looking, there is no P _D .
Protected Area	12 m.	3 seconds	12 m. / 4m/s = 3 seconds	Active IR	.08	Assuming adversary is using no tool.
Controlled Building Area						
Controlled Room						
Target Enclosure						

Fill in the information for each path element.

Protection Layer Between <u>Offsite</u> and <u>Limited Area</u>						
Path Element Code	Path Element Description	Delay Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate
	Concrete Fence	10 sec.	Climb fence without any tools	None	0	There is no detection on or around this fence
	Vehicle Gate (P3)	15 sec.	Routine Entry	Badge Check	0.1	Picture Badge
	Vehicle Gate (P4)	60 sec.	Routine Entry	Badge Check, Paperwork	0.1	Picture Badge
	Personnel Entrance (P2)	30 sec.	Routine Entry	Badge Check	0.1	Picture Badge
Protection Layer Between <u>Limited Area</u> and <u>Protected Area</u>						
Path Element Code	Path Element Description	Delay Time	Basis for Time Estimate	Detection Means	P _D	Basis for P _D Estimate
	Continue as above for each element between each additional protection layer.					

Application Considerations

1. Are there any facilities that an ASD cannot be constructed for?
2. Is an ASD the best way to determine most-vulnerable paths?
3. In addition to identifying possible paths, an ASD can also help you determine shortest delay pathways, delay balance between areas, and delay protection in depth. How can this information benefit your facility?

ASD Subgroup Instructor Guide

Key Points to Emphasize

- The purpose of this subgroup is to be sure that the group can develop an ASD and populate it with data.
- Identifying physical areas properly is critical. Make sure the students identify the areas in proper order before trying to identify path elements.
- We are interested in identifying “characteristically different” path elements that connect adjacent physical areas. If two elements have the same delay and detection characteristics, they can be represented by a single element.
- We use conservative data in the ASD. This means that we will take the shortest distance across a physical area when determining transit time and will use the minimum delay time and minimum probability of detection within the capabilities of the DBT when assigning these values.

Facilitation of the Module

- The difficult part of physical area identification is getting the PTR Admin Building and the Reactor Hall treated properly. The Admin Building should be above the Reactor Hall on the ASD. Note that the longest path from offsite to the product vault goes through the Admin Building first, so it should precede the Reactor Hall on the list of physical areas.
- Emphasize the importance of tracing the boundaries between physical areas when identifying the path elements that connect them. Don’t let the students just start naming the path elements they see by inspection of the drawings. Using colored pens to mark the boundaries is a good idea.
- Double layer elements usually cause confusion. Review the concept before they begin identifying path elements.
- Before we can do path analysis, every path element and every physical area will need a P_D and T . In this exercise, we will use data from the data book and exercise instructions to determine values for the physical areas and for a few of the path elements. Students just need to demonstrate that they understand how to do it for a few examples in this exercise. Select one or two protection layers for which data must be determined. It might be good to have different sub-subgroups work on different layers and report results and rationale to the group.

Areas to Avoid

- The students may think they have to use the same labels for physical areas that were used in the presentation. This is not necessary or desired. They should develop physical area names that make sense for the facility they are modeling.

Data Collection Facility Characterization

Module 5

Vulnerability Analysis Training Course
Date:

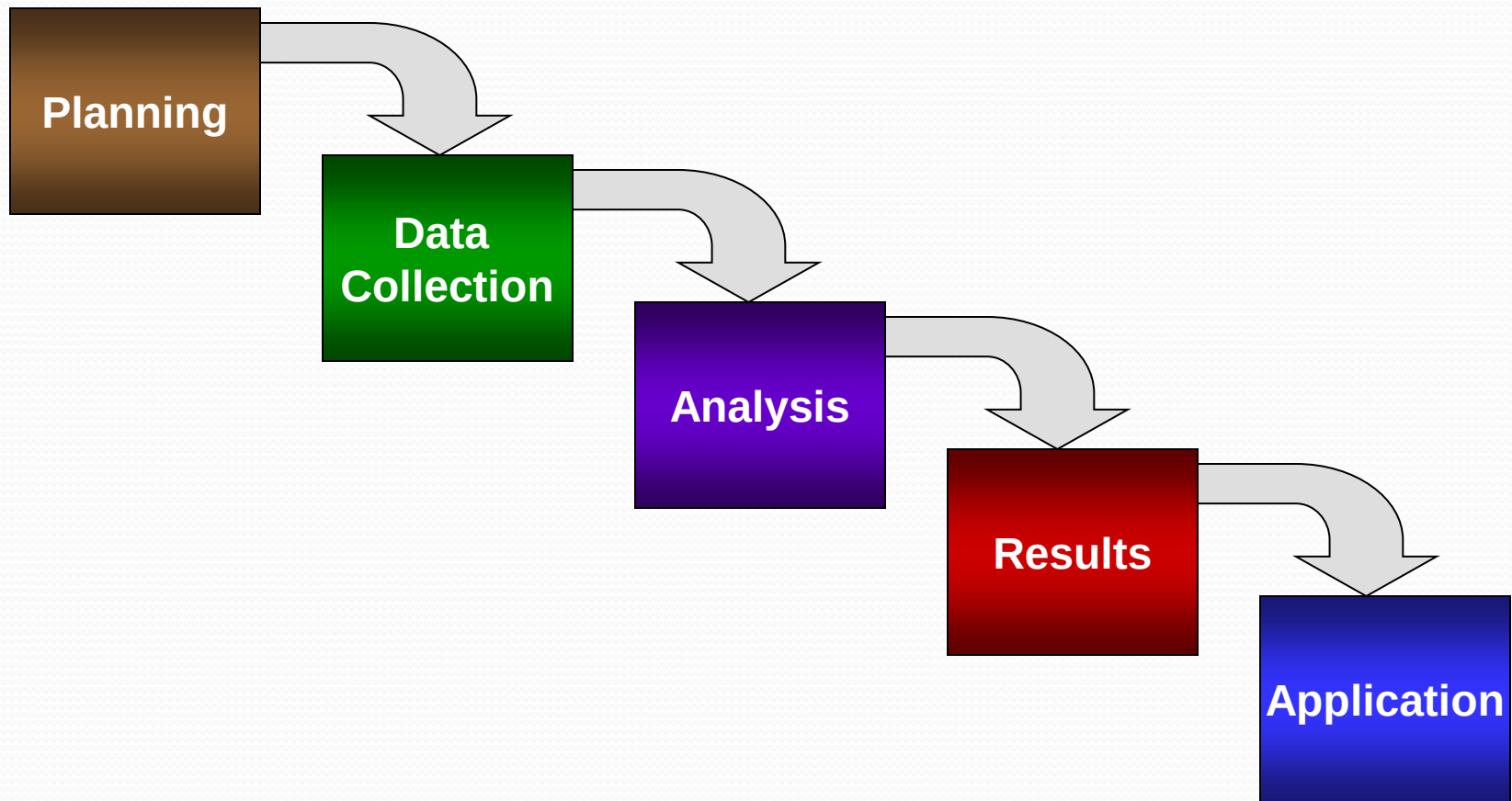


Student Learning Objectives

After completing this module, you should be able to:

- Discuss the facility characterization approach
- Complete the data worksheets for specific protection elements at the facility
- Discuss types of information that should be gathered during facility characterization

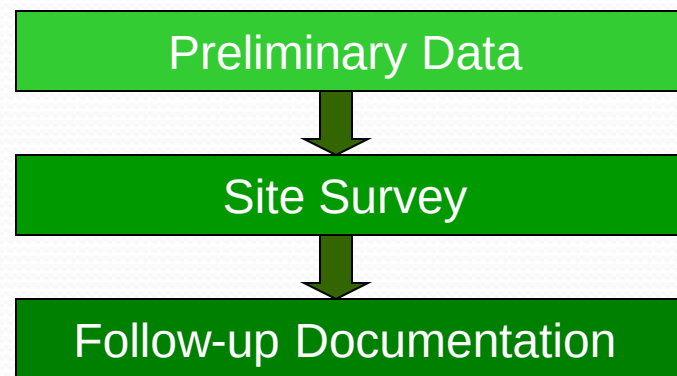
Phases of Vulnerability Analysis



Data Collection – Types of Data

**Data
Collection**

- Facility Characterization
 - PPS documentation
 - Open sources
 - Site survey
 - Test data
- Design Basis Threat
 - State
 - Regional or local
 - Facility (including insiders)
- Target Identification/Consequences
 - Types and characteristics of material
 - Location of material and vulnerable equipment
 - Prioritized targets for theft and vital areas for sabotage



***May take three phases to
complete the picture***



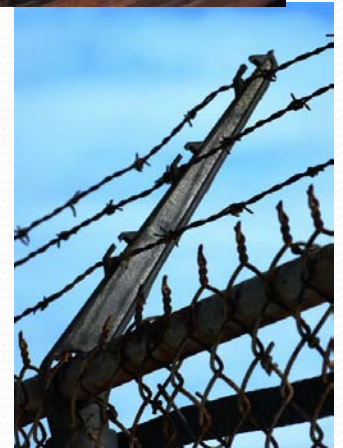
Facility Characterization

Investigating anything that impacts the performance of the system

- Site Information
- PPS
- Material Accountancy and Control System
- Information Sources
 - Documentation
 - Open sources
 - Site survey
 - Test data
 - Military and police
- Types of Information
 - Physical conditions
 - Facility operations
 - Facility policies and procedures
 - Insider access/authority/knowledge and insider groups
 - Regulatory requirements
 - Safety considerations
 - Legal issues
 - Organizational protection goals and objectives
 - Others?

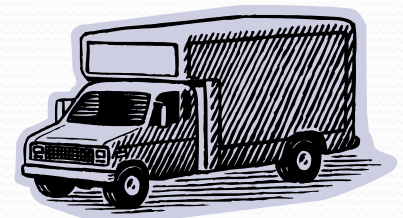
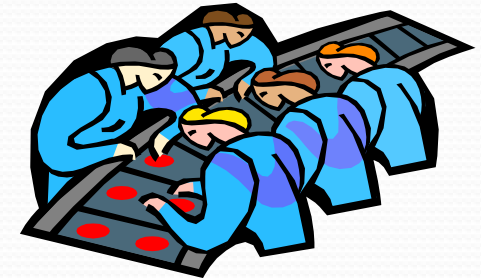
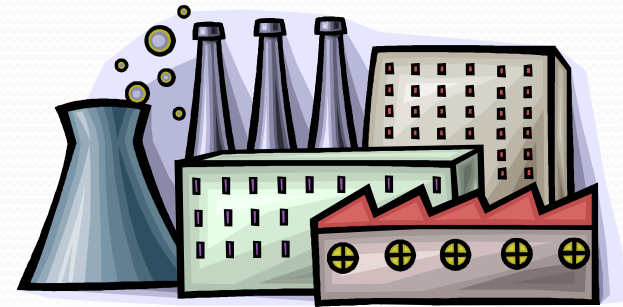
Physical Conditions

- Site boundaries, fences, barriers,
- Topography, weather, and environment
- Buildings construction materials for walls, ceilings, floors, doors, windows, etc.
- Areas and rooms
- Access points
- Heating, ventilation, air conditioning
- Communication paths and types
- Power distribution system
- Environmentally controlled areas
- Locations of nuclear materials and vulnerable equipment
- Locations of non-target, hazardous material



Facility Operations

- Operational activities
 - Products and processes
 - Operational hours
 - Number, types, and locations of employees
 - Visitors and vendors
 - Assess management
- On-site location and movement of materials
 - Shipping and receiving process
 - Intra-site movements/convoy
 - Internal processes
 - Tracking mechanisms





Facility Policies and Procedures

- Operations policies and procedures
- Training policies and procedures
- Other indications of organization culture



Regulatory Requirements

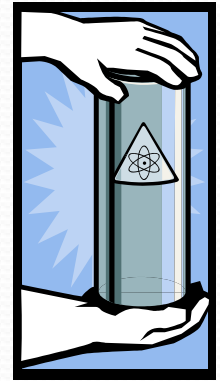
- State and local
- Competent authority
- Industry codes and regulations
- Construction codes
- Security system standards



**Physical Security Systems should be configured
so that the licensee complies with regulations**

Safety and Security Considerations

- Safety regulations and requirements
- Security regulations and requirements
- Interaction between safety and security
 - Safety is concerned primarily with the prevention of accidental events (injuries)
 - Security is concerned primarily with the prevention of intentional malicious attacks (theft, sabotage)



Safety is not Security

Legal Issues

- Complex and difficult
- Legal issues include:
 - Security liability
 - Provide reasonable security
 - Failure to protect
 - Negligence liability
 - Overreaction
 - Excessive force, lethal force, invasion of privacy, and rules of engagement
 - Labor/employment issues
 - Labor unions, work practices



Organization Protection Goals and Objectives

- View of security by management
- Support of protection goals by management
- Determination of security culture
 - Underlying assumptions
 - Attractive target?
 - Values that have been adopted by the facility
 - Intent of management?
 - Visible artifacts
 - Equipment and practices?



Other Information

- Political environment
- Surrounding community relations
- Facility and local law enforcement liaison
- Mutual aid agreements
 - Memoranda of understanding with military organizations, local law enforcement agencies, other facilities, etc.



Characterize the PPS

- Identify targets and target locations
- Identify security areas and layers of protection for the facility for Adversary Sequence Diagrams (ASDs)
- Determine facility states
 - Characterize protection elements that apply for different facility states
- Describe PPS functions (detection, delay, response)





Characterize the Material Control and Accountability System

- Material Balance Areas (MBAs) for physical control
- Control
 - Movements of materials between MBAs
 - Use of/tampering with material through tags and seals
- Accountability
 - Inventories
 - Measurement programs
 - Documentation
- MC&A systems can help detect theft and diversion and identify what material is missing



Identify Layers and Associated Areas

- Typical Layers:
 - Limited access area
 - Protected area (PA)
 - Inner area
 - Vital area
- Some protection systems may have more or fewer areas than these three areas
 - An area may surround the PA
 - E.g., limited access area
 - There may be other distinct areas within the inner area
 - The storage area may also be the inner area
- Identify MBAs

Example Area/Layers Worksheet

Area/Layers Worksheet					
Area No.	Area Name	Traversal Mode	Distance Across Area (meters)	Assumptions	Notes/Comments
Off-site	Off-site	☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
1	PA	☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
2	Bldg	☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
3	Room	☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
4	Vault	☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
Target	NM				

Area Number linked to Material Balance Area _____



List Facility States

- Shift, day of week, time of day, holiday, etc.
- Status of vault – open/closed
- Status of gates – open/closed
- Nuclear material movement
- Maintenance
- Emergency
- Unusual weather: fog, rain, wind, snow, hurricane, etc.
- Labor dispute

Facility States Matrix Example

Condition	Protected Area	Inner Area
Operational (day)	Open	Open
Operational (night)	Open	Closed
Non-operational (holiday)	Closed	Closed
Fire alarm during normal day*	Open	Open

* Uncontrolled exit during fire alarms

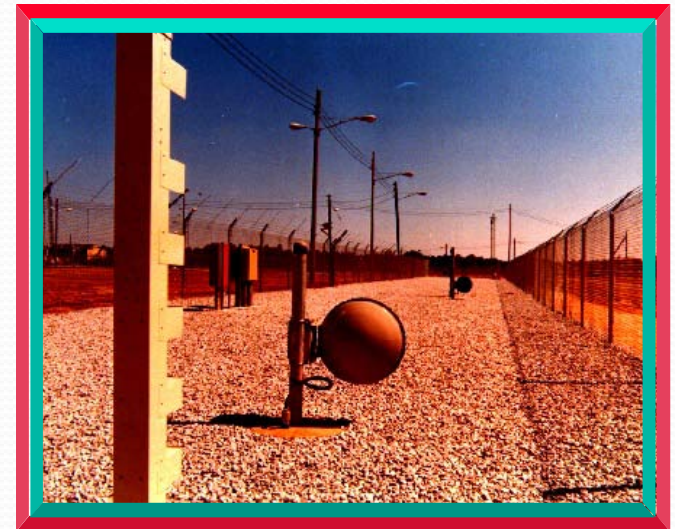
Describe Detection, Delay, and Response Elements

- Associated with PPS
 - Describe the alarm and assessment system
 - Describe the access control system
 - Describe the delay mechanisms
 - Characterize the response
- Associated with MC&A, operational, and safety systems
 - Describe detection features against the insider
 - Describe insider-related response procedures



Performance Measures for Alarm and Assessment System(s)

- Methods used by facility to assess various sensors and alarms
- Sensor types, locations
 - Installation, maintenance, and testing
- Protection of alarm communications lines
- Redundancy of alarm system
 - Sensors
 - Communications lines
 - Alarm stations
 - Alarm-handling procedures
 - Power supply
 - Spare parts
- Quality of computer security
- Adequacy of lighting and assessment systems
- Performance measures for alarm reporting

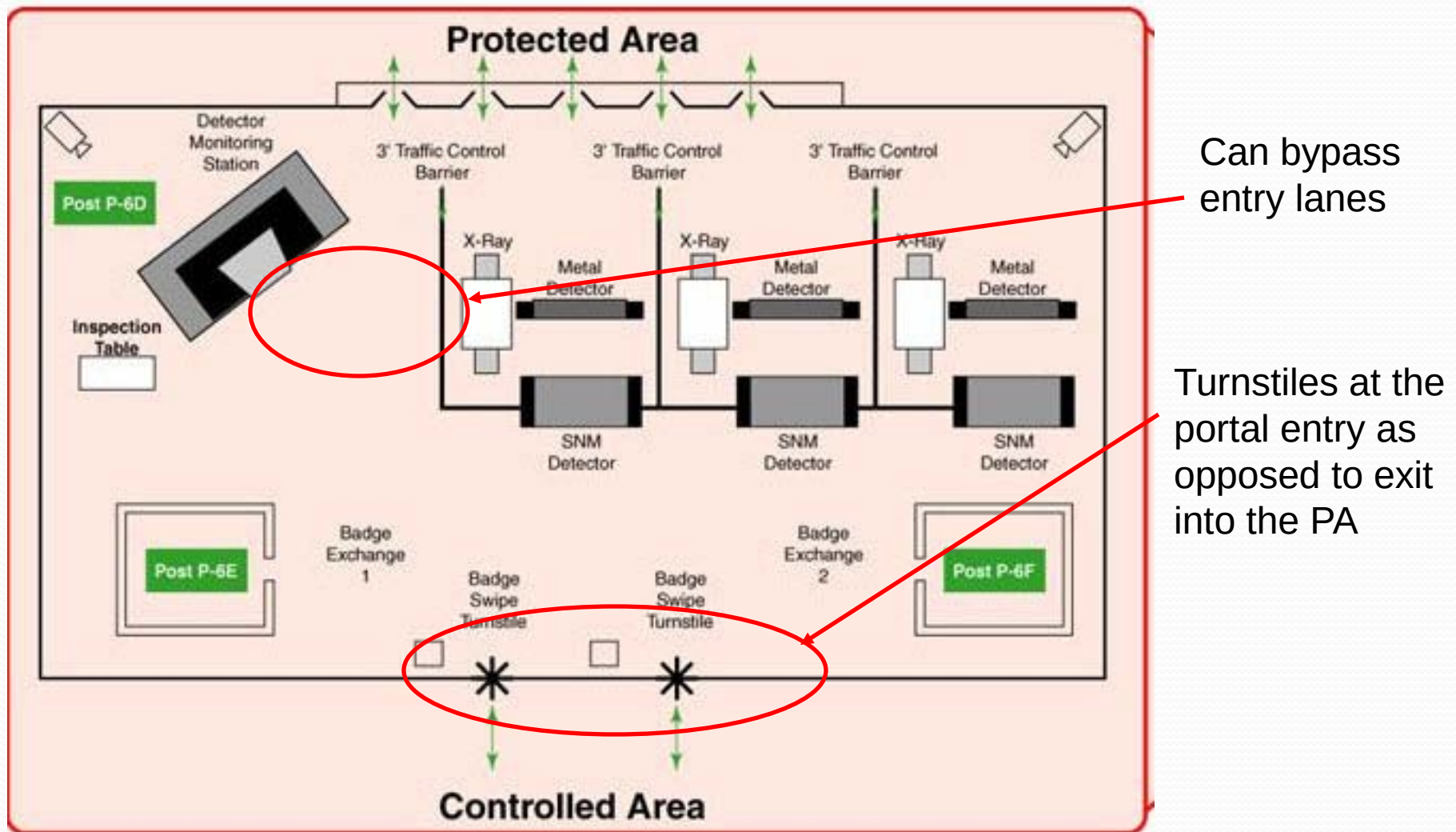


Characterize the Access Control System

- Types, locations, and configurations
- Entry control interface with guards
 - Timeliness of and capacity to assess entry control alarms
 - Methods of alarm resolution
- Contraband detection systems
 - Types
 - Installation, calibration, and maintenance
- Bypass systems



Example of a Personnel Portal Configuration

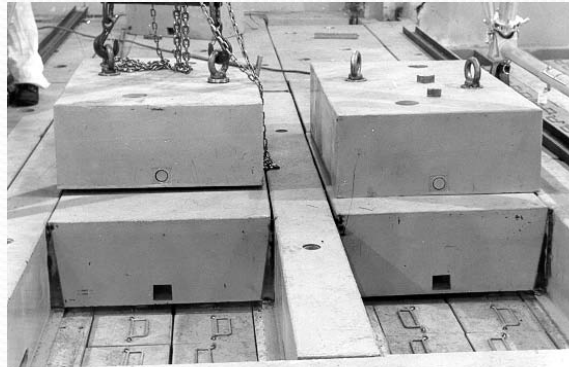


Other Detection Capabilities of MC&A, Operational, and Safety Systems

- Security System
 - Signal line protection
 - Security surveillance
- Nuclear Material Accountability Programs
- Operations System
 - Observation by co-workers or supervisors
 - Operational process alarms
 - Quality assurance
- Safety System
 - Criticality/fire alarms
 - Safety inspections

Characterize the Delay System(s)

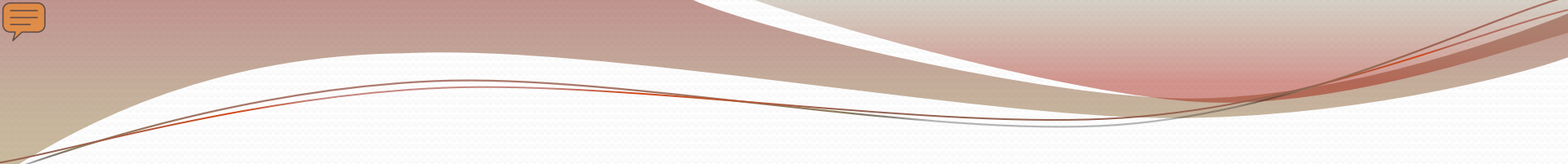
- Types and locations
- Installation and maintenance
- Amount of delay for the given adversary capabilities
- Detection location with respect to the delay
- Failure condition (loss of power, etc.)



Characterize the Response for Outsiders

- Characterize response force initial locations and deployment positions
- Determine types of response
 - Number of responders
 - Response times
 - Rules of engagement
 - Roles and trained capabilities
 - Weapons, equipment, vehicles
 - Tactics, strategies, and access
- Review response procedures
 - Normal operating procedures
 - Contingency procedures
- Review assessment, communication, and deployment times



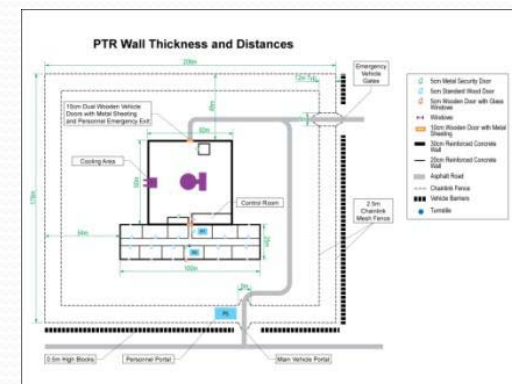
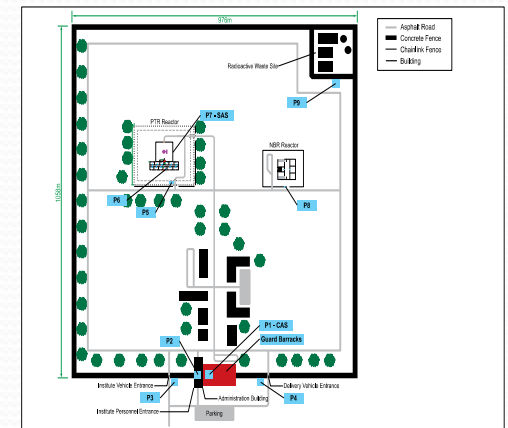


Tools to Characterize the Response

- ***Picture in Time:*** A description of the guard and/or response forces at a single point in time, indicating date and time, location of each unit, and possibly including some or all of the following information:
 - Status of each person's weapon, radio, and other equipment
 - Status of any vehicle each person controls
 - Weather conditions
- ***Time Motion Studies:*** Tests responders arriving to a designated response point during a required time
 - Such studies are considered the foundation for the response element
 - Determines and validates required response times to arrive at various response locations derived from a contingency plan

Guard and Response Force Picture-in-Time

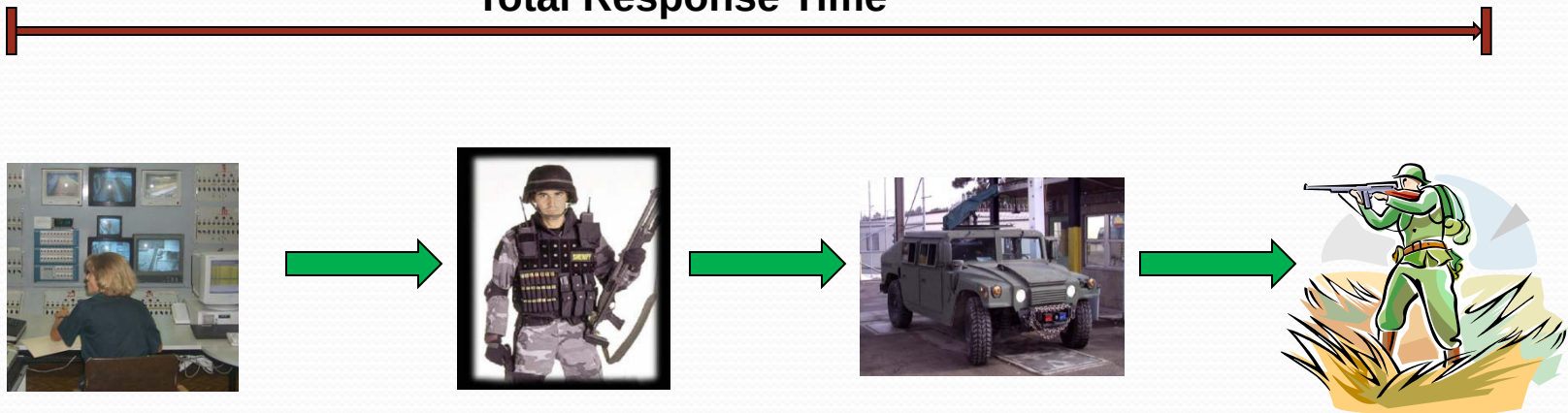
- Picture-in-time provides the stakeholders with:
 - Contingency plan
 - Post and patrol
 - Locations
 - Activities
 - Equipment status
 - Numbers
- How to collect pictures-in-time



Time Motion Study - How It Works

- Time begins at the responders origination point and ends at the dedicated response point
- Included in the overall response time:
 - Don all required equipment and firearms
 - Travel or traverse time
 - Enter through entry gates, doors, or other types of barriers

Total Response Time





Characterizing Response Against Insiders

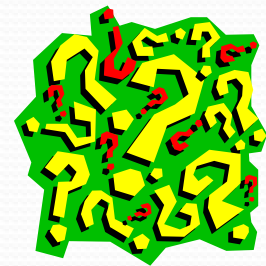
- Similar process to characterizing response against outsider threats
- Two types of response
 - The immediate response to prevent the malicious action from occurring/continuing
 - Can include co-workers as well as guards and response force
 - Immediate operational action taken by the system and operating personnel to prevent the undesired consequences

Characterizing Response Against Insiders (cont'd)

- Issues related to immediate response against insiders
 - Non-violent insiders are assumed to give up once detected
 - For violent insiders:
 - Is the insider identified?
 - Type of alarm?
 - Role for employees?
 - Where to respond?
- Issues related to operations and safety systems
 - What abnormal condition(s) initiate(s) immediate action to prevent the undesirable consequence?
 - Operations emergency plans

Summary

- Facility characterization involves gathering data that impacts the performance of the PPS
- Gather the following information during the facility characterization process
 - Security areas and layers of protection for the facility for the ASD
 - Targets and target locations
 - Facility states
 - Material Control and Accountability System
 - Operations and safety systems
 - Alarm and assessment system
 - Access control system
 - Delay mechanism descriptions
 - Response force capability



Subgroup Exercise: Facility Characterization

- Characterize the facility protection layers and elements
- Complete the worksheets for the protection elements for the targets
 - Detection
 - Delay
 - Response
- Define the protection elements that will be used for the path in outsider analysis

Module 5

Vulnerability Analysis Threat Worksheet

Adversary Action: _____ Theft _____ Sabotage _____ Other

Motivation: _____ Ideological _____ Economic _____ Personal

Capabilities: (Describe each)

Number of attackers:

Type of attackers:

Type of weapons:

Explosives (type and quantity):

Transportation:

Power and hand tools:

Technical skills:

Level of funding:

Infrastructure:

Collusion with Insider: _____ No _____ Yes: _____ passive _____ active support

Other Considerations:

Module 5: Data Collection and Facility Characterization Exercise

Session Objectives

After the session, you will be able to:

1. Document the facility protection layers and elements
2. Fill in the worksheets with detection, delay, and response information for the targets analyzed earlier

Exercise 1 – Characterize Facility Protection Layers and Elements

Step 1: Identify Facility Protection Layers

Using a poster of the LNRI facility, identify each of the protection areas with a different color of marker. Keep this poster on the wall for future reference.

Step 2: Review the LNRI Facility ASD

Review the LNRI Facility ASD. Ensure that the areas match the areas you drew on the map; if not, reconcile the differences. This ASD will be used for the rest of the VA.

Exercise 2 – Complete the worksheets for the Protection Elements for Identified Targets

Step 1: Fill in Protection Element Data Collection Worksheet

Protection element data should be collected for each element on each layer of the facility. Worksheets are a good way to gather this information. For this exercise, you will focus on the elements for the protection layer between the Institute Limited Area and the PTR Protected Area. Fill in the element with its corresponding detection, assessment, and delay for each element. The additional element layer data will be provided to you.

Protection Element Data Collection Worksheet

Protection Layer: Between Institute Limited Area and PTR Protected Area

[illegible]

Exercise 3 – Protection Areas/Layers Worksheet

Use your Adversary Sequence Diagram (ASD) to complete the Protection Areas/Layers worksheet for your team's assigned target. In the second column list each area name. In the Traversal Mode column, determine whether vehicle travel is possible or limited to foot travel only. Determine the distance across the area. The distance across the area may vary depending on which path is taken. Determine a distance and document the assumption associated with the estimated distance. Add any additional notes or comments in the last column of the worksheet.

Areas/Layers Worksheet					
Area No.	Area Name	Traversal Mode	Distance Across Area (meters)	Assumptions	Notes/Comments
Offsite	Offsite	☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
1.		☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
2.		☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
3.		☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
4.		☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			
5.		☐ Limited to Foot Traversal ☐ Vehicle Traversal Possible			

Exercise 4 – Collect Guard and Response Force Data

The following types of Guard and Response Force information should be collected from the data book for each target in a facility:

- Response Force Posture data, containing information about weapons, response strategy, number of guards or response forces, transport, and time components of PPS Response Time
- Rules of Engagement
- Order of Battle data

Note that the same Order of Battle form can be used to collect response arrival information for specific paths and scenarios. There is a direct link between the critical events on the Order of Battle form and the Response Storyboard.

Step 1: Collect and review data about the Guard and Response Force Posture

For a specific site target, Response Force Posture data contain information about number of guards or response forces, their weaponry, equipment and transport, as well as the response strategy, which units are involved in the response, and time components of PPS Response Time. This information is captured in two forms, shown below:

- The Guard and Response Force Description Data Form, collecting information about each guard and response unit that is generally valid for a specific shift.
- The PPS Response Time Data Form, collecting information about who responds and at what time to a specific target during a specific shift.

Please fill out the PPS Response Time Data Form for the operational shift (day shift or closed) that your subgroup is analyzing.

Guard and Response Force Description Data

Shift: _____

Post No.	Description/Location	Guard/ RF Type	Numbers	Weapons	Body Armor	Transport	Equipment	Communications
P1	Institute Personnel Entrance	Guard		Baton	No	Car	Hand cuffs, Flashlight	Hand-held (HH) radio
		Totals						
Offsite	Description							

*HG = Handgun; **SAR = Semi-Automatic Rifle

Shift: _____

Response Strategy:_____

Step 2: Collect Rules of Engagement Information about Groups/Types of Guards and Responders

The purpose of this subgroup exercise is to identify the Rules of Engagement that the response force will use against an adversary strategy of sabotage at the Institute. Complete the table below, using information from the *Exercise Data Book*.

Target: _____

Shift: _____

Adversary Objective: _____

Response Strategy: _____

Rules of Engagement Form

Response Group or Type	Strategy	Objective	Tactic	Technique
Target posts	Denial	Delay, Evacuate	Avoid	Non-lethal
Other posts				
Patrols				
Tactical teams onsite				
Local Law Enforcement Agencies (LLEAs)				
Military units				
Other				

Strategies could include, but may not be limited to:

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

Each strategy should have an objective, which may include:

- Observation
- Delay
- Evacuate personnel
- Interruption
- Neutralization
- Arrest
- Backup

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

- Avoid engagement
- Engage at will
- Engage on command
- Engage on necessity
- Co-ordinated engagement

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

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

Exercise 5 – Physical Protection System Features Summary Worksheet

Determine whether each physical protection feature requires a review during the site visit. If it is determined that a specific physical protection feature is not going to be included in the analysis, document the rationale for the decision (last column). If the physical protection feature does not exist, record a not applicable (“NA”) in the second column. Note: more physical protection features may be included during the site visit and should be recorded on this worksheet at a later time.

Physical Protection System Features Summary Worksheet		
Site:	Date:	Recorded by:
Physical Protection Features Summary	Review? Yes / No / NA	Justification (Comments)
1. Boundary and perimeter		
Fencing		
Vehicle barriers		
Isolation/clear zones near perimeter		
Other:		
Boundary entrances		
Personnel and vehicle		
Entrance construction		
Entrance locks		
Entrance barriers		
Other potential entry (egress gates, culverts, drains, manholes, etc.)		
Physical Protection Features Summary	Review? Yes / No / NA	Justification (Comments)
Distance between boundary and building		
Building 1 construction:		
Entrance construction (doors, windows, vents, skylights, etc.)		
Entrance locks		
Entrance barriers		
Distance from building entrance to critical assets		
Building 2 construction:		
Entrance construction (doors, windows, vents, skylights, etc.)		
Entrance locks		
Entrance barriers		
Distance from building entrance to critical assets		

Building 3 construction:		
Entrance construction (doors, windows, vents, skylights, etc.)		
Entrance locks		
Entrance barriers		
Distance from building entrance to critical assets		
Additional Notes:		

Physical Protection System Features Summary Worksheet (cont'd)		
Physical Protection Features Summary	Review?	Justification (Comments)
	Yes / No / NA	
2. Entry control features		
a. ID/authorization verification		
b. Access controls		
3. Contraband detection (persons, packages, vehicles)		
4. Alarms and assessment capability		
a. Methods: video, employees, security personnel, other		
b. Monitors and alarm stations (if applicable)		
c. Where displayed		
d. Where controlled		
e. Alarm destination (commercial company, P _D , etc.).		
f. Tamper-indicating measures		

5. Communication lines/methods		
6. Security personnel and response force		
a. Onsite security guards/officers		
b. Communications		
c. Patrols		
d. Secondary response forces? (e.g., state/local law enforcement agencies, military, emergency response, etc.)		
7. Other:		
a. Item:		
b. Item:		
c. Item:		
d. Item:		
Additional Notes:		

Area Requiring Verification Worksheet		
Describe Area Requiring Verification:		
	Description	Comments
Reason for Activity		
Test Type		
Equipment Needed		
Personnel Required		
Conditions for Test		
Time Required for Test		
When Test Is Preferred to Be Conducted		
Expected Operational impacts		
Other:		

Module 5. Data Collection and Facility Characterization Exercise

Solutions

Session Objectives

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

1. Document the facility protection layers and elements
2. Fill in the worksheets with detection, delay, and response information for the targets analyzed earlier

Exercise 1 – Characterize Facility Protection Layers and Elements

Step 1: Identify Facility Protection Layers

Using a poster of the LNRI facility, identify each of the protection areas with a different color of marker. Keep this poster on the wall for future reference.

Step 2: Review the LNRI Facility ASD

Review the LNRI Facility ASD. Ensure that the areas match the areas you drew on the map, if not reconcile the differences. This ASD will be used for the rest of the VA.

Exercise 2 – Complete the worksheets for the Protection Elements for Identified Targets

Step 1: Fill in Protection Element Data Collection Worksheet

Protection element data should be collected for each element on each layer of the facility. Worksheets are a good way to gather this information. For this exercise, you will focus on the elements for the protection layer between the Institute Limited Area and the PTR Protected Area. Fill in the element with its corresponding detection, assessment, and delay for each element. The additional element layer data will be provided to you.

Protection Element Data Collection Worksheet

Protection Layer: Between Institute Limited Area and PTR Protected Area

Element	Detection	Assessment	Distance/Delay	Comments
PTR Isolation Zone	Fence sensor on outer fence Active IR between fences Four sectors	CCTV cameras, Two per sector	1.5-m-high concrete blocks 2.5-m chain link fence (2) 12-m between fences	See page 21, 22 LNRI Data Book
Portal P5	Badge swipe Picture badge exchange BMS	Guard	20-cm reinforced concrete wall Guard 5-cm wood door with window	See page 22, 23 LNRI Data Book
Roof over P5	None	Guard (daytime only)	20-cm reinforced concrete roof	See page 23 LNRI Data Book
Main Vehicle Portal	BMS Active IR 2 m high	CCTV cameras (2)	Active barrier High-security padlock	See page 21, 22 LNRI Data Book
Emergency Vehicle Portal	BMS Active IR 2 m high	CCTV cameras (2)	Active barrier High-security padlock	See page 21, 22 LNRI Data Book

Exercise 3 – Protection Areas/Layers Worksheet

Use your Adversary Sequence Diagram (ASD) to complete the Protection Areas/Layers worksheet for your team's assigned target. In the second column list each area name. In the Traversal Mode column, determine whether vehicle travel is possible or limited to foot travel only. Determine the distance across the area. The distance across the area may vary depending on which path is taken. Determine a distance and document the assumption associated with the estimated distance. Add any additional notes or comments in the last column of the worksheet.

Areas/Layers Worksheet					
Area No.	Area Name	Traversal Mode	Distance Across Area (meters)	Assumptions	Notes/Comments
Offsite	Offsite	☐ Limited to Foot Traversal ☒ Vehicle Traversal Possible			
1.	Institute Limited Area	☐ Limited to Foot Traversal ☒ Vehicle Traversal Possible	About 200 M	Using minimum distance to PA from Institute Fenceline	
2.	PTR Protected Area	☐ Limited to Foot Traversal ☒ Vehicle Traversal Possible	33 m	Using minimum distance (Isolation zone to P6) page 23	
3.	PTR Reactor Building	☒ Limited to Foot Traversal ☐ Vehicle Traversal Possible	5 m	Using minimum distance across (P6 to D60/1 portal)	
4.	PTR Reactor Hall	☒ Limited to Foot Traversal ☐ Vehicle Traversal Possible	4 m	Using minimum distance across (D60/1 to CR door)	
5.	Control Room Interior	☒ Limited to Foot Traversal ☐ Vehicle Traversal Possible	4 m	Nominal distance not knowing exact locations	

Exercise 4 – Collect Guard and Response Force Data

The following types of Guard and Response Force information should be collected from the data book for each target in a facility:

- Response Force Posture data, containing information about weapons, response strategy, number of guards or response forces, transport, and time components of PPS Response Time
- Rules of Engagement and
- Order of Battle data.

Note that the same Order of Battle form can be used to collect response arrival information for specific paths and scenarios. There is a direct link between the critical events on the Order of Battle form and the Response Storyboard.

Step 1: Collect and review data about the Guard and Response Force Posture:

For a specific site target, Response Force Posture data contain information about number of guards or response forces, their weaponry, equipment and transport, as well as the response strategy, which units are involved in the response, and time components of PPS Response Time. This information is captured in two forms, shown below:

- The Guard and Response Force Description Data Form, collecting information about each guard and response unit that is generally valid for a specific shift.
- The PPS Response Time Data Form, collecting information about who responds and at what time to a specific target during a specific shift.

Please fill out the PPS Response Time Data Form for the operational shift (day shift or closed) that your subgroup is analyzing.

Guard and Response Force Description Data

Shift: __Dayshift as Example__

Post No.	Description/Location	Guard/ RF Type	Numbers	Weapons	Body Armor	Transport	Equipment	Communications
P1	Institute Personnel Entrance	Guard	2	Baton	No	Car	Hand cuffs, Flashlight	Hand-held (HH) radio
P2	HAW Facility Entrance (SAS)	Guard	1	Baton	No	Foot	Hand cuffs, Flashlight	Hand-held radio
P3	Vehicle Entrance (Main Gate)	Guard	1	Baton	No	Car	Hand cuffs, Flashlight	Hand-held radio
P4	Delivery vehicle entrance (Main Gate)	Guard	0					
P5	PTR Personnel and Vehicle Portals	Guard	1	Baton	No	Foot	Hand cuffs, Flashlight	Hand-held radio
P6	PTR Building Personnel Portal	Guard	1	Baton	No	Foot	Hand cuffs, Flashlight	Hand-held radio
P7	CAS (includes commander)	Guard	2	Baton	No	Foot	Hand cuffs, Flashlight	Hand-held radio
P8	PTR Emergency Vehicle Portal	Guard	0					
P9	PTR Emergency Vehicle Portal	Guard	2	Baton	No	Foot	Hand cuffs, Flashlight	Hand-held radio
		Totals	10					
Offsite	Description							
Police	Two 2-man Police Patrols	Police patrols	4	9-mm HG,* one SAR** per car	No	Car	Hand cuffs, Flashlight	Hand-held radio
Two	2 5-man military tactical response teams	Military Tactical Units	10	SAR** + baton one 7.62-mm sniper per team	Yes	Two trucks	Hand cuffs, Flashlight	Hand-held radio

*HG = Handgun; **SAR = Semi-Automatic Rifle

PPS Response Time Data

Target: PTR Control Room

Shift: Dayshift as Example PP1 has # deployed=0 during nights weekends

Adversary Objective: Sabotage Reactor

Response Strategy: Blank, no data

Unit	Type	Include?	Number Deployed	(1)	(2)	(3)	(4)	(5)	(1)+....(5)
				Alarm Communication	Assessment	Communication	Preparation	Travel and Deployment	Arrival Time
P1	Guard	Yes	1*	1	45	25	30 locking	stays	101s
P2	SAS Guard	Yes	0						
P3	Guard	Yes	1	1	45	25	30 locking	45	146s
P5	Guard	Yes	1	1	45	25	30 locking	45	146s
P6	Guard	Yes	1	1	45	25	30 locking	45	146s
P7	Guards at CAS	Yes	1***	1	45	25	30	45	146s
P9	Guards	Yes	2	1	45	25	30	45	146s
Police	Patrols	Yes	2	1	45	25	15	240	326s
Military	Teams	Yes	10	1	45	25	90	600	761s

*during day one guard responds while the other stays to lock up P1 and stand-by for the offsite response. At night the one guard at P1 stays and locks up and stands-by for offsite response. *** commander only

Step 2: Collect Rules of Engagement Information about Groups/Types of Guards and Responders

The purpose of this subgroup exercise is to identify the Rules of Engagement that the response force will use against an adversary strategy of sabotage at the Institute. Complete the table below, using information from the *Exercise Data Book*.

Target: PTR Control Room

Shift: All

Adversary Objective: Sabotage Reactor

Response Strategy: Blank no data

Rules of Engagement Form

Response Group or Type	Strategy	Objective	Tactic	Technique
Target posts	Denial	Delay, Evacuate	Avoid	Non-lethal
Other posts	Denial	Delay, Evacuate	Avoid	Non-lethal
Patrols	Denial	Observe	Avoid	Non-lethal
Tactical teams onsite	NA	--	--	--
Local Law Enforcement Agencies (LLEAs)	Containment	Arrest	Engage on necessity	Deadly force
Military units	Denial of task	Neutralize	Coordinated engage	Deadly force
Other	-			

Strategies could include, but may not be limited to:

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

Each strategy should have an objective, which may include:

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

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

- Avoid engagement
- Engage at will,
- Engage on command,
- Engage on necessity, and
- Co-ordinated engagement.

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

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

Exercise 5 – Physical Protection System Features Summary Worksheet

Determine whether each physical protection feature requires a review during the site visit. If it is determined that a specific physical protection feature is not going to be included in the analysis, document the rationale for the decision (last column). If the physical protection feature does not exist, record a not applicable (“NA”) in the second column. Note: more physical protection features may be included during the site visit and should be recorded on this worksheet at a later time.

Physical Protection System Features Summary Worksheet		
Site:	Date:	Recorded by:
Physical Protection Features Summary	Review?	Justification (Comments)
	Yes / No / NA	
1. Boundary and perimeter		
Fencing		
Vehicle barriers		
Isolation / clear zones near perimeter		
Other:		
Boundary entrances		
Personnel and vehicle		
Entrance construction		
Entrance locks		
Entrance barriers		
Other potential entry (egress gates, culverts, drains, manholes, etc.)		
Physical Protection Features Summary	Review?	Justification (Comments)
	Yes / No / NA	
Distance between boundary and building		
Building 1 construction:		
Entrance construction (doors, windows, vents, skylights, etc.)		
Entrance locks		
Entrance barriers		
Distance from building entrance to critical assets		
Building 2 construction:		
Entrance construction (doors, windows, vents, skylights, etc.)		
Entrance locks		
Entrance barriers		
Distance from building entrance to critical assets		

Physical Protection System Features Summary Worksheet		
Building 3 construction:		
a. Entrance construction (doors, windows, vents, skylights, etc.)		
b. Entrance locks		
c. Entrance barriers		
d. Distance from building entrance to critical assets		
Additional Notes: 		

Physical Protection System Features Summary Worksheet (cont'd)		
Physical Protection Features Summary	Review?	Justification (Comments)
	Yes / No / NA	
2. Entry control features		
a. ID/authorization verification		
b. Access controls		
3. Contraband detection (persons, packages, vehicles)		
4. Alarms and assessment capability		
a. Methods: video, employees, security personnel, other		
b. Monitors and alarm stations (if applicable)		
c. Where displayed		

Physical Protection System Features Summary Worksheet (cont'd)

d.	Where controlled		
e.	Alarm destination (commercial company, P _D , etc.).		
f.	Tamper-indicating measures		
5. Communication lines/methods			
6. Security personnel and response force			
a.	Onsite security guards/officers		
b.	Communications		
c.	Patrols		
d.	Secondary response forces? (e.g., state/local law enforcement agencies, military, emergency response, etc.)		
7. Other:			
a.	Item:		
b.	Item:		
c.	Item:		
d.	Item:		
Additional Notes:			

Area Requiring Verification Worksheet		
Describe Area Requiring Verification:		
	Description	Comments
Reason for Activity		
Test Type		
Equipment Needed		
Personnel Required		
Conditions for Test		
Time Required for Test		
When Test Is Preferred to Be Conducted		
Expected Operational impacts		
Other:		

Module 5: LNRI ASD

O	PD		T(sec)		Offsite									
	Institute Wall		Portal P1		Portal P3		Portal P4		Admin Bldg Roof					
	PD	0.01	PD	0.1	PD	0.1	PD	0.1	PD	0.02				
	T(sec)	10	T(sec)	35	T(sec)	5	T(sec)	5	T(sec)	10				
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:					
A	PD	0	T(sec)	60	Institute Limited Area									
	Portal P5		Main Veh Portal		Emg. Veh Portal		Isolation Zone		Roof over P5					
	PD	0.15	PD	0.15	PD	0.15	PD		PD	0.52				
	T(sec)	63	T(sec)	83	T(sec)	53	T(sec)		T(sec)	0.87				
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:					
B	PD	0	T(sec)	9	PTR Protected Area									
	Portal P6		Window		20 cm Surface		Cooling Duct		S/R Veh Door		Emg. Door		30 cm surface	30 cm roof
	PD	0.45	PD	0	PD	0.95	PD	0.1	PD	0.76	PD	0.76	PD	0.95
	T(sec)	20	T(sec)	0	T(sec)	180	T(sec)	174	T(sec)	30	T(sec)	12	T(sec)	195
	JUMP:		JUMP:		JUMP:		JUMP:	To D	JUMP:	To D	JUMP:	To D	JUMP:	To D
C	PD	0	T(sec)	2	PTR Reactor Building									
	Portal at D60		30 cm Surface											
	PD	0.6	PD	0.1										
	T(sec)	43	T(sec)	195										
	JUMP:		JUMP:											
D	PD	0	T(sec)	7	PTR Reactor Hall									
	C. Rm. Door		C.Rm. Windows		C.Rm. Walls									
	PD	0.02	PD	0.02	PD	0.02								
	T(sec)	12	T(sec)	6	T(sec)	180								
	JUMP:		JUMP:		JUMP:									
F	PD	0	T(sec)	2	Control Room Interior									
	Target Sab Task													
	PD	0.02												
	T(sec)	780												
	JUMP:													
G	PD		T(sec)											

Protection Element Data Collection Worksheet

Protection Layer: Between Offsite and Institute Limited Area

Element	Detection	Assessment	Distance/Delay	Comments
Institute Wall			Concrete Fence	See page 8 LNRI Data Book
Portal P1	Single Guard	Single Guard		See page 11 LNRI Data Book
Portal P3	Single Guard	Single Guard		See page 11 LNRI Data Book
Portal P4			High Security Padlock	See page 11 LNRI Data Book
Admin Building Roof				See page 8 LNRI Data Book

Protection Element Data Collection Worksheet

Protection Layer: Between Institute Limited Area and PTR Protected Area

Element	Detection	Assessment	Distance/Delay	Comments
Four	Fence sensor on outer fence Active IR between fences 4 sectors	CCTV cameras, Two per sector	1.5-m-high concrete blocks 2.5-m chain link fence (2) 12 m between fences	See page 21, 22 LNRI Data Book
Portal P5	Badge swipe Picture badge exchange BMS	Guard	20-cm reinforced concrete wall Guard 5-cm wood door with window	See page 22, 23 LNRI Data Book
Roof over P5	None	Guard (daytime only)	20-cm reinforced concrete roof	See page 23 LNRI Data Book
Main Vehicle Portal	BMS Active IR 2 m high	CCTV cameras (2)	Active barrier High-security padlock	See page 21, 22 LNRI Data Book
Emergency Vehicle Portal	BMS Active IR 2 m high	CCTV cameras (2)	Active barrier High-security padlock	See page 21, 22 LNRI Data Book

Protection Element Data Collection Worksheet

Protection Layer: Between PTR Protected Area and Reactor Building

Element	Detection	Assessment	Distance/Delay	Comments
Portal at P6	Balanced Magnetic Switch on Both Doors Door1: Badge Swipe Reader Door 2: Card Reader & PIN Keypad Metal Detector	CCTV Camera, ½-in. format 800 pixels	Door 1: 5-cm Wooden Door with Glass Windows Door 2: 5-cm Metal Security Door	See page 23,24 LNRI Data Book
Window				See page 24, 25 LNRI Data Book
20 cm Surface			20-cm Reinforced Concrete Wall	See page 24,25 LNRI Data Book
20 cm Surface			20-cm Reinforced Concrete Wall	See page 24, 25 LNRI Data Book
Cooling Duct			Mild Steel, 0.3 cm thick with 13-mm rebar grill on 15-cm centers	See page 20 LNRI Data Book
Shipping Door	Balanced Magnetic Switch	CCTV Camera, ½-in. format 800 pixels	2 High Security Padlocks	See page 24, 25 LNRI Data Book
Emergency Door?				
30 cm Surface			30-cm Reinforced Concrete Wall	See page 24, 25 LNRI Data Book
30 cm Roof			3- cm Reinforced Concrete Wall	See page 24, 25 LNRI Data Book

Protection Element Data Collection Worksheet

Protection Layer: Between PTR Reactor Building and PRT Reactor Hall

[illegible]

Protection Element Data Collection Worksheet

Protection Layer: Between PTR Reactor Hall and Control Room Interior

Element	Detection	Assessment	Distance/Delay	Comments
Control Room Door		CCTV Camera, ½-in. format 800 pixels	5-cm Wooden Door with Glass Window	No data for wooden doors See Pages 24, 25 LNRI Data Book
Control Room Window				See Pages 24, 25 LNRI Data Book
Control Room Walls			20-cm Reinforced Concrete Wall	See Pages 24, 25 LNRI Data Book



Data Collection Site Visit

Module 6

Vulnerability Analysis Training Course
Date:

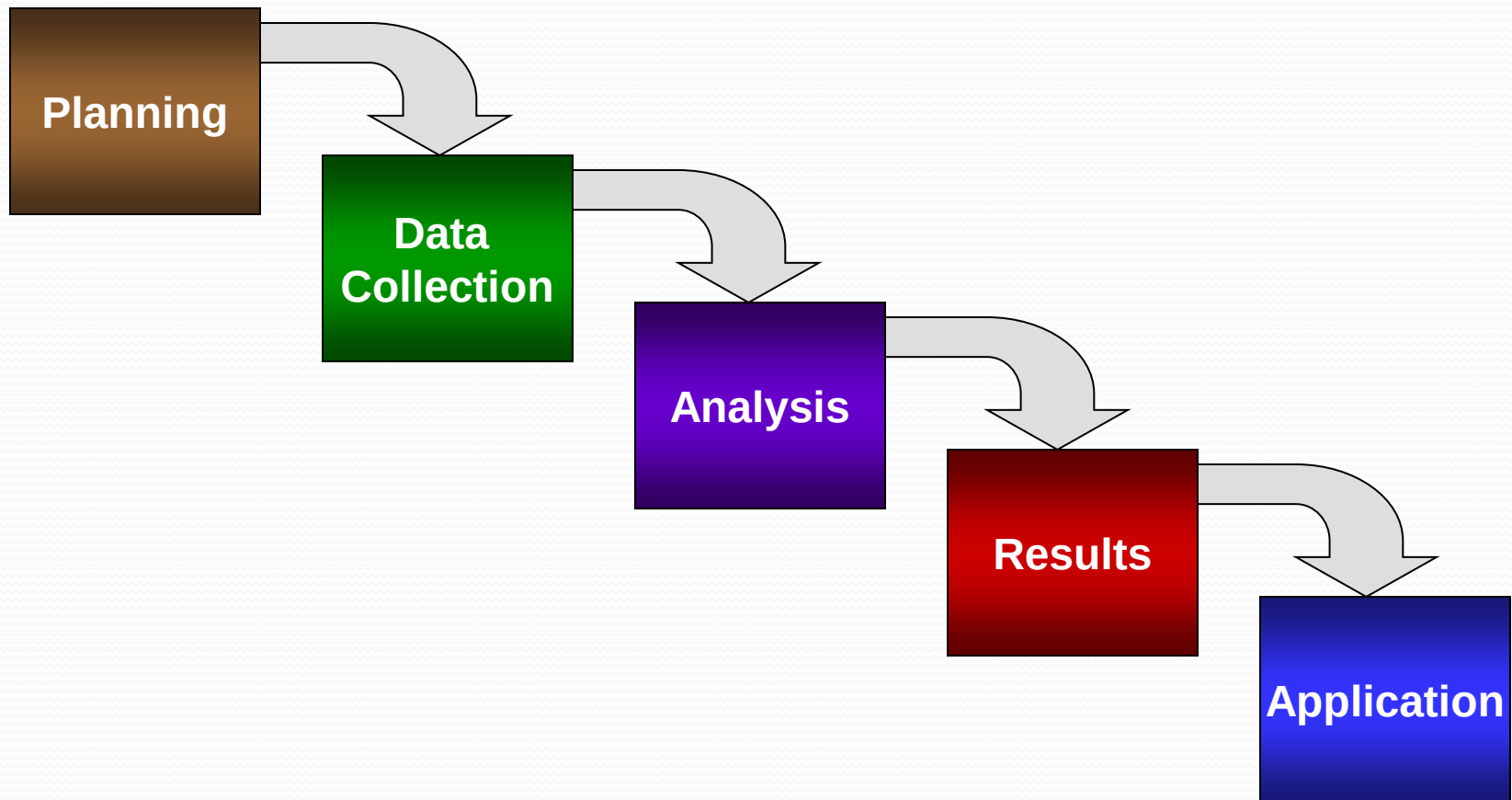


Student Learning Objectives

After completing this module, you should be able to:

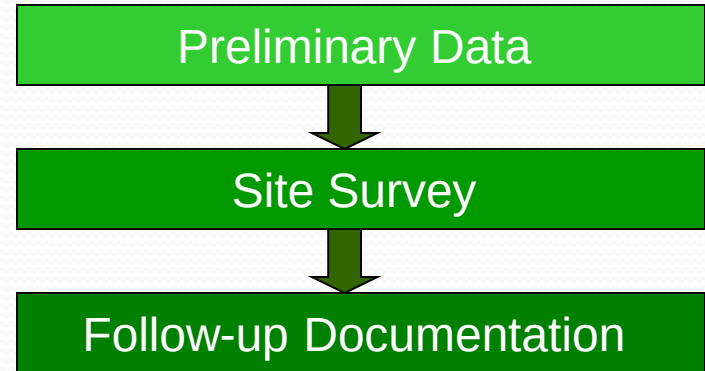
- Describe the purpose and general format of a site visit
- List specific activities to be completed during the visit
- Identify techniques to organize and distill gathered information
- Identify post-visit activities

Phases of Vulnerability Analysis



Data Collection – Types of Data

- Facility Characterization
 - PPS documentation
 - Open sources
 - Site survey
 - Test data
- Design Basis Threat
 - State
 - Regional or local
 - Facility
 - Outsider and insider
- Target Identification/Consequences
 - Types and characteristics of material
 - Location of material and vulnerable equipment
 - Prioritized theft targets and sabotage vital areas



May take three phases to complete the picture



Purpose of Site Visit

- Visually orient against received documentation
- Verify received data
- Complete missing information on the site-specific selected worksheets
- Confirm assumptions
- Interview appropriate site personnel to collect required data
 - Review security policies and procedures
 - Print versus practice



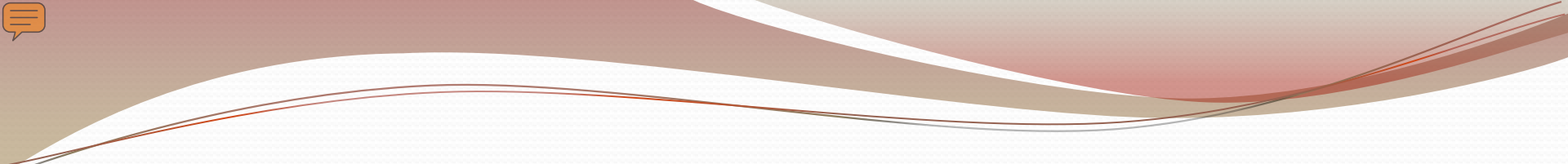
Knowledge of Site Before Visit

- The site visit team should have an deep knowledge of the data collected during preliminary data collection:
 - Mission and mission objectives
 - Site drawings, facility, and building layouts
 - Reports (safety, security, periodic, etc.)
 - Targets and locations
 - Types of threats to be considered – outsider and insider
 - Security culture
 - Maintenance and repair records
 - Site operating procedures
 - Emergency management operations plans
 - Security policies and procedures
 - Currently existing security features (physical, information protection, consequence mitigation, etc.)



Site Visit Process

- Stakeholders/management pre-briefing
- Conduct site tours
- Conduct interviews of facility personnel
- Validate data
- Post-brief



Site Visit Pre-briefing

- Introductions
- Purpose and approach for VA
- Summarize information gathered prior to the site visit
 - Protection objectives
 - Target set
 - Threat model
 - Assumptions
- Summarize areas requiring additional information
- Provide detailed descriptions of the activities needed and rationale
- Negotiate schedule to meet site's safety and security requirements during the planned activities
- Discuss an approach for conflict or information resolution
- Obtain permission for photos and videos

Obtain concurrence on information and activities

Conduct Site Tour

- Resolve the issues raised during the pre-site-visit document review
- Watch for new areas of potential information
- Look for problems previously not identified
- Review new documents
- Interview management, operational, and security personnel
- Build relationships with contacted personnel



Verify Data

- Observe the site's processes and procedures
- Visit each of the target areas
- Verify and validate previous opinions
- Performance testing in accordance with developed procedures
 - To verify physical security function
 - To complete data (preliminary data are inadequate or inconsistent)
 - To observe circulation control



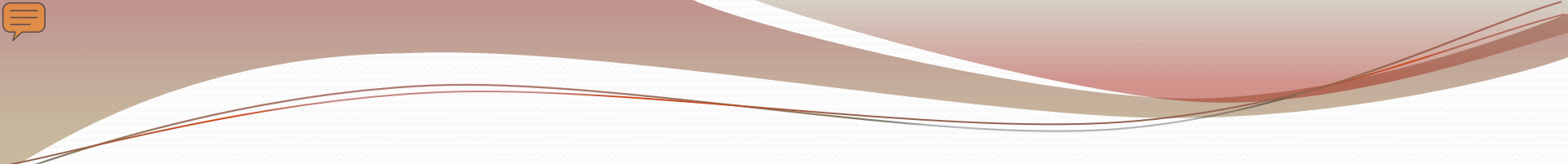
Follow Procedures for Site Activities

- Use planned procedures for
 - Testing equipment
 - Operational tests
 - Sensitivity tests
 - Personnel
 - Access control
 - Operating procedures
 - Time to perform tasks
- Develop procedures for impromptu activities
 - Describe needs to site hosts
 - Work cooperatively to arrive at an agreed procedure
 - Respect the site concerns about conducting unplanned activities



Example Form for Verification Activities

Item	Response
Reason for activity	
Test type	
Equipment needed	
Personnel required	
Conditions for test	
Time required	
When test is to be conducted	
Expected operational impacts	



Example Form for Verification Activities

Item	Response
Reason for activity	<i>Need to verify visual capabilities at night along perimeter</i>
Test type	<i>Observation from towers for activity between fences</i>
Equipment needed	<i>None</i>
Personnel required	<i>Escort, tower personnel, person moving in perimeter</i>
Conditions for test	<i>Dark with lighting on</i>
Time required	<i>1 hr</i>
When test is to be conducted	<i>In two days at 11 pm</i>
Expected operational impacts	<i>Shouldn't impact normal operations. All protection personnel on shift should be informed of test</i>



Conducting Interviews

- Build relationships with personnel
- Interview individuals, not groups
- Assure confidentiality
- Ask open-ended questions. For example:
 - Please give a description of your job.
 - Describe the processes or operations you are involved in and your responsibilities.
 - What do you do when unusual or abnormal situations occur?
- Paraphrase interviewee's responses and verify information
- Acquire information for both an outsider and insider perspective

Insider Access Discussion Points

- Authorized in work areas
- Special temporary access
- Escorted or unescorted access
- Emergency access (fire, medical, police)
- Access control systems
- Access to target
 - Duration of target exposure
 - Conditions of target during insider access
- Protection equipment and process tools
- Special site equipment

Insider Knowledge Discussion Points

- Targets
 - Locations, characteristics and details of targets
 - Details of facility layout
- Security Systems
- Processes, procedures and operations
- Safety and radiation protection systems
- Available tools and equipment

Insider Authority Discussion Points

- Over People
 - Designated authority over others
 - Personal influence over others
- Over Tasks and Equipment
 - Assessment of alarms
 - Preparation of sensitive forms
 - Authorization of processes and procedures
- Temporary Authority?
- Falsified Authority?
- Exemption From Procedures?

Photos and Videotapes

- Help document what was observed
- Log
 - Photo number
 - Content of photo
 - Location of photo
 - Date and time
- Better to take too many photos than not enough
 - Especially if there is not an opportunity to return to site
 - Very useful for final report and debriefings



Daily Updates While on Site

Start of Day (site personnel and site team survey)

- Site survey team usually attends
- Meet with all site personnel who desire an update
- Work to assure inclusion of the affected individual and areas
- Build rapport rather than criticize – remember the site wants to improve
- Apply the agreed approach for conflict and discrepancy resolution if needed
- Outline direction and activities for the day

End of Day (site survey team only)

- Coordinate obtained information
- Identify additional data needs and/or confirmation
- Document information, actions, and issues

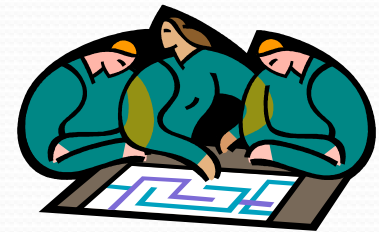


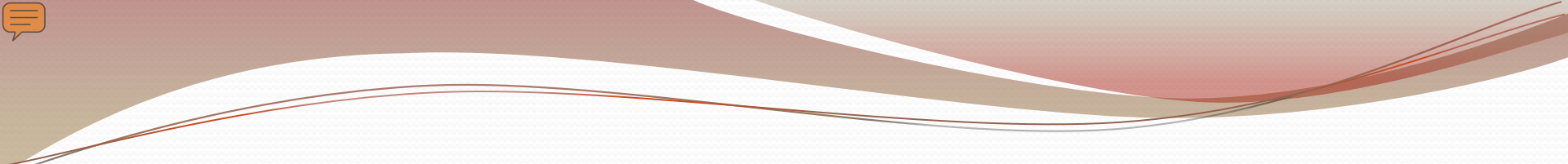
Approach for Resolution

- Resolve issues between the team and the site personnel
 - Discuss with all involved parties
 - Make sure all know the reason for the issue
 - Discuss potential solutions for resolution
 - Invite site ideas on resolution
 - Make sure advantages and disadvantages are completely discussed
- If issues cannot be resolved, then establish an oversight review panel to make decisions
 - Panel could include the VA team lead and a site manager

Organizing for the Post-Briefing

- Prepare for post-briefing
 - Document ideas before the post-briefing
 - Solidify team concurrence
- Update
 - Site diagrams
 - Adversary Sequence Diagrams (ASDs)
 - Worksheets
- Identify discrepancies
 - Identify areas needing clarification and resolution
- Invite all affected parties





Post-Briefing

Presented by site visit team to site management

- Review team activities
 - Review purpose of VA
- Emphasize site contributions and cooperation
- Review observations and potential weaknesses associated with observations
- Encourage site discussion on observations
- Emphasize that any conclusions are preliminary pending full analysis
- Outline team's next steps
 - Analysis
 - Final report
- Establish process for further issue resolution



Post-Visit Activities

- VA team discusses results
 - Review results and obtain team consensus
 - Incorporate additional findings into system descriptions
- List items or information that site personnel agreed to provide at a later date
- Address any issues and questions that could not be resolved on the site visit
- Assign responsibility for resolving issues and obtaining additional information
- Validate changes with the site soon after the visit
- Conduct the necessary analysis and documentation

Summary

- The purpose of a site visit is to collect data at the site by taking photos, drawing sketches, obtaining on-site drawings and policies, and interviewing facility personnel to collect required data.
- The site visit should consist of:
 - Pre-briefing
 - Site tour(s)
 - Daily updates
 - Post-briefing
- Post-visit activities include reviewing results and planning next steps



Subgroup Exercise:

Conducting the Site Visit

- Review the more site-specific information about the site
- Update the site drawings
 - Add new items gathered during the site visit
- Add details to drawings for both site and facility entry control portals
- Update your ASD for the facility
- Update the log worksheet as questions and issues arise
 - Make notation for previous issues that have been resolved

Site Visit Post-Briefing

Module 6

Vulnerability Analysis Training Course
Date:

Site Visit Post-Briefing Overview

- Introductions
- Purpose and approach for VA
- Summarize information gathered prior to the site visit
 - Protection objectives
 - Target set
 - Threat model
 - Assumptions
- Purpose of site visit
- Discuss information gathered during site visit

VA Methodology/Approach

- Describe the purpose and approach you will be using to generate the expected outcomes
- Expected outcomes
 - Determine the relative effectiveness of alternative protective strategies and systems
 - Ensure that systems provide balanced protection of assets
 - Identify strengths and weaknesses in existing or planned protection systems
 - Support cost-benefit studies for system design alternatives

Site Briefing

- PPS Objectives
- Design Basis Threat
- Materials and Targets
- Possible Impact to Site
- Major Assumptions

Site Visit Plan

- Schedule
- Additional data request
- Daily briefings
- Documentation control and protection
- Describe what activities will be performed and rationale
- Operational accommodations
- Approach for conflict or information resolution
- Obtain permission for photos/videos

Activities to be Performed

- TBD

Information Gathered

- TBD

Next Steps

- TBD

Module 6: Data Collection- Site Visit Exercise

Session Objectives

After the session, you will be able to:

1. Develop a site visit plan.
2. Interview the available experts from the LNRI facility.

Introduction

This exercise includes planning for and conducting a VA site visit. (This may be a mock site visit if a real site is not available.) Follow the directions listed below to complete this exercise.

Exercise 1 – Develop a site visit plan

During the Module 4 exercises, you reviewed data that was sent to your VA team before your site visit. Now as you prepare to visit the site, you learn that you will be assigned to meet with and interview the site security manager, who is knowledgeable about both the guard force and the offsite response forces. Next you will interview the security system manager. You will have a discussion with the VA site survey team delay expert about the delay for the shipping door, who will give you some insight on how delay numbers are developed. You will also have the opportunity to meet with a site representative who will provide you additional information about the site. Given this new information, you need to prepare for the site visit.

1. Review the site information that you have gathered up to this point in the course.
2. Identify gaps and areas where you would like to gather additional information.
3. Draft questions that you will ask the site security manager.
4. Draft questions that you will ask the security system manager.
5. Draft questions that you want to ask the delay specialist about the shipping door.
Document any tests that you need to run, pictures you need to take, or other additional information.

Remember, this is your chance to gather data, so plan carefully.

Exercise 2 – Site Visit

We are now going to simulate a site visit. Each of the four interviewees will come talk to your group about their particular topic. The experts may not visit you in the same order listed here. Have your site visit plan ready and make the best of your time with each expert.

Be sure to follow good interviewing techniques, as described in the lecture:

- Assure confidentiality.
- Be courteous and respectful of the person you are interviewing; to the extent possible, establish relationships with contacted personnel.
- Ask open-ended questions (e.g., “Please give a description of your job.”).
- Try not to define your observations in terms of good and bad – that is, say “How long has that sensor not been operating?” instead of “How long has that sensor been performing badly”)
- Paraphrase interviewee’s responses and verify information.

Topic 1: Site Security Manager Interview

Review the data forms you filled in during the Facility Characterization exercise:

- The Guard and Response Force descriptive data
- The PPS Response Time data
- The Rules of Engagement form.

Discuss any data gaps you have with the manager and attempt to gain more insight into how the response by guards and response force members is performed.

Enter any notes here that do not fit on the data forms:

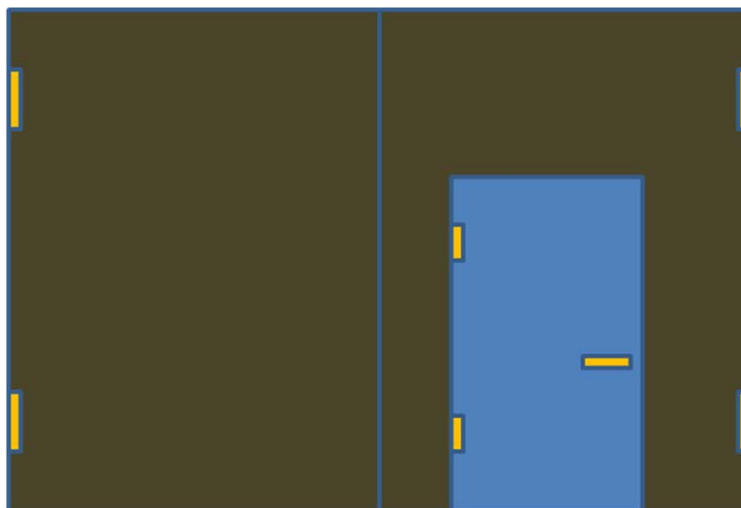
Topic 2: Security System Manager Interview

Here you will have a chance to talk to the security system manager about the intrusion sensors at the PTR Reactor area and to review alarm logs. The objective is to provide an opportunity to review an example alarm log and to understand the value of sorting this data by sensor, by cause, and by type of event.

Enter your notes here (and feel free to record information in your hypothetical facility description):

Topic 3: VA Site Survey Team Delay Expert

You will now have a chance to talk to the Site Survey Team delay expert about the PTR shipping door (illustrated below). The objective is to interview this expert to achieve a better understanding of how they develop adversary defeat methods for a door and then plan tests to develop a delay time for individual defeat methods.



Enter your notes here:

Topic 4: Interviews with a site representative who provides new information

You will be provided some additional site information by a site representative.
Formulate some questions quickly to get more insight into the topic.

Enter your notes here:

Exercise 3 – Develop Post Briefing

Follow the guidelines in the presentation from Module 5 to organize a post-briefing for this site visit. Each group will present its post-briefing to the class. There is a template available for this presentation, but there is no requirement to use it.

This briefing should include:

- The tasks that were conducted during the visit
- Observations based on your interviews (Remember not to make conclusions at this stage!)
- Next steps

Module 6

Site Visit Exercises: Instructor Notes

Exercise Part 1 – Site Visit Observations

Students will break up into three groups and rotate through these stations.

Note: These stations will present exercises to reveal site information about the LNRI facility during a simulated site visit and will present exercises about vulnerability concepts using the training facility that this course is being held in.

Station 1. Analyzing Adversary Task

1. Using the facility in which the course takes place, select a room to use as the target location.
2. Take students outside the facility and designate a perimeter.
3. Have students measure the time it takes to move from the perimeter to the entrance. Students may use 4 meters/second and the distance to calculate the time.
4. Discuss different tactics that might be used to get to the entrance and the affect on adversary time.
5. Have the students observe access control procedures:
 - a. What does it take for a vehicle to enter the site?
 - b. What does it take for a person to enter the facility?
6. Have students document actions and time each stage of movement to the target location.
7. Have students build an adversary task time diagram.

Station 2. Delay Elements

Using the plastic sheet holders with printed brick inserts,

1. Have students brainstorm how to penetrate the wall.
2. Discuss what tools and power they would need for each method.
3. Discuss the role of delay in increasing adversary task time.

Station 3. Response Force

1. Using the classroom as the alarm control center, have students describe the relationship between the alarm control center and each of the security forces: site guards, local police, response forces.
2. Discuss roles and responsibilities.
3. Discuss procedures during normal operations and during an alarm event to understand when each of the forces is engaged.
4. Discuss security force response times, the probability of interruptions, and the probability of neutralization.
5. Have students estimate response force times for the classroom facility scenario.

Exercise Part 2 – Putting Things Together

1. As a result of part one, students should have
 - a. developed an adversary task timeline
 - b. be able to define the critical detection point

- c. documented the relationship between detection, delay, response, and adversary task time
2. In part 2, students will build a basic ASD to depict the paths studied during part 1.

Site Visit – Additional Data Collected (This data is located in the Hypothetical Facility Exercise Data Book)

With Instructor Notes

Mission of LNRI

As a premier nuclear research reactor, the LNRI is host to a number of scientific experiments. The mission of the site is to support nuclear research.

Discuss how the mission relates to the role of security.

Safety Record

A review of the safety records indicates that the LNRI supports a culture of safety and shows only minor personnel accidents (slips, trips, and falls) related to traversing LNRI grounds during icy conditions. There were no safety incidents associated with the reactor operation.

Security Record

A review of security incidents revealed a less than satisfactory security culture. Security incidents seem to occur not from resident staff, but from the visiting research scientists who do not follow all the security procedures. Upon further inquiry, it was determined that visiting research scientists do not undergo site security training upon arrival, nor do they have security policies and procedures given to them as part of an orientation. Most violations relate to scientists being in unauthorized areas.

Discuss how this might be discovered during a site visit. Discuss the importance of understanding different security procedures for permanent personnel versus visiting personnel or temporary personnel. Discuss how security incidents might be different than physical protection alarms.

Recent Construction

Recent construction activity improved the drainage at the site. Most work was conducted from outside the site, but did require the temporary disabling of Sector 2 for two weeks. Guards were posted to monitor the construction and that section of the perimeter for the duration of the construction. During those two weeks, alarms from Sector 2 were masked. After construction, the sector was reactivated and performance-tested to ensure proper operation.

Discuss how abnormal events such as construction might be handled. Discuss the role of compensatory measures.

Emergency Management Operations Plans

A review of emergency management operation plans for LNRI revealed that safety is a higher priority than security. Personnel will make every attempt to secure their workspace before exiting, but not at the risk of their personal safety. Personnel are trained to notice anyone

deviating from emergency procedures and report such behavior to the nearest guard after evacuation. The team was not able to obtain copies of emergency procedures for either the guards or operators.

Discuss what these procedures might look like from a security point of view. What might be suggested for these procedures to enhance security?

Alarm Logs

Attached is a sample of the alarm log and daily activity reports from the site. A review indicated that these are typical for the site.

Discuss how trends analysis plays an important role. If the site is conducting trends analysis, they could reveal problem areas in the physical protection system related to seasons, weather, or recognizance.

Module 6: Site Visit Exercises – Additional Data Collected (This data is NOT located in the Hypothetical Facility Exercise Data Book)

With Instructor Notes

Topic 1: Site Security Manager Interview

Instructions: Go over information in Module 5 (on LNRI Site Layout and Response Force Location) and Module 8 (Response Force Data) as if this were a site briefing. Be aware of Section 7 (Entry Control Operations at LNRI Gates and Portals) to answer any procedural questions regarding entry control (or access control). Note that Module 5's name ought to cover Guard Force Locations, not RF locations.

The following information about the response is missing from their data sheets (highlighted in the figure below in dark red):

Notes on Guards:

1. *During the day, one guard responds from P1 and the other stays to lock it up and to stand by for the offsite response.*
2. *P3 deploys to that gate after locking it up during preparation; thus travel and deployment times are actually 0 (resulting in 101 s arrival time).*
3. *P5 deployment time is 50 seconds, which is above the estimated time of 45 seconds; this is due to a particularly complex set of deployment tasks.*
4. *P3, P5, and P6 all lock their posts as part of preparation.*
5. *The unit deploying from P7 is actually the guard commander; he is already armed and ready to go, so his preparation time is 0 seconds.*
6. *The P9 unit is actually a mobile unit, with response travel and deployment times that vary between 40 and 75 seconds. The 50 seconds used is more of a time-average across all such times and appears to be sufficient 90% of the time.*
7. *Regarding the Rules of Engagement form from the Module 4 exercise:*
 - a. *The patrols have a **Denial** strategy; their part is merely to **Observe** what is going on and relay the information to CAS/SAS/ and the Guard Force Commander.*
 - b. *Local law enforcement's objective is to arrest perpetrators and to engage if their lives or a civilian's life is threatened by the adversary. They cannot shoot if no-one is being threatened.*
 - c. *The Military units' strategy is denial of task (that is, the adversaries can get into the target room but cannot complete their sabotage task). Note: Please compare a strategy of denial of entry (you've got to make sure adversary doesn't enter the target room – e.g., a vital area) versus denial of task. Ask which is harder to protect against? (denial of entry). The Military unit's tactic is to engage the adversary team with a coordinated engagement (e.g., fire and perform close-quarters battle to protect the nuclear material) rather than wait until the adversary fires first.*

PPS Response Time Data

Target: _____

Shift: _____

Adversary Objective: Sabotage Reactor

Response Strategy: **Denial of Task**

Unit	Type	Include?	Number Deployed	(1) Alarm Communication	(2) Assessment	(3) Communication	(4) Preparation	(5) Travel and Deployment	(1)+....(5) Arrival Time
P1	Guard	Yes	1	1	45	25	30	45	146s
P2	SAS Guard	No	0						
P3	Guard	Yes	1	1	45	25	30 L	0: Deploys to P3 itself	101s
P5	Guard	Yes	1	1	45	25	30 L	50	151s
P6	Guard	Yes	1	1	45	25	30 L	45	146s
P7	Guards at CAS	Yes	1	1	45	25	0	45	116s
P9	Guards	Yes	2	1	45	25	15	50 ave.	136s
Police	Patrols	Yes	2	1	45	25	15	240	326s
Military	Teams	Yes	10	1	45	25	90	600	761s

L = Lock up portal as part of Preparation

Rules of Engagement Form

Response Group or Type	Strategy	Objective	Tactic	Technique
Target posts	Denial	Delay, Evacuate	Avoid	Non-lethal
Other posts	Denial	Delay, Evacuate	Avoid	Non-lethal
Patrols	Denial	Observe	Avoid	Non-lethal
Tactical teams Onsite	NA	--	--	--
Local Law Enforcement Agencies (LLEAs)	Containment	Arrest	Engage on Necessity	Deadly Force
Military Units	Denial of Task	Neutralize	Coordinated Engagement	Deadly Force

Other information for the Site Manager to point out:

BCompensatory Measures

When either of the two alarms or an assessment camera in a perimeter sector are not operating as expected, one of the patrols from P1 will be assigned to watch that sector.

Topic 2: Alarm Technician Interview

Here you will have a chance to talk to the alarm technician about the intrusion sensors at the PTR Reactor area and to review alarm logs.

Instructions: Go over information in Module 11 on exterior elements and Module 15 on interior elements. Go over each one of the elements on the diagrams: sensors, cameras, and vehicle barriers/lighting, where appropriate.

Go over the alarm log as discussed below.

Alarm Logs

Attached is a sample of the alarm log and daily activity reports from the site. A review indicated that these are typical for the site.

Discuss how trends analysis plays an important role. If the site is conducting trends analysis, they could reveal problem areas in the physical protection system related to seasons, weather, or recognizance.

Site Visit – Additional Data Collected (This data is located in the Hypothetical Facility Exercise Data Book)

With Instructor Notes

Topic 3: VA Site Survey Team Delay Expert

You will now have a chance to talk to the Site Survey Team delay expert about the PTR shipping door (illustrated below). The objective is to interview this expert to achieve a better understanding of how they develop delay times for a door and then plan tests to develop a delay time for individual defeat methods.

Discuss how to analyze hand, power, thermal tools (cutting rates) as well as explosive attacks as setup, retreat, wait, return, and cut through (if applicable) times.

Topic 4: Interviews with a Site Representative Who Provides New Information

You will be provided some additional site information by a site representative. Formulate some questions quickly to get more insight into the topic.

Mission of LNRI

As a premier nuclear research reactor, the LNRI is host to a number of scientific experiments. The mission of the site is to support nuclear research.

Discuss how the mission relates to the role of security.

Safety Record

A review of the safety records indicates that the LNRI supports a culture of safety and shows only minor personnel accidents (slips, trips, and falls) related to traversing LNRI grounds during icy conditions. There were no safety incidents associated with the reactor operation.

Security Record

A review of security incidents revealed a less than satisfactory security culture. Security incidents seem to occur not from resident staff, but from the visiting research scientists who do not follow all the security procedures. Upon further inquiry, it was determined that visiting research scientists neither undergo site security training upon arrival nor do they have security policies and procedures given to them as part of an orientation. Most violations relate to scientists being in unauthorized areas.

Discuss how this might be discovered during a site visit. Discuss the importance of understanding different security procedures for permanent personnel versus visiting personnel or temporary personnel. Discuss how security incidents might be different than physical protection alarms.

Recent Construction

Recent construction improved drainage at the site. Most work was conducted from outside the site, but did require the temporary disabling of Sector 2 for two weeks. Guards were posted to monitor the construction and that section of the perimeter for the duration of the construction. During those two weeks, alarms from Sector 2 were masked. After construction, the sector was reactivated and performance-tested ensure proper operation.

Discuss how abnormal events such as construction might be handled. Discuss the role of compensatory measures.

Emergency Management Operations Plans

A review of emergency management operation plans for LNRI revealed that safety is a higher priority than security. Personnel will make every attempt to secure their workspace before exiting, but not at the risk of their personal safety. Personnel are trained to notice anyone deviating from emergency procedures and report such behavior to the nearest guard after evacuation. We were not able to obtain copies of emergency procedures for either the guards or operators.



Performance Testing

Module 7

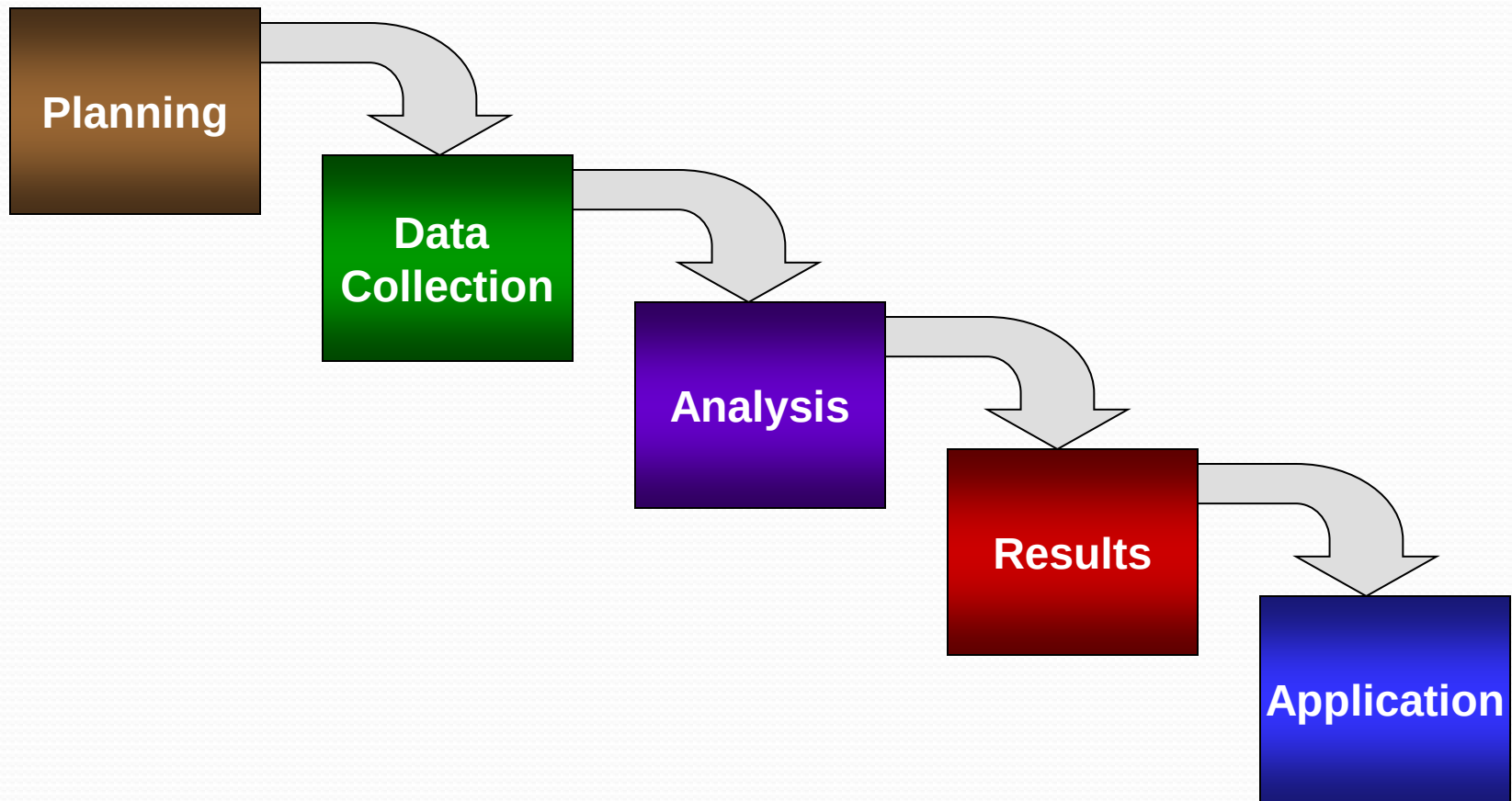
Vulnerability Analysis Training Course
Date:



Student Learning Objectives

- After completing this module, you should be able to:
 - Explain what a performance test is
 - Identify the purpose and importance of testing
 - Differentiate between different kinds of testing
 - Outline testing processes
 - Identify key elements for the test plan and test report
 - Define probability of detection and confidence levels

Phases of Vulnerability Analysis



Performance Tests

- *Performance test:* A test to evaluate the ability of an operating system element or total system to meet an established requirement
- Performance tests are methodical means to:
 - Establish or confirm a performance level of a PPS element
 - Provide comprehensive assurance of performance on a required basis
 - Determine element's baseline performance for system design
 - Test PPS elements over their planned range of operation
- Performance testing results
 - Identify whether element(s) tested performed adequately
 - If not, identifies the weakness or substandard performance



Purpose and Objectives

- Purpose of performance testing is to evaluate the performance of
 - People
 - Procedures
 - Equipment, technology, hardware
- Objectives of performance testing
 - Validate vulnerability analysis input data, assumptions, activities, results, and conclusions
 - Demonstrate protection capabilities
 - Ensure that the performance of protection elements provide adequate protection and acceptable risk





Performance Testing Program

- A testing program is needed to ensure elements implemented comply with requirements
 - All elements of the PPS function at the appropriate level of performance and work together as an effective system
- A performance testing program must be developed to:
 - Validate system performance
 - Evaluate operational continuity of all protection system components
 - Test protection elements whose failure would reduce PE to an unacceptable level
- Testing program activities and results must be documented
 - Integral part of the overall physical protection program

Types of Testing

- Example types of tests that can measure effectiveness
 - Operability and functional tests
 - Sub-system performance test
 - Whole system performance tests



Operability and Functional Tests

- Simple measure of operability – is it working?
- Simple measure of functionality – does it function as intended?
 - Performed on a frequent basis
 - Looks for significant malfunctions or outages
 - If the test fails, call maintenance and possibly take compensatory measures
- Examples (each shift):
 - Metal detectors
 - x-ray machines
 - Walk test a certain number of perimeter sectors to verify alarms are generated



Sub-system Performance Testing

- Sub-system performance testing focuses on the performance and effectiveness of either individual components or parts of the overall PPS
- Sub-system tests are conducted to:
 - Evaluate the skills, capability, or knowledge of personnel
 - Test operations, procedures, or policy requirements
- Sub-system tests should be conducted realistically—they may be either scheduled or unannounced
 - Example: protective force response to an alarm



Whole System Performance Tests

- Whole System Performance Tests are conducted to evaluate the overall effectiveness of all elements of an entire system
 - Or large portions of an entire system
 - 1st Example: Force-on-force security exercise tests the overall effectiveness of all elements involved in a response to a site-specific threat and adversary capabilities
 - 2nd Example: Used to determine how effectively individual elements perform together to form an entire system



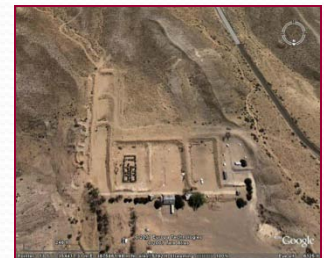
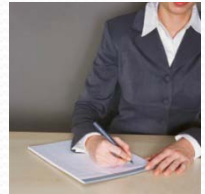
When to Conduct Performance Tests

- On new and proposed PPS equipment to determine effectiveness and limitations
- On PPS equipment after initial installation and after maintenance to verify component performance
- On new and existing security procedures – determine whether
 - Personnel understand and follow the procedures
 - Personnel and equipment interact effectively
- As necessary to ensure that protection elements are performing as designed and provide the required protection level



Performance Testing Process

- Plan the performance test
- Define test purpose, objectives, and standards
- Create a test plan
- Identify protection elements to be tested
 - Identify test locations
- Identify threats (capabilities) and develop scenarios
- Define testing methodology and evaluation criteria
- Define test controls
- Identify resource requirements
- Coordinate the tests and obtain approvals
- Identify compensatory measures
- Collect data
- Analyze, document, and critique test



Planning a Performance Test

- Before performance testing is conducted, it must be planned to ensure that the testing:
 - Will be effective
 - Will provide valid VA data
 - Will provide valid PPS performance data
- Requires developing a written test plan
 - Contains specific and detailed information necessary for efficient and effective testing
- Time and effort spent in testing can be significant
 - Want to ensure that a proper test is conducted safely with minimal impact on operations and security



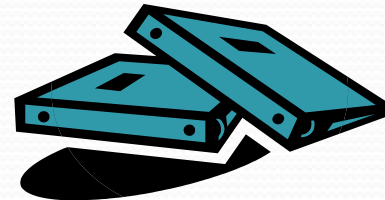
Purpose, Objectives, and Standards

- For a performance test to be clearly understood, state the purpose, objectives, and performance standards
- *Purpose*: General statement of the overall desired outcome of the performance test (describes the expected result)
- *Objectives*: Elaboration of the purpose that describes the specific test objectives to be achieved
 - Test goals
 - Tasks to be tested
 - Conditions for the test
- *Performance standards*: Describes the level of performance that is expected
 - Ensure that the protection element tested performs as required
 - Maintain high PE and low risk



Key Elements of Written Test Plans

1. Test purpose and objectives
2. Performance measures/standards
3. Test location
4. Element to be tested
5. Scenario description
6. Test methodology and evaluation criteria
7. Test controls
8. Resource requirements
9. Test coordination
10. Compensatory measures
11. Approval of performance test plans



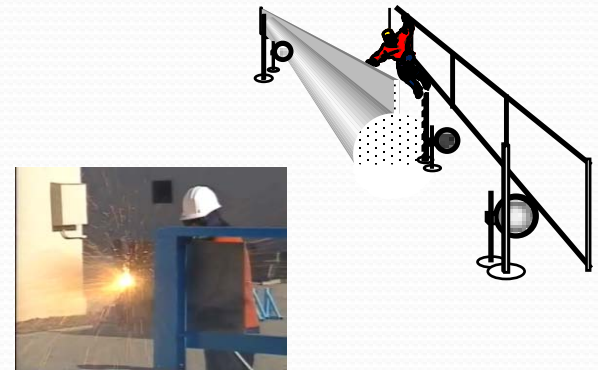
Security Elements to Be Tested and Test Location

- Identify/describe the specific security element(s)
- May need to performance test many security elements over the full spectrum of the protection system
 - Personnel, procedures, equipment/technology/hardware
- The test location should be consistent with
 - Security element(s) to be tested
 - Adversary threat (capabilities) and scenarios
- The test location should be realistic and incorporate



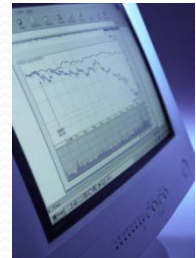
Adversary Threats, Capabilities, and Scenarios

- The PPS protection elements need to protect against the defined threat and capabilities
 - Based on the Design Basis Threat (DBT), what defeat methods may be applied to the element to be tested?
- Identify modes of attack (adversary capabilities) and develop scenarios
 - Run, walk, crawl, jump, tunnel, bridge
 - Use vehicle (air, land, water)
 - Cut, penetrate (hand/power tools)
 - Explosively penetrate
 - Deceive (falsify credential)
- Conservative approach for developing scenarios assumes skillful and cautious adversary



Test Methodology and Evaluation Criteria

- Test methodology describes how the test will be conducted
 - List steps for planning and execution of test
 - Describe statistical models or mathematical formulas
 - Number of tests to be performed for each scenario
 - Pass/fail criteria
 - Methods for data analysis
 - Record calibration settings and equipment configurations
 - Test evaluation criteria describe how the test will be assessed or scored
 - Criteria checklist for each objective listed
 - Criteria should be rated as pass or fail



Performance Test Controls

- Performance test controls are put in place to limit the test activity
- Test controls are imposed to:
 - Maintain test integrity and validity
 - Ensure that the correct data are collected
 - Minimize risk of injury or impact on security
- Performance test controls are required to mitigate testing artificialities and environmental concerns
 - Some actions must be simulated by using a stimulus equivalent to the actual adversary action
 - Certain environmental conditions may be expected to degrade performance and should be tested
 - Day/night, weather, birds/animals



Resource Requirements

- Resources includes anything it takes to conduct the performance test
- Some examples of resources are
 - Personnel
 - Time for the test
 - Equipment
 - Facility
 - Location
 - Funding
 - Adversaries
 - Weapons and equipment/tools
 - Logistical support
 - Safety requirements



Test Coordination and Approval Process

- Identify and brief everyone involved in the test
 - Or make them aware that a test will be conducted
- Various stakeholders need to be coordinated:
 - Safety and security
 - Facility operations, Management
 - Quality assurance, Human factors
 - Others
- Safety is very important - always an element of risk in performance testing
 - Conduct realistic testing without undue safety hazards
- The approval process describes:
 - How the test plan is approved
 - Who has to approve the test



Compensatory Measures

- Determine necessary compensation for any degradation of readiness experienced while conducting the test
- For example:
 - Are more post and patrols needed to ensure adequate protection during the performance test?
 - Does the test area need to be shut down or segregated to ensure the test is conducted safely and securely?
- Describe what will need to be implemented in the event of a test failure
 - If a security element fails during testing, what has to be done to compensate for the failure in the event that risk increases?



Analyze, Document, and Critique

- Analyze the performance testing data to determine if the performance level is achieved
 - And if deficiencies exist
- Document the performance test results and mitigation measures if required
 - Test Report = test plan + data collected + analyses + results + conclusions
- Provide critique after the performance tests
 - Critical self-analysis, even after success, is essential to improvement
 - Critiques are an effective way to draw out lessons learned
 - Should involve all test participants



May Need to use Preliminary Tests

- Use preliminary tests to practice on unknown elements
 - Allow for exploratory testing
- Tests will help refine the actual testing through initial data collection
 - Characterization of element
 - Interaction with environment
- Determine proper installation and configuration
 - Determine settings to minimize high NAR
- Determine areas of concern or uncertainty
 - Fully characterize the performance





Summary

- Many types of tests can measure effectiveness
 - Operability and functional tests
 - Component, sub-system, and whole system performance test
- Performance testing should include:
 - Evaluation of people, procedures, equipment/hardware/technology
 - Test against the defined threat (insider and outsider)
- The results of performance testing provide a statistical basis for the calculation of P_E
- Testing provides performance assurance and data for analysis tools
- Performance tests should be planned, evaluated, reviewed, analyzed, and reported

Module 7

Performance Test for Response Force Times

Session Objectives:

After the session, you will be able to:

1. Develop and conduct a general Time Motion Study (TMS) for Response Force Times (RFT).
2. Review the practical TMS for RFT in the classroom.
3. Conduct the practical TMS in an outside environment at the test facility.

Exercises:

1. Develop and conduct a general TMS for RFTs.
2. Review and conduct the practical TMS for the outside environment application at the test facility.

Estimated Time:

Sixty (60) minutes is allotted for each exercise.

Large Group Discussion:

An appointed representative from the subgroup will present the group's scoping briefing to the large group for input and discussion.

Exercise 1 – Evaluating a Response Path and Conducting a Time Motion Study

If a response plan requires a responder to arrive at a certain location within a certain time, a mechanism must be in place to determine if the time can be realistically achieved. The goal of this exercise is for you to understand how to collect data points along a response path and evaluate the data for upgrades to response time. In this exercise, you will time tasks for a response path in your classroom. These times will also enable you to implement and evaluate upgrades.

The Picture-in-Time: The responder is sitting in a chair with shoes removed. Response backpack and simulated weapon are in storage locations in opposite corners of the room. Response force personnel have key card to facility (room) in pocket.

The tasks and response force path are:

- Communicate Response
 - o Communication to respond and location for response
 - o Responder communication is responding with confirmation of location
- Prepare to Respond
 - o Put shoes on
 - o Grab and completely don the backpack from the corner of the room
 - o Grab the simulated weapon from the other corner of the room
- Respond
 - o Walk around the table once
 - o Exit room, closing door on exit
 - o Enter room with key card
 - o Touch the telephone

Collect the task times for the actual response time for three team members to perform the response.

Note: The remaining team members are the controllers with responsibilities to ensure safety of the player and to collect the data. Use the stop watch provided by your sub-group exercise instructor and input the necessary data points along the response path in the table below.

First Iteration

Task	Description	Time (sec)	Note Any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Second Iteration

Task	Description	Time (sec)	Note Any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Third Iteration

Task	Description	Time (sec)	Note Any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Document the total response time (Task 3):

Minimum: _____sec Maximum: _____sec Average: _____sec

Determine upgrades that could improve response time:

1. _____
2. _____
3. _____
4. _____

If there is sufficient time, implement the upgrades and determine new response time:

First Iteration - upgrades

Task	Description	Time (sec)	Note Any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Second Iteration - upgrades

Task	Description	Time (sec)	Note Any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Third Iteration - upgrades

Task	Description	Time (sec)	Note Any Delays/Comments
1	Communicate Response		
2	Prepare to Respond		
3	Respond		

Document the total response time after upgrades (Task 3):

Minimum: _____sec Maximum: _____sec Average: _____sec

Exercise 2 – Evaluating a Simulated Offsite Response Path and Conducting a Time Motion Study

During this exercise you will gain hands-on experience in conducting a TMS to justify a required response force time.

The Picture-In-Time: Two mobile patrol responders are located at a post with a vehicle parked and ready for response as communicated by the Central Alarm Station. Response equipment – backpack and simulated weapons – is located in the rear of the vehicle.

There are four tasks and associated paths to time:

- Communicate Response Required
 - o Communication to respond and location for response
 - o Responder communication is responding with confirmation of location
- Prepare to Respond
 - o Acquire and don equipment
 - o Enter vehicle (and fasten seat belts)
 - o Start vehicle
- Respond to Response Location 1
 - o Drive to Response Location 1
 - o Let Responder out
 - o Responder moves to Response Location 1
- Respond to second location
 - o Exit and secure vehicle
 - o Move to Response Location 2

For this exercise three teams will be required, one at each of three locations, to time each of the tasks. Radios are provided for communication between responders.

1. Team 1 stands at the mobile patrol response force “post” to log the Communicate Response Required and Prepare to Respond times. Log Communicate Response time when responders have radio confirmation of response location.
2. Team 2 stands near Response Location 1 and will log the Respond to Location 1 time. (Time begins when communication is initiated and ends when the responder radios he is in position.)
3. Team 3 stands near Response Location 2 and will log the Respond to Location 2 time. (Time begins when communication is initiated and ends when the second responder radios he is in position.)

Prior to the start of the Time Motion Study, the Subgroup Instructor, with Subject Matter Expert, will conduct a radio check with all participants. This is to ensure all participants are on the same radio channel to ensure definitive communication with all personnel.

The Subgroup Instructor will simulate being the Central Alarm Station (CAS) and will open the exercise by notifying the mobile patrol (Patrol 1 or P1) that containment is required using the following script.

CAS---“CAS to Patrol 1 Alpha and Bravo.” – Start stopwatch for all timed activities

P1 Bravo---“P1 Bravo, go ahead.”

CAS---“Respond to alarm activation inside building 6600 and establish containment.”

P1 Bravo --- “Understood. P1 Alpha and Bravo en route.”

P1 Bravo--- “P1 Bravo to CAS, P1 Bravo is in position.”

CAS---“Understood. P1 Bravo in position.”

P1 Alpha---“P1 Alpha to CAS, P1 Alpha in position have containment at this time.”

CAS---“Understood. 6600 containment in place.”

Example Time Motion Study Instructions

Title: Off-site Response Time Validation

Purpose: This TMS will determine the required response time to a response locations outside of the Lagassi Institute (TA-III Testbed). The responders will be timed from a designated point/area of their assigned post or patrol to their response locations. Also included in the overall time is the time it takes to don all required equipment and simulated firearms (if applicable), and use of entry gates, doors, and fences.¹

Details: Two Sandia National Laboratories (SNL) Security Police Officers (SPOs) will be used as the responders. The responders will also use a designated patrol vehicle to travel from the designated starting point to designated response points.

The Subgroup Instructor will be the Controller for this exercise.

Safety conditions and instructions: (Brief the Responders on the following)

- Drive safely, obey all posted speed limit signs, and use extreme caution in congested areas.
- **Adjust speed** according to weather, visibility, and vehicle and pedestrian traffic conditions.
- If **responding on foot** to response locations, be alert for **tripping hazards**.
- Ensure radio communication with Subgroup Instructor in the event of safety or security incidents.
- Advise the Subgroup Instructor prior to initiation and termination of TMS runs.
- In the event of a safety or security incident, the TMS will be halted immediately.

Time-motion conditions of the test (Brief the Responders on the following):

- The start and finish locations (show them the location(s) if needed before starting).
- The responders will be in a regular duty configuration without weapons.
- Subgroup instructor shall inspect vehicle and personnel to ensure there are no weapons.
- Instruct the responders to proceed to the starting location and contact Subgroup Instructor when in position.
- During exercise use the shortest route possible to the response location.
- If there is traverse time on foot, instruct the responders to **jog or walk moderately** from the vehicle or post with all appropriate equipment to their final response location.
- No real weapons will be used in the TMS.
- Should a real world incident occur the TMS will be immediately terminated.

¹ The description for the Time Motion Study may be deploying from a vehicle, locking gates, or carrying equipment through predestined positions and moving to a specified location within an area.

Data Collection

1. This response will be run from start to finish - from initial communication to response to Response Location 2 – for up to three iterations.
2. Each team shall record the completion time for the designated tasks in the charts below. The start time for each task is the start of the initial communication by the Subgroup Instructor (CAS). Also record any comments.
3. Calculate the average response times for each responder.
4. Recommend potential upgrades.

Data Sheet

Date: _____

Weather Conditions: _____

Team 1

Communicate Response Required	
Iteration	Time (sec)
1	
2	
3	
Prepare to Respond	
Iteration	Time (sec)
1	
2	
3	

Team 2

Respond to Location 1	
Iteration	Time (sec)
1	
2	
3	

Team 3

Respond to Location 2	
Iteration	Time (sec)
1	
2	
3	

Document the total response time (Team 3 time):

Minimum: _____sec Maximum: _____sec Average: _____sec

Recommend potential upgrades:

Remarks/Comments:

Module 7

Performance Testing Guard and Response Force Subgroup Instructor Guide

Key Points

1. Emphasize purposes and importance of guard/response testing.
2. Recognize the four levels of response performance testing.
3. Recognize the various types of response performance tests and exercises associated to each level
4. Focus on the Time Motion Study for Response Force Times identified in Level 1.

Facilitation

Things to consider when conducting Exercise 1:

1. Ensure the audience is familiar with a basic Response Force Time. Make sure the students do not make it complex, as the exercise is designed to show how to collect data points along a simple response path.
2. The exercise is designed to have hands-on interaction in a fun environment. Get the students motivated to participate in the exercise and keep the attentiveness for the next exercise.
3. Make sure you have some of the students be controllers. The controllers need to make sure that the player is going through each step safely and collecting the necessary data points along the response force path.

Things to consider when conducting Exercise 2:

1. Ensure the students are familiar with the basic Response Force Time derived from Exercise 1 and prepare to conduct a similar exercise in an exterior application.
2. Make sure the students follow the instructions on the TMS Data Collection Sheet. The responsibilities for Teams 1 and 2 are provided in detail.
3. The exercise is designed to have hands-on interaction in a safe and fun environment. As the exercise is conducted, ensure that the controllers are

maintaining a safe environment that enables collecting the necessary data points along the response force path.



Analysis Overview

Module 8

Vulnerability Analysis of Physical Protection Systems

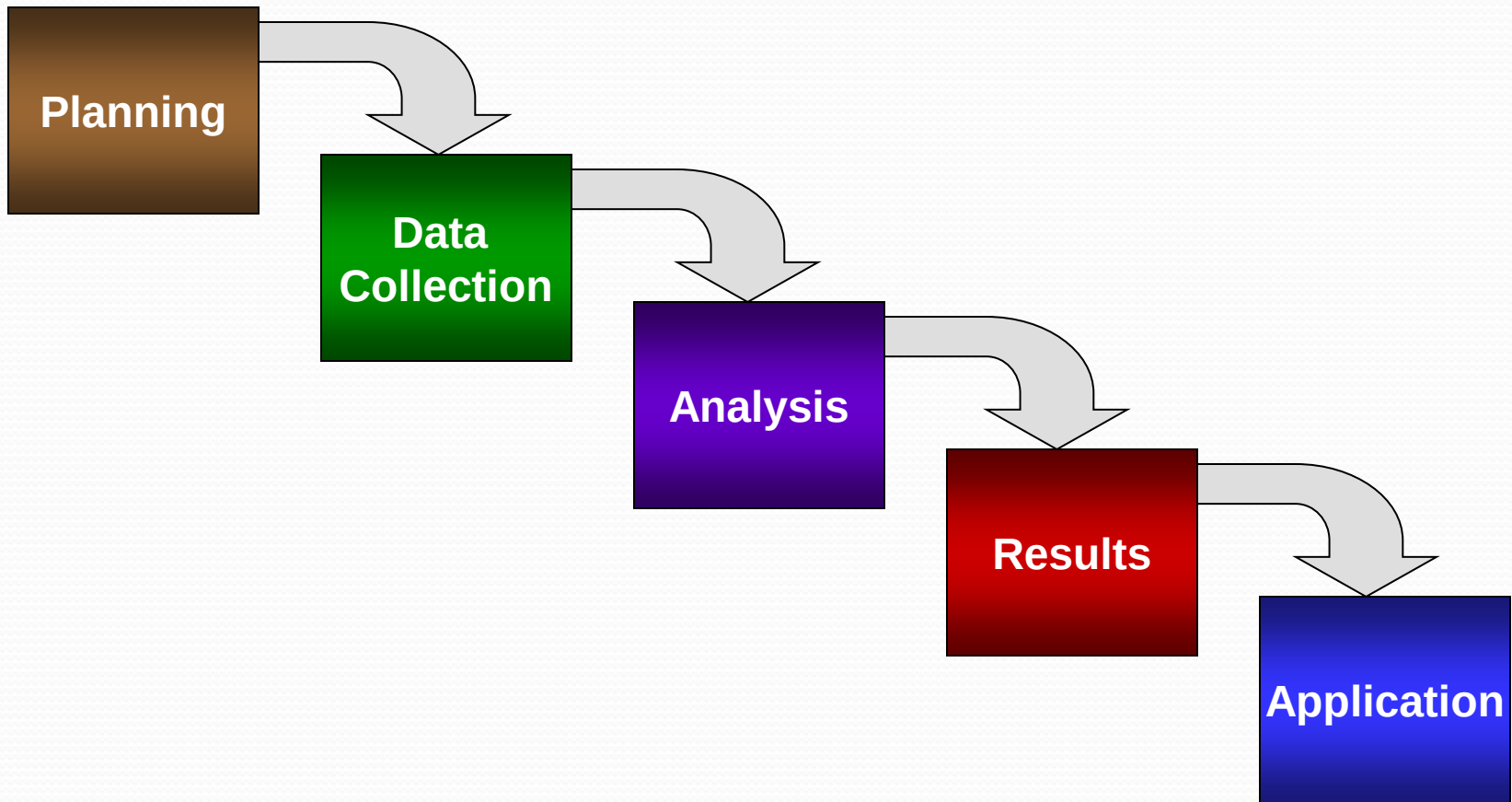
Date:

Student Learning Objectives

After completing this module, you should be able to:

- Describe the activities in each of the three steps in the analysis process
- Describe the strengths and weaknesses of both quantitative and qualitative evaluations
- Identify target scoping issues that arise in performing vulnerability analyses

Phases of Vulnerability Analysis



Three Performance Metrics

- Three metrics are commonly used during analysis of the PPS:

- System Effectiveness (P_E)

The probability that the physical protection system will defeat the adversary

- $P_E = P_I * P_N$

- Probability of Interruption (P_I)

Probability that the response force arrives in time to stop the adversary

- Probability of Neutralization (P_N)

The probability, given interruption of the adversary by the response force, that the response force kills or captures the adversary or causes the adversary to flee

The Analysis Process Estimates The Three Performance Metrics Qualitatively or Quantitatively

1. Assign Element Performance

Assign Delay and Detection to Subsystems, ASD

Assign PPS Response Time

Determine Blast Effects

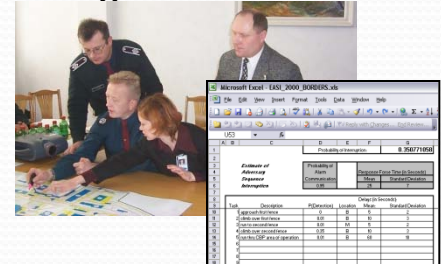
Collected Site and Testing Data

2. Path Analysis (P_I , Crude P_N)

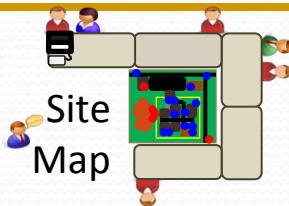
A. Timely Detection Analysis

B. Overt Attack Analysis

Determine minimum P_I path by software or using “manual” method

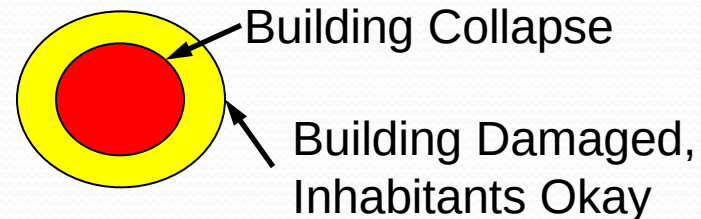
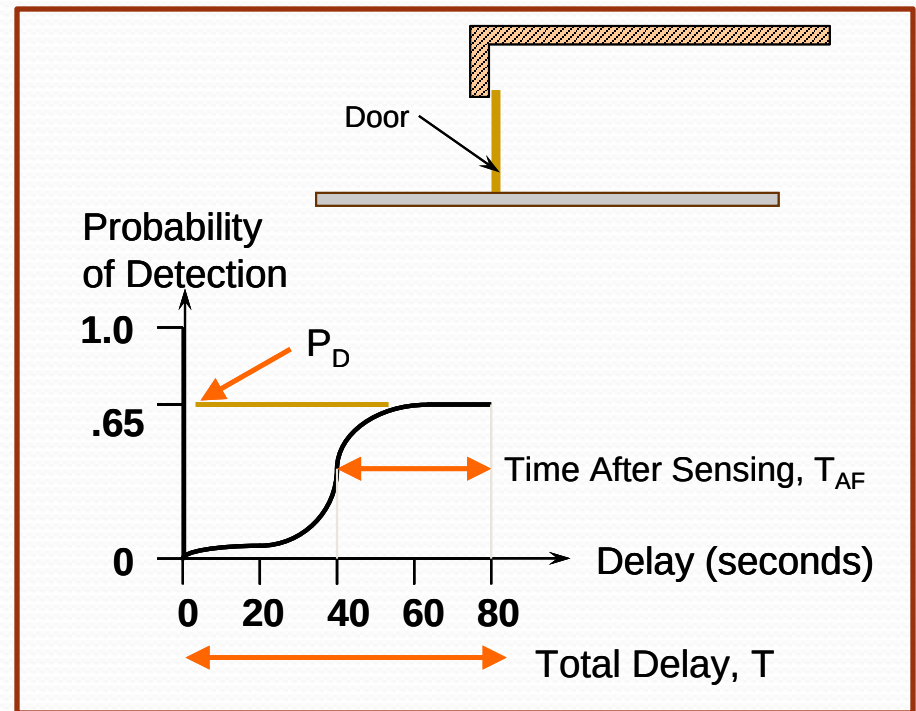


3. Scenario Analysis (P_N , P_E)

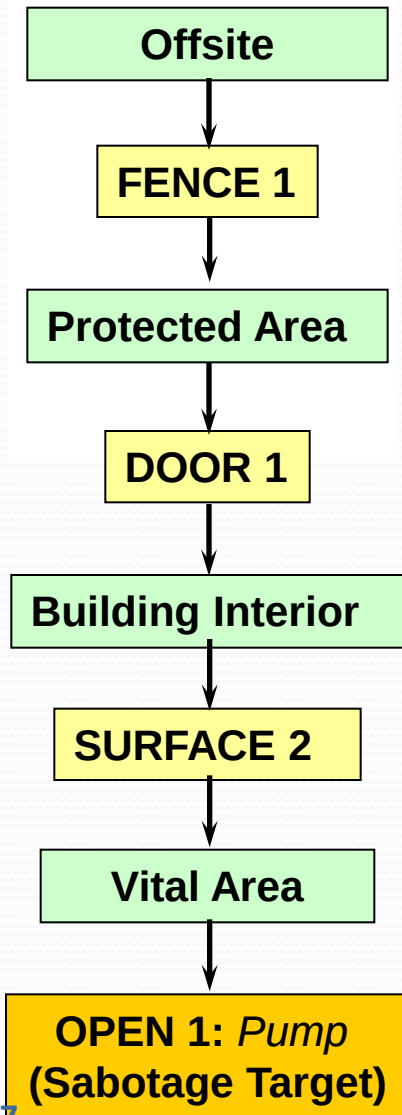


1. Assign Element Performance

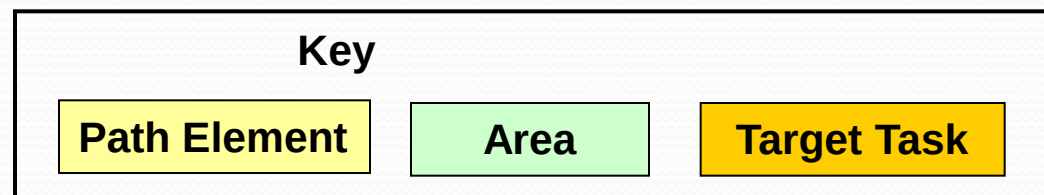
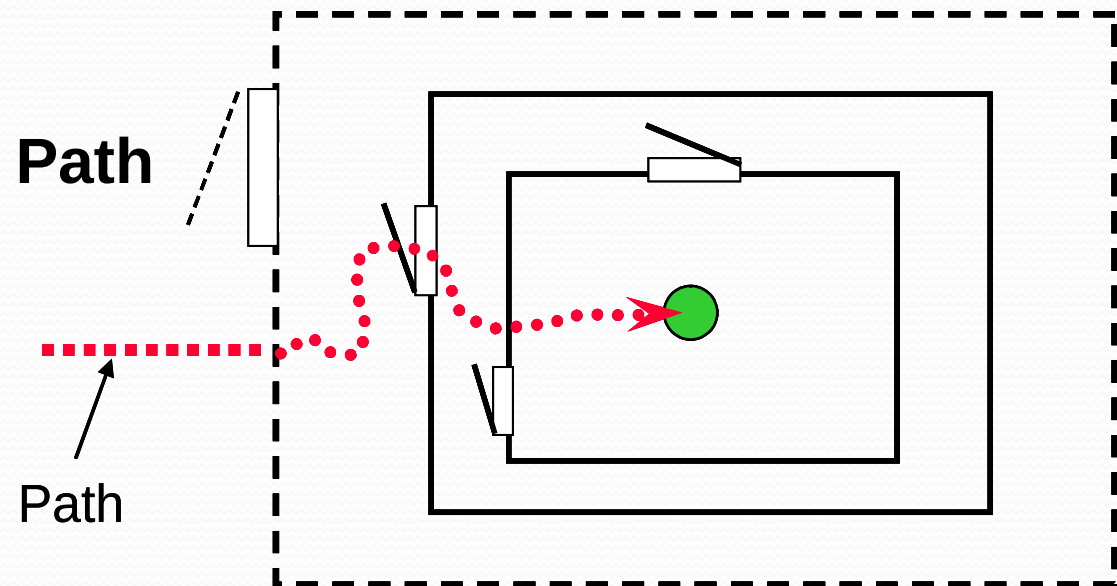
- Assign Subsystem Performance
- ASD Elements and Areas
 - Probability of Detection, P_D
 - Total Delay Time, T
 - Time After Sensing, T_{AF}
- Response Force
 - PPS response time based on order-of-battle data
- Blast Effects
 - Effects on personnel and structures based on blast circles



2. Path Analysis Focuses on Adversary Paths

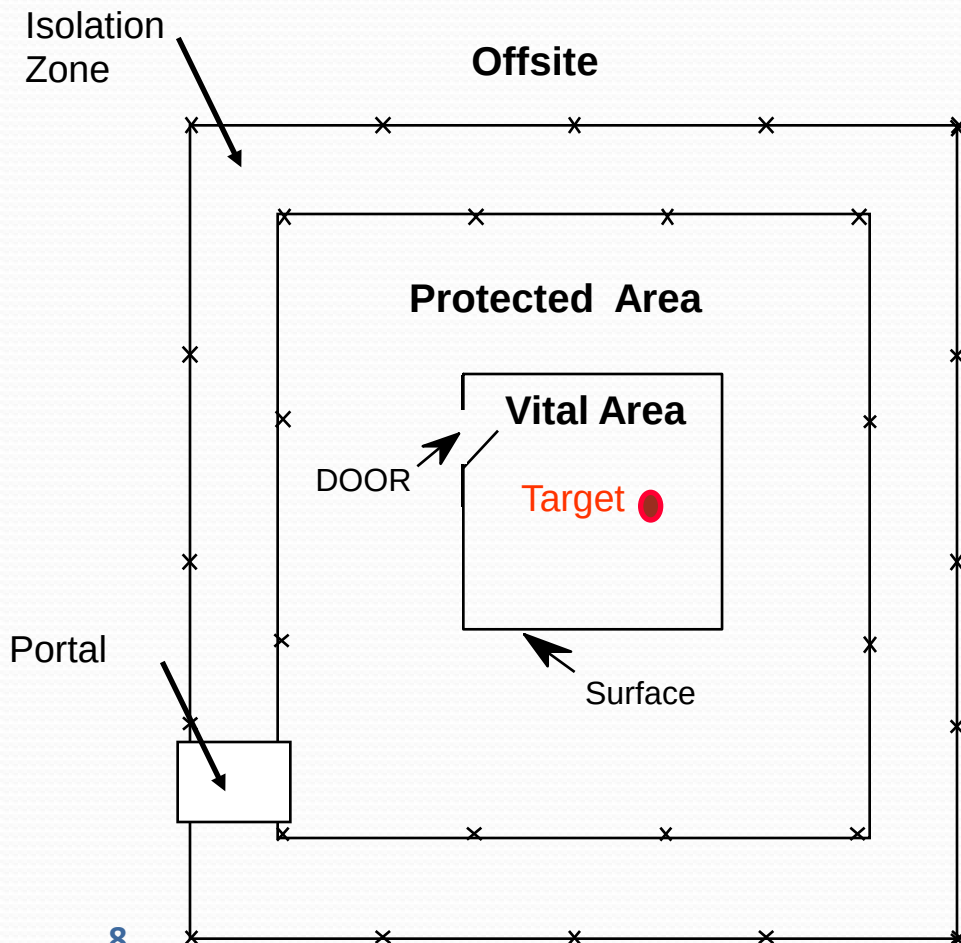


Adversary Path—Time-ordered sequence of path elements, areas, and a target task that the adversary must traverse to complete an attack



Path Analysis Uses ASDs and PPS Response Time Data

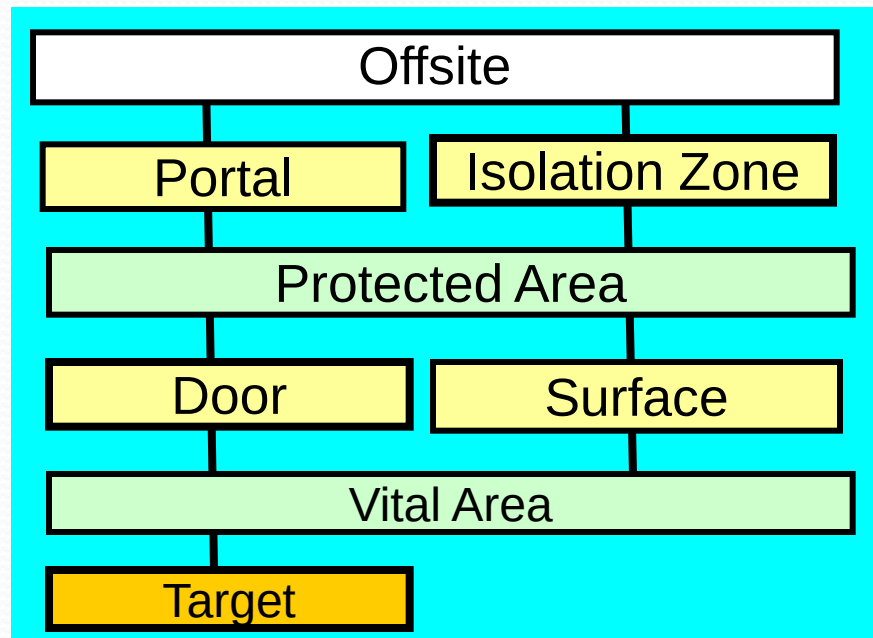
Example Facility



Corresponding ASD

Each Area and Element in the ASD have Performance Values

- Total Time, T
- Time After Sensing, T_{AF}
- Probability of Detection, P_D





Path Analysis Includes Two Sub-Analyses

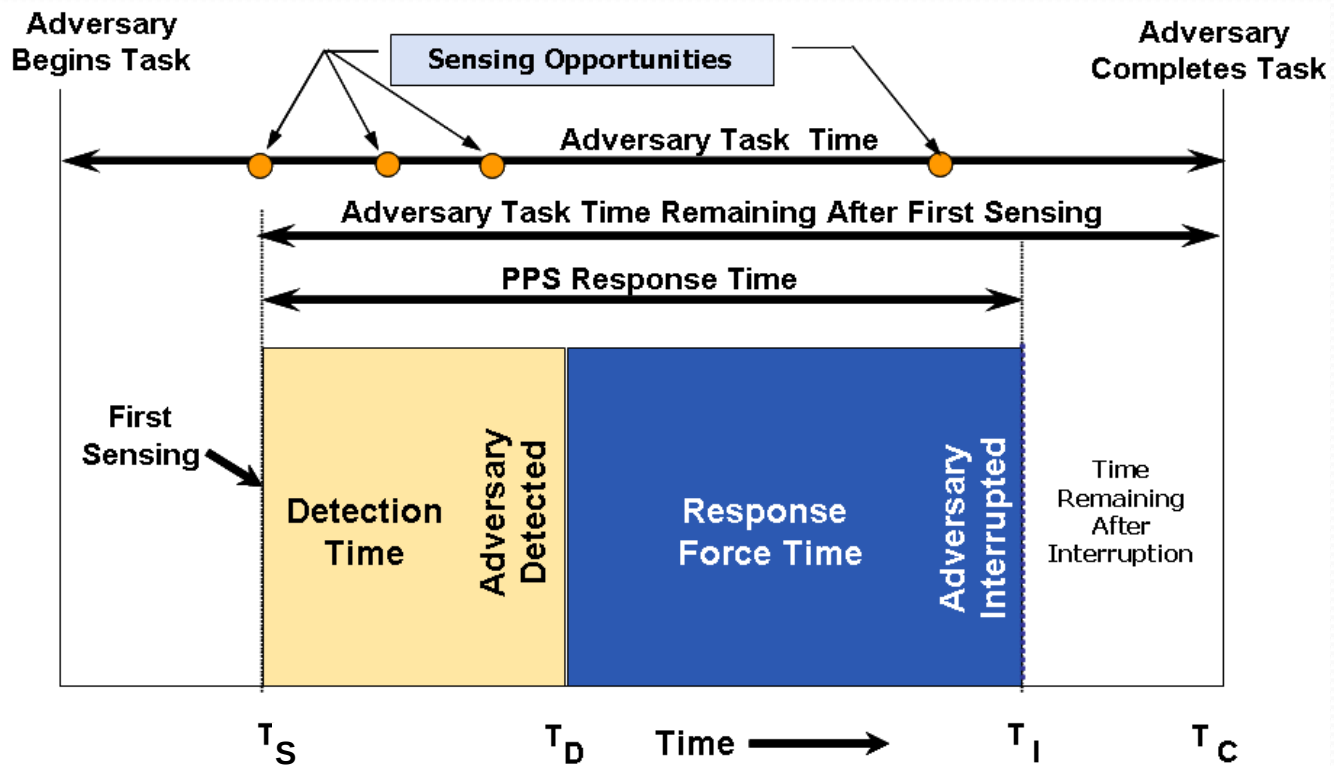
A. Timely Detection Analysis

- Determines whether Probability of Interruption (P_I) is adequate along all adversary paths
 - Is site detection and delay sufficient so the response force arrives in time to interrupt?

B. Overt Attack Analysis

- Determines whether there are paths that have inadequate Probability of Neutralization (P_N)
 - Example: paths that include attacks on the response force
 - Typically, $P_D = 1$ at some point on these paths
 - P_N is determined approximately, by expert judgment and simple numerical models

A. Timely Detection Analysis Uses Adversary and PPS Timelines to Evaluate P_i



B. Overt Attack Analysis

- Examine ways the adversary may reduce P_N
- Compare response force to adversary
 - Types of Weapons and Equipment: Equal match to DBT?
 - Numbers: Do the response force numbers meet or exceed the DBT?
 - Procedures/Plans: Appropriate ? Training adequate?
- Consider, also, adversary paths that provides adversary tactical advantages
 - Examine response survivability: Armored vehicles, fighting positions, tactics
 - Consider possible adversary use of ambushes and explosives
 - Determine if surviving Response Force capability and numbers meet competent authority requirements for interruption and neutralization
 - This course will use simple P_N Tables to determine sufficiency

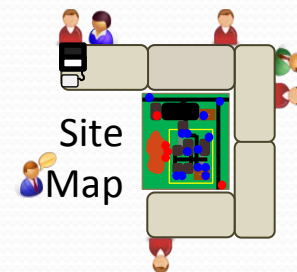


Scenario Analysis

- Determines whether the PPS effectiveness, P_E , is adequate across a range of detailed attack scenarios within the DBT
- Evaluates P_E directly or uses formula $P_E = P_I * P_N$ and then combines P_I and P_N estimates
- Evaluates only a small number of scenarios (e.g., 3-10)
 - Cannot claim to have found a “most-vulnerable” scenario (the scenario with the lowest P_E)
 - Requires a process for developing and selecting good scenarios
 - Scenarios are typically evaluated using data from simulations

Scenario Analysis Requires

- Methods to develop “good” scenarios
 - Start from lowest P_I or delay time paths perhaps after modifying PPS Response Time or ASD delays and/or P_D 's
 - Develop around adversary attacks on response force by:
 - Minimizing P_N (Overt Attack Analysis)
 - Minimizing P_E (Red Team Analysis, using an expert “red team”)
- Process for deciding which of these scenarios to evaluate
- One or more types of simulations to provide data to evaluate effectiveness
 - Tabletop exercises
 - Computer combat simulations
 - Force-on-force (FOF) exercises



1. Assign Element Performance

Assign Delay and Detection to Subsystems, ASD

Response Force: Assign PPS Response Time

Determine Blast Effects on People and Structures

Collected Site and Testing Data

2. Path Analysis

A. Timely Detection Analysis: Identify Paths With Lowest P_I in ASDs

B. Overt Attack Analysis: Identify Paths With Low P_N

Analysis Process

Scenario Development:

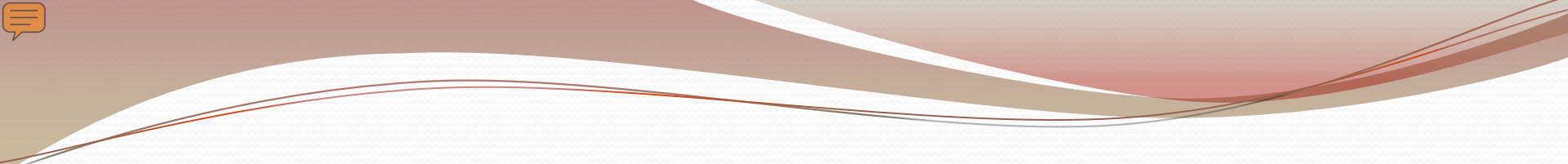
- Based on Low P_I/P_N or Delay Paths
- By Expert RedTeams

Decide Which Scenarios to Evaluate

3. Scenario Analysis

Scenario Evaluation of P_N , P_E based on

- Table-top Exercise
- Computer Combat Simulation
- Force-on-Force (FoF) Exercises



Quantitative and Qualitative Analysis

- Quantitative Analysis: Analysis that assigns a metric as a number
 - Probabilities such as P_S , P_A , P_D , P_I , P_N , P_E
 - Times such as Delay times or PPS Response Times
- Qualitative Analysis: Analysis that assigns a metric, such as P_N , a categorical description
 - Acceptable/unacceptable
 - Range from Very Low to Very High
- Numerical information, such as delay times, are typically used in both types of analyses



Two Example Analysis Approaches

Pure Quantitative Analysis Approach

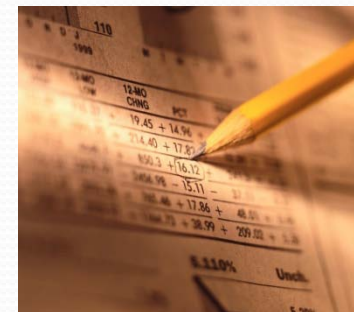
- P_I determined quantitatively
- P_N determined quantitatively, based on a mix of computer simulations and force-on-force exercises

Mix of Quantitative and Qualitative Approaches

- P_I determined quantitatively
- P_N determined qualitatively, by review of numerical data collected during force-on-force exercises
 - Example metrics reviewed:
Response force surviving to arrive at target, time of arrival during exercise
 - Competent Authority determines P_N to be acceptable or unacceptable based on criteria

Scoping Issue: Limiting Number of Targets to Be Analyzed

- The number of individual targets may be too large to allow all of them to be analyzed
- Ways to reduce the number of targets to be analyzed
 - Combine targets by type, protection, and location
 - Prioritize targets and analyze the highest priority ones
 - Example: Based on adversary attractiveness or categorization
 - Eliminate targets that fall below an acceptable risk level when the VA is performed as part of a risk assessment



Summary

- The three steps in the process for conducting analysis of the data that were collected
 - Assign element performance
 - Path analysis
 - Scenario analysis
- Quantitative and qualitative evaluations each have strengths and weaknesses
- It is not always possible to analyze every target; therefore it may be necessary to reduce the number of targets for analysis



Characterizing Element Performance

Module 9

Vulnerability Analysis Training Course
Date:

Student Learning Objectives

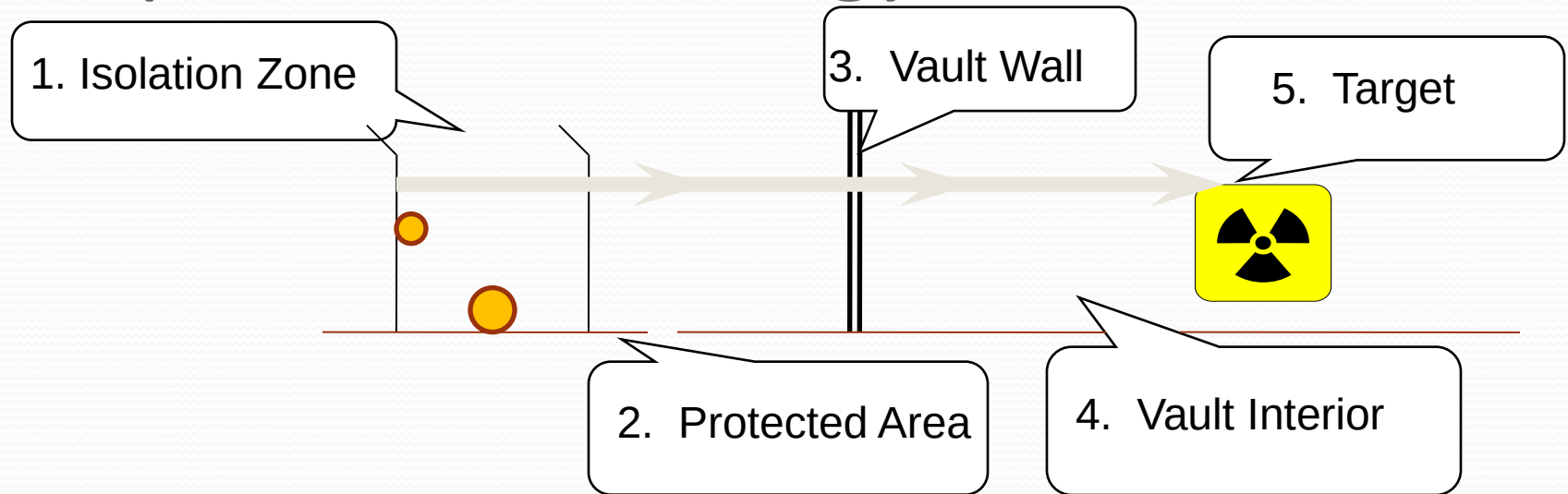
At the end of this module, you should be able to:

- Define and illustrate adversary methods for compromising protection systems and elements
 - Adversary strategies, element defeat strategies, and component defeat methods
- Characterize effectiveness of protection elements in terms of detection, delay, and response parameters
 - Determine ASD element/area performance data: P_D , T , and T_{AF} values
 - Determine PPS response times based on response data
- Discuss the process of evaluating the effect of explosive blast against personnel and structures

Definitions

- ***Scenario***—Outline of a sequence of events by which an adversary may achieve the objective
- ***Path***—Route and related path/area elements used in a scenario by the team attacking the asset

Examples of Terminology



Path consists of elements/areas:

1. Isolation Zone
2. Protected Area
3. Vault Wall
4. Vault Interior
5. Target

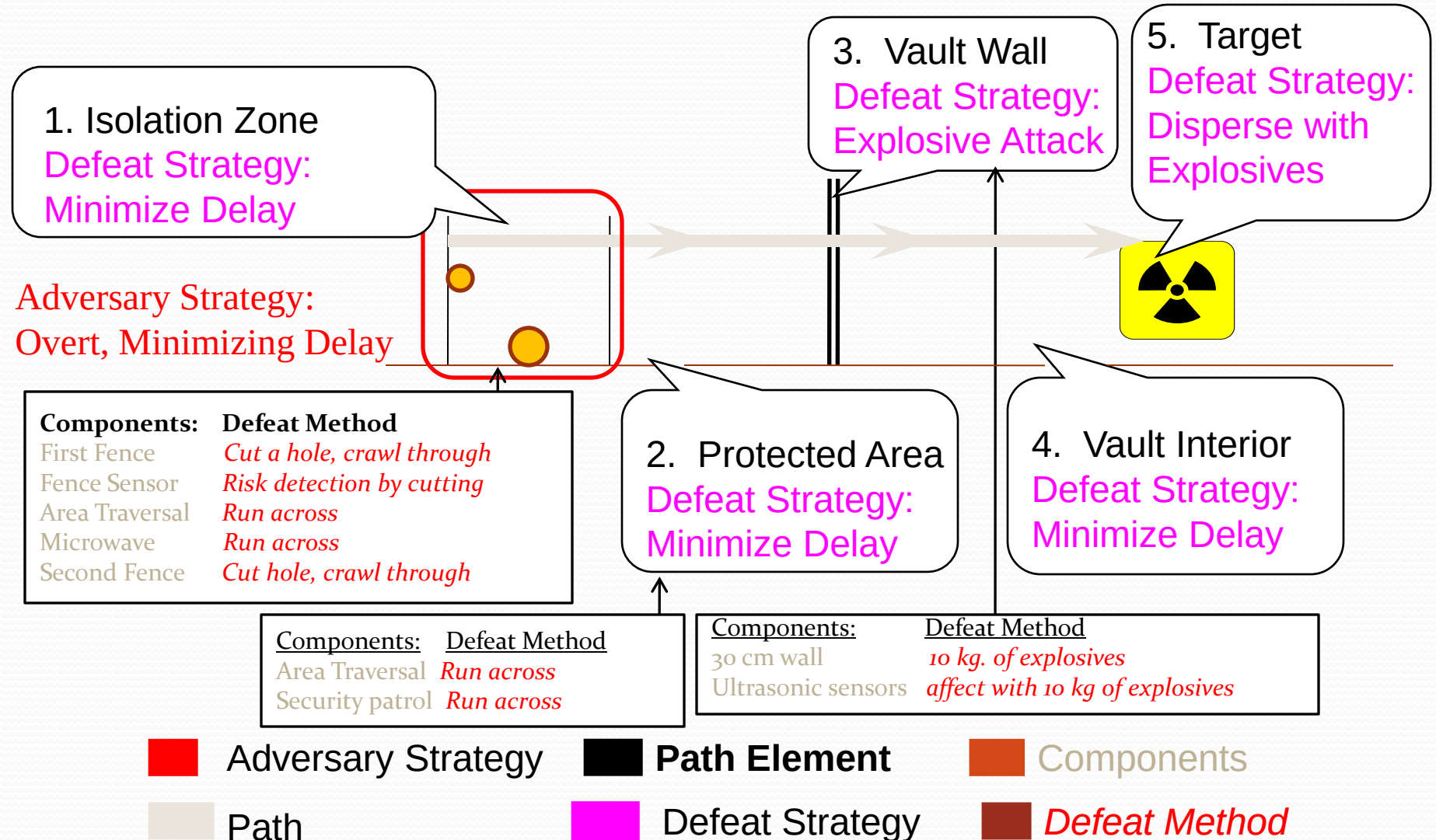
 Path

 Path Element

New Definitions

- ***Adversary Strategy***—Short description of the scenario used to achieve the adversary's objective
- ***Defeat Strategy***—General method used to defeat a path element or a PPS function
- ***Defeat Method***—Way to prevent a component within a path element from accomplishing its purpose or function

Examples of Terminology



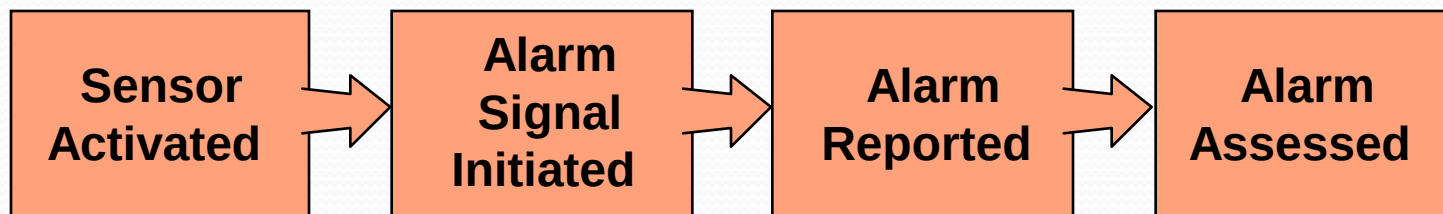
Developing Defeat Strategies and Methods

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



Avoid, Degrade, or Disable Detection

- Sensing
 - Bypass or defeat sensors
- Alarm Reporting (Communication and Display)
 - Defeat alarm communication or annunciation
- Assessment
 - Defeat the ability to assess what caused the alarm





Degrade, Disable, or Circumvent Delay

- Attack when delays are inactive
 - Doors and gates unlocked or open
 - Material in use
- Disable or circumvent activated delays
 - Deployed guards
 - Pop-up vehicle barriers
- Attack when delays are present
 - Walls and other surfaces
 - Fences

Degrade or Eliminate Response

- Attack
 - Ambush response
- Divert
 - Multiple attack points
- Confuse
 - Prevent security communications
- Slow
 - Damage vehicles



Many attacks will use a combination of these efforts

Defeat Methods for PPS components

<i>Function</i>	<i>Defeat method</i>
● Detection ● Sense unauthorized condition ● Communicate the alarm ● Assess the alarm	Bypass, spoof, tamper, stealth Jamming, tampering Avoid
● Delay systems ● Barrier ● Activated delay	Penetrate Disable or circumvent
● Response	Disable, divert, confuse, or delay

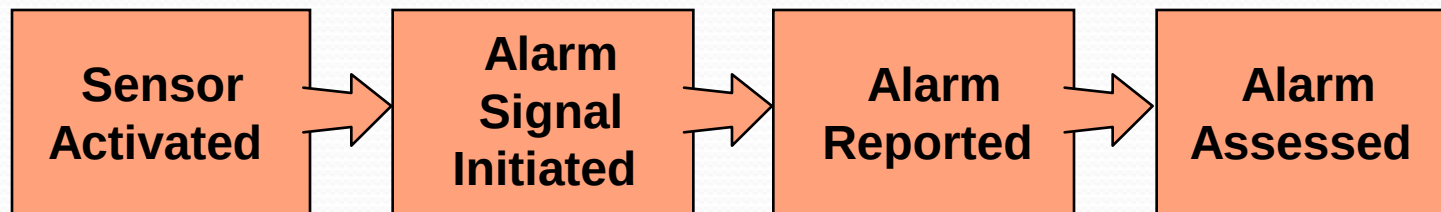
Examples of Element Defeat Strategies – Entry Into a Vault

- Penetrate the vault door
 - Blow door open (force)
 - Tamper with intrusion detection system and quietly penetrate door (stealth)
 - Pose as an inspector (deceit)
- Penetrate the vault wall
 - Explosively breach the wall (force)
 - Defeat with power tools (force)



Detection Performance Measures

- Process
 - Sensor activated
 - Alarm signal initiated
 - Alarm reported
 - Alarm assessed
- Performance measures
 - Probability of detection
 - Time for communication and assessment
 - Frequency of nuisance alarms





Relationship of Detection, Sensing, and Assessment

$$P_D = P_S * P_A$$

where

P_D = Probability of Detection

P_S = Probability of Sensing

P_A = Probability of Assessment
(given sensing)

Delay Performance Measures

- Encountering obstacles
 - Physical barriers
 - Protective force personnel
 - Distances
- Performance measure
 - Total Time (T) to defeat obstacles
 - Time after sensing (T_{AF})

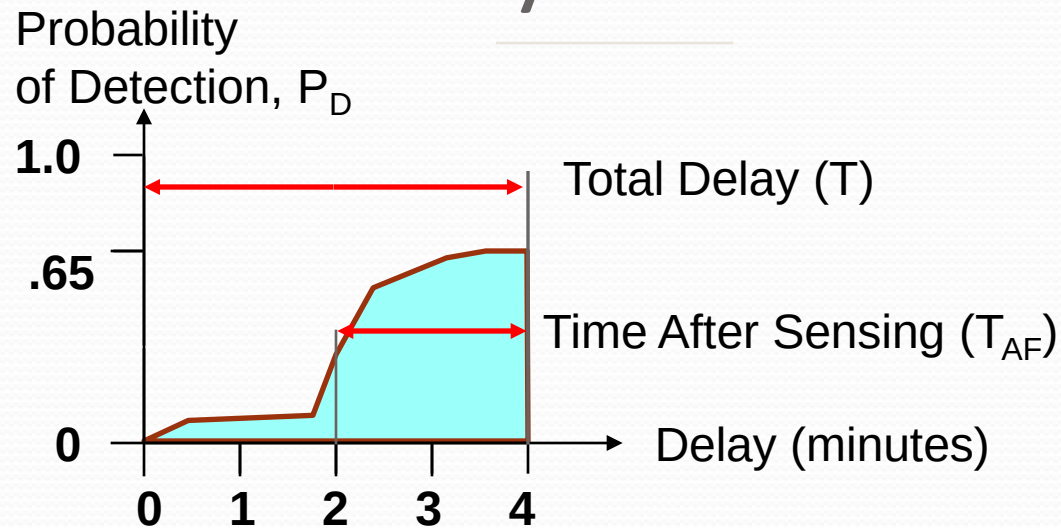


Delay Characterization

- Select combinations of tools (hand, power, or thermal tools; explosives; vehicles) to be used
- Determine what delay and detection is produced by different tool combinations
- Keep track of additional factors:
 - Tool weight
 - Number of personnel and skills required
 - Tactical factors—need for transportation and to retreat, collateral effects



How to Represent the Relationship of Detection Versus Delay at an Element



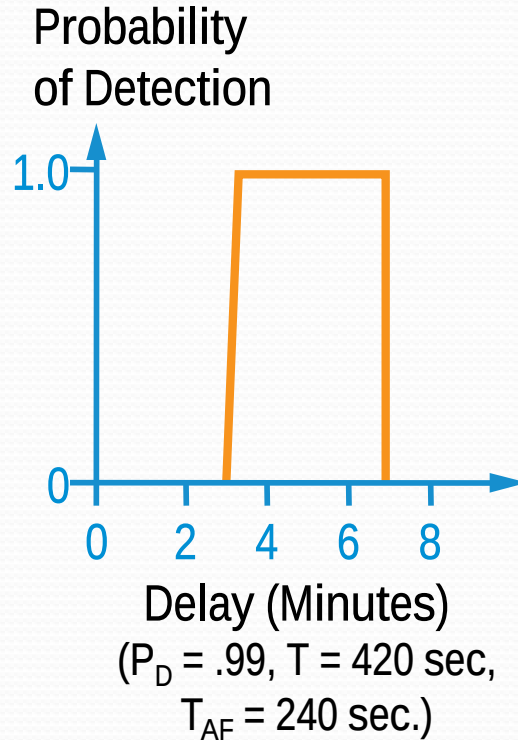
- Performance values for each area/element
 - Estimate P_D , delay at the element
 - Determine the Total Delay, T
 - Determine how much delay exists after sensing at this element, T_{AF} , assuming detection occurs here for the first time
- For this example
 - $P_D = 0.65$, $T = 240$ seconds, $T_{AF} = 120$ seconds

How to Determine When Sensing Occurs

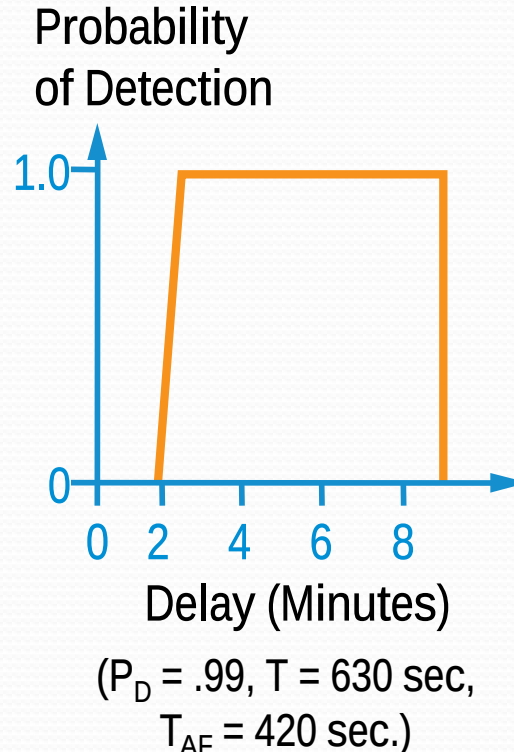
- Location of sensors typically when detection occurs
 - Before barrier: $T_{AF} = T$
 - After barrier: $T_{AF} = 0$
 - During explosive breaching task: T_{AF} = time after explosives go off but before adversary finishes crawling through hole

Relation Between Detection and Delay for Different Defeat Strategies

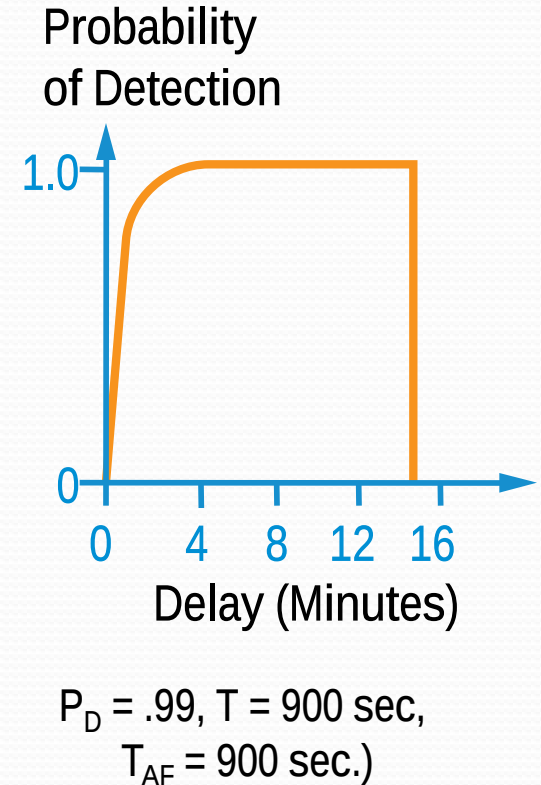
45 kg of explosives
Large Plate



10 kg of Explosives
Plus Cutting Tool



Power Tools



Comparison of Additional Factors

	45 kg explosives	10 kg explosives, cutting tool	Power Tools
Equipment Weight	<i>100 kg</i>	<i>50 kg</i>	<i>60 kg</i>
Number of Adversaries	<i>3</i>	<i>2</i>	<i>1</i>
Advanced Skills	<i>Explosives</i>	<i>Cutting Tool</i>	<i>Power tool</i>
Tactical Factors	<i>Retreat Vehicle Needed Collateral Damage</i>	<i>Retreat Collateral Damage</i>	

Response Process and Performance Measures



- Performance measures
 - Probability of communication to response force
 - Communication time
 - Effectiveness of deployment
 - PPS response time
 - Probability of neutralization

Techniques to Characterize Response

- Use these techniques to determine when an adequate number of responders will arrive in time to interrupt
 - Review time data making up response times
 - Develop response picture-in-time
 - Review response command and control procedures
- Exercises can provide clues about
 - Gaps in planning
 - Adherence to procedures
 - Untenable positions or tasks



Determining The PPS Response Time

- Collect times for components of PPS response time
 - Detection time, consisting of alarm communications and assessment times
 - Response time, consisting of communications, preparation, travel, and deployment times
- Record the response on what we will call a response picture-in-time that records:
 - Where guards/response forces respond to (on/off site), number, and timing
 - Tactical considerations
- Note that time estimates should be conservatively high, so that in most cases interruption will occur *earlier*

A Form Can Be Used to Calculate Arrival Times for Guards and/or Response Forces

Components of PPS Response Time Form

Unit	Include?	Number Deployed	(1) Alarm Communica- tion	(2) Assess- ment	(3) Communica- tion	(4) Prepara- tion	(5) Travel and Deployment	(1)+....(5) Arrival Time

These Arrival Times Can Be Used to Create an Initial Order-of-Battle Form

Order-of-Battle Form

Target: XYZ

Adversary Strategy: Sabotage

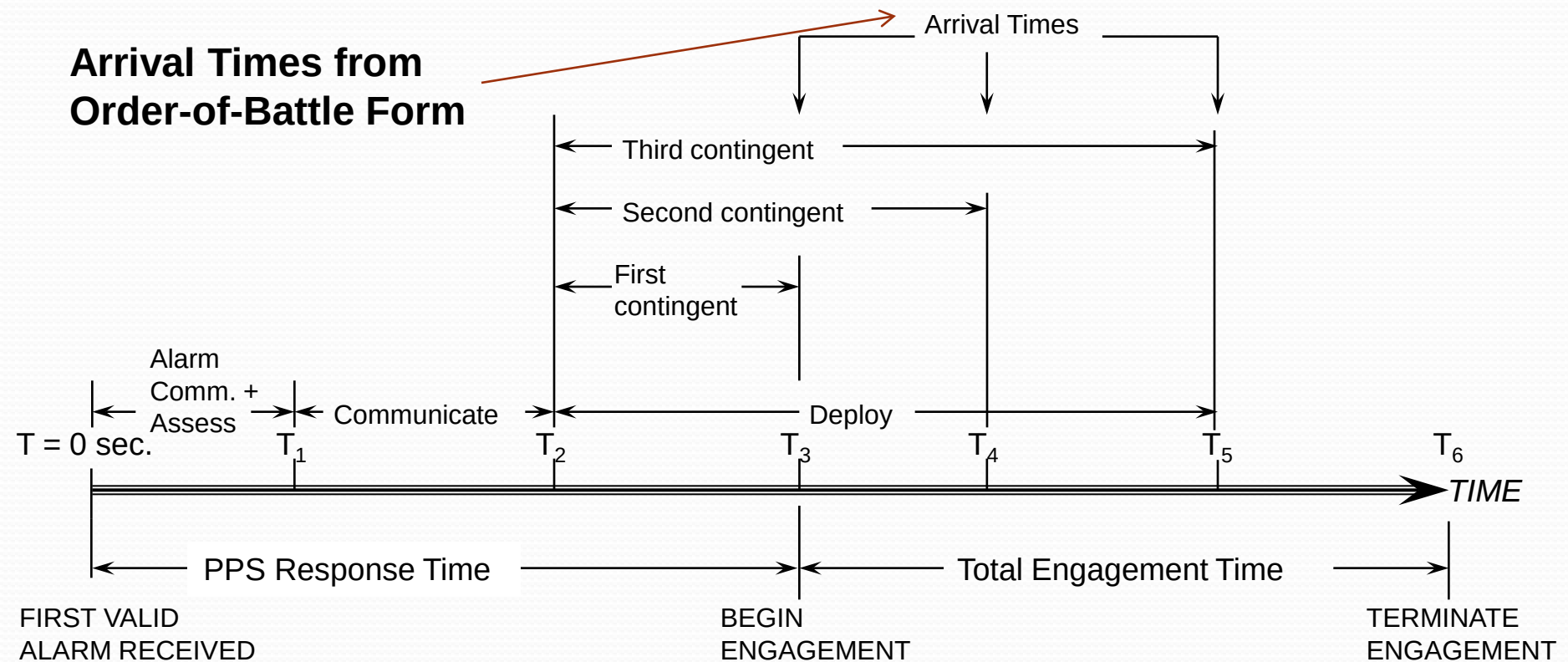
Response Force Strategy: Denial

Critical Event Number	Time (sec.)	Description of Event (e.g., Arrival of unit x)	Total Killed By Other Attacks (e.g., IEDs)	Total Number Arrived	Total Number Engaged
1	30s	Patrol arrives	0	1	0
2	60s	Tactical Team (SRT) Arrives	0	11	0
3	90s	Entry Team of 6 enters building	0	11	6

- This focuses on the response process as a function of time
- Initially performed for general response to a target

PPS Response Time Records When Sufficient Forces Have Arrived to Interrupt

Arrival Times from Order-of-Battle Form



Command, Control, and Communications (C3) Overview

Command: Exercise of authority (decision making) by response force leaders

Control: Direction by response force leaders over assigned personnel to accomplish the mission

Communications: Allows real-time communication between the central alarm station, tactical leaders and response force in the field and allows tactical leaders to direct the actions of the response based on adversary actions



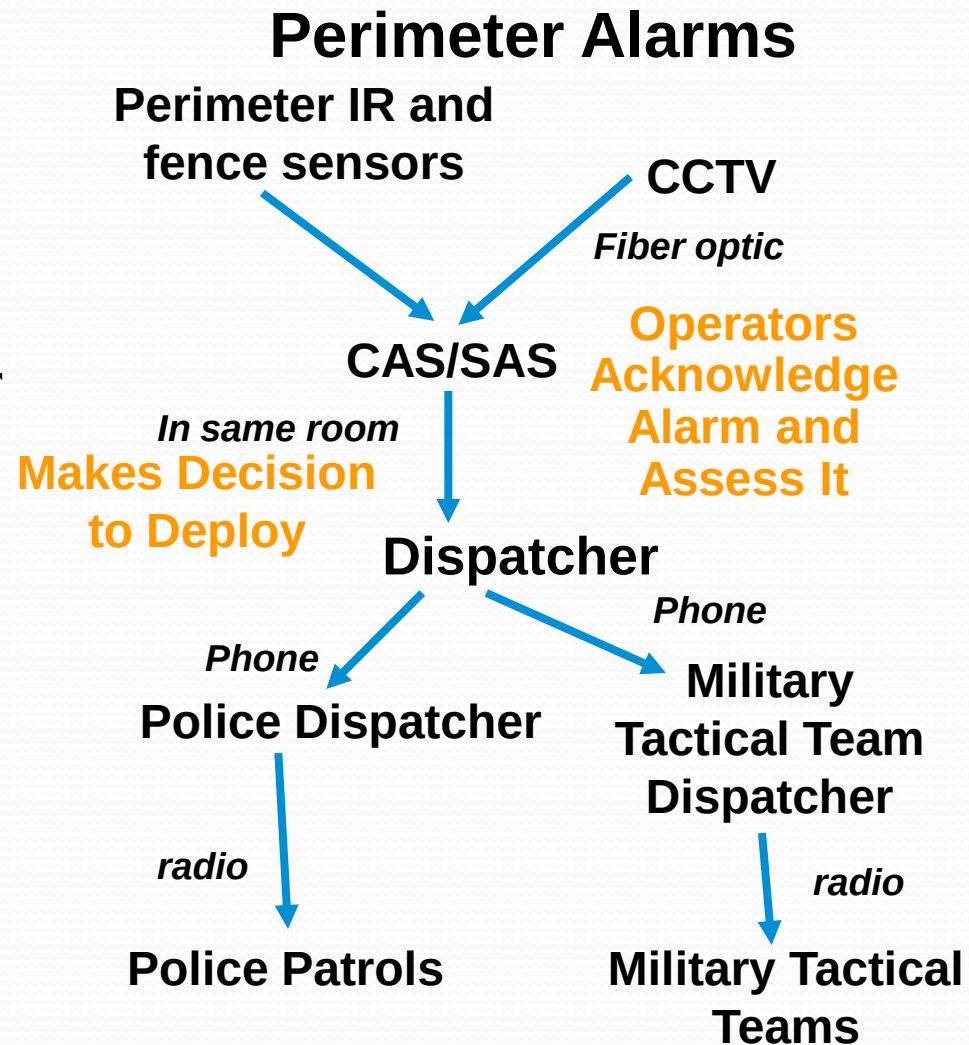
Communications Systems

- Vital to command and control
- A robust communication system uses multiple systems to ensure functionality is not lost
- Most common is simple radio frequency communication system
 - Most systems are conventional, narrow-band frequency modulation, clear-voice systems, with encryption
 - Typical radios operate on any one of several frequencies or channels
 - Approximate range is 2 to 5 km

Defeat Methods For Response Communications

Given the following system and response procedures, think of ways to defeat the system

An alarm is received from the perimeter alarm system. This alarm is communicated to the CAS/SAS alarm console, the operator is alerted, acknowledges the alarm, and looks at the video image of the alarmed area. The operator alerts the dispatcher, who then alerts the Police Dispatcher and Military Tactical Team Dispatcher.



Response Force Picture-in-Time Technique

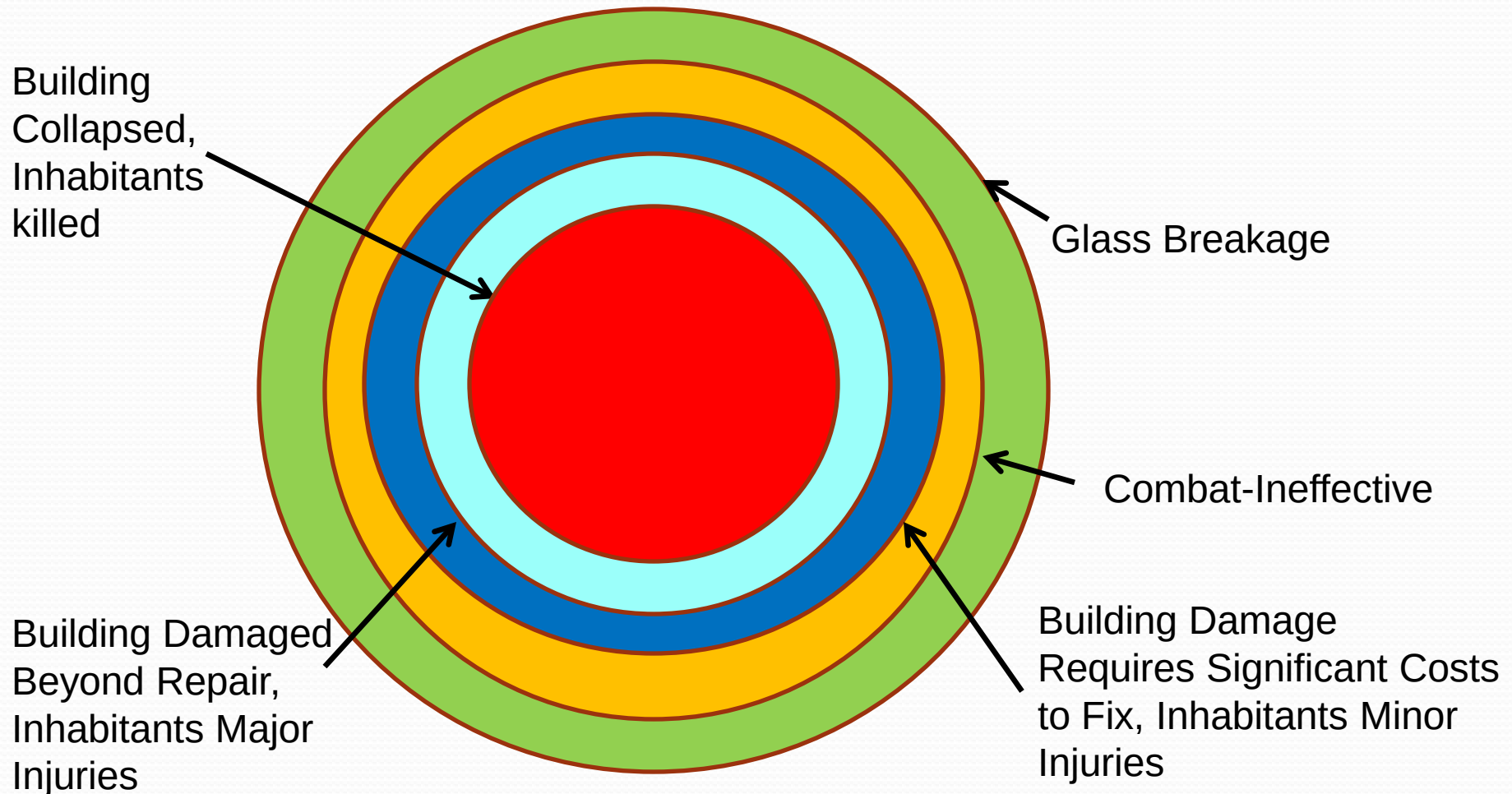
- Can use picture-in-time technique to determine the response force time based on time and location of forces
 - At this point, we are only showing where the response force deploys
- For each adversary strategy targeting the response, fill in the response portion of the picture-in-time
 - Where officers respond to (on and off site)
 - Numbers and timing
 - Tactical considerations
- Given the response, place adversaries and/or the response to adversary's best advantage



Evaluate the Effect of Explosive Blast Against Personnel and Structures

- Approach presented is simplification of complex methodology
- Consider adversary use of explosives against personnel during scenario analysis
 - People in the open becoming combat-ineffective
 - Distance at which glass breaks into fragments
 - Significant blast damage against buildings with humans inside
- Also consider possible use of explosives to create unacceptable blast damage against targets

For This Course Use Hypothetical Blast Effect Circles (Inside the Circle the Effect Happens)



Summary

- Three basic adversary defeat strategies
 - Avoid, degrade, or disable detection systems
 - Degrade, disable, or circumvent delay systems
 - Degrade or eliminate response
- Use various techniques to determine ASD element/area performance data for each element and element strategy:
 - P_D , T, and T_{AF} Values
- Use tools to demonstrate PPS response times based on response time data and deployment locations
- Use tools to evaluate the effect of explosive blast against personnel and structures

Module 9

Characterizing Element Performance

Session Objectives

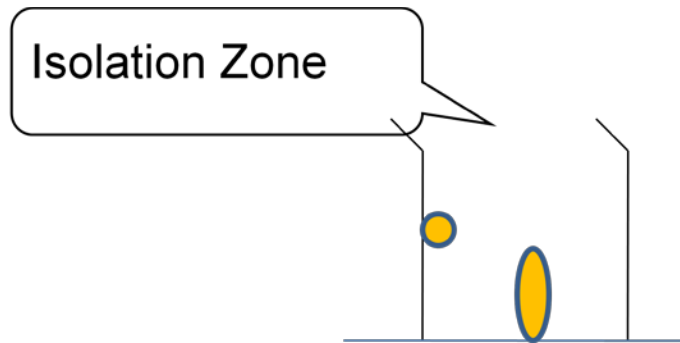
After the session, you will be able to:

1. Assign Detection and Delay values for ASD elements and areas.
2. Create an Order-of-Battle data form to determine a PPS response time based on numbers of responders.

Exercise 1 – Assign Detection and Delay Values for an ASD Element at the PTR Protected Area Boundary

In this exercise, you will assign performance values (Probability of Detection, P_D ; Total Delay Time, T ; and Time After Sensing, T_{AF}) for elements on the protection layer between the Institute Limited Area and the PTR Protected Area.

1. Identify what facility state and adversary transport mode your subgroup is analyzing.
2. For the isolation zone element in the protection layer between the Institute Limited Area and the PTR Protected Area, apply the following process to determine performance values:
 - a. Brainstorm some defeat strategies for the element, such as covert entry, minimizing delay, etc. Fill the form on the next page in for an element-defeat strategy you want to analyze.
 - b. For that element defeat strategy,
 - i. Think through some good defeat methods for defeating components at that element. For example, to develop defeat methods for exterior sensors, look at Attachments 1 and 2 to see how an adversary might take advantage of weaknesses in sensor coverage or susceptibility to nuisance alarms.



Element Defeat Strategy: _____

Component	Defeat Method	Time (sec)	Ps
Outer Fence	Cut through	10	
Fence Sensor	Cut through, ignoring detection		0.95
Area Traversal	Run across 12m at 4 m/s	3	
Passive IR	Run through		0.95
Inner Fence	Cut through	10	
Total Probability of Sensing, Ps			0.99
PA (based on CCTV + recording)			0.95
Probability of Detection, $P_D = P_S * P_A$			0.94
Total Delay Time, T		23 sec	
Time After Sensing, T_{AF}		23 sec	

Equipment Required for Defeat Strategy: _____

Weight of Equipment (Kg.) _____

Number of Adversaries Involved in Defeat Strategy: _____

Advanced Skills Required: _____

Tactical Factors: _____

- ii. Determine Probability of Sensing for all sensor components at the element using Table 6 in Section 16 of the Hypothetical Facility Data Book. If you have more than one component, combine these values as taught in the International Training Course: that is, to combine P_{S1} and P_{S2} , the combined P_S is $P_S = 1 - (1 - P_{S1}) * (1 - P_{S2})$.
- iii. Determine delay times for barriers and for transit based on defeat methods that are consistent with the element strategy. (For example, using explosives against a fence is usually not consistent

with a covert entry through a perimeter.) **Note that all defeat methods must be consistent with the Design Basis Threat.**

- iv. Select Probability of Assessment, P_A , from the following list, based on all defeat methods identified in i. and iii (Note that an element strategy might target the assessment, also.):
 - $P_A = .25$ Humans are the primary means of assessment, either directly or through surveillance;
 - $P_A = .5$ Assessment depends upon live video, or the assessment is not timely enough for the operator to see the adversary intrusion; and
 - $P_A = .95$ Highly-effective assessment system with recording during all facility states, using an alternate means during times when video cameras are not effective.
- v. Lay out the adversary activities determined in i., iii., and possibly iv., in a sequence.
- vi. Determine total delay, $P_D = P_S * P_A$, and judge Time After Sensing, T_{AF} . Enter these into the correct Layer Performance form.
- vii. If you have the data, determine the equipment required to defeat this element for the given element strategy and record the weight of that equipment; the number of adversaries and any advanced skills required to perform the strategy at the element; and any tactical factors that may enter into employing this strategy (e.g., use of explosives within a building might collapse it).
- viii. Copy the information about this defeat strategy for the isolation zone into column 8 of the summary table on the next page, under the heading "Iso zone."

Layer Performance Values

Protection Layer: PTR Protected Area Boundary

From Area: Institute Limited Area

To Area: PTR Protected Area

[illegible]

Protection Layer: _____

From Area: _____

To Area: _____

[illegible]

Exercise 2 – Create Order-of-Battle Data

A PPS response time should be determined for each target in a facility. This time may vary between operational conditions or weather conditions, so the influence of such factors on the PPS response time should be studied.

For the operational condition you are analyzing, use the information you collected in the Guard and Response Force Description data form, the PPS Response Time data form, and the Rules of Engagement form to complete the Order-of-Battle form below.

Order-of-Battle Form

Target: _____

Adversary Strategy: _____

Response Force Strategy: _____

Critical Event Number	Time (sec)	Description of Event (e.g., Arrival of Unit x)	Total Killed By Other Attacks (e.g., IEDs)	Total Number Who Arrived Armed	Total Number Engaged	Comments

*Unarmed

Note: Most critical events will occur at some time after a valid alarm is generated. For events that may occur before the alarm is generated, enter in the Time column the time since the beginning of the path and put a B in front of the time. For example, if an IED is exploded when the adversary has proceeded 50 seconds into the path (and that time is before the CDP) enter B50 in the Time column as the time.

Exercise 3 – Assign Detection and Delay Values for an ASD Element at the Lagassi Institute Outer Boundary

1. Apply the same process described in Exercise 1 to an element within the protection layer between Offsite and the Institute Limited Area on the same forms.
2. Assign performance data for the Institute Limited Area itself based on whatever facility state and adversary transport mode your subgroup has been assigned to analyze.

Element Name: _____

Element Defeat Strategy: _____

Component	Defeat Method	Time (sec)	Ps
Total Probability of Sensing, Ps			
PA (based on: _____)			
Probability of Detection, PD			
Total Delay Time, T			
Time After Sensing, T _{AF}			

Equipment Required for Defeat Strategy: _____

Weight of Equipment (kg) _____

Number of Adversaries Involved in Defeat Strategy: _____

Advanced Skills Required: _____

Tactical Factors: _____

Layer Performance Values

Protection Layer: Lagassi Site Boundary

From Area: Offsite To Area: Institute Limited Area

Element	P1	P1	P3	P3	P4	P4	P4	P4	Wall	Over P1
Element Strategy	Force, on foot	Deceit on foot	Force, with car	Deceit, with car	Force, with car	Deceit, with car	Force, on foot	Deceit on foot	Stealth	Stealth
<i>Element Performance</i>										
Probability of Detn, Pd	0.45	0.1	0.45	0.1	0.1	0.1	0.1	0.1	0.01	0.02
Total Delay Time, T	35	35	5	5	5	5	10	10	10	10
Time After Sensing, TAF	35	35	5	5	5	5	5	5	5	5
<i>Other Information</i>										
Equipment Weight										
Number of Adversaries										
Advanced Skill										
Tactical Factors:										

Protection Layer: _____

From Area: _____ To Area: _____

Element										
Element Strategy										
<i>Element Performance</i>										
Probability of Detn, Pd										
Total Delay Time, T										
Time After Sensing, TAF										
<i>Other Information</i>										
Equipment Weight										
Number of Adversaries										
Advanced Skill										
Tactical Factors:										

Attachment 1 – Some Representative Qualitative Estimates of P_D

Key: VL = very low A = active
L = low P = passive
M = medium C = covert
H = high V = visible
VH = very high TF = terrain following
N/A = not applicable LOS = line-of-sight

System Type									
Defeat Method	Electric Field	Microwave	Infrared	Fence Motion	Taut-Wire	Seismic	Seismic/Magnetic	Ported Coax	Video Motion
Walking	VH	VH	VH	N/A	N/A	VH	VH	VH	H
Slow Walk	VH	H	VH	N/A	N/A	H	H	H	M
Running	VH	H	VH	N/A	N/A	H	H	VH	H
Crawling	H	M-H	M-H	N/A	N/A	M	M	VH	M-H
Rolling	VH	M-H	M-H	N/A	N/A	M	M	VH	M-H
Jumping	VH	M-H	H	VH	VH	M	M	H	H
Tunneling	VL	VL	VL	L	VL	L	L	M	VL
Trenching	L	L-M	L	L	VL	M	M	VH	L-M
Bridging	L	LOS	VL	VL	VL	L	L	L	M
Cutting	N/A	N/A	N/A	M-H	H	N/A	N/A	N/A	N/A
Climbing	N/A	N/A	N/A	H	H	N/A	N/A	N/A	N/A
Adverse Environment	Surface Snow	Surface Snow		Ice Coat		Frozen Ground			Shadows, snow fog, heavy rain
Defeat Methods	Trench	Trench	Bridge, Trench	Bridge, Trench	Bridge, Trench	Bridge	Magnetically Clean	Stilts	
Characteristics									
Active or Passive	A	A	A	P	P	P	P	A	P
Covert or Visible	V	VH	V	V	V	C	C	C	V
LOS	TF	LOS	LOS	TF	TF	TF	TF	TF	LOS

Attachment 2 – Relative Susceptibility to Nuisance Alarms

Environment	System Type								
	Electric Field	Microwave	Infrared	Fence Motion	Taut-Wire	Seismic	Seismic/Magnetic	Ported Coax	Video Motion
<u>Weather</u>									
Wind Speed <47 km/hr	L	VL	VL	L	VL	L	L	VL	L
Wind Speed (WS)									
47 km/hr < WS < 115 km/hr	M	L	L	H	VL	M	M	VL	M
Wind Speed > 115 km/hr	M	L-M	L-M	VH	L	H	H	VL	M
Rain	L-H	L	L	M	VL	L	L	M	L
Runoff, Standing Water	VL	M-H	L	L	VL	L	L	H	M
Snow	M	L-M	M	L	VL	L	L	L	M
Fog	VL	L	M	VL	VL	VL	VL	VL	L
Hail	M	L	L-M	L	VL	H	M-H	M-H	M
<u>Animals</u>									
Small (Rabbits, Squirrels)	M	M-H	M	L	VL	L	L	VL	L
Large (Dogs, Deer)	VH	VH	VH	M	L	VH	VH	M	H
<u>Birds</u>									
Small	L	VL	L	L	VL	VL	VL	VL	L
Large	M	M	M	L	VL	VL	VL	VL	M
<u>Electrical Interference</u>									
Lightning	M	L-M	L	L	VL	L	H	M	H
Overhead Power Lines	VL	L	VL	VL	VL	L	M	VL	VL
Buried Power Lines	VL	VL	VL	VL	VL	M	H	VL	VL

Key: VL = very low
L = low
M = medium
H = high
VH = very high
N/A = not applicable

Attachment 3 – Climatic and Weather Information

Weather Element	Type of Information	Use or Significance of Information
Wind	• Prevailing direction • Mean speed • Peak gust speed • Speed and direction distribution	If wind speed is 47 km/hr, fence sensors may be activated If wind speed is 32 km/hr, wind-induced noise from trees, bushes, grass, buried posts, poles, and guy wires may activate seismic sensors Ground pressure waves caused by strong winds may activate seismic sensors Windblown debris and subsequent accumulation on fences may cause false alarms and reduce visibility
Temperature	• Extreme minimum • Mean minimum • Mean maximum • Extreme maximum • Mean days/month >38 °C or < -18 °C • Frost depth	Equipment must operate under extremes of temperature Seismic sensors may be desensitized if frost depth exceeds specified limits
Rain	• Mean total per year • Maximum in 24 hours • Rate and duration distribution	Indicated soil moisture in general and its variability Excessive rain may dictate soil erosion control Some seismic sensors are unreliable in extremely wet soil Periods of hard rain will increase seismic background noises Visibility will be reduced during hard rain
Snow	• Mean total per year • Maximum in 24 hours • Maximum accumulations • Drifting (depth, prevalence) • Rate and duration distribution • Water content	Increases amount of soil moisture Decreases visibility if heavy; may require supplementary assessment measures Snow depth >15 cm may require use of snow control measures Can decrease detection capability of some sensors if snow is sufficiently deep or has a hard surface crust
Hail	• Mean days of occurrence per year • Mean and maximum hailstone size • Mean and maximum accumulation • Rate and duration distribution	Hail produces seismic signals and false alarms from seismic sensors Low, dense ground cover may attenuate the seismic effect Large hailstones or prolonged hailstorm may physically damage aboveground sensors. Like other forms of precipitation, hail reduces visibility and assessment capability

Weather Element	Type of Information	Use or Significance of Information
Visibility	• Mean days vs. visibility range • Time of day	Poor visibility due to rain, hail, snow, fog, dust, smoke, smog, etc, can seriously reduce assessment capability, depending on intensity and duration Localized conditions can affect concentrations
Airborne Corrosive Elements	• Types of elements • Frequency of occurrence • Concentration in parts per million (ppm)	Protective coverings or other measures may be necessary Equipment must operate in this environment
Electrical Storms	• Mean days • Duration	Lightning can damage equipment Creates electromagnetic interference

Path Analysis

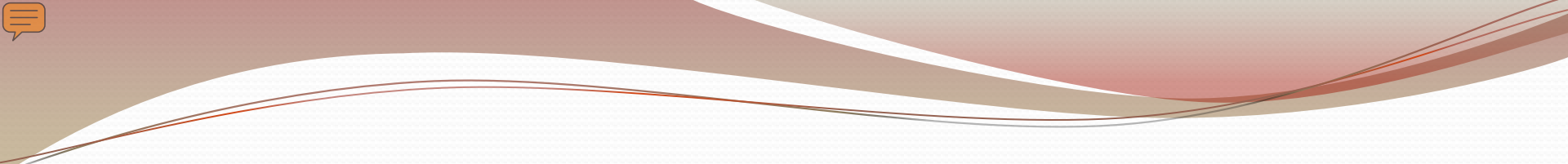
Module 10

Vulnerability Analysis Training Course
Date:

Student Learning Objectives

After completing this module, you should be able to:

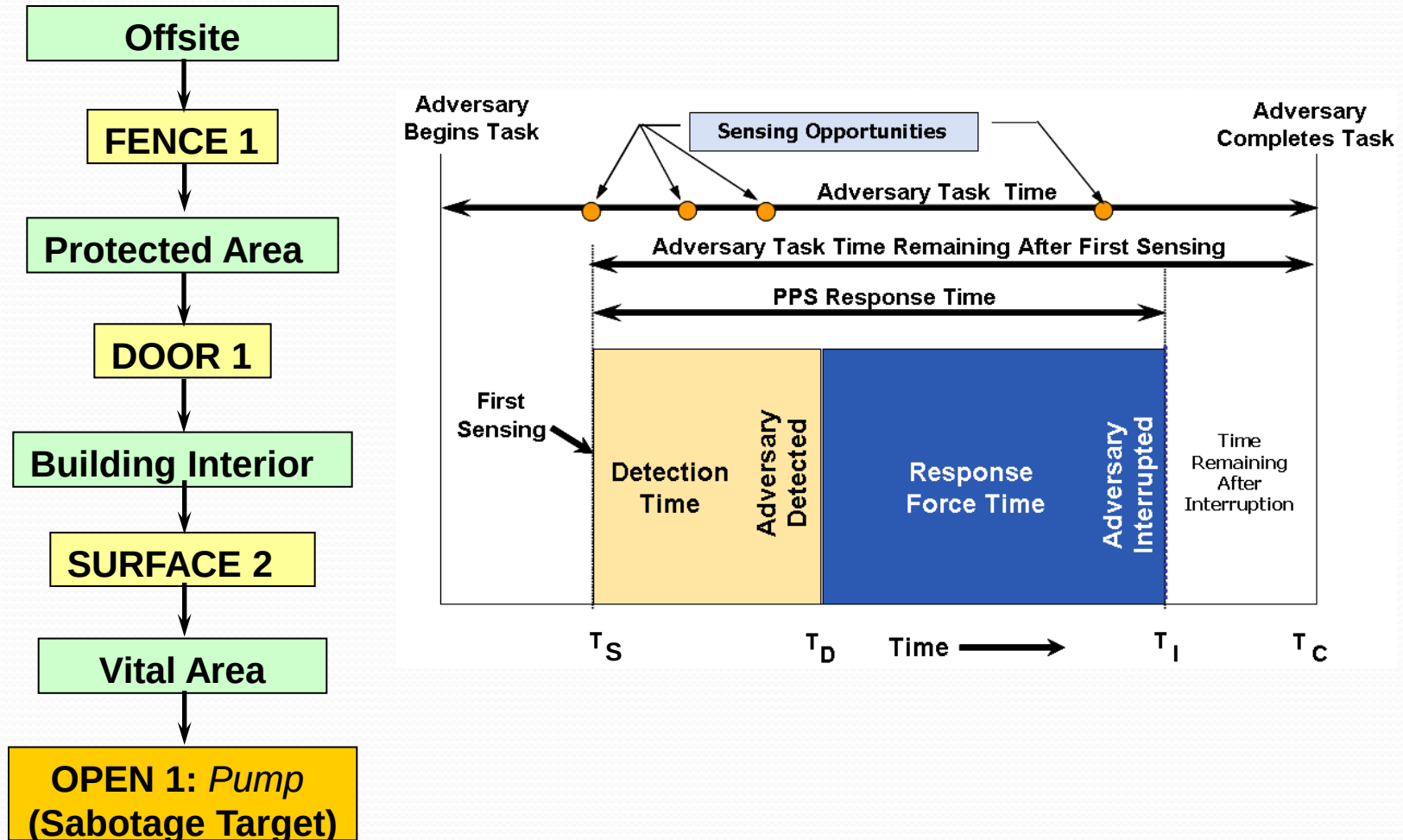
- Perform a single path analysis by hand, including identifying the critical detection point and calculating the probability of interruption
- Perform a timely detection multipath analysis by hand, including
 - Identifying areas and elements having timely detection
 - Evaluating minimum P_I effectiveness
 - Identify most vulnerable paths for the site's ASD
- Describe how to perform an Overt Attack Analysis



Path Analysis Includes Two Sub-Analyses

- Timely Detection Analysis
 - Determines whether Probability of Interruption (P_I) is adequate along all adversary paths
- Overt Attack Analysis
 - Determines whether there are paths that are susceptible to overt attacks that reduce Probability of Neutralization (P_N)
 - Overt in sense that adversary attacks the response force or key response capabilities
 - Typically, $P_D = 1$ at some point on these paths
- Both types of analysis focus on adversary paths within the DBT and account for response regulatory requirements

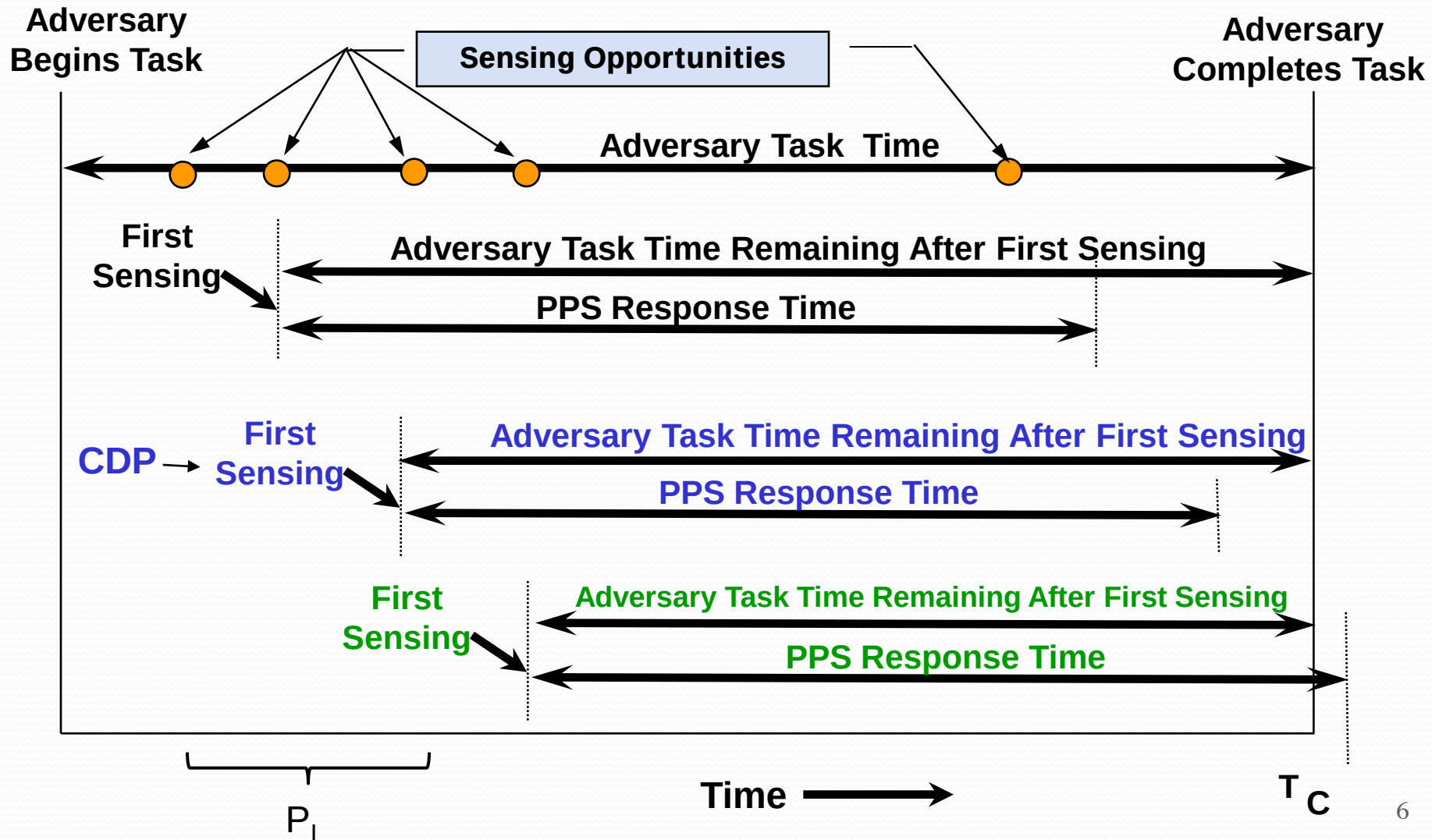
Timely Detection Analysis Uses Adversary and PPS Timelines to Evaluate P_i



Relation of Critical Detection Point to Timely Detection and P_I

- The critical detection point (CDP) is the last sensing opportunity along a path where the PPS response time is less than the adversary task time remaining after first sensing
- Timely detection
 - PPS response time must be less than system delay time after first alarm to achieve adversary interruption
- P_I is the cumulative probability of detection on the path before or at the CDP
 - P_I is also the cumulative probability of timely detection

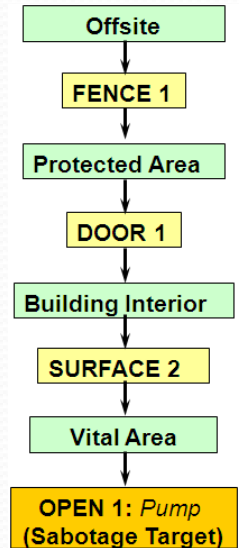
Finding the Critical Detection Point



Evaluating P_i for a Single Adversary Path

Start with Form Describing the Adversary Path

Step	Path Element or Area	Defeat Strategy	P_D	Delay, T(sec)	T_{AF} (Sec)	Equipment	Weight
1	Fence 1	Climb	0.1	6	3		
2	Protected Area	Run Across	0.1	4	0		
3	Door 1	Explosives	0.6	80	35	Explosives	.5 Kg
4	Building Interior	Run Across	0.1	5	0		
5	Surface 2	Power Tools	0.7	110	50	Saw	15 Kg
6	Vital Area	Run Across	0	5	0		
7	Pump	Sabotage	1	50	0	Explosives	30 Kg
8							



Use Data to Build a Schematic of the Adversary Timeline

	Begin Mission						Complete Mission					
Element/Area:	FENCE 1	PA	DOOR 1	BLDG INTERIOR	SURF 2	VITAL AREA	PUMP	← Areas and elements				
P_D								← Delay data				
T (Seconds)	6	4	80	5	110	5	50					

Evaluating P_i for a Single Adversary Path (Cont'd)

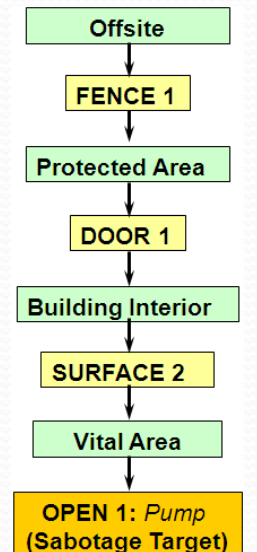
- Determine Adversary Task Time Remaining After First Sensing (*Task Time Remaining* on the form) from right to left
- Stop when Task Time Remaining exceeds the PPS Response Time (120 seconds for this example) to see which elements/areas are timely
- Assign CDP to last timely element/area

	Begin Mission													Complete Mission
Element/Area:	FENCE 1	PA	DOOR 1	BLDG INTERIOR	SURF 2	VITAL AREA	PUMP							
P(Detection)														
T (Seconds)	6	4	80	5	110	5	50							
TAF(Seconds)					50									
Task Time Remaining*					105									
Timely Detn?	Yes	Yes	Yes	Yes	No	No	No							

With a CDP, We Can Explicitly Calculate P_I

- The CDP is the last sensing opportunity that provides timely detection
- $P_I = 1 - (1 - P_{D1}) * (1 - P_{D2}) * ... * (1 - P_{DCDP})$, where P_{Dj} is the Probability of Detection at the j^{th} opportunity
- Explicit Evaluation of P_I (RFT = 120 seconds)

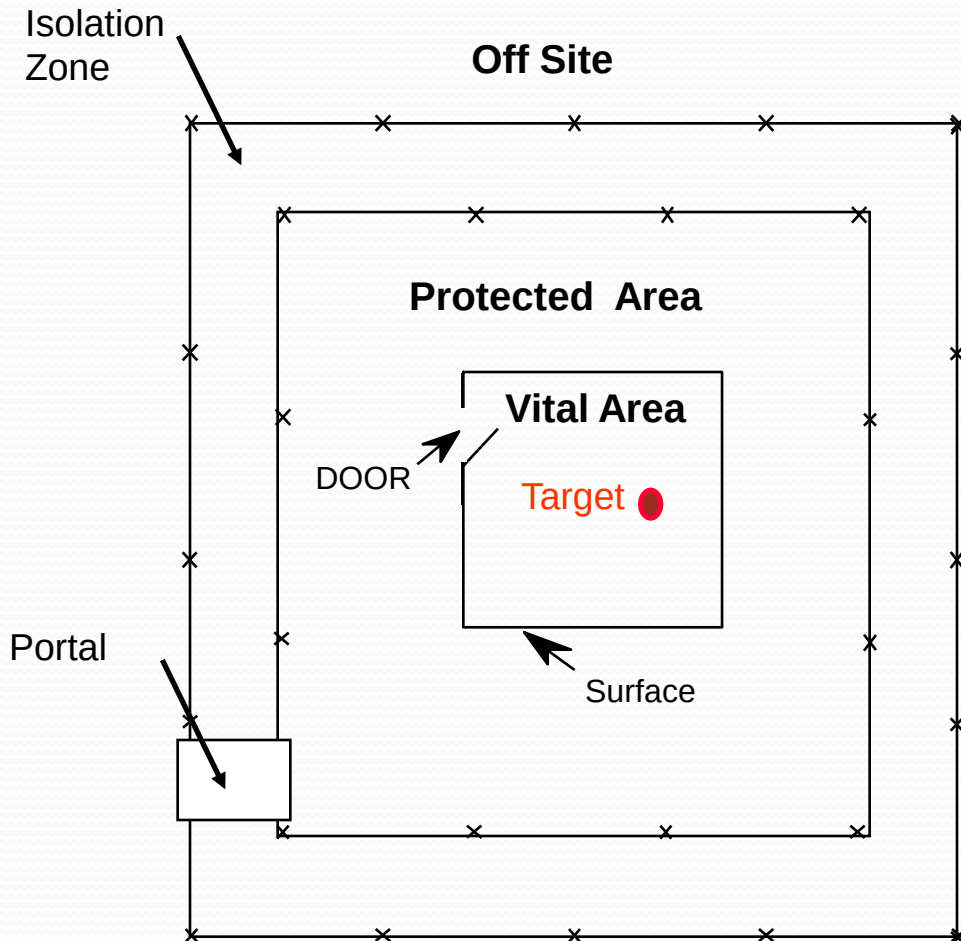
$$\begin{aligned}
 P_I &= 1 - (1 - .1)(1 - .1)(1 - .6)(1 - .1) \\
 &= 1 - (.9)(.9)(.4)(.9) \\
 &= 1 - .292 \\
 &= .708 \sim .71
 \end{aligned}$$



	Begin Mission				Critical Detection Point (CDP)				Complete Mission			
Element/Area:	FENCE 1	PA	DOOR 1	BLDG INTERIOR	SURF 2	VITAL AREA	PUMP					
P(Detection)	0.1	0.1	0.6	0.1								
T (Seconds)	6	4	80	5	110	5	50					
TAF(Seconds)					50							

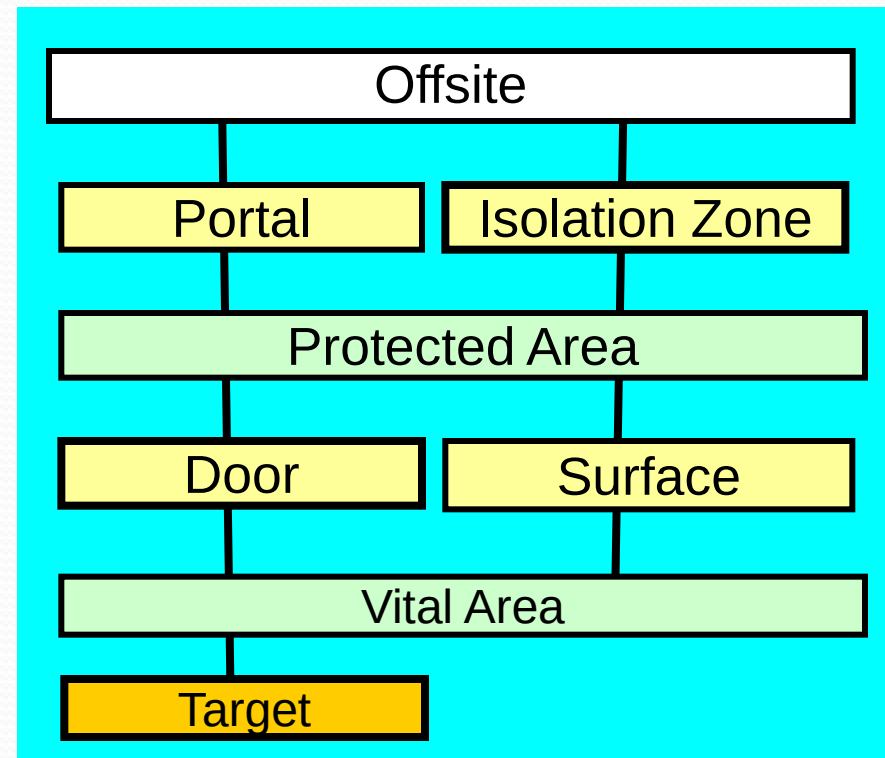
Example Facility for Multipath Analysis

Example Facility



Corresponding ASD

Each Element and Area has Performance Values (T , T_{AF} , P_D)



Perform a Timely Detection Multipath Analysis Selecting the Most Vulnerable Path*

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

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

Offsite

Iso. Zone $P_D = 0.35$
 $T = 25 \text{ s} \mid T_{AF} = 12 \text{ s}$

Portal: $P_D = 0.5$
45 s | 45 s

Protected Area

$P_D = 0.1$ 10 s | 5 s

Door $P_D = 0.9$
60 s | 30 s

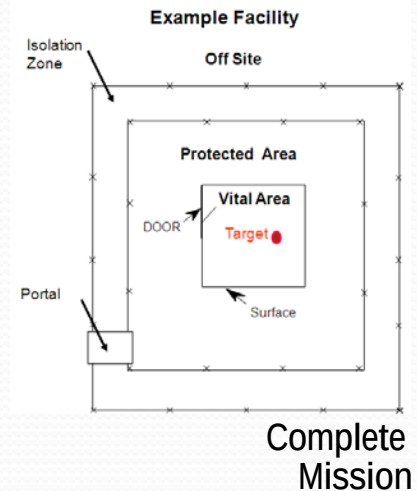
Surface $P_D = .99$
480 s | 240 s

Vital Area

$P_D = 0.0$ 30 s | NA

Start at Target and Enter Target Time on Path Event Timeline

PPS Response
Time = 120 sec



Begin Mission

Pump $P_D = 0.5$
50 s | 50 s

Win Point

PUMP ↓

Element/Area:

						50					
						50					

Task Time

Remaining*

						50					12



Offsite

Iso. Zone $P_D = 0.35$
 $T = 25 \text{ s} \mid T_{AF} = 12 \text{ s}$

Portal: $P_D = 0.5$
 $45 \text{ s} \mid 45 \text{ s}$

Protected Area

$P_D = 0.1$ 10 s | 5 s

Door $P_D = 0.9$
60 s | 30 s

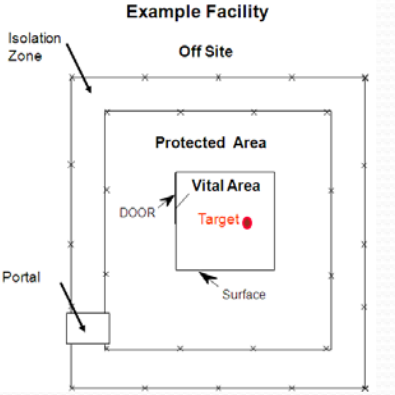
Surface $P_D = .99$
480 s | 240 s

Vital Area

$P_D = 0.0$ 30 s | NA

Enter Data for Vital Area
and Best Vital Area
Perimeter Element

PPS Response
Time = 120 sec



Begin
Mission

Pump $P_D = 0.5$
50 s | 50 s

Win Point

Complete
Mission

Element/Area:

Door Vital Area PUMP

P(Detection)													
T (Seconds)					60	30	50						
TAF(Seconds)					30								
Task Time													
Remaining*					110								
Timely Detn?					NO	NO	NO						13



By Checking Other Elements,
We Can Determine Which
Are Timely (green boxes)

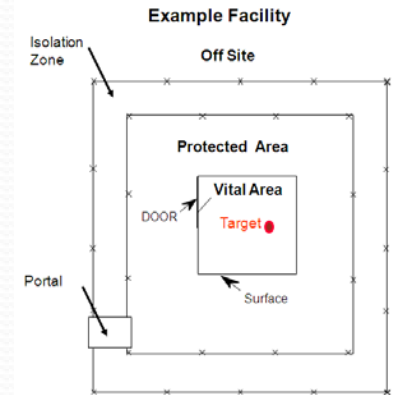
Offsite	
Iso. Zone $P_D = 0.35$ $T = 25\text{ s} \mid T_{AF} = 12\text{ s}$	Portal: $P_D = 0.5$ $45\text{ s} \mid 45\text{ s}$
Protected Area	$P_D = 0.1$ $10\text{ s} \mid 5\text{ s}$

Door $P_D = 0.9$ $60\text{ s} \mid 30\text{ s}$

Surface $P_D = 0.99$ $480\text{ s} \mid 240\text{ s}$

Vital Area	$P_D = 0.0$ $30\text{ s} \mid \text{NA}$

PPS Response
Time = 120 sec



Pump $P_D = 0.5$ $50\text{ s} \mid 50\text{ s}$

Begin
Mission

Critical Detection Point (CDP)

Complete
Mission

Element/Area

Win Point

Wall Vital Area PUMP

P(Detection)												
T (Seconds)				480	30	50						
TAF(Seconds)				240		50						

Task Time

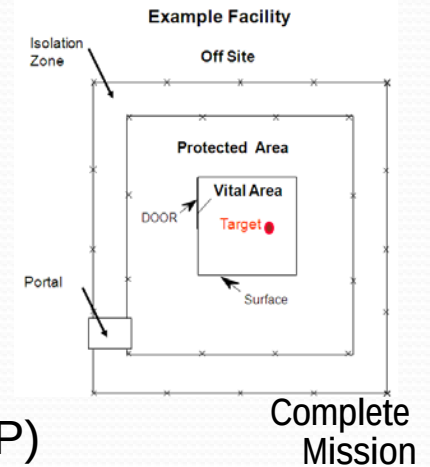
Remaining*

Timely Detn?

				320								
				Yes	NO	NO						14



Once CDP Is Found,
Minimize Detection From
Front of Path and
Determine P_i



PPS Response
Time = 120 sec

Adversary:

Minimizes

P_D

(CDP)

Minimizes

Delay

Offsite

Iso. Zone $P_D = 0.35$
 $T = 25$ s | $T_{AF} = 12$ s

Portal: $P_D = 0.5$
45 s | 45 s

Protected Area $P_D = 0.1$ 10 s | 5 s

Door $P_D = 0.9$
60 s | 30 s

Surface $P_D = .99$
480 s | 240 s

Vital Area $P_D = 0.0$ 30 s | NA

Pump $P_D = 0.5$
50 s | 50 s

Begin
Mission

Critical Detection Point (CDP)
Win Point

Complete
Mission

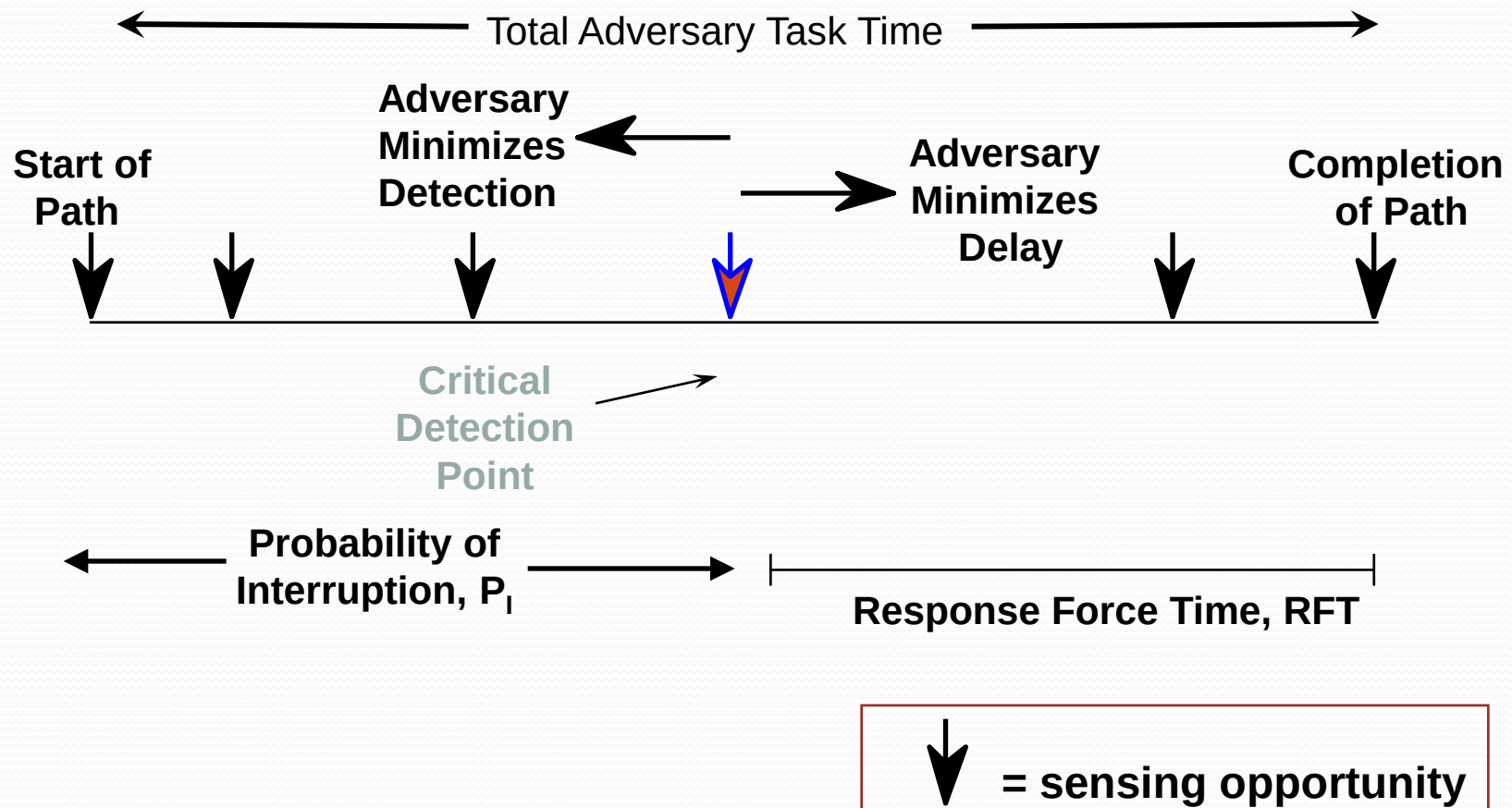
Element/Area

Iso. Zone PA Door Vital Area PUMP

P(Detection)			0.35	0.1								
T (Seconds)				10	60	30	50					
TAF(Seconds)				5	30		50					

$$P_i = 1 - (1 - .35)(1 - .1) = 1 - (.65)(.9) = 1 - .585 = .415 \sim .41$$

Relationship of Multipath Algorithm to Assumed Adversary Planning Preferences





Issue of Where Sensing Occurs Within Elements on a Layer

Offsite

Iso. Zone $P_D = 0.35$
 $T = 25 \text{ s} \mid T_{AF} = 12 \text{ s}$

Portal: $P_D = 0.5$
 $45 \text{ s} \mid 45 \text{ s}$

Protected Area

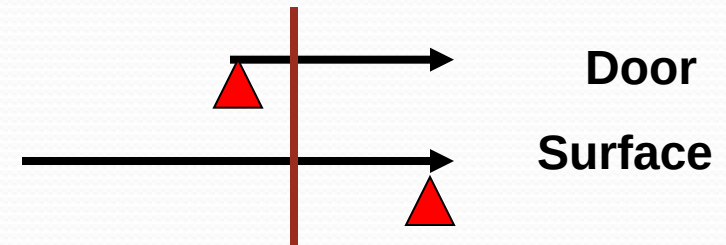
$P_D = 0.1 \quad 10 \text{ s} \mid 5 \text{ s}$

Door $P_D = 0.9$
 $60 \text{ s} \mid 60 \text{ s}$

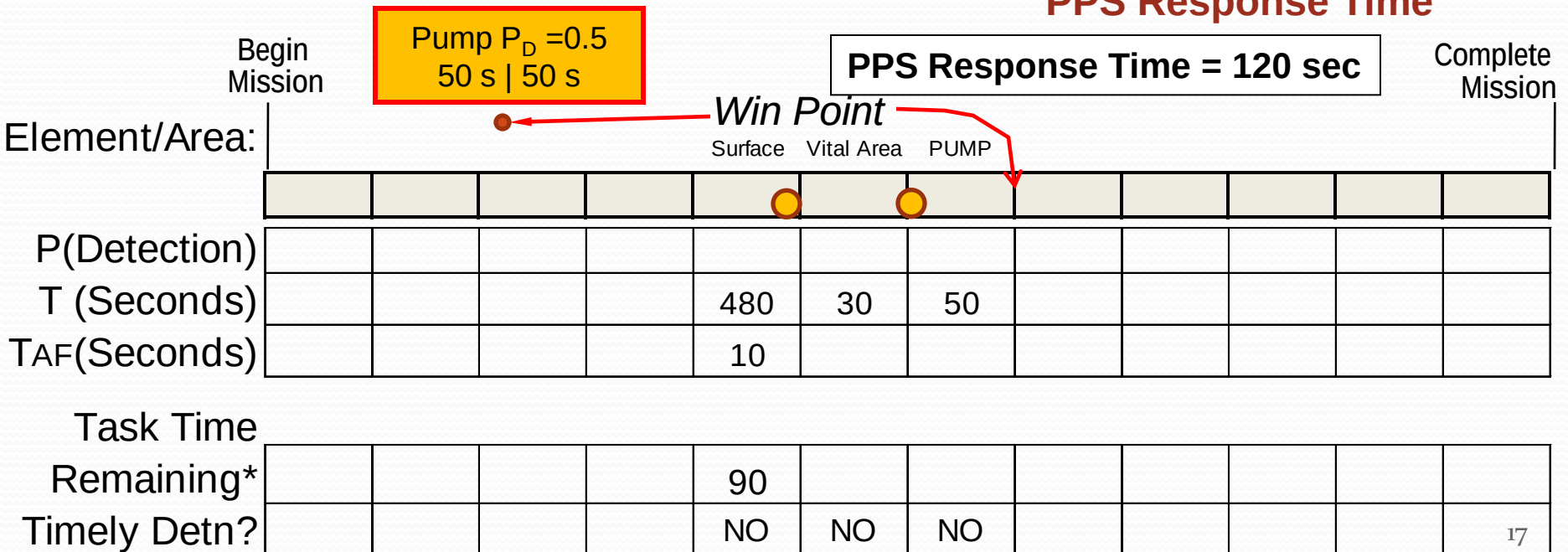
Surface $P_D = .99$
 $480 \text{ s} \mid 10 \text{ s}$

Vital Area

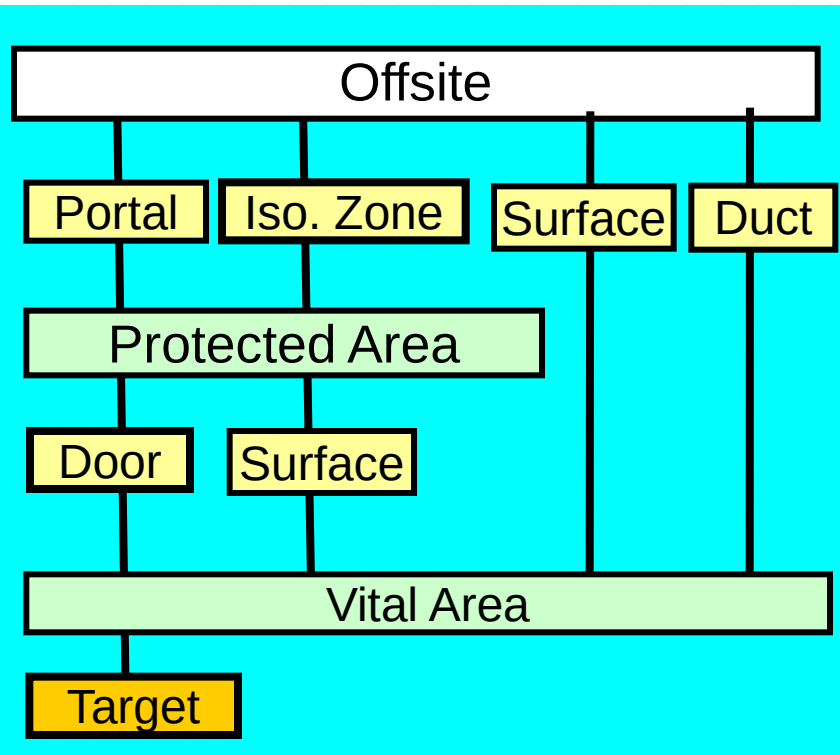
$P_D = 0.0 \quad 30 \text{ s} \mid \text{NA}$



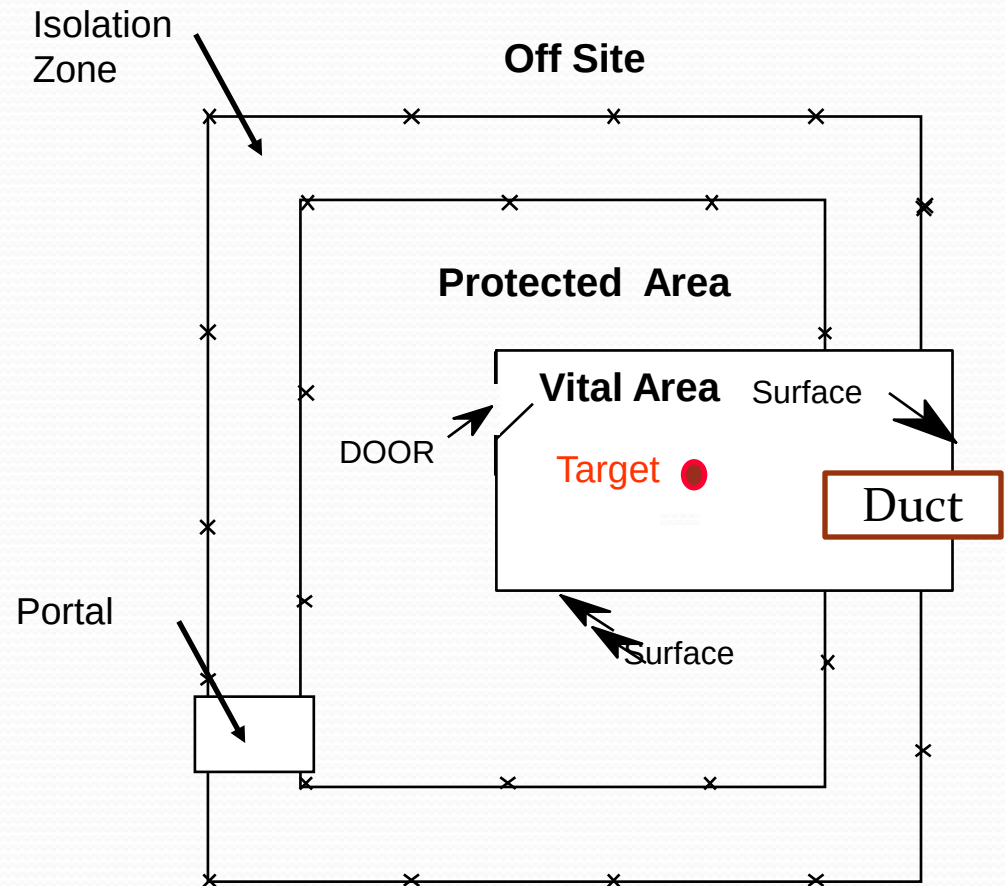
PPS Response Time



If the ASD Has Jumps



Example Facility





O

Offsite

~~Iso. Zone $P_D = 0.35$
 $T = 25\text{ s} \mid T_{AF} = 12\text{ s}$~~

~~Portal: $P_D = 0.5$
 $45\text{ s} \mid 45\text{ s}$~~

Surface: $P_D = 0.7$
 $T = 90\text{ s} \mid T_{AF} = 60\text{ s}$

Duct: $P_D = 0.5$
 $T = 120\text{ s} \mid T_{AF} = 60\text{ s}$

A

Protected Area

$P_D = 0.1$ 10 s | 5 s

~~Door $P_D = 0.9$
 $60\text{ s} \mid 30\text{ s}$~~

~~Surface $P_D = .99$
 $480\text{ s} \mid 240\text{ s}$~~

B

Vital Area

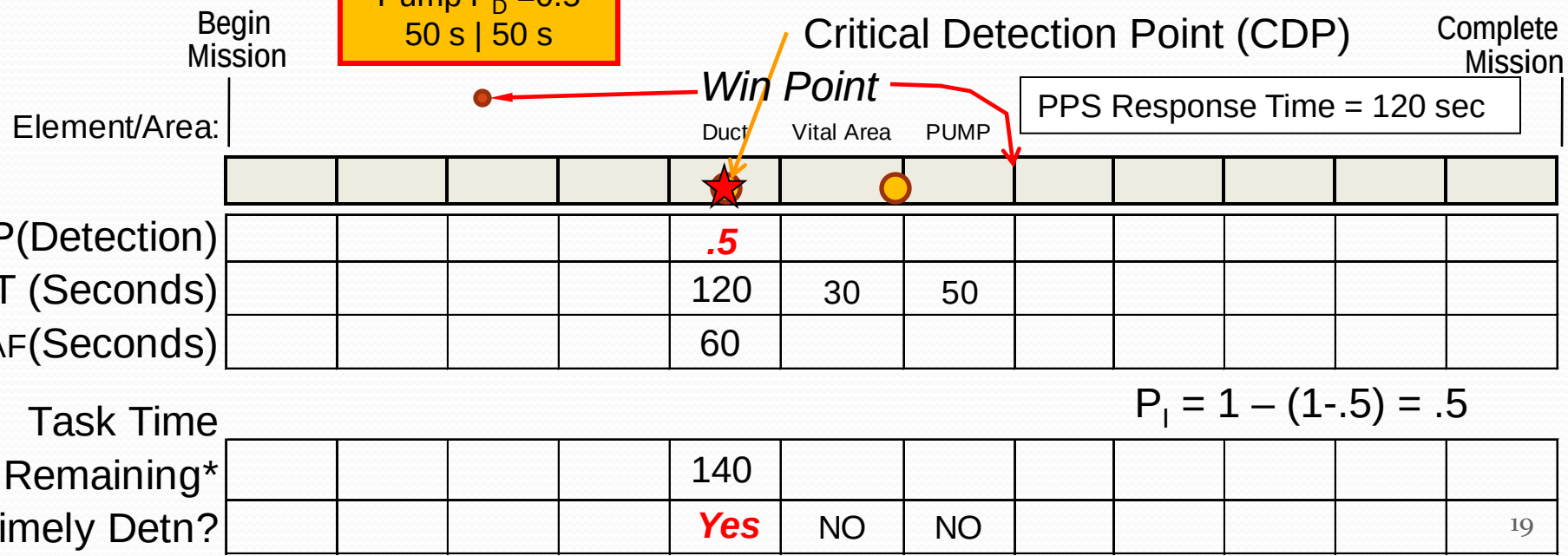
$P_D = 0.0$ 30 s | NA

Jump to B

Jump to B

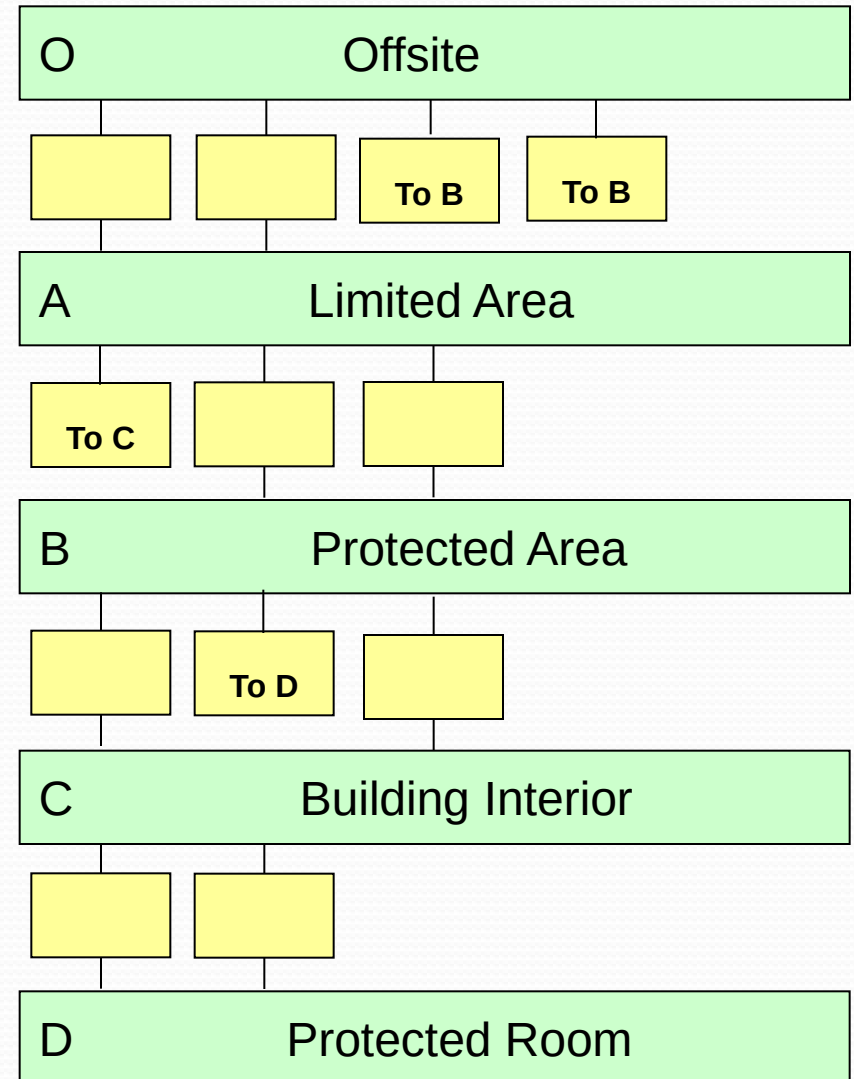
If the ASD Has Jumps,
Treat Each Combination
of Similar Jumps As
Separate Analysis Cases

Pump $P_D = 0.5$
 $50\text{ s} \mid 50\text{ s}$



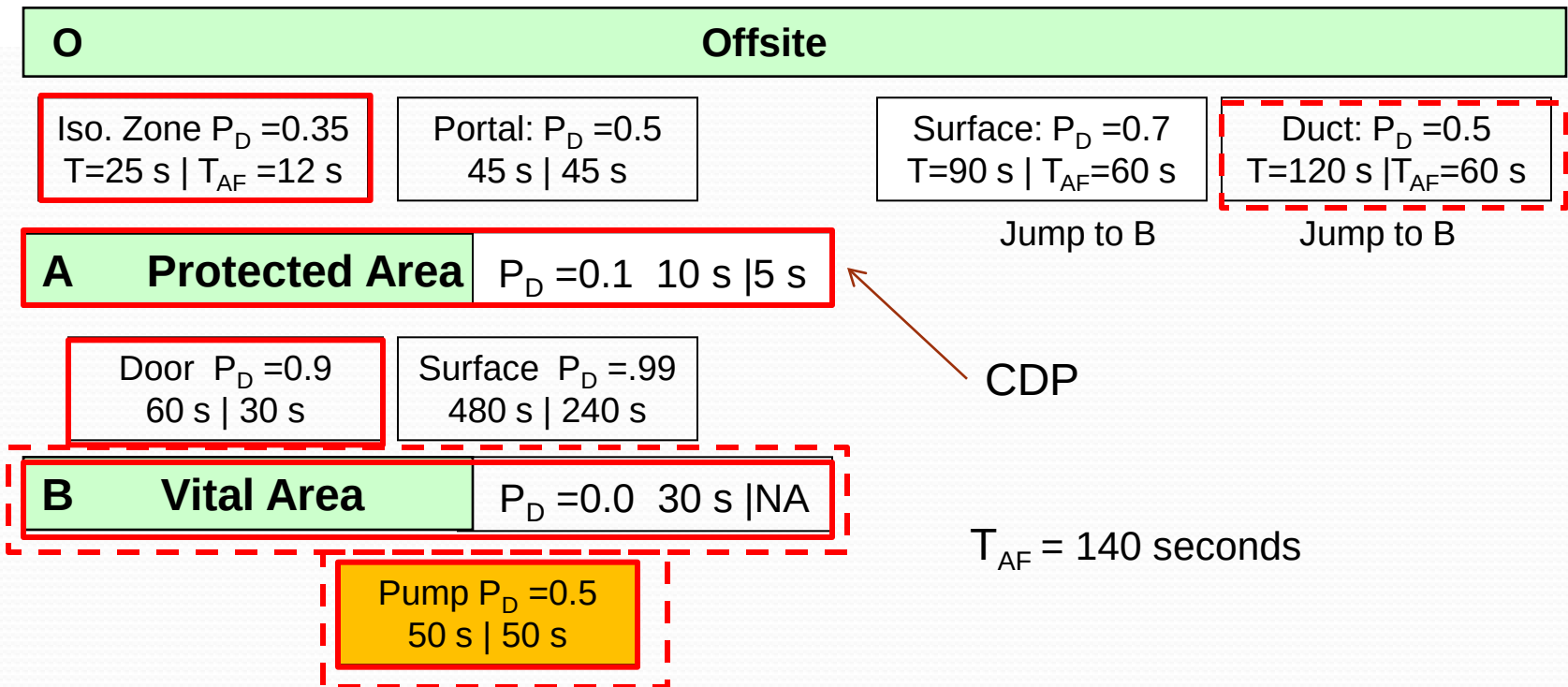
Determining the Number of Separate Analysis Cases to Analyze

- Analysis Cases = 1 for no jumps + number of combinations of jumps
- Ignore elements not included in the case
- Example ASD has 5 cases:
 - No jumps
 - O To B jumps
 - A To C jumps
 - B To D jumps
 - O To B, then B To D jumps in succession



Determining the Most Vulnerable of Two Paths, Each From a Different Analysis Case

- The path with the smaller P_I is the most vulnerable of the two
 - Path 1 (Non-jump part of ASD) $P_I = .41$
 - Path 2 (Jump part of ASD): $P_I = .5$
 - Then Path 1 is most vulnerable



Determining the Most Vulnerable of Two Paths (Cont'd)

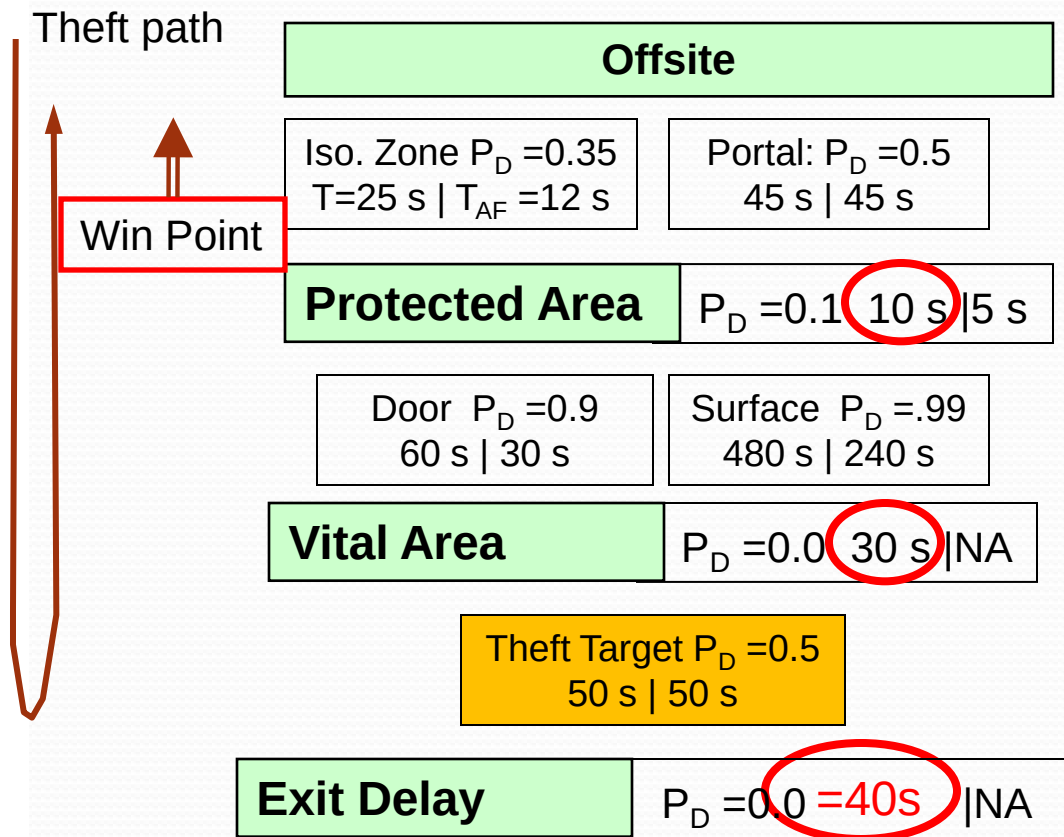
- If both paths have the same P_I , the path with the smaller task time remaining (after the CDP) is most vulnerable of the two
 - Path 1: $P_I = .5$, *Task Time Remaining(After the CDP) = 140 seconds
 - Path 2: $P_I = .5$, *Task Time Remaining(After the CDP) = 130 seconds
 - Then Path 2 is most vulnerable

*Task Time Remaining on the form is Adversary Task Time Remaining After First Sensing

Containment Response: Make Worst-Case Assumptions for Exit, and Count Area Delay Times

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

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



Examining Balance on Each Protection Layer

- Balanced Protection: Compare both P_D and Delay Times for Elements Within a Protection Layer
 - Values do not have to be identical but there should not be any big differences

Vehicle Door $P_D = 0.8$ $T = 60$ s $T_{AF} = 30$ s

Fence: $P_D = 0.1$ 8 s 8 s

Gate $P_D = 0.8$ 60 s 30 s

- Protection in Depth: Compare Detection Probabilities and Delay Times Across Multiple Layers



Given a Most-Vulnerable Path, See If Coverage of Target Is Adequate

- Update the “Response only” response picture-in-time to show where adversaries would be on the path, given detection at an assumed sensing opportunity
 - Timely Detection: at the CDP
 - Overt Attack: at a point on the path that is virtually certain (e.g., when big vehicle bomb is exploded)
- Place adversaries and/or sabotage the response to adversary's best advantage
- Determine if target building or room is adequately covered to allow interruption

Simple P_N Methodology for Path Analysis

- Let X = number of adversaries fighting
- Let Y = number of responders who 1) match adversary capabilities and 2) actually fight
- Find P_N in table at row Y , column X

Number of
Responders,
 Y

Number of Adversaries, X

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
1	0.50	0.17	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.84	0.50	0.23	0.08	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
3	0.96	0.78	0.50	0.26	0.11	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	0.99	0.92	0.74	0.50	0.29	0.14	0.06	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00
5	1.00	0.98	0.89	0.72	0.50	0.30	0.16	0.07	0.03	0.01	0.00	0.00	0.00	0.00	0.00
6	1.00	0.99	0.96	0.86	0.70	0.50	0.32	0.18	0.09	0.04	0.02	0.01	0.00	0.00	0.00
7	1.00	1.00	0.99	0.94	0.84	0.68	0.50	0.33	0.20	0.10	0.05	0.02	0.01	0.00	0.00
8	1.00	1.00	1.00	0.98	0.93	0.82	0.67	0.50	0.34	0.21	0.12	0.06	0.03	0.01	0.01
9	1.00	1.00	1.00	0.99	0.97	0.91	0.81	0.66	0.50	0.35	0.22	0.13	0.07	0.04	0.02
10	1.00	1.00	1.00	1.00	0.99	0.96	0.90	0.79	0.65	0.50	0.35	0.23	0.14	0.08	0.04
11	1.00	1.00	1.00	1.00	1.00	0.98	0.95	0.88	0.78	0.65	0.50	0.36	0.24	0.15	0.09
12	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.94	0.87	0.77	0.64	0.50	0.37	0.25	0.16
13	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.93	0.86	0.76	0.64	0.50	0.37	0.26
14	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.99	0.96	0.92	0.85	0.75	0.63	0.50
15	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.98	0.96	0.91	0.84	0.75	0.63	0.50
16	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.91	0.83	0.74	0.62
17	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.92	0.95	0.90	0.82	0.73
18	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.89	0.82
19	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.88
20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.96	0.93

Example: 10 responders and 6 adversaries: $P_N = .96$

$P_I = .41$; $P_E = P_I * P_N = .4$



Overt Attack Analysis Examines Ways The Adversary May Reduce P_N

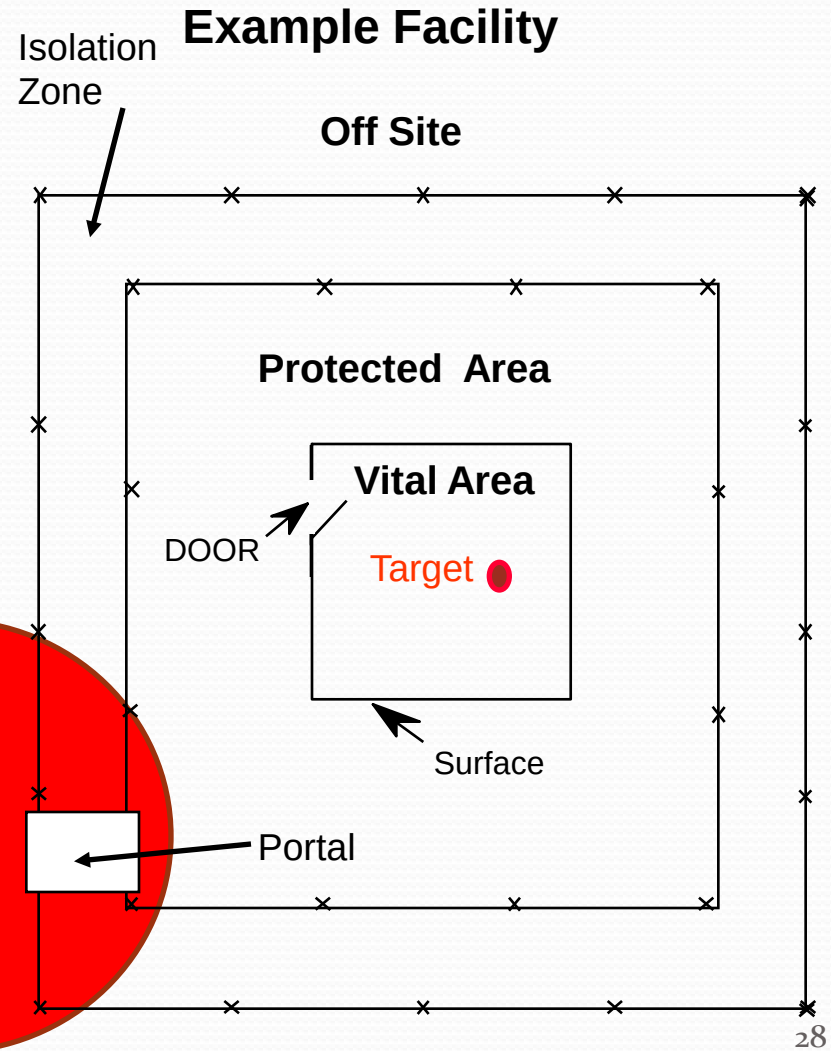
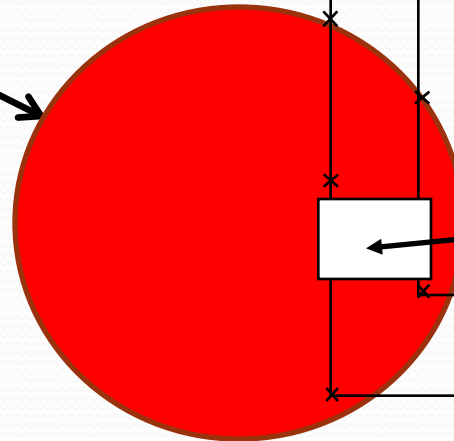
- Compares Response Force to Adversary:
 - Types of Weapons and Equipment: Equal match to DBT?
 - Procedures/plans appropriate and training adequate?
- Considers, also, adversary paths that reduce numbers of responders or provides adversary tactical advantages
 - Examines response force survivability: Armored vehicles, fighting positions
 - Considers possible adversary use of ambushes and explosives
 - Judges if surviving response force capability and numbers meet requirements for interruption and neutralization
 - This course will use simple P_N tables to determine sufficiency

Overt Attack: Blow Up Portal Containing Responders

- Concept: Kill 6 immediate responders, so size of response force falls from 10 to 4

- Assume 6 adversaries

Building
Collapsed
Inhabitants
killed



Offsite

Portal: $P_D = 1.0$
5 s | 5 s

Protected Area

$P_D = 0.1$ 10 s | 5 s

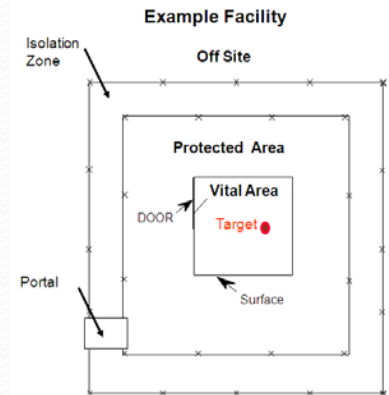
Door $P_D = 0.9$
60 s | 30 s

Surface $P_D = .99$
480 s | 240 s

Vital Area

$P_D = 0.0$ 30 s | NA

Overt Attack: Blow Up Portal Containing Responders



Pump $P_D = 0.5$
50 s | 50 s

PPS Response
Time = 120 sec

Complete Mission

Begin Mission

Win Point

Element/Area:

Portal

PA

Door

VITAL
AREA

PUMP

[illegible]

Task Time

Remaining*

Offsite

Portal: $P_D = 1.0$
45 s | 45 s

Protected Area	$P_D = 0.1$ 10 s 5 s

Door $P_D = 0.9$
60 s | 30 s

Surface $P_D = .99$
480 s | 240 s

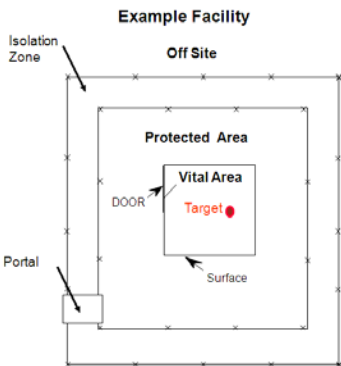
Vital Area	$P_D = 0.0$ 30 s NA

$P_D = 0.0$ 30 s | NA

Revised ASD and Path Analysis

$$P_I = 1 - (1-1)(1-.1) = 1$$

$$P_N = .14 = P_E$$



PPS Response Time = 120 sec

Begin Mission

Pump $P_D = 0.5$
50 s | 50 s

Critical Detection Point (CDP)
- *Win Point*

Complete Mission

Element/Area:

											
		1	0.1								
			10	60	30	50					
			5	30							

Task Time

Remaining*

Timely Detn?

			145	110							
			Yes	NO	NO	NO					30

Evaluating P_i for a Single Adversary Path (Cont'd)

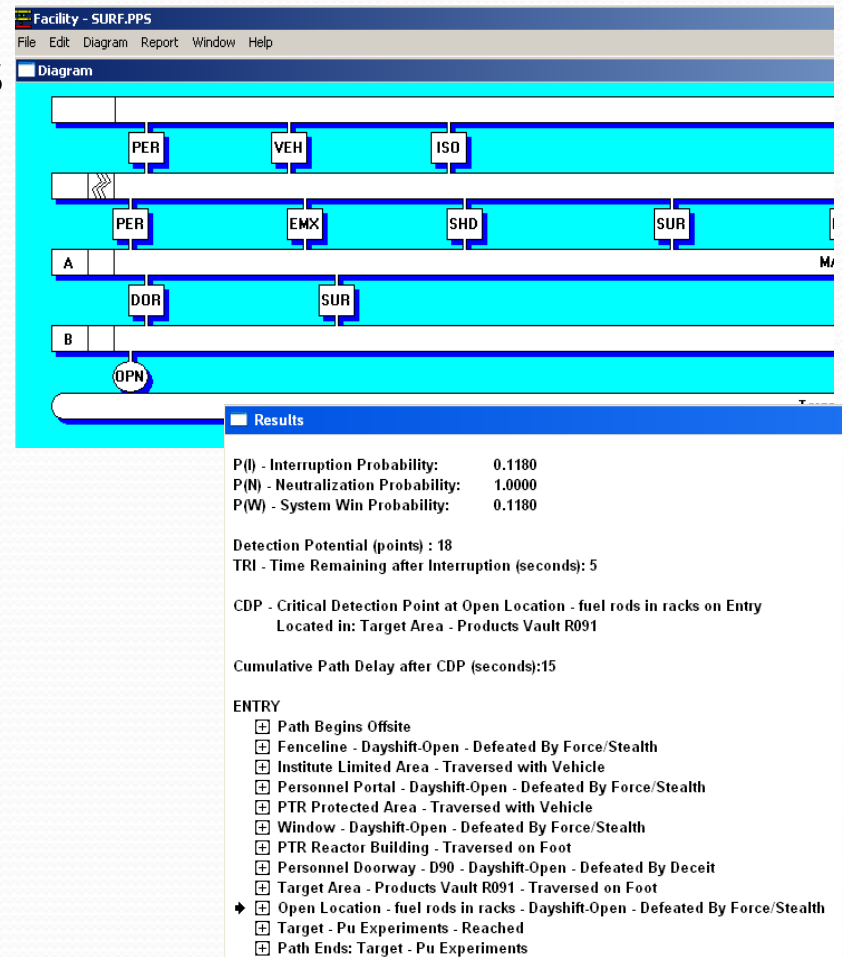
- Implicit Evaluation (e.g., CDP by regulation at PA or closer to target)
 - Timeliness Requirements: Fence 1 and PA are timely (met)
 - Detection Requirements: Fence P_D should be .90 and PA P_D should be .25 (unmet)

	Begin Mission				CDP								Complete Mission
Element/Area:	FENCE 1	PA	DOOR 1	BLDG INTERIOR	SURF 2	VITAL AREA	PUMP						
P(Detection)	0.1	0.1	0.6	0.1									
T (Seconds)	6	4	80	5	110	5	50						
TAF(Seconds)	3	0	35	0	50	0	0						

In Some Countries, Path Analysis Computer Tools Can Be Used to Find Paths With Lowest P_I

- Use: Identifies adversary paths with the lowest P_I among all paths through a PPS
- Examples:
 - U.S. competent authorities
 - NRC for commercial reactors: No such tools are used
 - Department of Energy: SAVI (shown here)
 - Russia: Vega
 - France: EVA
 - Korea: SAPE

Note: software can develop outsider, insider, and collusion paths



Summary

- Conduct a single path analysis to identify the CDP and calculate the P_I
- A multipath analysis is used to:
 - Identify areas and elements
 - Evaluate the minimum P_I effectiveness
 - Identify the most-vulnerable path for the site's ASD
- An overt attack analysis examines ways the adversary may reduce P_N

10. Path Analysis Subgroup

Session Objectives

After this session, you will be able to:

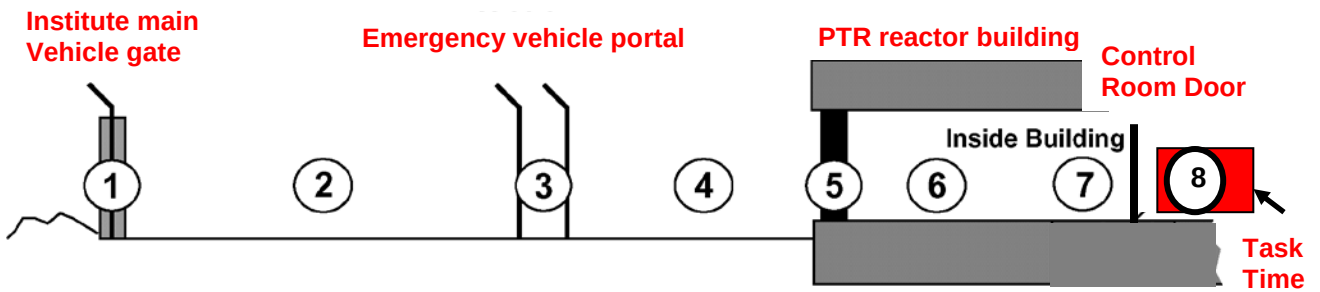
1. Determine CDP and Probability of Interruption for a single path to the PTR Reactor facility, based on a Timely Detection analysis.
2. Determine how to find a most-vulnerable path through an ASD based on a Timely Detection Analysis and determine P_I .
3. Determine how to alter the values in the ASD to perform an Overt Attack Analysis and determine an approximate P_N and P_E for this analysis.

Exercise 1 – Timely Detection Analysis: Determining Probability of Interruption and Critical Detection Point for a Single Outsider Path

An adversary force sized to match your Design Basis Threat (DBT) equipped with a truck, a 1.0-kg explosive charge, and a 25-kg set of special tools intends to sabotage the PTR reactor by attacking the Control Room vital equipment. The adversaries intend to:

1. Crash a truck through the outer main vehicle gate of the Institute.
2. Drive to the emergency vehicle portal at the PTR reactor.
3. Penetrate the emergency vehicle portal using a fast defeat strategy that you calculated detection and delay values for in the Characterizing Element Performance Subgroup
4. Drive to the PTR reactor building shipping door.
5. Penetrate the shipping door with 1.0 kg of explosives.
6. Run to the reactor control-room door.
7. Break the glass in the door and open it.
8. Sabotage the vital equipment in the control room.

1) Use the Path Event Timeline Worksheet to record the information about attacking the emergency vehicle portal (defeat strategy, P_D , T , T_{AF} , equipment involved in that step, and weight of that equipment).



Barrier Number	Type	Specification
1	Main Gate	2.4-m x 4-m-wide padlocked, chain-link gate on metal pipe (construction and maintenance gate)
2	Distance	1-km road
3	Vehicle portal	Two active barriers, 2.4-m x 4-m wide, manually operated, chain-link gates on metal pipe (12 m apart)
4	Distance	125-m paved surface
5	Reactor shipping door	10-cm thick wooden door with metal sheeting
6	Distance to control room door	60 m to door
7	Control room door	5-cm wooden door with glass windows
8	Task Time	Time to sabotage vital equipment in control room

Exercise 1 – Adversary Path Worksheet

Path Event Timeline Worksheet

Step	Path Element or Area	Defeat Strategy	P_D	Delay, T(sec)	T_{AF} (sec)	Equipment	Weight (kg)
1	Vehicle Entrance, P3	Crash truck	0.45	6	3	truck	1,500
2	Institute Area	Drive 1 km	0.2	36	18		
3	Emergency Vehicle Portal						
4	Protected Area	Drive 125 m	0	12	6		
5	PTR Building Shipping Door	Penetrate w. 1-kg explosive	0.95	114	20	explosive	1
6	Reactor Hall	Run 60 m	0	15	7.5		
7	Control-Room Door	Break glass	0.5	6	3		
8	Control Room	Sabotage task	0.9	780	780	tools	25

2) Fill out the Adversary Timeline Schematic below for this path:

- First, by entering the delays, T, and Time After Sensing, T_{AF} ;
- Determining the Adversary Task Time Remaining After First Sensing (Task Time Remaining) for all sensing opportunities;
- Determining which sensing opportunities are timely and finding the CDP; and
- Entering the Probability of Detection just for the timely detection locations.

Adversary Timeline Schematic

Begin Mission									
Element/Area:									
P(Detection)									
T (Seconds)									
T_{AF} (Seconds)									
Task Time Remaining*									
Timely Detn?									

PPS Response Time Seconds

*Adversary Task Time Remaining After First Sensing

3) What is the Probability of Interruption, P_I ? The P_I is found by multiplying the non-detection probabilities down to and including the CDP:

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

Exercise 2 – Timely Detection Analysis: Determining the Most-Vulnerable P_I Path Through an ASD and Evaluating Timely Detection, P_I , and Critical Detection Point for That Single Outsider Path

In this exercise, we will evaluate system effectiveness against radiological sabotage at the PTR Reactor by a terrorist attack. For this analysis, use the data appropriate for the facility state and type of transport your subgroup is analyzing. The ASD in Figure 1 has data for all elements except the protection layer between offsite and the Limited Area, the Limited Area itself, and the protection layer between the Limited Area and the Protected Area.

- 1) Fill in the missing values on the ASD in Figure 1 for the Limited Area and two protection layers for the facility state and type of adversary transport your subgroup is analyzing.
- 2) Record the PPS Response Time here: _____
- 3) Determine the most-vulnerable timely detection path through the ASD for the PPS Response Time, starting from the end of the path. Record your progressing definition of the path in the Path Event Timeline Worksheet and Adversary Timeline Schematic included below.

What elements are timely? (explain verbally) _____

Where is the Critical Detection Point on the Most-Vulnerable Path? _____

What is the Probability of Interruption? _____

Figure 1 – Delay and Detection Values for PTR Areas and Elements

O	PD		T(sec)		Offsite											
	Institute Wall		Portal P1		Portal P3		Portal P4		Admin Bldg Roof							
	PD	0.01	PD	0.1	PD	0.1	PD	0.1	PD	0.02						
	T(sec)	10	T(sec)	35	T(sec)	5	T(sec)	5	T(sec)	10						
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:							
A	PD	0	T(sec)	60	Institute Limited Area											
	Portal P5		Main Veh Portal		Emg. Veh Portal		Isolation Zone		Roof over P5							
	PD	0.15	PD	0.15	PD	0.15	PD		PD	0.52						
	T(sec)	63	T(sec)	83	T(sec)	53	T(sec)		T(sec)	0.87						
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:							
B	PD	0	T(sec)	9	PTR Protected Area											
	Portal P6		Window		20 cm Surface		Cooling Duct		S/R Veh Door		Emg. Door		30 cm surface		30 cm roof	
	PD	0.45	PD	0	PD	0.95	PD	0.1	PD	0.76	PD	0.76	PD	0.95	PD	0.95
	T(sec)	20	T(sec)	0	T(sec)	180	T(sec)	174	T(sec)	30	T(sec)	12	T(sec)	195	T(sec)	195
	JUMP:		JUMP:		JUMP:		JUMP:	To D	JUMP:	To D	JUMP:	To D	JUMP:	To D	JUMP:	To D
C	PD	0	T(sec)	2	PTR Reactor Building											
	Portal at D60		30 cm Surface													
	PD	0.6	PD	0.1												
	T(sec)	43	T(sec)	195												
	JUMP:		JUMP:													
D	PD	0	T(sec)	7	PTR Reactor Hall											
	C. Rm. Door		C.Rm. Windows		C.Rm. Walls											
	PD	0.02	PD	0.02	PD	0.02										
	T(sec)	12	T(sec)	6	T(sec)	180										
	JUMP:		JUMP:		JUMP:											
F	PD	0	T(sec)	2	Control Room Interior											
	Target Sab Task															
	PD	0.02														
	T(sec)	780														
	JUMP:															
G	PD		T(sec)													

Path Event Timeline Worksheet

Step	Path Element or Area	Defeat Strategy	P _D	Delay, T(sec)	T _{AF} (sec)	Equipment	Weight (kg)
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

Adversary Timeline Schematic

	Begin Mission												Complete Mission
Element/Area:													
P(Detection)													
T (Seconds)													
T _{AF} (Seconds)													
Task Time													
Remaining*													
Timely Detn?													

PPS Response Time

Seconds

*Adversary Task Time Remaining After First Sensing

- 4) We will now calculate an approximate P_N , based on the number of adversaries who can use weapons versus the number of responders who a) match the adversaries in terms of skills and b) actually engage the adversaries.

What is the total number of adversaries who can engage the response forces (as opposed to work on target tasks, etc.)? _____

What is the total number of response forces who a) match the adversaries in terms of skills and b) actually engage the adversaries? _____

From the following table, what is an approximate P_N for this path? _____

		Number of Adversaries														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number of Response Forces	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	1	0.50	0.17	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.84	0.50	0.23	0.08	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	3	0.96	0.78	0.50	0.26	0.11	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	4	0.99	0.92	0.74	0.50	0.29	0.14	0.06	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	5	1.00	0.98	0.89	0.72	0.50	0.30	0.16	0.07	0.03	0.01	0.00	0.00	0.00	0.00	0.00
	6	1.00	0.99	0.96	0.86	0.70	0.50	0.32	0.18	0.09	0.04	0.02	0.01	0.00	0.00	0.00
	7	1.00	1.00	0.99	0.94	0.84	0.68	0.50	0.33	0.20	0.10	0.05	0.02	0.01	0.00	0.00
	8	1.00	1.00	1.00	0.98	0.93	0.82	0.67	0.50	0.34	0.21	0.12	0.06	0.03	0.01	0.01
	9	1.00	1.00	1.00	0.99	0.97	0.91	0.81	0.66	0.50	0.35	0.22	0.13	0.07	0.04	0.02
	10	1.00	1.00	1.00	1.00	0.99	0.96	0.90	0.79	0.65	0.50	0.35	0.23	0.14	0.08	0.04
	11	1.00	1.00	1.00	1.00	1.00	0.98	0.95	0.88	0.78	0.65	0.50	0.36	0.24	0.15	0.09
	12	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.94	0.87	0.77	0.64	0.50	0.37	0.25	0.16
	13	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.93	0.86	0.76	0.64	0.50	0.37	0.26
	14	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.96	0.92	0.85	0.75	0.63	0.50	0.38
	15	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.98	0.96	0.91	0.84	0.75	0.63	0.50
	16	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.91	0.83	0.74	0.62
	17	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.90	0.82	0.73
	18	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.89	0.82
	19	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.88
	20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.96	0.93

Exercise 3 – Overt Attack Analysis: Determining the Most-Vulnerable Path Through an ASD and Evaluating Timely Detection, Probability of Interruption (P_I), and Critical Detection Point for That Single Outsider Path

In this exercise, we will evaluate system effectiveness against radiological sabotage at the PTR Reactor by a terrorist attack. This time we will incorporate some forceful attack against the PPS and/or Response Force.

For this analysis, use the data appropriate for the facility state and type of transport your subgroup is analyzing. The ASD in Figure 2 has data for all elements *except* the protection layer between offsite and the Limited Area, the Limited Area itself, and the protection layer between the Limited Area and the Protected Area.

- 1) Think of a way to use a vehicle bomb against the PTR facility. Use the blast circles to determine whether the blast would cause a result against the PPS that you, the adversary, would like to achieve: _____
- 2) Fill in the missing values on the ASD in Figure 2 for the Limited Area and two protection layers for the facility state and type of adversary transport your subgroup is analyzing, along with any modifications to cover the overt attack.
- 3) Look back at your calculations for the PPS Response Time. Would the PPS Response Time change? Record the appropriate PPS Response Time here:

- 4) Determine the most-vulnerable timely detection path through the ASD as modified in 2) for the PPS Response Time given in 3), starting backward from the end of the path. Record your progressing definition of the path in the Path Event Timeline Worksheet and Adversary Timeline Schematic included below.

What elements are timely? _____

Where is the Critical Detection Point on the Most-Vulnerable Path? _____

What is the P_I ? _____

Figure 2 – Delay and Detection Values for PTR Areas and Elements

O	PD		T(sec)		Offsite								
	Institute Wall		Portal P1		Portal P3		Portal P4		Admin Bldg Roof				
	PD 0.01		PD 0.1		PD 0.1		PD 0.1		PD 0.02				
	T(sec) 10		T(sec) 35		T(sec) 5		T(sec) 5		T(sec) 10				
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:				
A	PD	0	T(sec)	60	Institute Limited Area								
	Portal P5		Main Veh Portal		Emg. Veh Portal		Isolation Zone		Roof over P5				
	PD 0.15		PD 0.15		PD 0.15		PD		PD 0.52				
	T(sec) 63		T(sec) 83		T(sec) 53		T(sec)		T(sec) 0.87				
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:				
B	PD	0	T(sec)	9	PTR Protected Area								
	Portal P6		Window		20 cm Surface		Cooling Duct		S/R Veh Door		Emg. Door	30 cm surface	30 cm roof
	PD 0.45		PD 0		PD 0.95		PD 0.1		PD 0.76		PD 0.76	PD 0.95	PD 0.95
	T(sec) 20		T(sec) 0		T(sec) 180		T(sec) 174		T(sec) 30		T(sec) 12	T(sec) 195	T(sec) 195
	JUMP:		JUMP:		JUMP:		JUMP: To D		JUMP: To D		JUMP: To D	JUMP: To D	JUMP: To D
C	PD	0	T(sec)	2	PTR Reactor Building								
	Portal at D60		30 cm Surface										
	PD 0.6		PD 0.1										
	T(sec) 43		T(sec) 195										
	JUMP:		JUMP:										
D	PD	0	T(sec)	7	PTR Reactor Hall								
	C. Rm. Door		C.Rm. Windows		C.Rm. Walls								
	PD 0.02		PD 0.02		PD 0.02								
	T(sec) 12		T(sec) 6		T(sec) 180								
	JUMP:		JUMP:		JUMP:								
F	PD	0	T(sec)	2	Control Room Interior								
	Target Sab Task												
	PD 0.02												
	T(sec) 780												
	JUMP:												
G	PD		T(sec)										

Path Event Timeline Worksheet

Step	Path Element or Area	Defeat Strategy	P _D	Delay, T(sec)	T _{AF} (sec)	Equipment	Weight (kg)
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

Adversary Timeline Schematic

	Begin Mission												Complete Mission
Element/Area:													
P(Detection)													
T (Seconds)													
T _{AF} (Seconds)													
Task Time Remaining*													
Timely Detn?													

PPS Response Time

Seconds

*Adversary Task Time Remaining After First Sensing

- 5) We will now calculate an approximate P_N , based on the number of adversaries who can use weapons versus the number of responders who a) match the adversaries in terms of skills and b) actually *survive and* engage the adversaries.

What is the total number of adversaries who can engage the response forces (as opposed to work on target tasks, etc.)? _____

What is the total number of response forces who a) match the adversaries in terms of skills and b) actually engage the adversaries? _____

From the following table, what is an approximate P_N for this path? _____

		Number of Adversaries														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number of Response Forces	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	1	0.50	0.17	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.84	0.50	0.23	0.08	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	3	0.96	0.78	0.50	0.26	0.11	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	4	0.99	0.92	0.74	0.50	0.29	0.14	0.06	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	5	1.00	0.98	0.89	0.72	0.50	0.30	0.16	0.07	0.03	0.01	0.00	0.00	0.00	0.00	0.00
	6	1.00	0.99	0.96	0.86	0.70	0.50	0.32	0.18	0.09	0.04	0.02	0.01	0.00	0.00	0.00
	7	1.00	1.00	0.99	0.94	0.84	0.68	0.50	0.33	0.20	0.10	0.05	0.02	0.01	0.00	0.00
	8	1.00	1.00	1.00	0.98	0.93	0.82	0.67	0.50	0.34	0.21	0.12	0.06	0.03	0.01	0.01
	9	1.00	1.00	1.00	0.99	0.97	0.91	0.81	0.66	0.50	0.35	0.22	0.13	0.07	0.04	0.02
	10	1.00	1.00	1.00	1.00	0.99	0.96	0.90	0.79	0.65	0.50	0.35	0.23	0.14	0.08	0.04
	11	1.00	1.00	1.00	1.00	1.00	0.98	0.95	0.88	0.78	0.65	0.50	0.36	0.24	0.15	0.09
	12	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.94	0.87	0.77	0.64	0.50	0.37	0.25	0.16
	13	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.93	0.86	0.76	0.64	0.50	0.37	0.26
	14	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.96	0.92	0.85	0.75	0.63	0.50	0.38
	15	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.98	0.96	0.91	0.84	0.75	0.63	0.50
	16	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.91	0.83	0.74	0.62
	17	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.90	0.82	0.73
	18	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.89	0.82
	19	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.88
	20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.96	0.93

- 6) Calculate $P_E = P_I * P_N$ _____

Module 8

Path Analysis Subgroup

Solutions

Session Objectives

After this session, you will be able to:

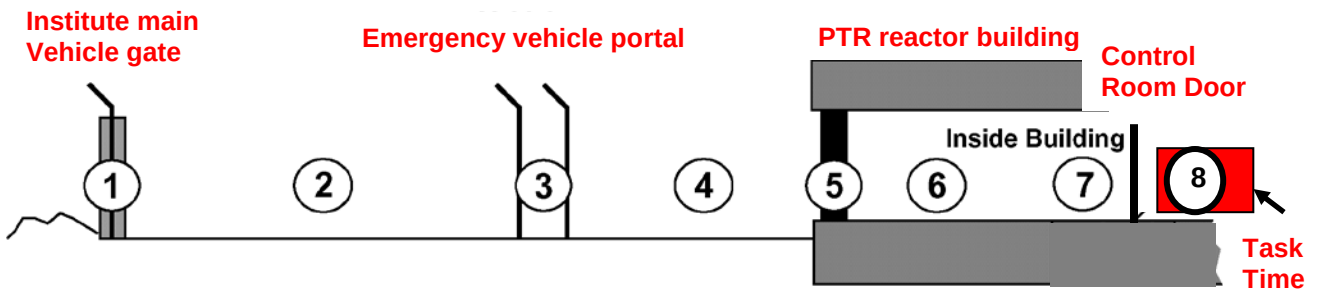
1. Determine CDP and Probability of Interruption for a single path to the PTR Reactor facility, based on a Timely Detection analysis.
2. Determine how to find a most-vulnerable path through an ASD based on a Timely Detection Analysis and determine P_I .
3. Determine how to alter the values in the ASD to perform an Overt Attack Analysis and determine an approximate P_N and P_E for this analysis.

Exercise 1 – Timely Detection Analysis: Determining Probability of Interruption and Critical Detection Point for a Single Outsider Path

An adversary force sized to match your Design Basis Threat (DBT) equipped with a truck, a 1.0-kg explosive charge, and a 25-kg set of special tools intend to sabotage the PTR reactor by attacking the Control Room vital equipment. The adversaries intend to:

1. Crash a truck through the outer main vehicle gate of the Institute.
2. Drive to the emergency vehicle portal at the PTR reactor.
3. Penetrate the emergency vehicle portal using a fast defeat strategy that you calculated detection and delay values for in the Characterizing Element Performance Subgroup.
4. Drive to the PTR reactor building shipping door.
5. Penetrate the shipping door with 1.0 kg of explosives.
6. Run to the reactor control-room door.
7. Break the glass in the door and open it.
8. Sabotage the vital equipment in the control room.

1) Use the Path Event Timeline Worksheet to record the information about attacking the emergency vehicle portal (defeat strategy, P_D , T , T_{AF} , equipment involved in that step, and weight of that equipment).



Barrier Number	Type	Specification
1	Main Gate	2.4-m x 4-m-wide padlocked, chain-link gate on metal pipe (construction and maintenance gate)
2	Distance	1-km road
3	Vehicle portal	Two active barriers, 2.4 m x 4 m wide, manually operated, chain-link gates on metal pipe (12 m apart)
4	Distance	125-m paved surface
5	Reactor shipping door	10-cm-thick wooden door with metal sheeting
6	Distance to control room door	60 m to door
7	Control room door	5-cm wooden door with glass windows
8	Task Time	Time to sabotage vital equipment in control room

Exercise 1 – Adversary Path Worksheet

Path Event Timeline Worksheet

Step	Path Element or Area	Defeat Strategy	P_D	Delay, T(sec)	T_{AF} (sec)	Equipment	Weight (kg)
1	Veh Entrance, P3	Crash truck	0.45	6	3	truck	1,500
2	Institute Area	Drive 1 km	0.2	36	18		
3	Emergency Vehicle Portal						
4	Protected Area	Drive 125 m	0	12	6		
5	PTR Building Shipping Door	Penetrate w. 1-kg explosive	0.95	114	20	explosive	1
6	Reactor Hall	Run 60 m	0	15	7.5		
7	Control-Room Door	Break glass	0.5	6	3		
8	Control Room	Sabotage task	0.9	780	780	tools	25

2) Fill out the Adversary Timeline Schematic below for this path:

- First, by entering the delays, T, and Time After Sensing, TAF;
- Determining the Adversary Task Time Remaining After First Sensing (Task Time Remaining) for all sensing opportunities;
- Determining which sensing opportunities are timely and finding the CDP; and
- Entering the Probability of Detection just for the timely detection locations.

Adversary Timeline Schematic

Begin Mission										
Element/Area:										
P(Detection)										
T (Seconds)										
T_{AF} (Seconds)										
Task Time Remaining*										
Timely Detn?										

PPS Response Time Seconds

*Adversary Task Time Remaining After First Sensing

3) What is the Probability of Interruption, P_I ? The P_I is found by multiplying the non-detection probabilities down to and including the CDP:

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

Exercise 2 – Timely Detection Analysis: Determining the Most-Vulnerable P_I Path Through an ASD and Evaluating Timely Detection, P_I , and Critical Detection Point for That Single Outsider Path

In this exercise, we will evaluate system effectiveness against radiological sabotage at the PTR reactor by a terrorist attack. For this analysis, use the data appropriate for the facility state and type of transport your subgroup is analyzing. The ASD in Figure 1 has data for all elements except the protection layer between offsite and the Limited Area, the Limited Area itself, and the protection layer between the Limited Area and the Protected Area.

- 1) Fill in the missing values for the ASD in Figure 1 for the Limited Area and two protection layers for the facility state and type of adversary transport your subgroup is analyzing.
- 2) Record the PPS Response Time here: _____
- 3) Determine the most-vulnerable timely detection path through the ASD for the PPS Response Time, starting from the end of the path. Record your progressing definition of the path in the Path Event Timeline Worksheet and Adversary Timeline Schematic included below.

What elements are timely? (explain verbally) _____

Where is the Critical Detection Point on the Most-Vulnerable Path? _____

What is the Probability of Interruption? _____

Figure 1 – Delay and Detection Values for PTR Areas and Elements Is this a printout from SAVI or something? It is really hard to read.

O	PD	T(sec)	Offsite					
	Institute Wall	Portal 'P1	Portal P3	Portal P4	Admin Bldg Roof			
	PD	PD	PD	PD	PD			
	T(sec)	T(sec)	T(sec)	T(sec)	T(sec)			
	JUMP:	JUMP:	JUMP:	JUMP:	JUMP:			
A	PD	T(sec)	Institute Limited Area					
	Portal P5	Main Veh Portal	Emg. Veh Portal	Isolation Zone	Roof over P5			
	PD	PD	PD	PD	PD			
	T(sec)	T(sec)	T(sec)	T(sec)	T(sec)			
	JUMP:	JUMP:	JUMP:	JUMP:	JUMP:			
B	PD	0	T(sec)	9	PTR Protected Area			
	Portal P6	Window	20 cm Surface	Cooling Duct	S/R Veh Door	Emg. Door	30 cm surface	30 cm roof
	PD	PD	PD	PD	PD	PD	PD	PD
	T(sec)	T(sec)	T(sec)	T(sec)	T(sec)	T(sec)	T(sec)	T(sec)
	JUMP:	JUMP:	JUMP:	JUMP:	JUMP:	JUMP:	JUMP:	JUMP:
C	PD	0	T(sec)	2	PTR Reactor Building			
	Portal at D60	30 cm Surface						
	PD	PD						
	T(sec)	T(sec)						
	JUMP:	JUMP:						
D	PD	0	T(sec)	7	PTR Reactor Hall			
	C. Rm. Door	C.Rm. Windows	C.Rm. Walls					
	PD	PD	PD					
	T(sec)	T(sec)	T(sec)					
	JUMP:	JUMP:	JUMP:					
F	PD	0	T(sec)	2	Control Room Interior			
	Target Sab Task							
	PD							
	T(sec)							
	JUMP:							
G	PD		T(sec)					

Path Event Timeline Worksheet

Step	Path Element or Area	Defeat Strategy	P _D	Delay, T(sec)	T _{AF} (sec)	Equipment	Weight (kg)
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

Adversary Timeline Schematic

	Begin Mission												Complete Mission
Element/Area:													
P(Detection)													
T (Seconds)													
T _{AF} (Seconds)													
Task Time Remaining*													
Timely Detn?													

PPS Response Time

Seconds

*Adversary Task Time Remaining After First Sensing

- 4) We will now calculate an approximate P_N , based on the number of adversaries who can use weapons versus the number of responders who a) match the adversaries in terms of skills and b) actually engage the adversaries.

What is the total number of adversaries who can engage the response forces (as opposed to work on target tasks, etc.)? _____

What is the total number of response forces who a) match the adversaries in terms of skills and b) actually engage the adversaries? _____

In the following table, what is an approximate P_N for this path? _____

		Number of Adversaries														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number of Response Forces	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	1	0.50	0.17	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.84	0.50	0.23	0.08	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	3	0.96	0.78	0.50	0.26	0.11	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	4	0.99	0.92	0.74	0.50	0.29	0.14	0.06	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	5	1.00	0.98	0.89	0.72	0.50	0.30	0.16	0.07	0.03	0.01	0.00	0.00	0.00	0.00	0.00
	6	1.00	0.99	0.96	0.86	0.70	0.50	0.32	0.18	0.09	0.04	0.02	0.01	0.00	0.00	0.00
	7	1.00	1.00	0.99	0.94	0.84	0.68	0.50	0.33	0.20	0.10	0.05	0.02	0.01	0.00	0.00
	8	1.00	1.00	1.00	0.98	0.93	0.82	0.67	0.50	0.34	0.21	0.12	0.06	0.03	0.01	0.01
	9	1.00	1.00	1.00	0.99	0.97	0.91	0.81	0.66	0.50	0.35	0.22	0.13	0.07	0.04	0.02
	10	1.00	1.00	1.00	1.00	0.99	0.96	0.90	0.79	0.65	0.50	0.35	0.23	0.14	0.08	0.04
	11	1.00	1.00	1.00	1.00	1.00	0.98	0.95	0.88	0.78	0.65	0.50	0.36	0.24	0.15	0.09
	12	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.94	0.87	0.77	0.64	0.50	0.37	0.25	0.16
	13	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.93	0.86	0.76	0.64	0.50	0.37	0.26
	14	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.96	0.92	0.85	0.75	0.63	0.50	0.38
	15	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.98	0.96	0.91	0.84	0.75	0.63	0.50
	16	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.91	0.83	0.74	0.62
	17	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.90	0.82	0.73
	18	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.89	0.82
	19	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.88
	20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.96	0.93

Exercise 3 – Overt Attack Analysis: Determining the Most-Vulnerable Path Through An ASD and Evaluating Timely Detection, Probability of Interruption, and Critical Detection Point for that Single Outsider Path

In this exercise, we will evaluate system effectiveness against radiological sabotage at the PTR reactor by a terrorist attack. This time we incorporate some forceful attack against the PPS and/or response force.

For this analysis, use the data appropriate for the facility state and type of transport your subgroup is analyzing. The ASD in Figure 2 has data for all elements *except* the protection layer between offsite and the Limited Area, the Limited Area itself, and the protection layer between the Limited Area and the Protected Area.

- 1) Think of a way to use a vehicle bomb against the PTR facility. Use the blast circles to determine whether the blast would cause a result against the PPS that you, the adversary, would like to achieve: _____

- 2) Fill in the missing values on the ASD in Figure 2 for the Limited Area and two protection layers for the facility state and type of adversary transport your subgroup is analyzing, along with any modifications to cover the overt attack.

- 3) Look back at your calculations for the PPS Response Time. Would the PPS Response Time change? Record the appropriate PPS Response Time here:

- 4) Determine the most-vulnerable timely detection path through the ASD as modified in 2) for the PPS Response Time given in 3), starting backwards from the end of the path. Record your progressing definition of the path in the Path Event Timeline Worksheet and Adversary Timeline Schematic included below.

What elements are timely? _____

Where is the Critical Detection Point on the Most-Vulnerable Path? _____

What is the Probability of Interruption? _____

Figure 2 – Delay and Detection Values for PTR Areas and Elements

O	PD		T(sec)		Offsite											
	Institute Wall		Portal 'P1		Portal P3		Portal P4		Admin Bldg Roof							
	PD		PD		PD		PD		PD							
	T(sec)		T(sec)		T(sec)		T(sec)		T(sec)							
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:							
A	PD		T(sec)		Institute Limited Area											
	Portal P5		Main Veh Portal		Emg. Veh Portal		Isolation Zone		Roof over P5							
	PD		PD		PD		PD		PD							
	T(sec)		T(sec)		T(sec)		T(sec)		T(sec)							
	JUMP:		JUMP:		JUMP:		JUMP:		JUMP:							
B	PD	0	T(sec)	9	PTR Protected Area											
	Portal P6		Window		20 cm Surface		Cooling Duct		S/R Veh Door		Emg. Door		30 cm surface		30 cm roof	
	PD	0.45	PD	0	PD	0.95	PD	0.1	PD	0.76	PD	0.76	PD	0.95	PD	0.95
	T(sec)	20	T(sec)	0	T(sec)	180	T(sec)	174	T(sec)	30	T(sec)	12	T(sec)	195	T(sec)	195
	JUMP:		JUMP:		JUMP:		JUMP:	To D	JUMP:	To D	JUMP:	To D	JUMP:	To D	JUMP:	To D
C	PD	0	T(sec)	2	PTR Reactor Building											
	Portal at D60		30 cm Surface													
	PD	0.6	PD	0.1												
	T(sec)	43	T(sec)	195												
	JUMP:		JUMP:													
D	PD	0	T(sec)	7	PTR Reactor Hall											
	C. Rm. Door		C.Rm. Windows		C.Rm. Walls											
	PD	0.02	PD	0.02	PD	0.02										
	T(sec)	12	T(sec)	6	T(sec)	180										
	JUMP:		JUMP:		JUMP:											
F	PD	0	T(sec)	2	Control Room Interior											
	Target Sab Task															
	PD	0.02														
	T(sec)	780														
	JUMP:															
G	PD		T(sec)													

Path Event Timeline Worksheet

Step	Path Element or Area	Defeat Strategy	P _D	Delay, T(sec)	T _{AF} (sec)	Equipment	Weight (kg)
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

Adversary Timeline Schematic

	Begin Mission												Complete Mission
Element/Area:													
P(Detection)													
T (Seconds)													
T _{AF} (Seconds)													
Task Time Remaining*													
Timely Detn?													

PPS Response Time

Seconds

*Adversary Task Time Remaining After First Sensing

- 5) We will now calculate an approximate P_N , based on the number of adversaries who can use weapons versus the number of responders who a) match the adversaries in terms of skills and b) actually *survive and* engage the adversaries.

What is the total number of adversaries who can engage the response forces (as opposed to work on target tasks, etc.)? _____

What is the total number of response forces who a) match the adversaries in terms of skills and b) actually engage the adversaries? _____

Looking up in the following table, what is an approximate P_N for this path? _____

		Number of Adversaries														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number of Response Forces	0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	1	0.50	0.17	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	2	0.84	0.50	0.23	0.08	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	3	0.96	0.78	0.50	0.26	0.11	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	4	0.99	0.92	0.74	0.50	0.29	0.14	0.06	0.02	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	5	1.00	0.98	0.89	0.72	0.50	0.30	0.16	0.07	0.03	0.01	0.00	0.00	0.00	0.00	0.00
	6	1.00	0.99	0.96	0.86	0.70	0.50	0.32	0.18	0.09	0.04	0.02	0.01	0.00	0.00	0.00
	7	1.00	1.00	0.99	0.94	0.84	0.68	0.50	0.33	0.20	0.10	0.05	0.02	0.01	0.00	0.00
	8	1.00	1.00	1.00	0.98	0.93	0.82	0.67	0.50	0.34	0.21	0.12	0.06	0.03	0.01	0.01
	9	1.00	1.00	1.00	0.99	0.97	0.91	0.81	0.66	0.50	0.35	0.22	0.13	0.07	0.04	0.02
	10	1.00	1.00	1.00	1.00	0.99	0.96	0.90	0.79	0.65	0.50	0.35	0.23	0.14	0.08	0.04
	11	1.00	1.00	1.00	1.00	1.00	0.98	0.95	0.88	0.78	0.65	0.50	0.36	0.24	0.15	0.09
	12	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.94	0.87	0.77	0.64	0.50	0.37	0.25	0.16
	13	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.93	0.86	0.76	0.64	0.50	0.37	0.26
	14	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.96	0.92	0.85	0.75	0.63	0.50	0.38
	15	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.98	0.96	0.91	0.84	0.75	0.63	0.50
	16	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.91	0.83	0.74	0.62
	17	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.95	0.90	0.82	0.73
	18	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.89	0.82
	19	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.97	0.94	0.88
	20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.96	0.93

- 6) Calculate $P_E = P_I * P_N$ _____



Scenario Analysis

Module 11

Vulnerability Analysis of Physical Protection Systems

Date:

Student Learning Objectives

After completing this module, you should be able to:

- Describe the purpose of *scenario analysis* in the context of evaluating PPS performance
- Discuss the four phases of the Scenario Analysis Process
- Create adversary attack scenarios
- Describe a process for selecting final attack scenarios



What Is Scenario Analysis?

Scenario analysis—A methodology for analyzing system effectiveness, P_E , by considering several alternative possible adversary attacks (scenarios).

- Allows more detailed analysis of the attack, the defense, and the results than path analysis
- Focus is on identifying gaps in planning and vulnerabilities



Purposes of Scenario Analysis

- Provide a basis for level of confidence about PPS performance
- Create robust security plans to match and use fully the capabilities of the PPS design
- How?
 - Develop details of realistic adversary attack plan
 - Specific, coordinated tasks and timeline for all attackers
 - Develop detailed characterization of how PPS and the response force should behave, based on performance testing and site plans
 - Simulate how PPS and the response force behave during attempted adversary attack scenario

IMPORTANT:

- *Overall physical protection system effectiveness is represented by effectiveness against a few specific scenarios*
- *No attempt to determine worst-case scenario*

Scenario Analysis Supports Development and Validation of Contingency Plans

- INFCIRC/225/Revision 5 (Planning and preparedness for and response to nuclear security events)*
- “Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned. (Fundamental Principle K: Contingency Plans).”
 - “3.58 – The State should establish a contingency plan. The State’s competent authority should ensure that the operator prepares contingency plans to effectively counter the threat assessment or design basis threat taking actions of the response forces into consideration.”

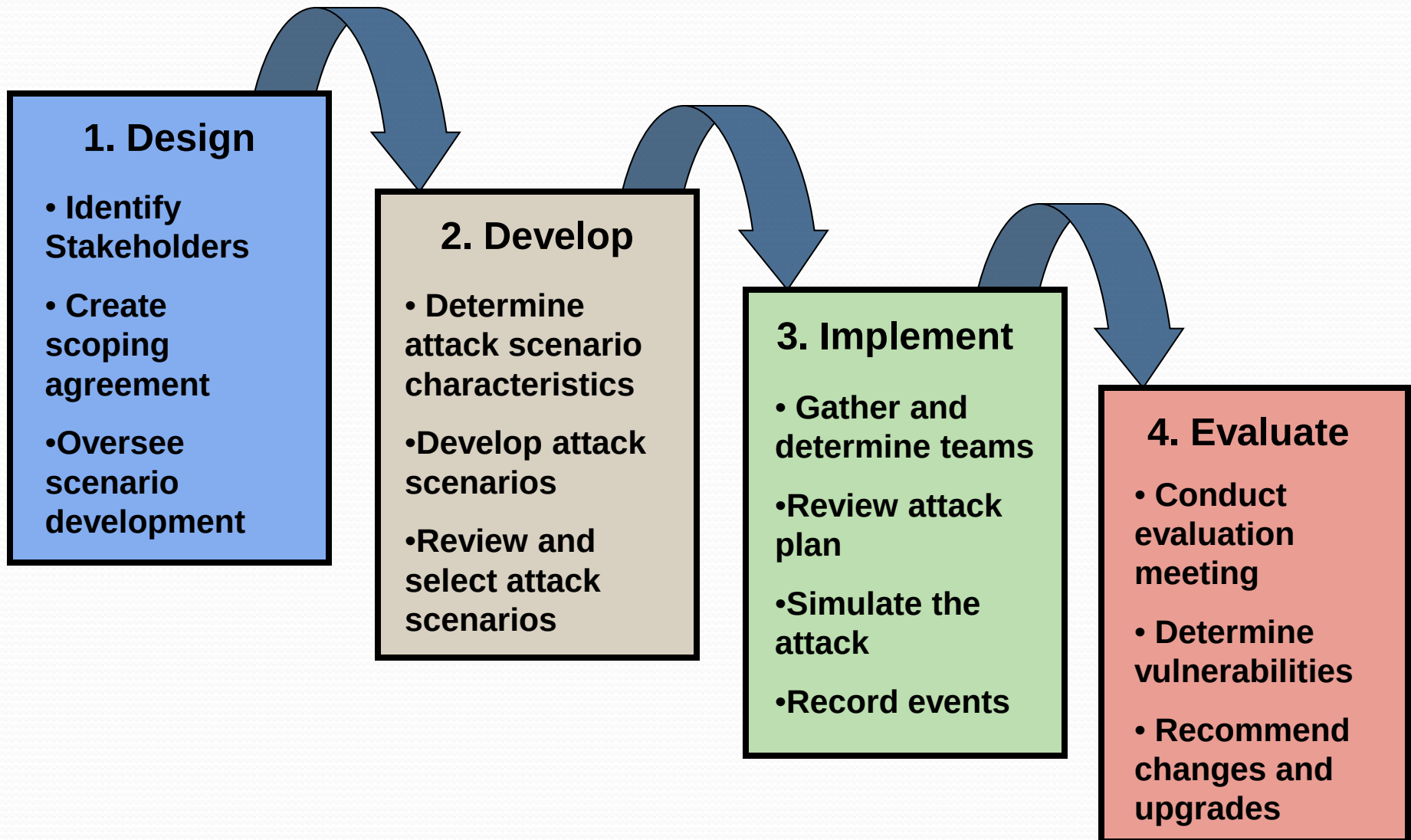
* Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No.13 The IAEA, January 2011.



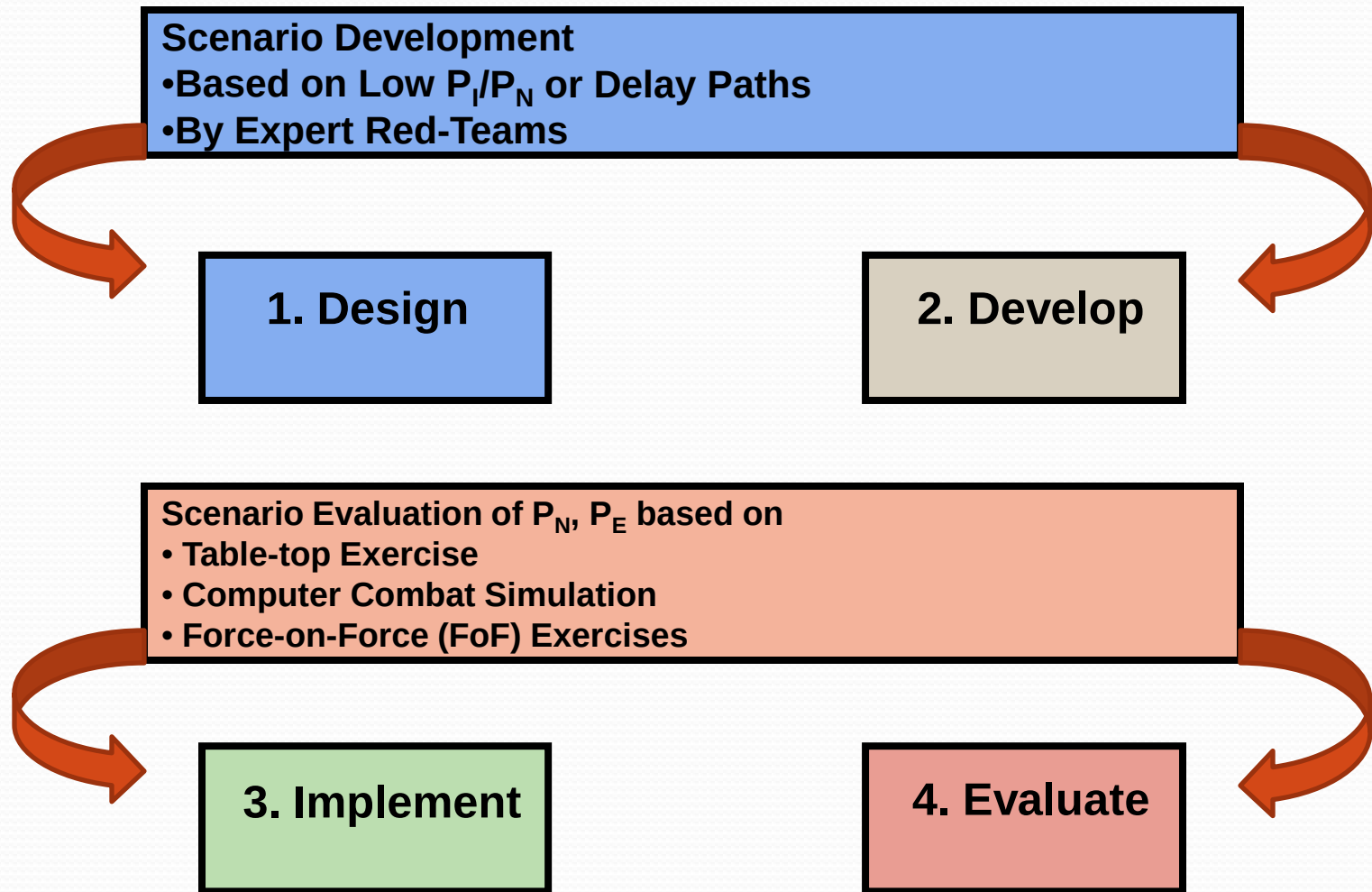
Scope of Scenario Analysis

- Identify key questions
 - How effective is the current PPS?
 - How effective is the existing response force strategy?
- Identify major considerations- sort by controllable/uncontrollable
 - Numbers and capabilities of adversary increase
 - Adversary tactics change to reflect current threat
 - State of the existing PPS
 - State of the existing guard/response force

Scenario Analysis Process



Scenario Analysis Process



1. Design

Identify Stakeholders

- Identify people who are responsible for the design, implementation, evaluation, and risk acceptance of the PPS
 - Competent Authority
 - Response Force Management
 - Vulnerability Analysis Team
 - Adversary Planning Subject Matter Experts (SME)
 - Security Management
 - Facility Operations
 - Other necessary people...

1. Design

Scoping Agreement

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

- Define requirements
- Design Basis Threat (DBT) Statement
- Facility Characterization
- Target ID (type of targets)
- Identify credible SMEs for attack planning
- Types of attacks and numbers of scenarios (sabotage/theft)
- Identify and agree on assumptions
- Determine type of Insider (passive/active, etc.)
- Memorandum of Understanding with government
- Review security posture
- Determine Picture-in-Time
- Agree on simulation tools and the process for using them

1. Design

Oversee Scenario Development

- Stakeholder(s) familiar with the design and evaluation of the PPS should be included in scenario development
- All Participants should:
 - Agree to confidentiality of all site/adversary information
 - Remain unbiased to site or adversaries
 - Ensure the adversary scenarios are within the parameters of the scoping agreement
 - Ensure accuracy of the PPS and target information
 - Thickness of vault walls
 - Assessment capability
 - Response capability

2. Develop

Scenario Characteristics

Scenario: A time-ordered, detailed description of an adversary attack used in analyzing physical protection system effectiveness (P_E)

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

Scenario Characteristics (Cont'd)

- Two classes of adversary scenarios
 - **Direct:** Adversary follows a direct path to target
 - **Adversary goal:** Minimize Probability of Interruption by defeating system detection or delay elements
 - **Indirect:** Adversary attacks PPS infrastructure before attacking target
 - **Adversary goal:** Minimize Probability of Interruption or Probability of Neutralization in order to:
 - Increase response time
 - Decrease response numbers
 - Disable critical systems

Structured Approach to Create Scenarios

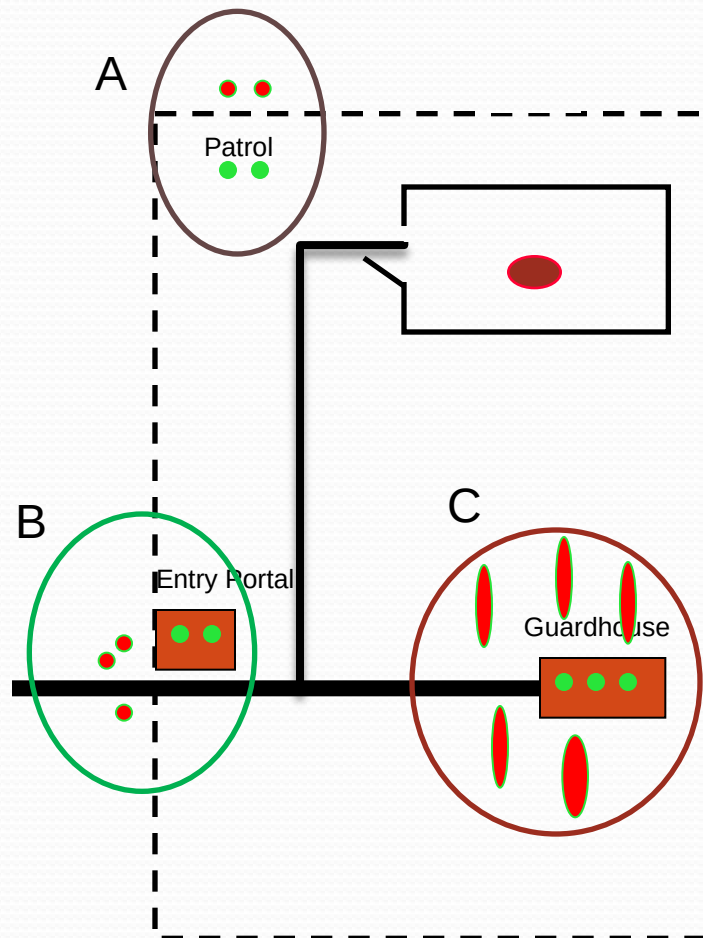
- **Create a range of scenarios**
 - Identify site vulnerabilities
 - Exploit the site identified vulnerabilities – build scenarios
 - Review and select final scenarios based on criteria

Identify Site Vulnerabilities

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

2. Develop

Example: Identify Site Vulnerabilities



Vulnerability: At times the guard force is divided

- Scenario conditions:
 - 2 guards on patrol
 - 2 guards at entry portal
 - 3 guards at guard house

Results from Path Analysis

Adversaries = 5 (DBT)

Guard Force = 7

Expected Results from vulnerability-based scenario

Task Plan A:

2 Adversaries vs. 2 Guards

Surprise advantage to adversaries

Task Plan B:

3 Adversaries vs. 2 Guards

Surprise advantage to adversaries

In coordination with Task Plan A (increased level of difficulty)

Task Plan C:

4 Adversaries vs. 3 Guards

Exploit Identified Site Vulnerabilities

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

Exploit Identified Site Vulnerabilities (Cont'd)

- Example
 - Vulnerability: At times the response force is divided
 - List of tasks to exploit vulnerability
 - A. Ambush guards on patrol concurrently with task plan B
 - B. Ambush guard post concurrently with task plan A
 - C. Attack remaining response force
 - D. Enter material storage building and remove material
 - E. Escape to safe house

2. Develop

Task Plan A

Start Time	Activity	End Time
00:00	A1 and A2 surreptitiously generates fence alarm and lie in wait for ambush	00:50
00:50	A1 and A2 engage P1 and P2	00:55
00:55	A1 and A2 climb over fence	01:00
01:00	A1 and A2 link up with A3, A4, and A5	02:00

2. Develop

Task Plan B

Start Time	Activity	End Time
00:00	A3, A4, and A5 drive vehicle up to the gate	00:40
00:40	A3 waits until P3 and P4 arrive at vehicle	00:50
00:50	A3 engages P3 while A4 and A5 exit vehicle	00:55
00:55	A4 and A5 engage P4	01:00
01:00	A4 and A5 breach gate	01:30
01:30	A3 drives vehicle through gate and picks up A4 and A5	01:45
01:45	A3, A4, and A5 standby for A1 and A2 to enter in vehicle	02:00

2. Develop

Task Plan C

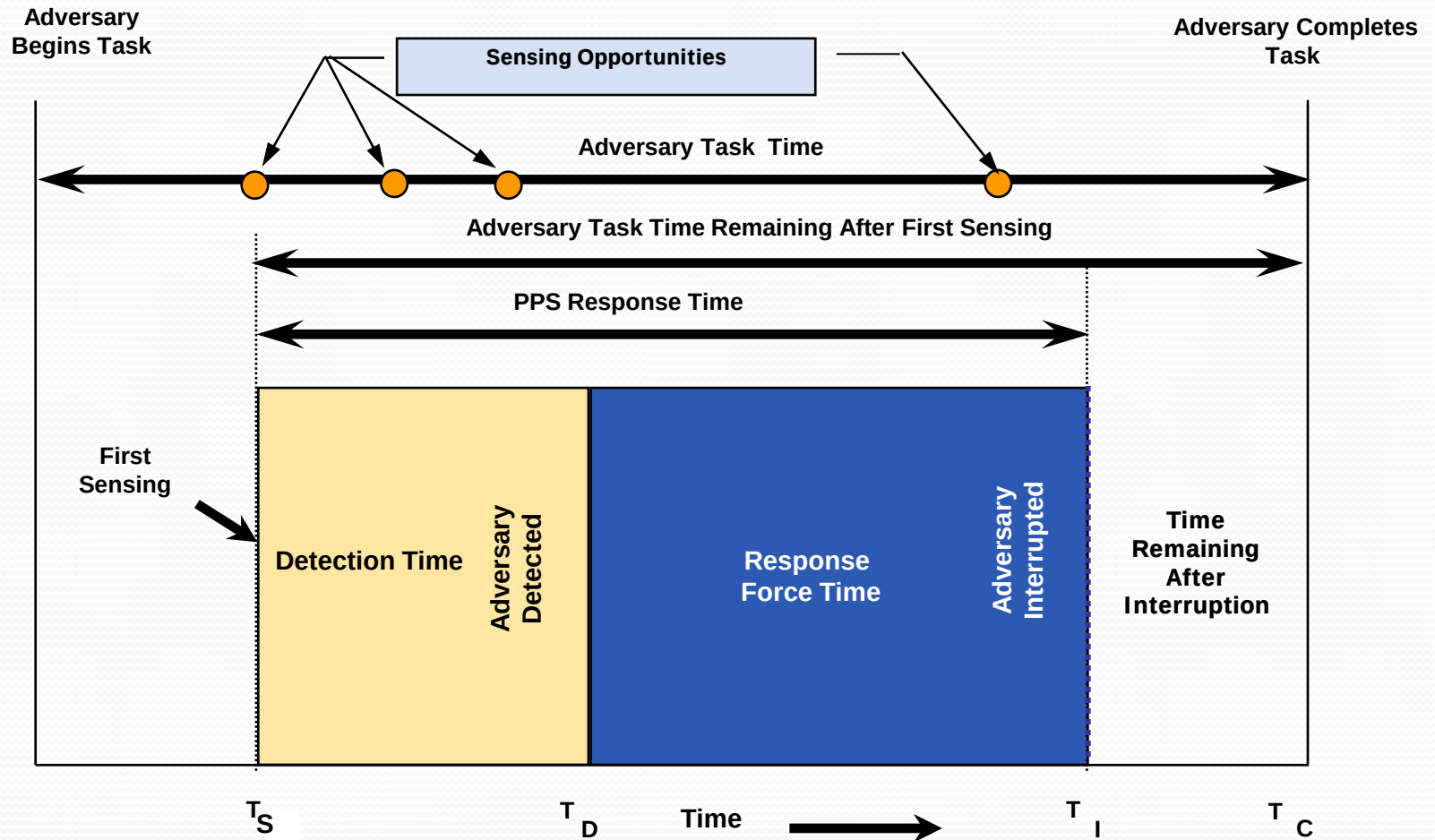
Start Time	Activity	End Time
02:00	A3 drives to guardhouse and A1, A2 A4, and A5 exit vehicle	03:00
03:00	A1, A2, A4, and A5 surround guardhouse and wait for guards to exit	03:30
03:30	Adversary team engages guards in guardhouse	04:00

Exploit Identified Site Vulnerabilities (Cont'd)

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

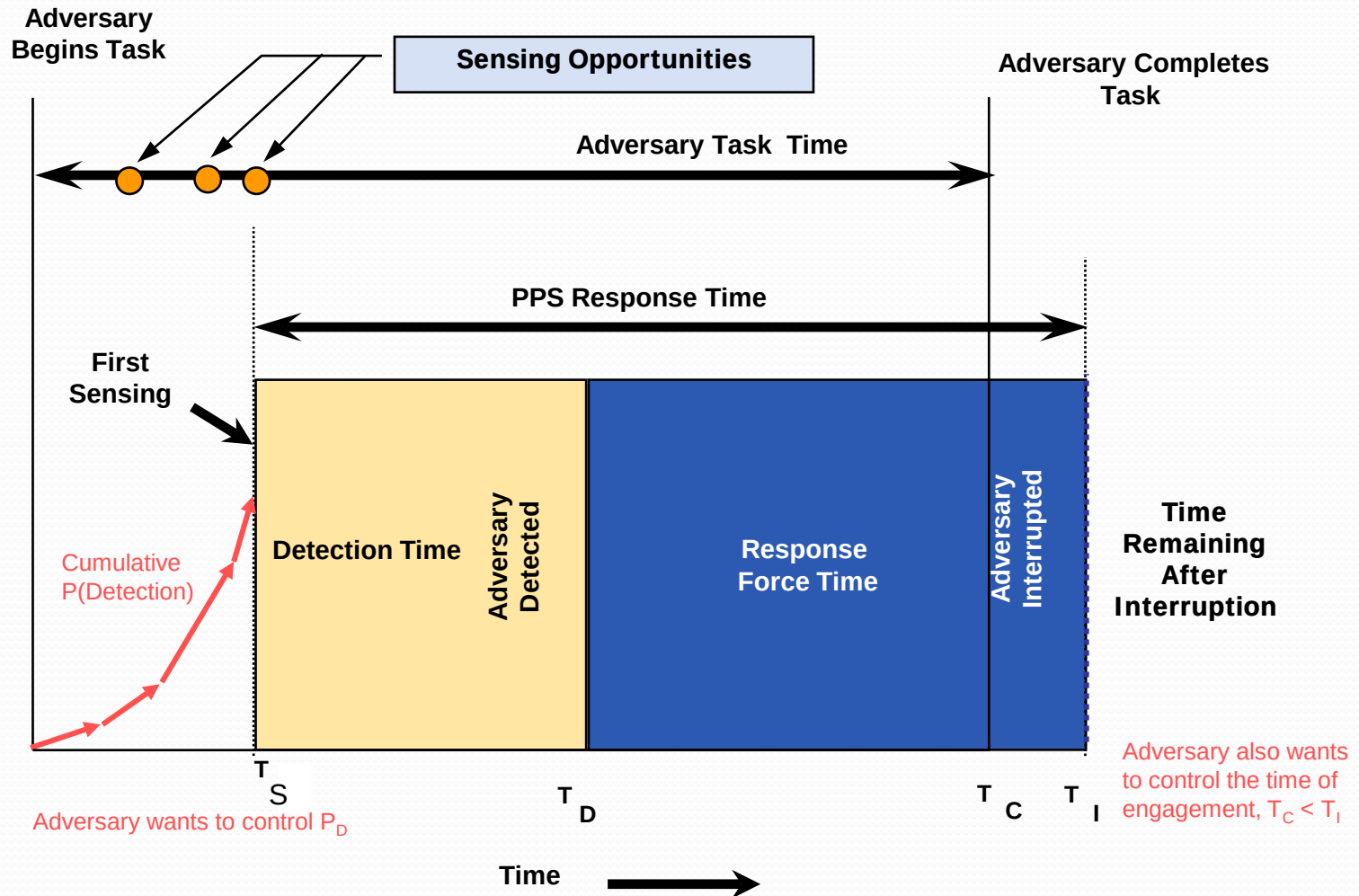
2. Develop

Adversary and PPS Timelines



2. Develop

Adversary's Perspective for Main *and* Supporting Teams



Scenario Development Planning and Complexity Factors

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

Review and Select Final Scenarios

(1 of 4)

- Include stakeholder in the review and selection process
- Review and select final scenarios based on scoping agreement criteria
- Are all analysis objectives covered?
 - Are conditions and states covered adequately?
 - Have we addressed several means of adversary approach (on foot, in land vehicles, on water, or by air) that apply, based on the Design-Basis Threat (DBT)?
- Are scenarios credible, limited by threats within the DBT, etc.?

Review and Select Final Scenarios

(2 of 4)

- Consider scenarios from Path Analysis
 - Start with minimum delay, minimum P_I , or minimum $P_I * P_N$ paths
 - Add scenario details to these paths
 - Add supporting team plans to assist these attackers
 - IMPORTANT: The most-vulnerable P_I path from Path Analysis may be a poor basis for a scenario

Review and Select Final Scenarios

(3 of 4)

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

Review and Select Final Scenarios

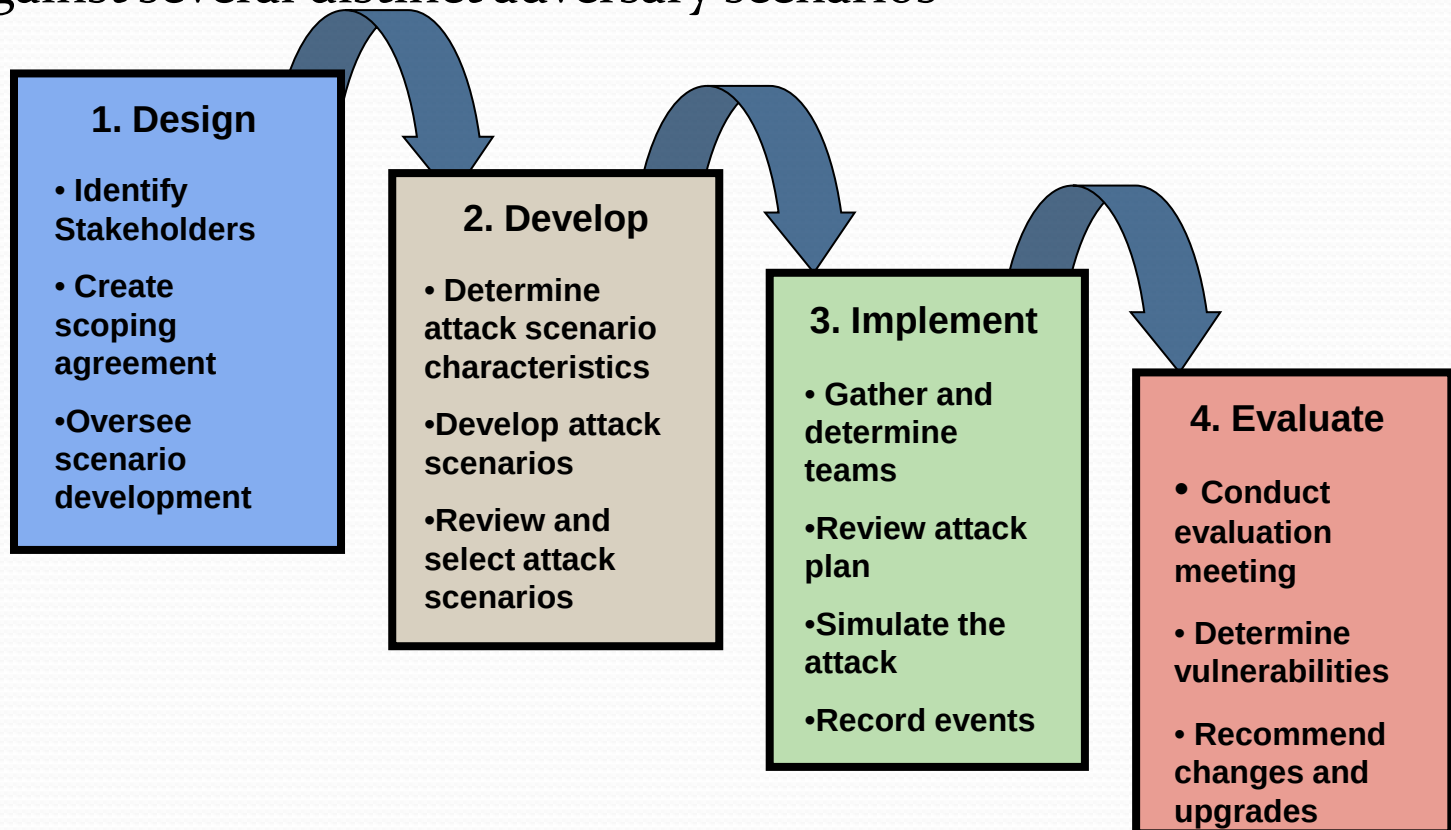
(4 of 4)

- Why do adversary attacks fail?
 - Early detection (adversaries detected earlier than expect)
 - Detection by intelligence organizations directly or by populace
 - Lead-up to the attack
 - Non-combat failures (typically due to failure to plan and stock for contingencies)
 - Logistic failures (inability to get weapons, etc.)
 - Breakdowns of vehicles, communications equipment
 - Exhaustion of team-members during the attack
 - Tool/explosive failure to breach
 - Timing and synchronization failures
 - Wrong plan due to bad information
 - Inadequate training and rehearsal

Even if adversary is not detected early *AND* there are no non-combat failures *AND* there is adequate training and rehearsal, the response force can win!

Summary

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



11. Scenario Development Subgroup

Session Objectives

After the session, you will be able to:

1. Recognize the steps needed to perform a scenario analysis.
2. Recognize how to create scenarios.

Exercise 1 – Develop an Attack Plan

Step 1: Collect and review the following documents:

- o Adversary Sequence Diagram (ASD) that you developed.
- o Design Basis Threat (DBT) that you were provided.
- o Exercise Data Book that you were provided.

Step 2: Review your ASD and determine the most-vulnerable pathway.

Step 3: Create a Picture-in-Time for your tabletop exercise, this should include:

- Time of day
- Procedures in place at that time of day
- Number and location of response force
- Other necessary information

Step 4: Write an attack plan using the information you have gathered and the following guidelines:

- o The adversary objective is sabotage the nuclear reactor to prevent shutdown and to drain the reactor pool.
- o All actions necessary to prevent shutdown and drain the reactor pool can be accomplished either in the reactor hall or from the control room.
- o The control room is considered to be the most viable vital area of the two due to the shorter task time.
- o Within the determined pathway (from Step 2), construct a scenario starting from offsite to the target; document this on the poster in the timeline and adversary task columns.



Tabletop Analysis

Module 12

Vulnerability Analysis of Physical Protection Systems

Date:

Student Learning Objectives

After completing this module, you should be able to:

- Describe a tabletop exercise
- Describe a critical event and engagement
- Describe how to document and track the critical events and engagements properly
- Recognize how to determine results of critical events and engagements



What is a Tabletop Exercise?

Tabletop exercise: A method to simulate an adversary attack on a site's existing or proposed physical protection system (PPS)

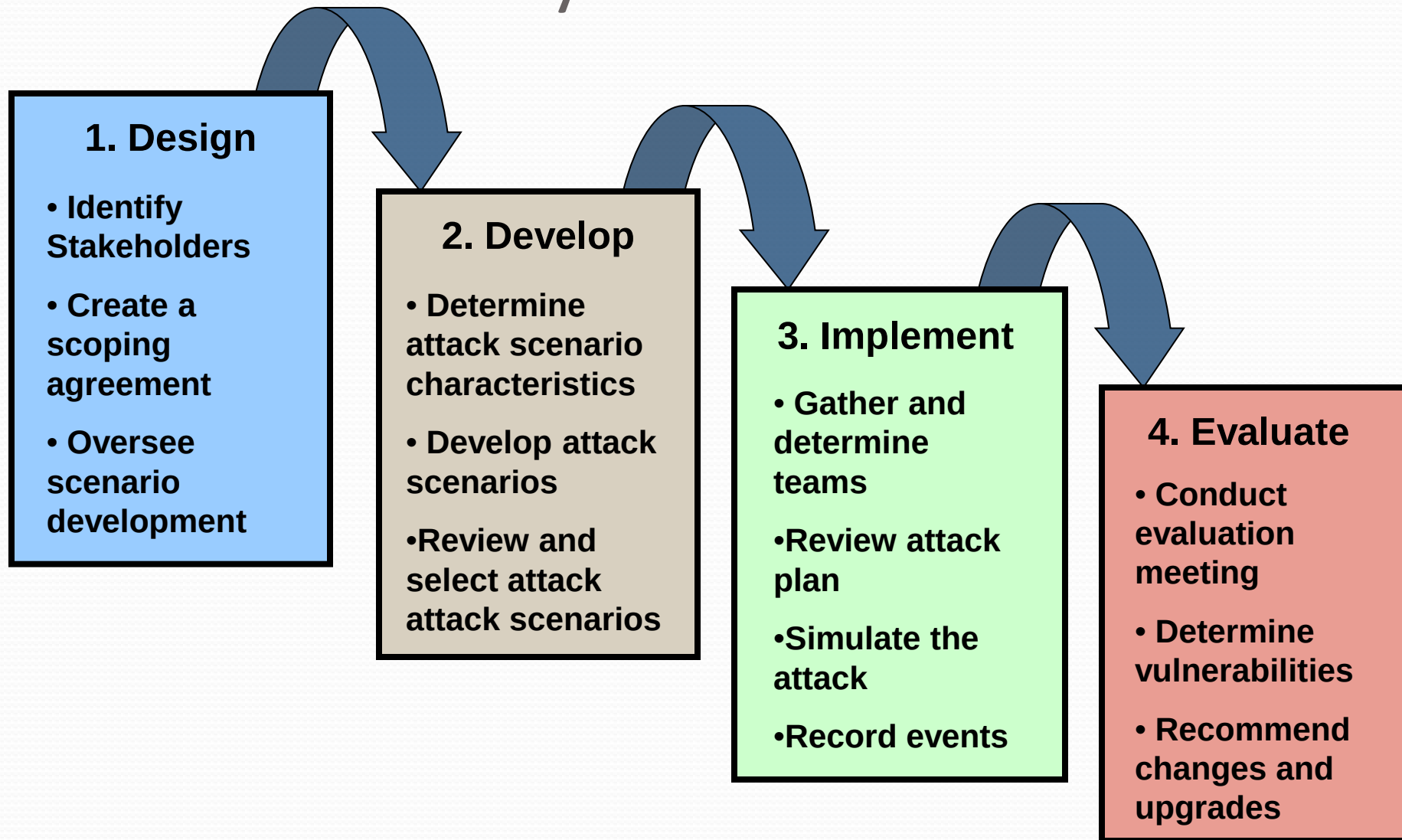
- Analyzes PPS elements:
 - Detection
 - Delay
 - Response
- Provides insight into a PPS that can stand alone or be used in other analysis tools
- Results can be used to make decisions regarding whether a PPS is deemed adequate
- Helps determine the most appropriate PPS upgrades



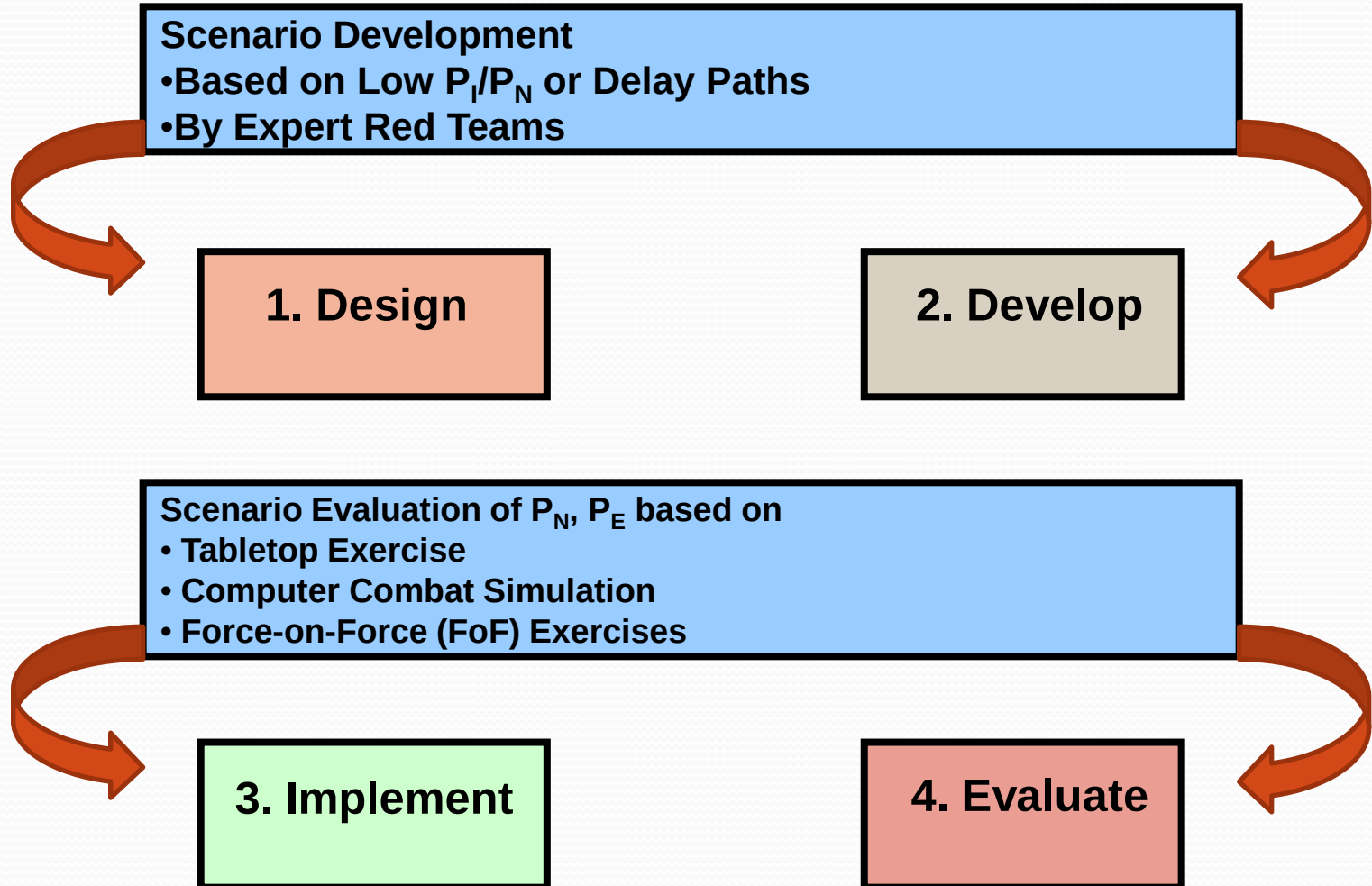
When to Conduct a Tabletop Exercise

- To evaluate:
 - Current and proposed PPSs
 - Current and changing (postulated) threats
 - Current and changes to targets
- As a training tool:
 - Identifies inconsistencies in response and site procedures
 - Maintains response force proficiency

Scenario Analysis Process



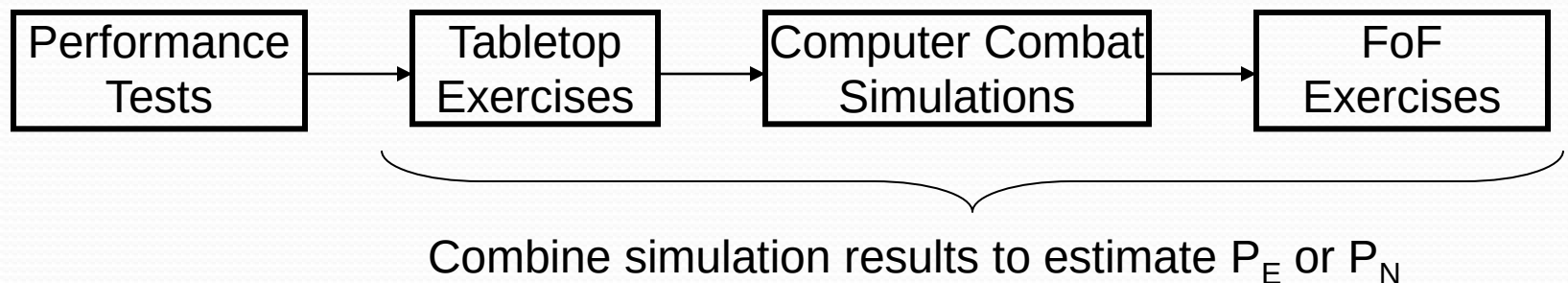
Scenario Analysis Process



3. Implement

Performing Simulations to Determine System Effectiveness Against Scenarios

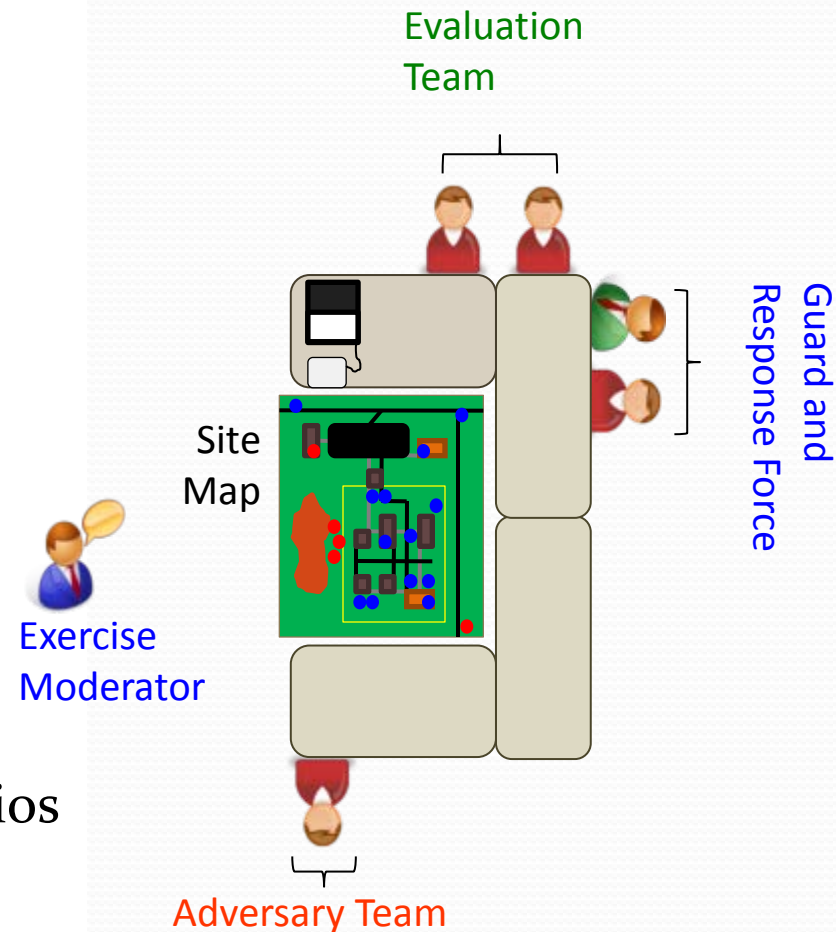
- Tabletop exercises will serve as the simulation technique taught in this course to determine P_E (qualitatively)
- When there is a choice of simulations, the best sequence of use is shown below
 - Performance tests provide necessary input to tabletop exercises
 - Tabletop exercises can often foresee the analysis and logistic issues that will arise in computer simulations and FoF exercises
 - In some cases, issues are identified in tabletops that have to be addressed before other simulations can be performed



3. Implement

Organize Tabletop

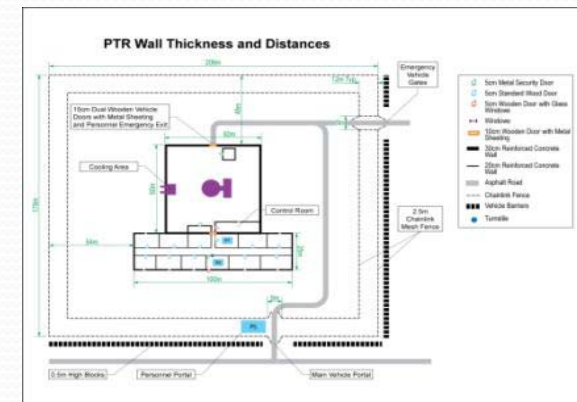
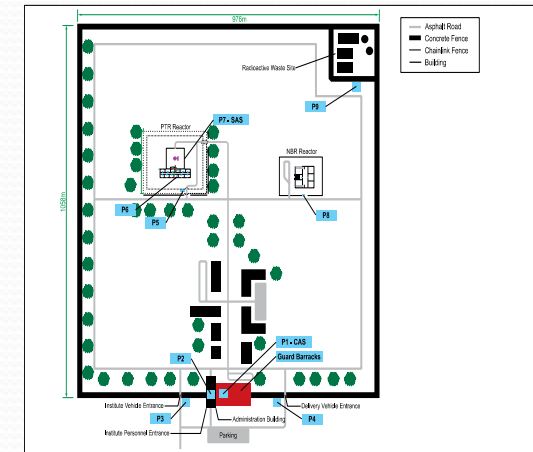
- Gather all necessary participants
- Determine teams
 - Guard and Response Force Team
 - Adversary Team
 - Evaluation Team
 - Exercise Moderator
- Review necessary information including:
 - Facility and PPS
 - Picture-in-time
 - Types of attacks, number of scenarios
 - Attack plan steps and timeline
 - Adversary Team briefs the attack plan to the stakeholders



3. Implement

Security Force Picture-in-Time

- Need to create a Picture-in-Time(s)
- Picture-in-Time provides the stakeholders with:
 - Security emergency response plan
 - Post and patrol
 - Locations
 - Activities
 - Equipment status
 - Numbers
- How to collect Picture-in-Time



Tabletop Preparation

- Review the type of equipment, vehicles, weapons, and tactics that the adversary and the response force will use
- Using the Picture-in-Time, lay out the response force positions on a map in a typical configuration
- Gather required documentation.
 1. DBT
 2. Adversary attack plans
 3. Security Emergency Response Plan
- Have resources readily available for the evaluation team to clarify adversary or response force assumptions made during the exercise

Implement Tabletop

Critical Event: Any event that requires attention and resources to overcome (detection, delay, engagement)

Engagement: An interaction that occurs between the guard and/or response force and the adversary along the adversary attack path

- Simulate the attack against PPS
 - Identify each critical event using Picture-in-Time
 - Determine outcome of each critical event
 - **Document** engagements, vulnerabilities, outcomes, performance test issues, etc.

3. Implement

Simulate the Attack

- Timeline should begin before the initial point of detection or engagement
- Work through the timeline until the first point where detection or engagement may occur
 - The Adversary timeline and Response Force Picture-in-Time are overlaid and any critical event or engagement are played through
 - Determine chance-based outcomes with random number generator (dice, pull number out of hat, group discussion, or exercise moderator decision)
- Assess and record engagements and critical events (who, what, when, where)
- Adjust the timeline and participant status and move forward to the next event in time
 - Update the clock every 10 seconds
 - Update the players on both sides to the time of the clock
 - Perform previously scheduled natural events (bomb detonation, detection, etc.)
- Continue simulation evaluating critical events until the win point

Analyzing Engagements

- Analyze each potential engagement to determine the following:
 - Verify:
 - Engagement feasibility
 - Line of sight between shooter and target
 - Within range of weapon system
 - Identify characteristics of the persons involved
 - Standing still, walking, running, prone, kneeling, in vehicle
 - Type of weapon and round, number of rounds, mounted, bipod, supported
 - Identify characteristics of target
 - In/out of vehicle, level of armor on vehicle, speed of vehicle
 - Body armor/level, behind cover, in prepared fighting position
 - Prone, kneeling, standing, walking, running, low crawling
 - Determine probability of casualty (P_{cas}) calculations and declare the results of the engagement

3. Implement

Hypothetical Probability of Casualty

- Probability of Casualty, P_{cas}
 - When a critical event occurs, use the following chart to determine if the shot causes a casualty

Distance	Probability of Casualty (Rifle)
25 to 0 meters	100%
50 to 25.1 meters	80%
100 to 50.1 meters	50%
Greater than 100 meters	0%

Distance	Probability of Casualty (Handgun)
5 to 0 meters	100%
15 to 5.1 meters	80%
25 to 15.1 meters	50%
50 to 25.1 meters	20%
Greater than 50 meters	0%

3. Implement

Random Number Generator

Probability	Outcome
0.05	Event Occurred

Instructions

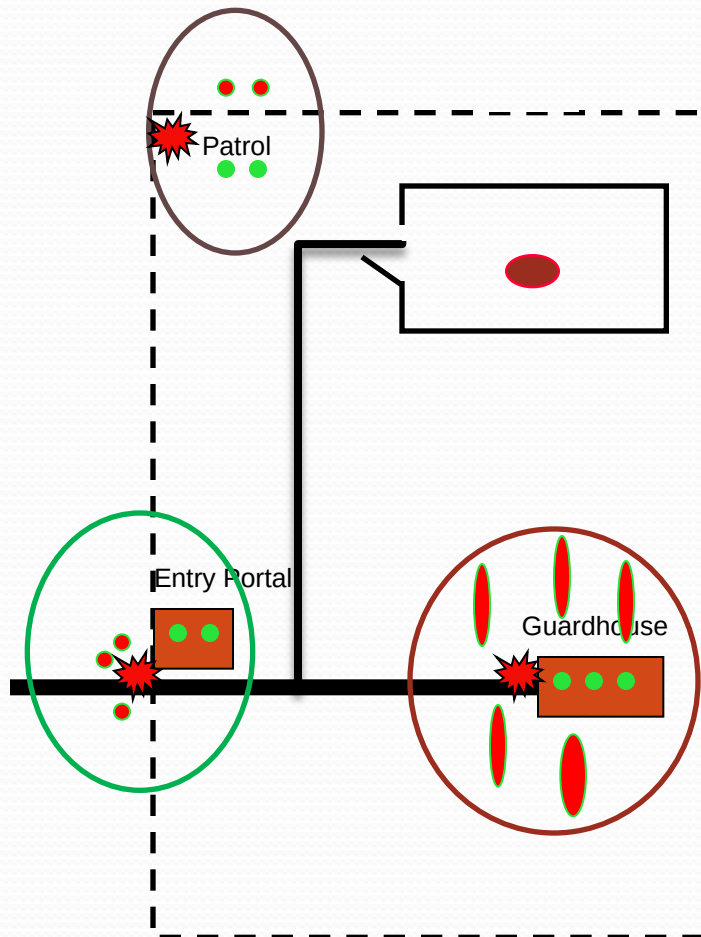
This functions requires entry of a probability (even the same one!) to achieve a new random number

Thus, if a guard had to shoot 3 times to kill an adversary, with a Probability of Hit and Kill of .35, you would enter .35 three times:

0.35	Event Did NOT Occur
0.35	Event Did NOT Occur
0.35	Event Occurred

3. Implement

Example: Identify Site Vulnerabilities



Vulnerability: At times the guard force is divided

- Scenario conditions:

- 2 guards on patrol
- 2 guards at entry portal
- 3 guards at guard house

Results from Path Analysis

Adversaries = 5 (DBT)

Guard Force = 7

Expected Results from vulnerability based scenario

Task Plan A:

2 Adversaries vs. 2 Guards

Surprise advantage to adversaries

Task Plan B:

3 Adversaries vs. 2 Guards

Surprise advantage to adversaries

In coordination with Task Plan A (increased level of difficulty)

Task Plan C:

4 Adversaries vs. 3 Guards

Task Plan A Engagement

Start Time	Adversary Activity	End Time	Start Time	Response Activity	End Time
00:00	A1 and A2 surreptitiously generate fence alarm and lie wait for ambush	00:50	00:10	Alarm is annunciated to CAS	00:15
			00:15	P1 and P2 receive dispatch from CAS, don equipment, and travel to alarm location	00:45
			00:45	P1 and P2 arrive on scene, dismount vehicle, and move on foot to alarm location	00:50
00:50	A1 engage P1 and A2 engage P2	00:53	00:50	P1 and P2 outcome?	00:53
00:55	A1 and A2 climb over fence	01:00			
01:00	A1 and A2 link up with A3, A4, and A5	02:00			

Task Plan B Engagement

Start Time	Adversary Activity	End Time	Start Time	Response Activity	End Time
00:00	A3, A4, and A5 drive vehicle up to the gate	00:40			
00:40	A3 waits until P3 and P4 arrive at vehicle	00:50	00:40	P3 and P4 exit gate house to speak to driver	00:50
00:50	A3 engages P3 while A4 and A5 exit vehicle	00:55	00:50	P3 outcome?	00:55
00:55	A4 and A5 engage P4	01:00	00:55	P4 outcome?	01:00
01:00	A4 and A5 breach gate	01:30			
01:30	A3 drives vehicle through gate and picks up A4 and A5	01:45			
01:45	A3, A4, and A5 standby for A1 and A2 enter in vehicle	02:00			

Task Plan C Engagement

Start Time	Adversary Activity	End Time	Start Time	Response Activity	End Time
02:00	A3 drives to guardhouse and A1, A2 A4, and A5 exit	03:00			
03:00	A1, A2, A4, A5 surround guardhouse and wait for guards to exit	03:30	00:40		
03:30	Adversary team engages guards in guardhouse	04:00	03:30	Guards outcome?	04:00

3. Implement

Results of Engagement(s)

Log results of each engagement

Engagement Start Time End Time		Shooter Status	Target Status	Weapon Type	Range (Meters)	Rate of Fire (Sec)	Results Miss/Neutralized
Task Plan A: A1 and A2 engagement between P1 and P2							
00:50	00:53	A1	P1	Rifle	30	3	P1 ?
00:50	00:56	A2	P2	Rifle	30	3	P2 ?
Task Plan B: A3, A4 and A5 engagement between P3 and P4							
00:50	00:55	A3	P3	Rifle	30	3	P3 ?
00:55	01:00	A4 /A5	P4	Rifle	30	3	P4 ?
Task Plan C: A1, A2, A3, A4, and A5 engagement between Guardhouse Guards (P5,P6,P7)							
00:55	00:60	A1/A2/A3/ A4/A5		Rifle	30	3	P5/P6/P7 ?

4. Evaluate

Evaluation Meeting

- Evaluation meetings are held with appropriate stakeholders and participants after the exercise is completed.
- Evaluation criteria:
 - Win or loss
 - Response force casualties
 - Access to target
 - Duration of engagement
 - Compensatory measures
 - Performance testing concerns
 - Response discrepancies
 - Vulnerabilities, where exploited

Note: Use the evaluation criteria to determine consistency with results from different analysis tools

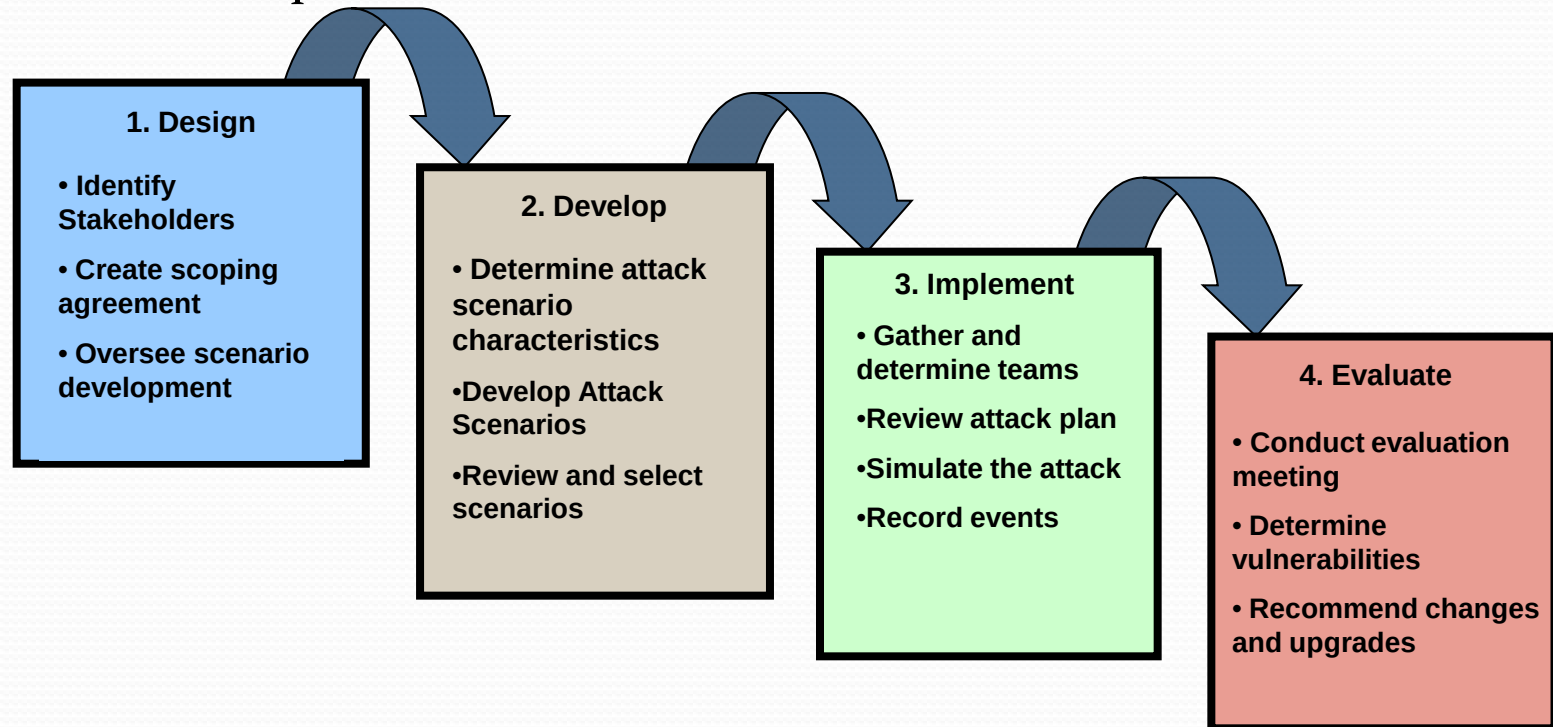
4. Evaluate

Evaluation Meeting (Cont'd)

- Discuss the assessment and capture lessons learned
- Possible discussion points may include:
 - Key attack points, scenarios considered but not used
 - System changes that could affect the attack scenarios
 - Ranking of vulnerabilities
 - Possible upgrades and acceptance options
- Analyze the attack scenario and provide different perspectives on what did and did not work
- Provide recommendations for improving the overall effectiveness of the PPS
- Identify and discuss potential upgrades that should be modeled in subsequent analyses
- Determine the qualitative effectiveness of the PPS

Summary

- A tabletop exercise is a method to simulate an adversary attack on a site's existing or proposed PPS
- Critical events and engagements must be documented and analyzed for a productive result
- Tabletops provide valuable insight, are simple and cost effective, and require minimal resources



12. Tabletop Exercise

Session Objectives

After the session, you will be able to:

1. Recognize issues that need to be addressed in the scoping stage of tabletop exercises.
2. Recognize how a tabletop is conducted and how to facilitate the exercise through the critical events and engagements along the adversary timeline.
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 – Conducting a Tabletop

Step 1: Break into two groups. One group will be the Response Force; the other group will be the Adversary.

Step 2: Lay out the map of Lagassi Institute and set up the figures on the map. Place adversaries and Guard/Response Force according to the Picture-in-Time.

Step 3: Use the task and timeline table that was created in Step 4 of Exercise 1 from the Scenario Analysis Subgroup Exercise to play out each task.

Step 4: Using the attack plan that the group developed and the posters of the facility, work through the tabletop exercise. Begin offsite using modes of transportation to the known target. When a critical event or critical engagement surfaces, roll the dice and use the random number generator (page 5 and 6) to determine the outcome. (If necessary, discuss and make a decision on the event.) Document each critical event or engagement on the poster provided. Move to the next critical event or engagement, all the way up to the target.

Note: Have discussion with participants in the groups to determine the outcome of the first critical event. Please describe it.

Exercise 2 – After-Action Activities

Involving all participants and observers, use the questions below 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.

Step 1: Review the critical events that were documented on the poster. Discuss and document the possible mitigation measures for each event.

Step 2: Discuss and answer the following questions.

A. Overall, how effective is the Lagassi Physical Protection System?

B. Were the adversaries able to exploit any vulnerabilities? _____

If so, what were they and how could the PPS be improved to prevent the exploitation?

C. Scenario analysis will often show vulnerabilities in how the response forces are normally deployed and used.

During the tabletop attack plan scenario, how effective were the response tactical team?

What mitigation measure could be implemented to achieve better effectiveness for the team?

What other mitigation measures and/or upgrades could be implemented to achieve better physical security system effectiveness? Note: Consider guard force and operations personnel emergency plans also.

Random Number Generation Using Dice

Die 1 Outcome	Die 2 Outcome	Probability (Cumulative)	
1	1	2.8%	
1	2	5.6%	
1	3	8.3%	
1	4	11.1%	
1	5	13.9%	
1	6	16.7%	
2	1	19.4%	
2	2	22.2%	
2	3	25.0%	
2	4	27.8%	
2	5	30.6%	
2	6	33.3%	
3	1	36.1%	
3	2	38.9%	
3	3	41.7%	
3	4	44.4%	
3	5	47.2%	
3	6	50.0%	
4	1	52.8%	
4	2	55.6%	
4	3	58.3%	
4	4	61.1%	
4	5	63.9%	
4	6	66.7%	
5	1	69.4%	
5	2	72.2%	
5	3	75.0%	
5	4	77.8%	
5	5	80.6%	
5	6	83.3%	
6	1	86.1%	
6	2	88.9%	
6	3	91.7%	
6	4	94.4%	
6	5	97.2%	
6	6	100.0%	

Use this table during a tabletop exercise when you want to know if some random event happened or did not happen.

To use this table, you need:

- o A probability, P, for the event you need an outcome for, expressed as a percentage. This probability may be a Probability of Detection that you found in the performance database; or it might be a Probability of Casualty for determining if someone firing a weapon at somebody else actually killed their target; these can be found on the next page. **ROUND THIS NUMBER UP OR DOWN TO MATCH SOME NUMBER IN THE TABLE (e.g., 61% becomes 61.1%; 40.5% becomes 41.7%; round up any probability greater than 0% but less than 2.8% to 2.8%).**
- o Two six-sided Die(note that in English 2 “dies” are called dice.) Designate Die1 in some fashion.

RULE: On the basis of the results on Die1 and Die2, select a value from the table corresponding to the number in the cell matching the results on Die1 and Die2. Assume the event happens if p is greater than or equal to this table value; otherwise, assume the event will/does not happen.

Examples: Throw 2 Dice. Suppose Die 1 shows 4 and Die 2 shows 3: then the event happened if p is greater than or equal to 58.3%; otherwise, it did not happen. If Die 1 shows 6 and Die 2 shows 1, then the event happened if p is greater than or equal to 86.1%; otherwise, it did not happen.

An application of this table to outcomes of security engagements is shown on the next page.

Hypothetical Probability of Casualty, P_{Cas} , Tables for Rifles and Handguns

The tables below show the Probability of Casualty, P_{Cas} , for firing a Rifle and a Handgun on a particular “turn” to fire in the tabletop. These are not based on any testing and should be viewed as plausible values.

Distance	Probability of Casualty (P_{Cas}) – Rifle	Distance	Probability of Casualty (P_{Cas}) – Handgun
25 to 0 meters	100%	5 to 0 meters	100%
50 to 25.1 meters	80%	15 to 5.1 meters	80%
100 to 50.1 meters	50%	25 to 15.1 meters	50%
> 100 meters	Assume won't fire	50 to 25.1 meters	20%
		> 50 meters	Assume won't fire

Example: To show how to use this table, assume an adversary with a rifle is 40 meters from a response force member who is armed with a handgun. Assume that the response force member fires first (perhaps because he notices the adversary before the adversary sees him).

First throw of 2 dice (responder firing with $P_{Cas} = 20\%$):

If Die 1 shows 4 and Die 2 shows 3, then the event happened if p is greater than or equal to 58.3%; otherwise, it did not happen. Since $p = 20\%$ the responder missed. If Die 1 shows 6 and Die 2 shows 1, then the event happened if p is greater than or equal to 86.1%; otherwise, it did not happen. Since $p = 20\%$, the responder missed.

Second throw of 2 dice (adversary firing with $P_{Cas} = 80\%$):

If Die 1 shows 4 and Die 2 shows 3, then the event happened if p is greater than or equal to 58.3%; otherwise, it did not happen. Since $p = 80\%$ the adversary killed the responder.

If Die 1 shows 6 and Die 2 shows 1, then the event happened if p is greater than or equal to 86.1%; otherwise, it did not happen. Since $p = 80\%$, the adversary missed.

Note: If some entity is killed before they can fire then they should not be allowed to fire. In this example, if the adversary had been killed by the responder who got the first shot then they would not be allowed to fire.



Insider Analysis

Module 13

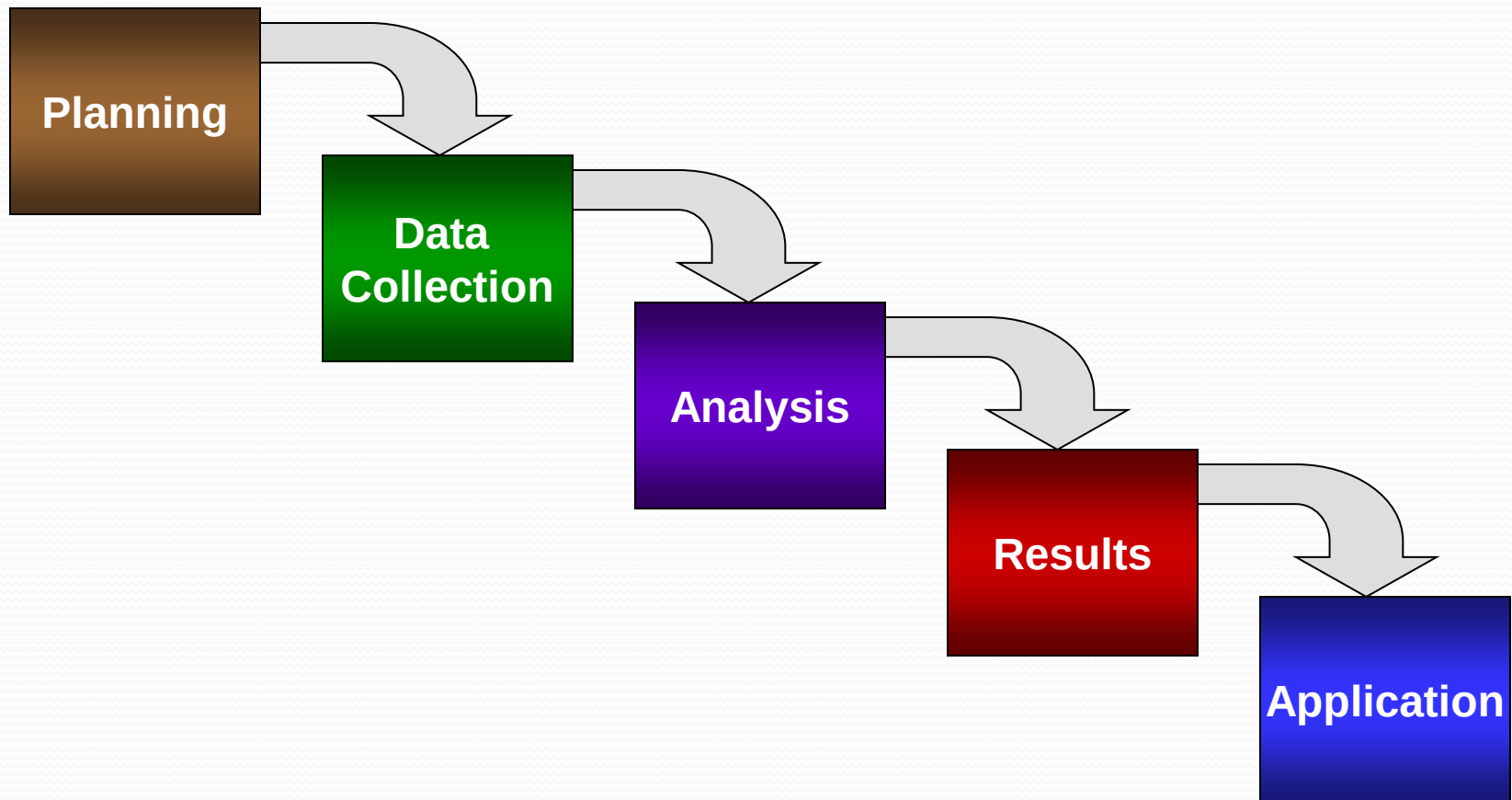
Vulnerability Analysis Training Course
Date:

Student Learning Objectives

After completing this module, you should be able to:

- Recognize an accepted description of an insider
- Identify insider unique issues and concerns
- Define potential insiders at a facility
- Use the system approach to apply techniques that prevent and protect against insiders
- Recognize the Insider Analysis Methodology
- Recognize the three steps in the Analysis Tool Sequence for conducting an insider analysis of the data that were collected

Phases of Vulnerability Analysis

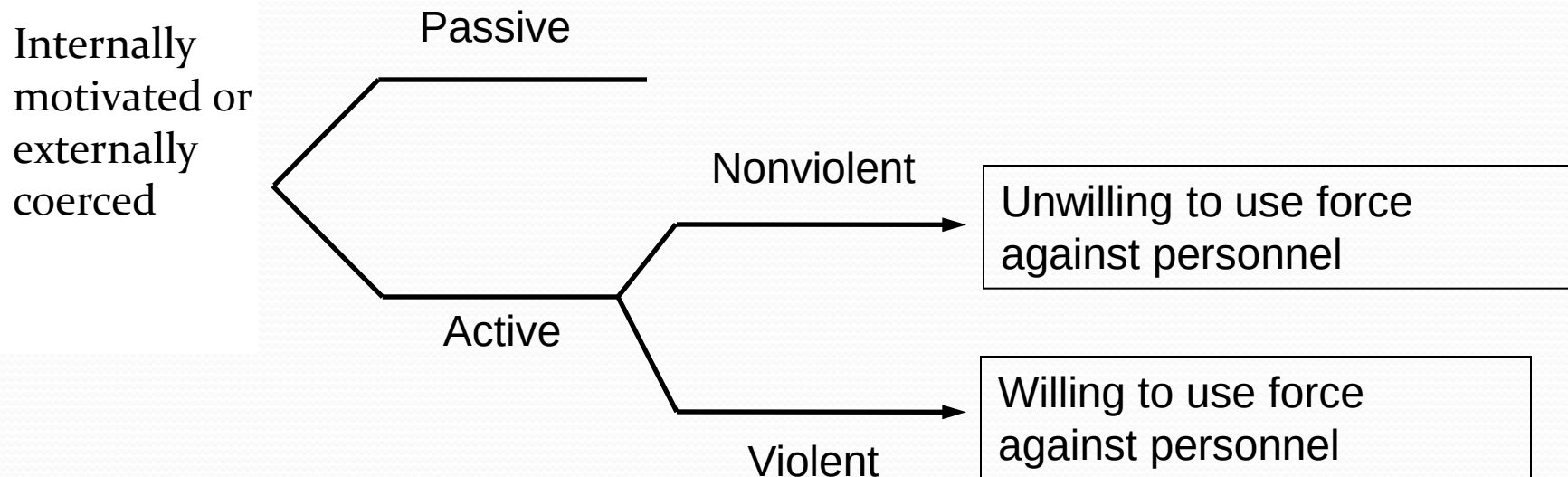


Insider Definition

Insider: One or more individuals with authorized access to *nuclear facilities* or *nuclear material* in *transport* who might attempt *unauthorized removal* or *sabotage*, or who could aid an external adversary to do so (INFCIRC/225/Rev.5 definition).

- Insiders might include, but are not limited to:
 - Management
 - Regular employees
 - Security personnel
 - Service providers
 - Visitors
 - Inspectors

Insider Categories



- All insiders can use stealth and deceit
- Insiders may be rational or irrational

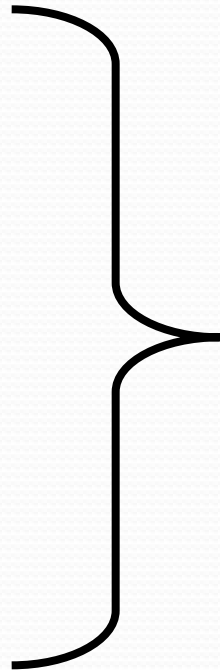


Insider Attributes

- Access
 - Authorized access to work areas
 - Special temporary access
 - Conditions of target during insider access
 - Access to special knowledge
- Authority
 - Over people
 - Over tasks and equipment
 - Temporary authority
 - Falsified authority
- Knowledge
 - Targets
 - Facility characteristics
 - Special tools and equipment

Opportunity

Access
Authority
Knowledge



*Insider
Opportunity*

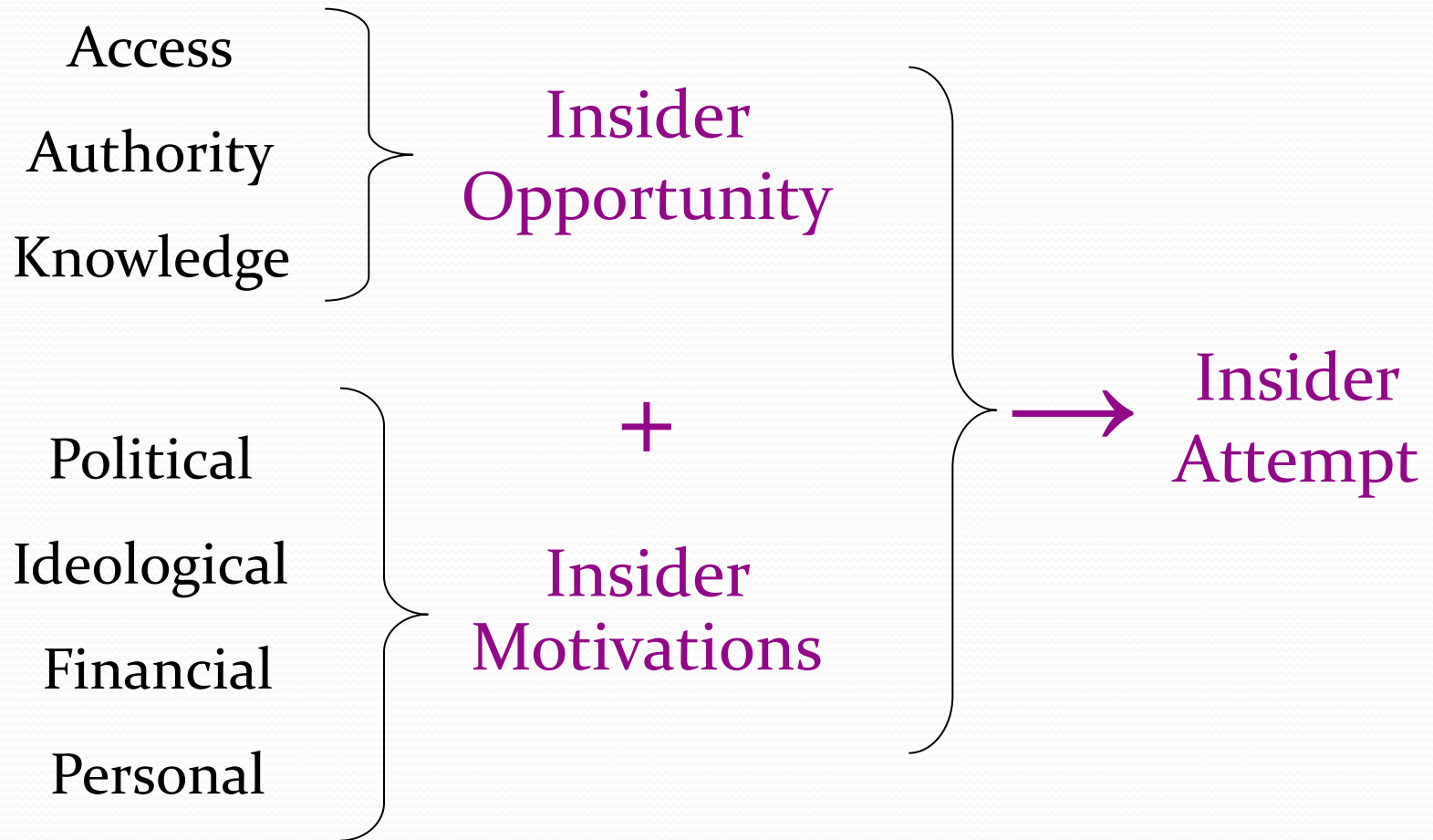


Insider Motivations

- Political
- Ideological – Fanatical conviction
- Financial – Wants/needs money
- Personal
 - Revenge – Disgruntled employee or customer
 - Ego – “Look what I am smart enough to do?”
- Psychotic – Mentally unstable but capable
- Coercion – Family or self threatened

Note: Motivation is an important indicator for both level of malicious intent and likelihood of attempt

Factors Affecting Insider Attempt

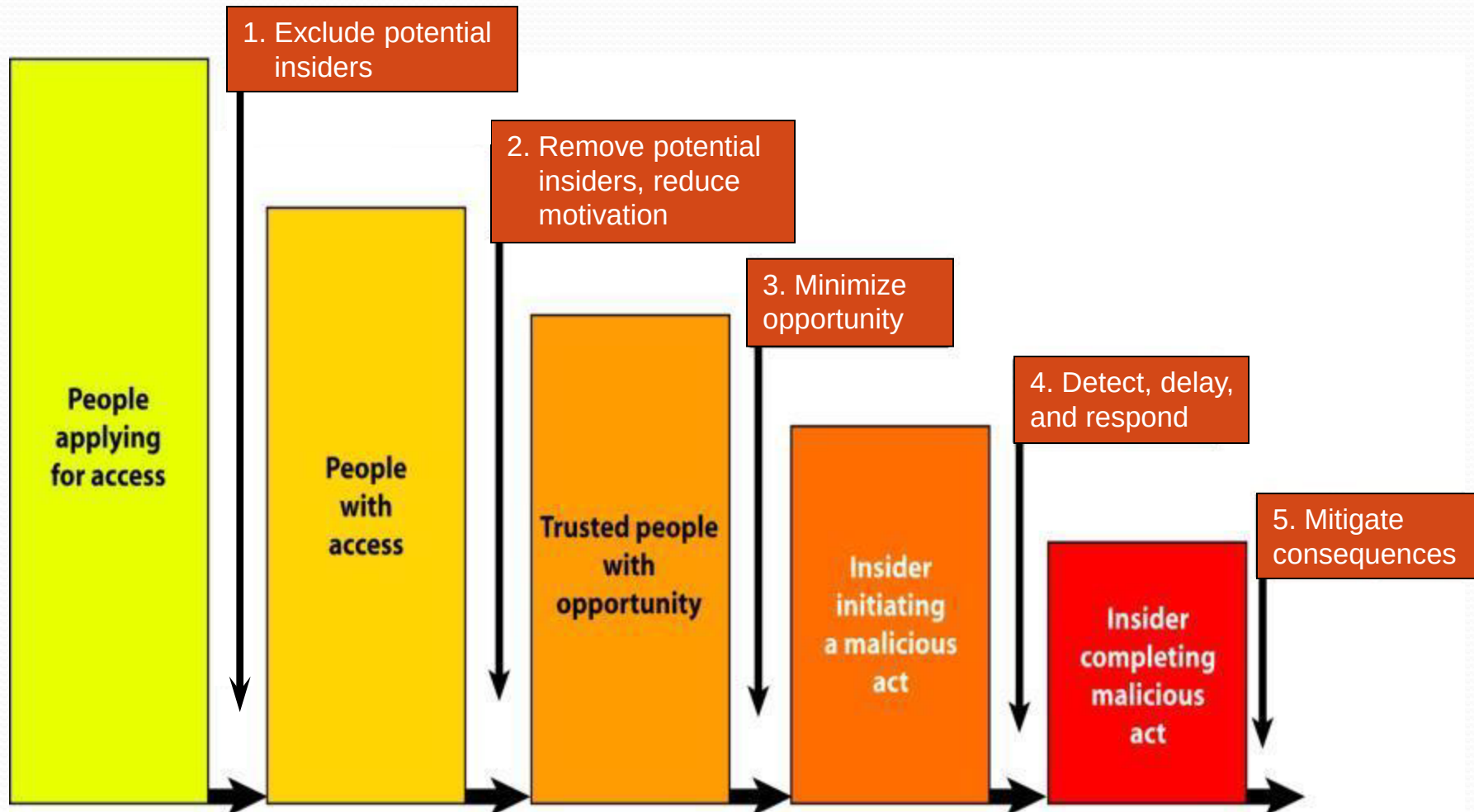




Insider Advantages

- Time
 - Can select optimum time to implement plan
 - Can extend actions over long periods of time
- Tools
 - Has knowledge of and capability to use tools already at work location
- Tests
 - Can test the system with normal mistakes
- Teamwork (collusion)
 - May recruit/collude with others, either insiders or outsiders

System Approach to Prevent and Protect Against Insiders



1. Exclude Potential Insiders



- Filtering
 - Pre-employment:
 - Background checks
 - Criminal
 - Ideological
 - Financial obligations
 - Work history
 - Drug/Alcohol testing
- Detection and deterrence achieved by the above measures
- Response – Do not hire

2. Remove Potential Insider Reduce Motivation

- For persons who are authorized to conduct activities at the site:
 - Security awareness
 - Periodic background checks
 - Fitness for duty programs
 - Employee Assistance Programs
 - Human Reliability Program
 - Quality control programs
- Invoke disciplinary action when any malicious act occurs (could be testing)
- Deterrence achieved by above and prosecution

3. Minimize Opportunity

- Confidentiality and partitioning of information
- Operational security program
- Compartmentalize facility
- Access (circulation) control
- Restrict vital equipment operations
- Inventory management
- Nuclear safety
- Nuclear facility design



4.1 Detection Measures

- Observation by co-workers or supervisors
 - Administrative or technology controlled
 - Two-person rule – no alone zones
 - Two-lock access – A lock and B lock
 - Procedure non-compliance
- Entry/exit control
 - Contraband searches (person and vehicle)
 - Special nuclear material detectors
 - Metal detectors
 - Explosive detectors
- Signal line supervision
- Nuclear material control and accountancy
 - Periodic inventory
 - Real-time accounting
 - Third-party verification
 - Plan of the day

4.2 Delay Measures

- PPS barriers
 - Vaults, tie-downs, locks
- Surveillance and escorts
- Compartmentalization and complexity of tasks
 - Multi-step processes
 - Separation of duties
- Special processes, tools, and operations
 - Material access verification
 - Material transfer verification
- Emergency exit controls and evacuation corrals
- False evacuation alarm prevention

Note: Insider may have authorized access or special knowledge to reduce delays.

4.3 Response Measures

- If Detection is timely
 - Passive insider (passing information) – respond, mitigate, investigate, prosecute
 - Active insider acting alone – respond, investigate, prosecute
 - Active violent insider must be neutralized by security measures
 - Active insider in collusion with outsiders – response similar to outsider response
- If Detection is delayed
 - Mitigate consequences
 - Investigate and prosecute as possible

Note: Measures are limited for response because detection is often late in sequence – response needs to be rapid

5. Mitigate Consequences

- For loss of information
 - Identify scope of loss
 - Change procedures if security could be compromised
- For unauthorized removal of nuclear material
 - Inventory to identify material loss
 - Search for material that might remain on facility grounds
 - Report to appropriate authorities
- For uncompleted sabotage activities
 - Repair, recover
- For completed sabotage activities
 - Follow emergency response plans, consequence mitigation plans

Insider Protection System Considerations (1 of 2)

- Deterrence
 - Cannot quantify effectiveness in either insider or outsider case
- Detection
 - Technology is the same, but insiders may be able to bypass
 - Nuclear Material Control and Accountability system for protracted theft
 - Detection of insiders includes more non-technical means
- Delay
 - Technology is the same
 - Insiders may be authorized access past many barriers
 - Insiders may have special knowledge and opportunities to defeat barriers
 - Insider protection relies more on non-technical means

Insider Protection System Considerations (2 of 2)

- Response
 - Includes safety, security, and operations
 - Containment strategy for theft
 - Denial strategy for sabotage
 - Mitigation if sabotage objective is achieved
 - Passive insider – usually no detection before the act
 - Violent and non-violent insider – response varies – assume worst-case
 - Response to insider activities must be quick

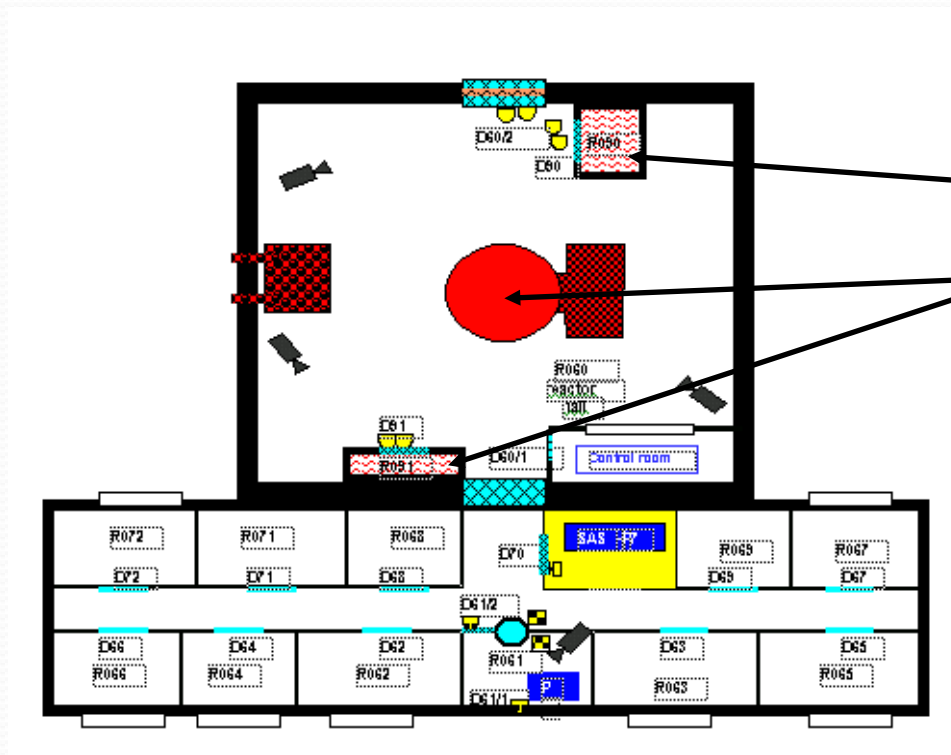
Analysis of Insider Events

- Passive insider (passing information)
 - Prevention is goal
 - Either detected and stopped or not detected
- Active insider in collusion with outsider
 - Modify outsider analysis to include insider contributions
- Active insider acting alone
 - Apply detection, delay, and response principles
 - Analyze credible scenarios

Facility-Specific Insider Analysis Methodology

- Identify targets of interest
 - Abrupt unauthorized removal
 - Protracted unauthorized removal
 - Single-event sabotage
 - Protracted multiple-event sabotage
- Define facility-specific threat (insider groups)
- Determine types of paths for insider using:
 - Adversary Action Sequence Diagram
 - Path Analysis
 - Scenario Analysis
 - Tabletop analysis
- Evaluate the preventive and protective measures in each physical area
- Summarize target/threat results

Target Identification for Unauthorized Removal



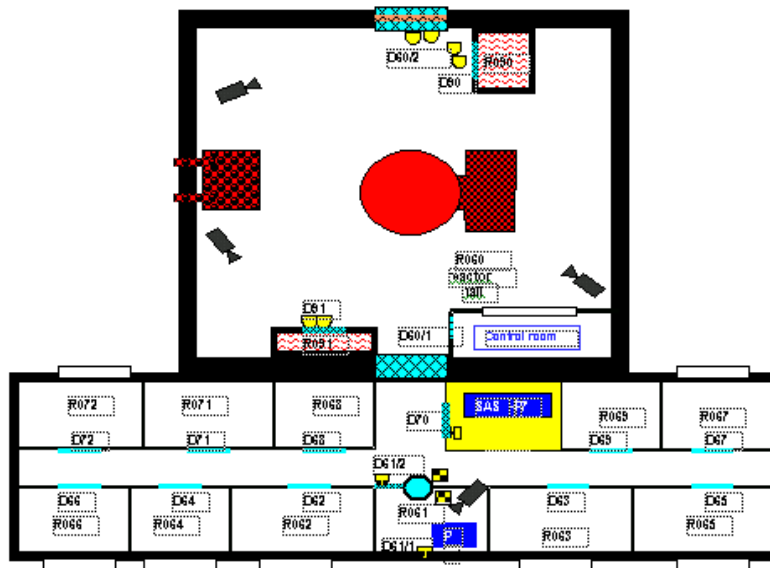
Target Acquisition
Locations

Material Vaults

Reactor Core

Define Facility-Specific Threats

- Review site documentation and organization chart
- Identify facility personnel types
- Recognize guidelines and methods for insider grouping
- Recognize attribute characterization for each group



Insider Groups

Managers

Operators

Technicians

Guards

Visitors

Determine Types of Paths for Insiders

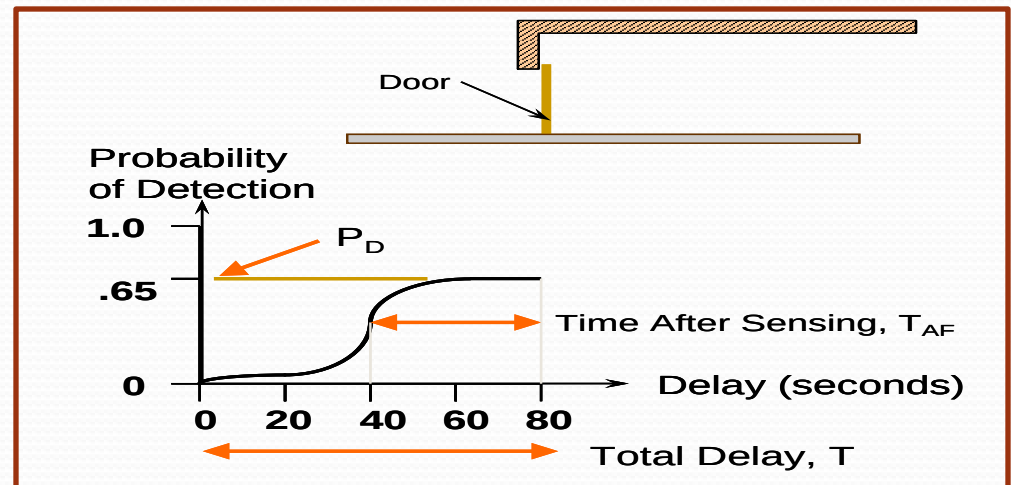
- Tools Used to Determine Insider Paths
 - Adversary Action Sequence Diagram
 - Path Analysis
 - Scenario Analysis
 - Tabletop Analysis

Adversary Action Sequence Diagram (1 of 3)

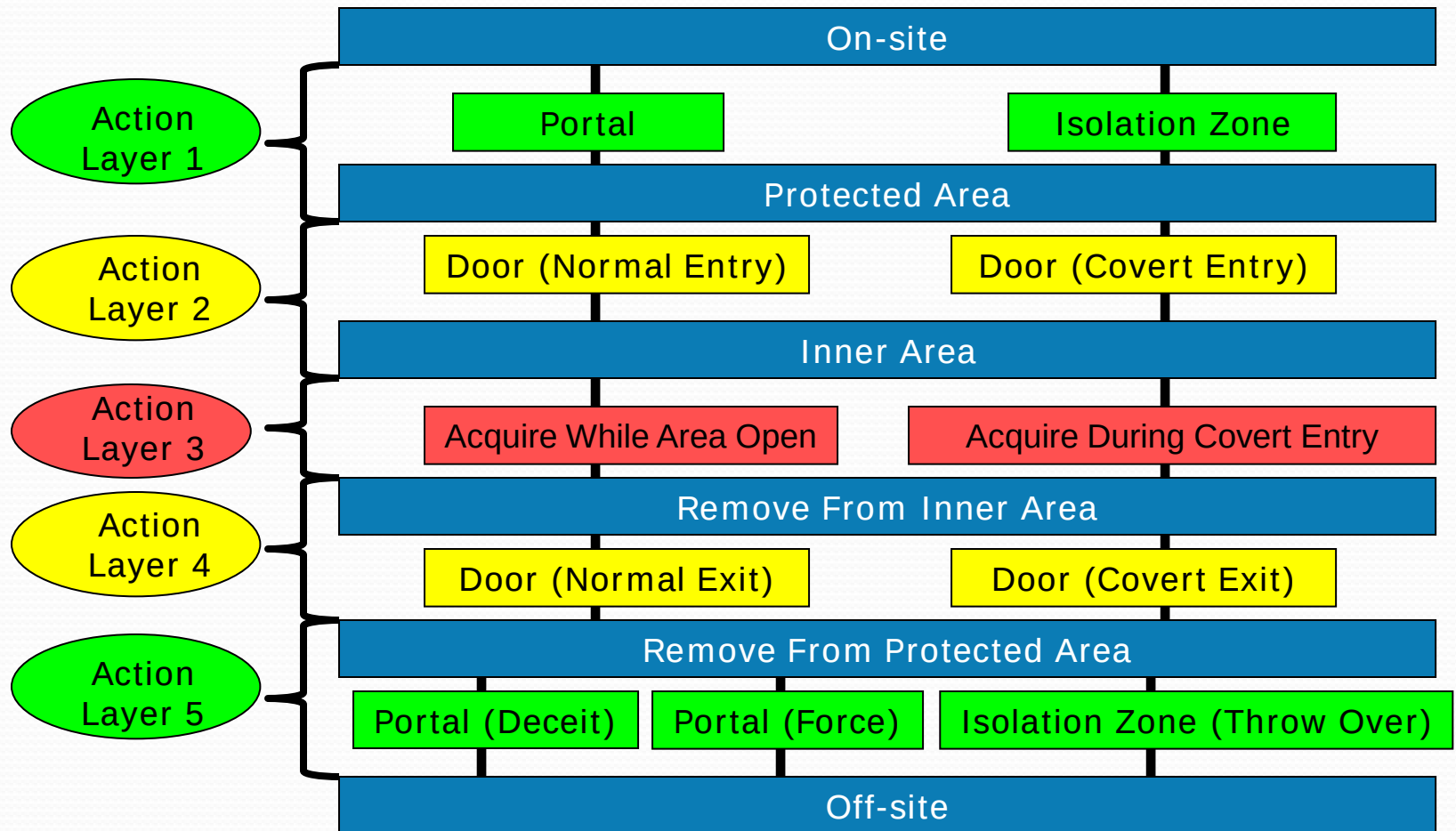
- Identifies action sequence rather than just a path sequence in ASD
- Capable of capturing more specific data for an insider analysis rather than an ASD
- Describes what should be mitigated rather than showing where it should be mitigated
- Sequence for a theft scenario
 - Define each physical area
 - Define an action sequence (steps) the insider must perform to succeed
 - Determine options for each step along the action sequence

Adversary Action Sequence Diagram (2 of 3)

- Assign element performance against an insider
- ASD actions are assigned
 - Probability of Detection, P_D
 - Also for Active, Violent Threat:
 - Total Delay Time, T
 - Time After Sensing, $T_{AF}=0$
- Response force
 - Can include “response” by personnel and/or response force
 - PPS Response Time based on Order-of-Battle Data Response Time Motion Studies



Adversary Action Sequence Diagram Theft in Inner Area (3 of 3)



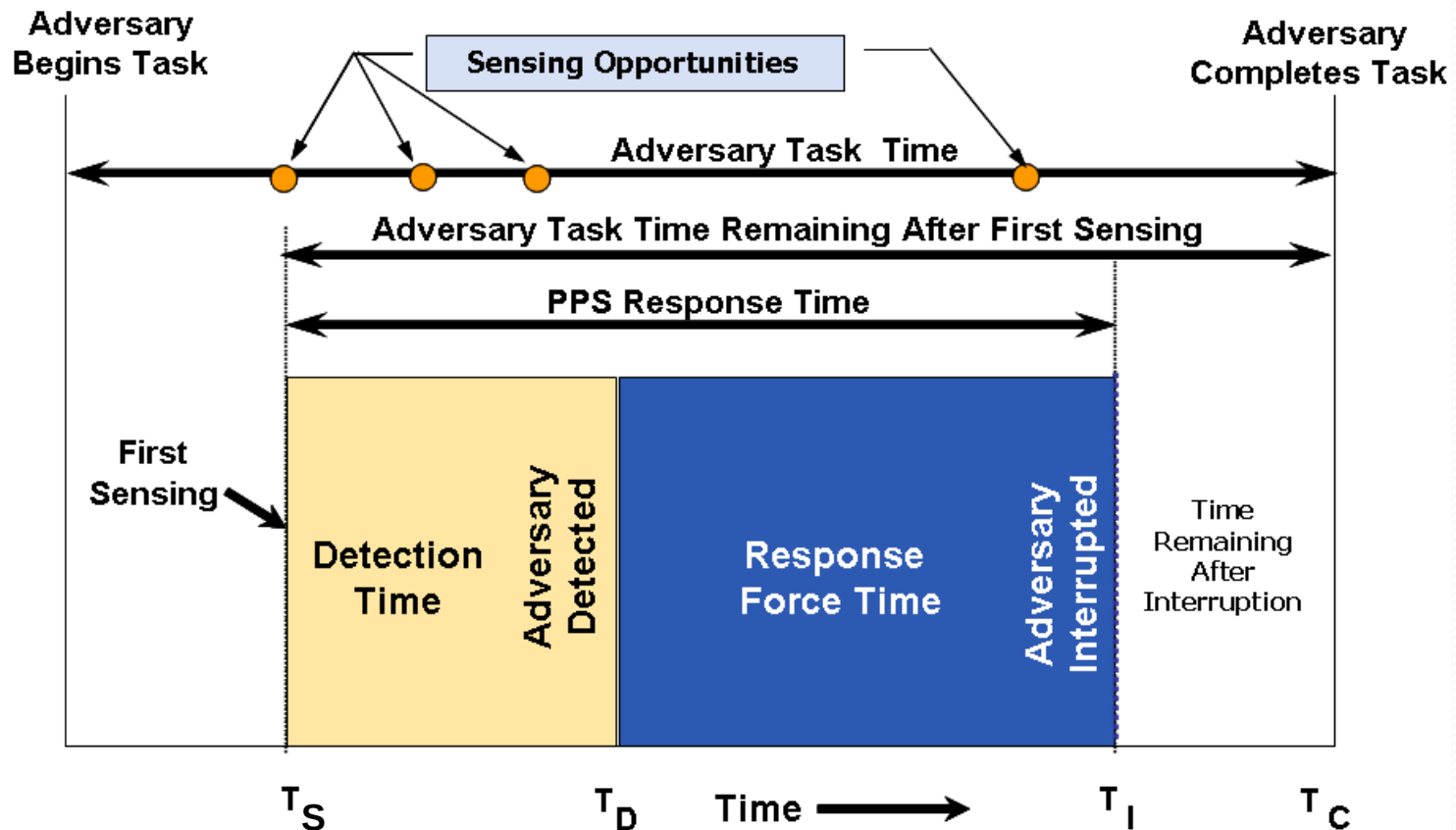


Path Analysis (1 of 2)

- Two types of sub-analysis are used for insiders:
 1. **Detection Analysis:** Determines whether Probability of Detection (P_D) is adequate along all adversary paths
 2. **Timely Detection Analysis:** Determines whether Probability of Interruption (P_I) is adequate along all adversary paths
- Technique for finding most-vulnerable insider paths
 - Use similar approach as used for Outsider
 - For non-violent insiders, assume all ASD elements are timely and minimize P_D
 - For violent insiders, use timelines to determine P_I

Path Analysis: (2 of 2)

- Uses Adversary and PPS Timelines to Evaluate P_I





Scenario Analysis

- Determines whether the PPS effectiveness, P_E , is adequate across a range of detailed adversary scenarios involving insiders within the Design Basis Threat
- Evaluates P_E directly or uses formula $P_E = P_I * P_N$ and then combines P_I and P_N estimates
- Evaluates only a small number of scenarios
 - Cannot claim to have found a most-vulnerable scenario (having the lowest P_E)
 - Requires a process for developing/selecting good scenarios
 - Scenarios are typically evaluated using data from simulations

Insider Analysis Tool Sequence

1. Assign Element Performance

Assign Delay and Detection To Subsystems, ASD

Response Force: Assign PPS Response Time

Determine Blast Effects on People and Structures

Collected Site and Testing Data

2. Path Analysis

A. Detection Analysis: Identify Paths With Lowest P_D in ASD's

B. Timely Detection Analysis: Identify Paths With Lowest P_I in ASD's

3. Scenario Analysis

Scenario Development:

- Based on Low P_I/P_N or Delay Paths
- By Expert RedTeams

Decide Which Scenarios to Evaluate

Scenario Evaluation of P_N , P_E :

- Tabletop Exercise
- Computer Combat Simulation
- Force-on-Force (FoF) Exercises

Summary

- **Insider:** One or more individuals with authorized access to *nuclear facilities* or *nuclear material in transport* who might attempt *unauthorized removal* or *sabotage*, or who could aid an external adversary to do so.
- Analysis process for insider
 - Target identification for insiders
 - Facility-specific insider threat definition
 - Determine types of paths for insider
 - Protection system evaluation
 - Summarize insider/target results
- There are three steps in the process for conducting an insider analysis of the data that was collected
 - Assign element performance
 - Path analysis
 - Scenario analysis

Module 13

Subgroup Insider Analysis

Session Objectives

After the session, you will be able to:

1. Apply the insider PPS design evaluation technique to the PTR hypothetical facility.
2. Use the methodology outlined in Module 13, Insider Analysis.
3. Suggest solutions to reduce the vulnerability to the insider threat of theft of special nuclear materials.

Session Instructions

In Exercise 1 take a comprehensive look at potential targets for insider adversaries in the hypothetical PTR facility. In Exercises 2-7, consider only the Pu experiments in R091 as targets for unauthorized removal by a single, active nonviolent insider. Begin the analysis on-site but outside of the PTR protected area.

Exercise 1 – Target Identification In this exercise, use your *Exercise Data Book* Section 3, Material Stored on Site, and Section 10, PTR Research Reactor Building Floor Plan, to identify potential insider theft targets, target acquisition locations, and sabotage Vital Areas. Rank the targets in order of importance to be protected based on consequence and attractiveness. You may use the subjective rankings of Very High (VH), High (H), Medium (M), Low (L), and Very Low (VL), or a ranking scheme of your choice.

Insider Unauthorized Removal (Theft) Targets

Target Acquisition Locations	Material	Form	Qty	Abrupt Theft	Protracted Theft	Consequence of Loss	Rank

Insider Sabotage Targets

Sabotage Vital Areas	Material	Form	Qty	Radiation Level	Consequence of Sabotage	Rank

Exercise 2 –Threat Definition: Facility Specific Insider Identification

The objective of this exercise is to define insider groups from the personnel access list for PTR for subsequent analysis. Information from the facility organization chart and from site visits and interviews has been compiled in Table 1. The table shows job category and access to three facility areas: the PTR protected area, the reactor hall R060, and the plutonium storage vault R091. For each access area in the table, the left column is the number of people per shift with authorized access and the right column is the number of people allowed access only with a dedicated escort, denoted by a capital “E” after the number. A blank entry means there is no authorized access. R091 is under Two-Person-Rule (TPR) control, which is in addition to the dedicated escort requirement.

Group these personnel for analysis as active nonviolent insiders who might attempt unauthorized removal of material from vault R091. Refer to lecture slides 33-38 for grouping guidelines. Use an EXCEL™ spreadsheet if possible during this exercise. You may have more or less than ten groups.

	Insider Group Description	Personnel Categories	Number (Total)	P.A.	R060	R091
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Table 1. PTR Personnel Access List

	Personnel Type	Accesses					
		PTR P.A.		R060		R091	
1	Plant manager	1		1			1E
2	Reactor Operations Shift Supervisor	1		1			
3	Senior Reactor Operator	1		1			
4	Reactor Operator	2		2			
5	Auxiliary Operator	2		2			
6	Control Room Support Personnel	5			5E		
7	Operations Support		2E		2E		
8	Maintenance Manager	1		1			1E
9	Electrical Maintenance	2		2			2E
10	Mechanical Maintenance	2		2			2E
11	Craft Maintenance	2		2			2E
12	Administrative Support	4		4			
13	Health Physics Technicians	3		3			3E
14	Guard Supervisor	1		1			
15	Alarm Station Operators	2		2			
16	Patrol Guards	2					
17	Post Guards	3		1			
18	Janitorial Staff	4			4E		4E
19	Material Balance Area Custodians	3		3		3	
20	Nuclear Material Technicians	6		6		6	
21	Nuclear Material Accounting Technicians	2		2		2	
22	Engineering Support	2		2			
23	Design Engineers		2E		2E		
24	Safety	5		5			5E
25	Scientists	6		6		6	
26	Analysts						
27	Vendors		2E				
28	State Safety Inspectors		4E		4E		4E
29	State Security Inspectors		4E		4E		4E
30	IAEA Inspectors		2E		2E		2E

Exercise 3 – Action Sequence for Unauthorized Removal from R091

The objective of this exercise is to develop the action sequence necessary for an active nonviolent insider to complete unauthorized removal of target material from R091. Referring to the PTR site schematic and the adversary sequence diagram that you have developed previously for outsider analysis, develop the action sequence in terms of movement between layers as well as tasks that must be accomplished at each layer. Remember that active nonviolent insiders will use primarily stealth and deceit, as well as their access, authority and knowledge, and will surrender if detected. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Step	Action
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

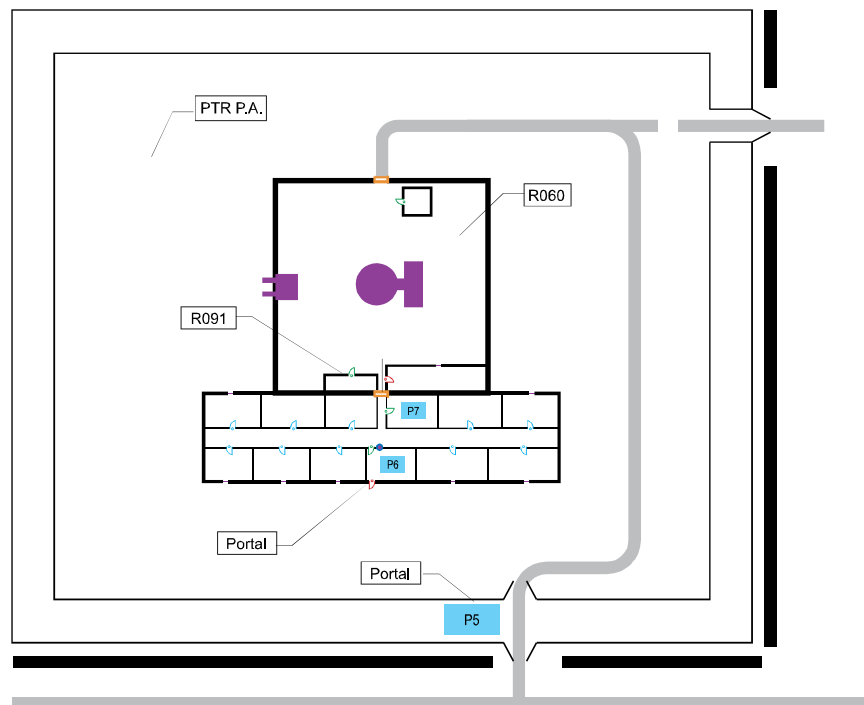


Figure -2. PTR Facility

Exercise 4 – Identify Path Elements and Protection Measures

The objective of this exercise is to identify path element options and protection measures along the insider action sequence developed in Exercise 3. Refer to the PTR site schematic and the adversary sequence diagram that you developed previously for outsider analysis. Use judgment in determining path elements applicable to insiders. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Step	Action	Path Elements	Protection Measures
1			
2			
3			
4			
5			
6			
7			
8			

Exercise 5 – Define Insider Defeat Strategies

The objective of this exercise is to define possible defeat strategies for the protection measures at each path element and action identified in Exercise 4. Refer to the PTR site schematic to ensure that all applicable PPS elements are accounted for in your defeat strategies. Table 2 lists some defeat strategies. Consider the access, authority, knowledge, and capabilities of each group on your insider group list and add other defeat strategies as appropriate. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Action	Path Element and Protection Measures	Defeat Strategy for:	
		Entry	Exit with target

Table 2. Example Defeat Strategies

Doors/portals with access control	Normal entry/exit
Doors/portals with alarms	Normal entry/exit
Fences and isolation zones	Climb over
Search and scan detection	Disguise contraband
Target acquisition	Appear authorized
	Distract Two-person Rule
Target removal	Hide on person

Exercise 6 – Determine Path Element Effectiveness

The objective of this exercise is to determine the protection measure detection probabilities for the strategies at each path element or action identified in Exercise 4. Consider at least two of the insider groups defined in Exercise 2 and be sure that at least one group has authorized access to R091. The detection probabilities may be estimated either quantitatively, as a single-digit decimal fraction between 0 and 1.0, or qualitatively, using very high (VH), high (H), medium (M), low (L), or very low (VL). However, qualitative values must be converted to quantitative numbers for probability accumulation using Table 3. Assume that sensor detection probability for insiders with unauthorized access is 0.9 and that detection by dedicated escorts is 0.7. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Table 3. Qualitative-to-Quantitative Detection Probability Conversion

Qualitative Effectiveness	Suggested Probability of Detection (P_D)
Very High	0.9
High	0.7
Medium	0.5
Low	0.3
Very Low	0.1

The suggested quantitative values must reflect the thinking of the evaluators and may not be exactly as shown above. Change the values if necessary.

Action	Path Element and Protection Measures	Defeat Strategy	Insider Group P _D				

Exercise 7 – Develop Most-Vulnerable Scenarios

The objective of this exercise is to develop the most-vulnerable scenarios for insiders trying to acquire and remove target material. Using the results of Exercise 6, find the combination of protection measure and defeat strategy with the lowest probability of detection for each action in the unauthorized removal sequence. This is the most-vulnerable scenario for each insider. Calculate the cumulative detection probability for each insider. Use an EXCEL™ spreadsheet if possible for this exercise.

Action	Insider Group ____			Insider Group ____		
	Strategy	P _D	P _E	Strategy	P _D	P _E
			----			----
			----			----
			----			----
			----			----
			----			----
Cumulative detection P_i	-----	-----		-----	-----	

From your analysis, identify the insider group that has the greatest probability of success (lowest P_E) in stealing Pu from the storage vault in the PTR (R091).

Insider group with greatest probability of success: _____

Starting with the worst-case insider identified above, for each insider group with P_E less than 0.9, choose one action and suggest at least one upgrade that will increase P_E to at least 0.9. Will this upgrade work for all strategies at that path element? Will the upgrade work for all path elements possible for that action?

Module 13

Subgroup Insider Analysis

Solutions

Session Objectives

After the session, you will be able to:

1. Apply the insider PPS design evaluation technique to the PTR hypothetical facility.
2. Use the methodology outlined in Module 13, Insider Analysis.
3. Suggest solutions to reduce the vulnerability to the insider threat of theft of special nuclear materials.

Session Instructions

In Exercise1 take a comprehensive look at potential targets for Insider adversaries in the hypothetical PTR facility. In Exercises 2-7, consider only the Pu experiments in R091 as targets for unauthorized removal by a single active non-violent insider. Begin the analysis onsite but outside of the PTR protected area.

Exercise 1 – Target Identification

In this exercise, use your *Exercise Data Book* Section 3, Material Stored on Site and Section 10, PTR Research Reactor Building Floor Plan, to identify potential Insider theft targets, target acquisition locations, and sabotage Vital Areas. Rank the targets in order of importance to be protected based on consequence and attractiveness. You may use the subjective rankings of Very High (VH), High (H), Medium (M), Low (L), and Very Low (VL), or a ranking scheme of your choice.

Insider Unauthorized Removal (Theft) Targets

Target Acquisition Locations	Material	Form	Qty	Abrupt theft	Protracted Theft	Consequence of Loss	Rank

Insider Sabotage Targets

Sabotage Vital Areas	Material	Form	Qty	Radiation Level	Consequence of Sabotage	Rank

Exercise 2 –Threat Definition: Facility Specific Insider Identification

The objective of this exercise is to define insider groups from the personnel access list for PTR for subsequent analysis. Information from the facility organization chart and from site visits and interviews has been compiled in Table 1. The table shows job category and access to three facility areas: the PTR protected area, the reactor hall R060, and the plutonium storage vault R091. For each access area in the table, the left column is the number of people per shift with authorized access and the right column is the number of people allowed access only with a dedicated escort, denoted by a capital “E” after the number. A blank entry means there is no authorized access. R091 is under Two-Person-Rule (TPR) control, which is in addition to the dedicated escort requirement.

Group these personnel for analysis as active nonviolent insiders who might attempt unauthorized removal of material from vault R091. Refer to lecture slides 33-38 for grouping guidelines. Use an EXCEL™ spreadsheet if possible during this exercise. You may have more or less than ten groups.

	Insider Group Description	Personnel Categories	Number (Total)	P.A.	R060	R091
1	Plant Manager	1	1	1	1	1E
2	Maintenance	8,9,10,11,13	10	10	10	10E
3	Operator	2,3,4,5,6	11	11	7/5E	0
4	Guard	14,15,16,17	8	8	4	0
5	NM Handlers	19,20,21,25	17	17	17	17
6	Janitor	18	4	4	4E	4E
7	Support	7,12,22,23	10	6/4E	6/4E	0
8	Safety	24	5	5	5	5E
9	Outside Agents	26,27,28,29,30	12	12E	10E	10E
10						

This is one possible way of grouping the personnel that we are considering insiders for this exercise. Make sure that each personnel type is accounted for.

Table 1. PTR Personnel Access List

	Personnel Type	Accesses					
		PTR P.A.		R060		R091	
1	Plant Manager	1		1			1E
2	Reactor Operations Shift Supervisor	1		1			
3	Senior Reactor Operator	1		1			
4	Reactor Operator	2		2			
5	Auxiliary Operator	2		2			
6	Control Room Support Personnel	5			5E		
7	Operations Support		2E		2E		
8	Maintenance Manager	1		1			1E
9	Electrical Maintenance	2		2			2E
10	Mechanical Maintenance	2		2			2E
11	Craft Maintenance	2		2			2E
12	Administrative Support	4		4			
13	Health Physics Technicians	3		3			3E
14	Guard Supervisor	1		1			
15	Alarm Station Operators	2		2			
16	Patrol Guards	2					
17	Post Guards	3		1			
18	Janitorial Staff	4			4E		4E
19	Material Balance Area Custodians	3		3		3	
20	Nuclear Material Technicians	6		6		6	
21	Nuclear Material Accounting Technicians	2		2		2	
22	Engineering Support	2		2			
23	Design Engineers		2E		2E		
24	Safety	5		5			5E
25	Scientists	6		6		6	
26	Analysts						
27	Vendors		2E				
28	State Safety Inspectors		4E		4E		4E
29	State Security Inspectors		4E		4E		4E
30	IAEA Inspectors		2E		2E		2E

Exercise 3 – Action Sequence for Unauthorized Removal from R091

The objective of this exercise is to develop the action sequence necessary for an active nonviolent insider to complete unauthorized removal of target material from R091. Referring to the PTR site schematic and the adversary sequence diagram that you developed previously for outsider analysis, develop the action sequence in terms of movement between layers as well as tasks that must be accomplished at each layer. Remember that active nonviolent insiders will use primarily stealth and deceit, as well as their access, authority, and knowledge, and will surrender if detected. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Step	Action
1	Enter PA
2	Enter R060
3	Enter R091
4	Acquire Material
5	Exit R091
6	Exit R060
7	Exit PA
8	
9	
10	

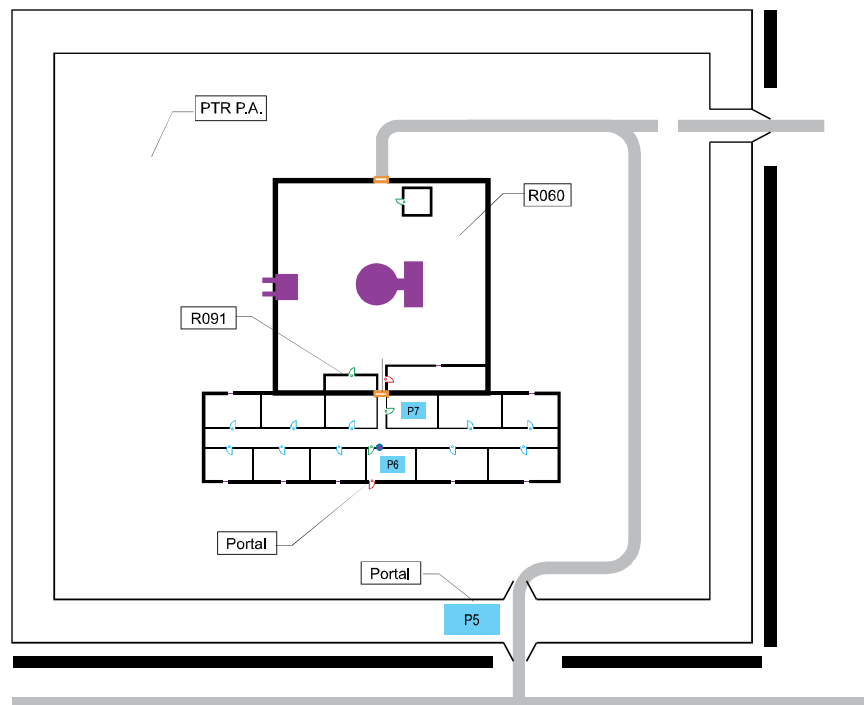


Figure 1. PTR Facility

Exercise 4 – Identify Path Elements and Protection Measures

The objective of this exercise is to identify path element options and protection measures along the insider action sequence developed in Exercise 3. Refer to the PTR site schematic and the adversary sequence diagram that you developed previously for outsider analysis. Use judgment in determining path elements applicable to Insiders. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Step	Action	Path Elements	Protection Measures
1	Enter PA	PER (P5)	Guard ID check, BMS, badge reader, magnetic locks
		VEH	Guard, locks, contraband check, alarm (accessed)
		VEH-EM	locks
		ISO	alarms
2	Enter R060 Reactor Hall	DOR D61-1, 61-2 and 60-1	BMS, badge exchange, badge and PIN, BMS, metal detector. Package inspection, locks
		SHP D60-2	Dual locks and BMS sensors
3	Enter R091 Product Vault	DOR D91	Dual locks, BMS and interior volumetric sensors
4	Acquire Material		2-person rule?
5	Exit R091	DOR D91	Same as step 1
6	Exit R060	DOR D61-1	Same as step 2
		DOR D61-2	
		DOR D60-1	
		SHP D60-2	
7	Exit PA	PER	Same as step 3
		VEH	
		VEH-EM	
		ISO	

In exercise 4 we should think not only about the path elements encountered in the action sequence, but also all of the protection measures. As with the Outsider, the protection measures may exist in one state or condition, but not in others (e.g., guard posted during working hours, locked and alarmed at night). Also, when going through a path element, many protection measures may be encountered, some of which apply and some t don't. Make sure that the students are thinking this way now; it will help when it comes to estimating protection measure effectiveness.

Exercise 5 – Define Insider Defeat Strategies

The objective of this exercise is to define possible defeat strategies for the protection measures at each path element and action identified in Exercise 4. Refer to the PTR site schematic to ensure that all applicable PPS elements are accounted for in your defeat strategies. Table 2 lists some defeat strategies. Consider the access, authority, knowledge, and capabilities of each group on your insider group list and add other defeat strategies as appropriate. Use an EXCEL™ spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Action	Path Element and Protection Measures	Defeat Strategy for:	
		Entry	Exit with target
Enter PA	Personnel portal with posted guard, ID check, magnetic locks and BMS sensors	Normal Entry	Normal Exit
		False Badge (deceit)	Hide in Package
	Vehicle portal with guard, contraband check, locked gate	Normal Entry	Normal Exit
			Hide in vehicle
	Emergency vehicle portal with locks and alarms	Deactivate alarm	Unauthorized traversal
		Claim false alarm	
		Acquire keys	
	Isolation Zone with alarms	Unauthorized traversal	Unauthorized traversal
			Throw over
Enter R060	Main entry portal (and subsequent doors) with guard, badge exchange, badge check, metal detection	Normal Entry	Normal Exit
	Shipping door with dual locks and BMS sensors	Acquire keys	Crash out
		Deactivate alarm	Deactivate alarm
Enter R091	Door with dual locks and BMS and Interior sensors	Normal Entry	Normal Exit
		Appear authorized	Appear authorized
		Acquire keys	Falsify forms
		Deactivate alarms	Hide on person
Acquire Target	Two-person rule	Authorized material access	
		Appear authorized	
		Distract TPR	
		Cause evacuation alarm	

In this exercise we need to think about defeat strategies for all the protection measures the insider may encounter. To do this we need to start thinking about when the insider will attempt his actions, because different protection measure may be in effect and different defeat methods would therefore apply. Here we are just brainstorming defeat

methods, but we need to start thinking about the end goal of determining protection measure effectiveness. To do that we need to think about what combination of strategies the insider will use at each path element, and how the combined effectiveness of the protection measures will be compromised by the insider.

Also, when doing something like this in practice and to save time in exercises, when normal entry is established as a viable insider strategy, no other strategies need to be examined. This is the default strategy if possible.

Table 2. Example Defeat Strategies

Doors/portals with access control	Normal entry/exit
	Deceit entry/exit
Doors/portals with alarms	Normal entry/exit
	Deactivate alarms
	Claim false alarm
Fences and isolation zones	Climb over
	Penetrate
	Unauthorized traversal
	Throw material over fence
Search and scan detection	
	Disguise contraband
	Bypass detector
	Claim false alarm
Target acquisition	Falsify authorization
	Claim false exemption from search
Target removal	Appear authorized
	Distract Two-person Rule
	Acquire during evacuation drill
	Acquire during evacuation alarm
	Falsify removal form
	Hide on person
	Hide in package
	Hide with tools or equipment
	Hide in vehicle
	Falsify shipment
	Append to authorized shipment

Exercise 6 – Determine Path Element Effectiveness

The objective of this exercise is to determine the protection measure detection probabilities for the strategies at each path element or action identified in Exercise 4. Consider at least two of the insider groups defined in Exercise 2 and be sure that at least one group has authorized access to R091. The detection probabilities may be estimated either quantitatively, as a single-digit decimal fraction between 0 and 1.0, or qualitatively, using very high (VH), high (H), medium (M), low (L), or very low (L). However, qualitative values must be converted to quantitative numbers for probability accumulation using the table below. Assume that sensor detection probability for insiders with unauthorized access is 0.9 and that detection by dedicated escorts is 0.7. Use an EXCEL[™] spreadsheet if possible for this exercise. Save the results for use in the following exercises.

Table 2. Qualitative-to-Quantitative Detection Probability Conversion

Qualitative Effectiveness	Suggested Probability of Detection (P_D)
Very High	0.9
High	0.7
Medium	0.5
Low	0.3
Very Low	0.1

Use this table to convert qualitative probabilities of detection into quantitative values. The suggested quantitative values must reflect the thinking of the evaluators and may not be exactly as shown above. Change the values if necessary.

Action	Path Element and Protection Measures	Defeat Strategy	Insider Group P _D				
Enter R091	D91 Locks, BMS, interior sensors	Normal entry					
		Appear authorized					
		Acquire keys, disable alarms					
Acquire material	TPR	Distract TPR					
		Acquire during evacuation ¹					
		Falsify removal form					
Exit R091	D91 Locks, BMS, interior sensors	Hide material on person					
		Hide material in package					
		Append to auth. removal					
		Remove during evacuation ¹					
Exit R060	D60-2 Locks, BMS	Hide material on person					
		Hide material in package					
		Hide material with tools					
		Remove during evacuation ¹					
	D60-1, D61-2, D61-1	Hide on person and bypass metal detector					
		Hide in package					
		Hide with tools					
Exit PA	PER Guard, ID check, mag. locks, BMS	Hide on person					
		Hide in package					
		Unauthorized traversal					
	VEH Contraband check, locks	Hide in vehicle					
	ISO	Throw over Isolation zone					
		Unauthorized traversal					
		Disable alarms					

A thing to note in this exercise is that some strategies are suited to follow other strategies. “Falsify removal form” is not well followed by “hide on person” because the material will seem to have disappeared, and that might be alerting.

Some strategies may apply over a string of actions. Emergency evacuations might be used to acquire material and to take material past several boundaries (but will only go so far).

Exercise 7 – Develop Most-Vulnerable Scenarios

The objective of this exercise is to develop the most-vulnerable scenarios for insiders trying to acquire and remove target material. Using the results of Exercise 6, find the combination of protection measure and defeat strategy with the lowest probability of detection for each action in the unauthorized removal sequence. This is the most-vulnerable scenario for each insider. Calculate the cumulative detection probability for each insider. Use an EXCEL™ spreadsheet if possible for this exercise.

Action	Insider Group ____			Insider Group ____		
	Strategy	P _D	P _E	Strategy	P _D	P _E
Enter R091	NE	0.0	----	Appear auth		----
Acquire mat.	Distract	0.7	----	...		----
Exit R091	Hide on per.	0.1	----			----
Exit R060	Bypass	0.1	----			----
Exit PA	NE	0.0	----			----
Cumulative detection P _i	-----	-----	0.76	-----	-----	

From your analysis, identify the insider group that has the greatest probability of success (lowest P_E) in stealing Pu from the Storage Vault in the PTR (R091).

Insider group with greatest probability of success: _____

Starting with the worst-case insider identified above, for each insider group with P_E less than 0.9, choose one action and suggest at least one upgrade that will increase P_E to at least 0.9. Will this upgrade work for all strategies at that path element? Will the upgrade work for all path elements possible for that action?

Complete contraband detection with bypass protection

Procedure to prohibit personal packages in R060

Material handoff and third-party verification on material transfers



Document the Results of the Assessment

Module 14

Vulnerability Analysis Training Course
Date:



Student Learning Objectives

At the end of this module, you should be able to:

- Organize a VA report
- Outline contents of each section of the report
- Recognize the importance of protecting information

Typical VA Report Outline

- Executive Summary
- Introduction
- Identification and Description of Targets
- Threat Definition
- Theft Vulnerability Analysis
- Radiological Sabotage Analysis
- Upgrades Analysis
- Adjusted Risk for Upgrade Options
- Conclusions and Recommendations
- Appendices



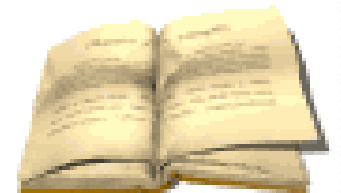
Executive Summary

- Provided to allow a broad spectrum of readers to understand the results quickly
- Should be short, one or two pages
- Include
 - Overview of the analysis approach
 - Specific issues of concern
 - Conclusions
 - High-level recommendations or upgrade options
- Likely to be the most-read portion of the report
 - Mostly likely the only section to be read by senior management
 - Should be an open, unclassified document



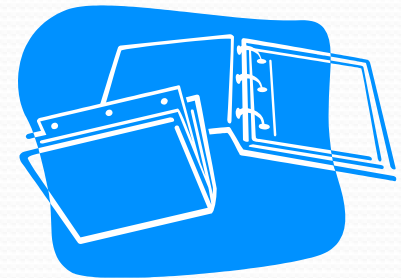
Introduction

- Background
- Objective of VA
- Scope of VA and customer requirements
- Report structure
- Assumptions made for the analysis
- Methodology used
- VA contributors
- Sensitivity of the information



Identification and Description of Targets

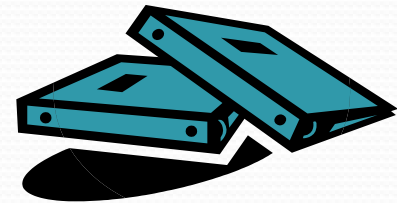
- Theft targets and potential consequences
 - Types, categories, and amounts
 - Locations
 - Attractiveness for weapons or dispersal off-site
 - Portability
 - Priority of targets
- Radiological sabotage
 - Types and amounts
 - Locations
 - Attractiveness for dispersal onsite
 - Radiological consequences
 - Priority of targets





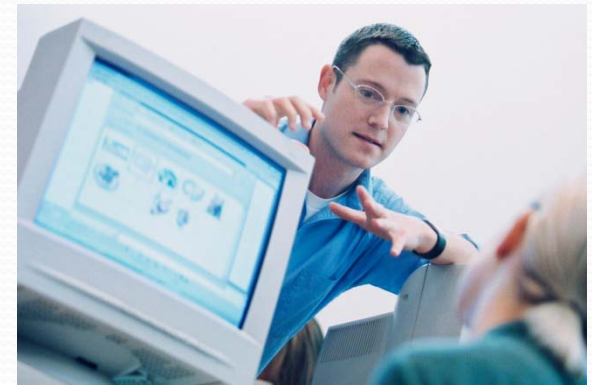
Threat Definition

- Outsider summary
 - DBT used
 - Modifications from DBT
 - Site-specific threat issues
- Insider summary
 - DBT used
 - Expansion on DBT basic threat
 - Site-specific threat categorizations
- Collusion summary



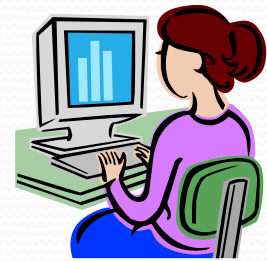
Vulnerability Analysis Concerning Theft

- Methods and tools used
- Confidence in data used
 - Data available
 - Testing done
 - Estimates and assumptions made
- Scenario development process
- Outsider
 - Scenarios evaluated
 - Facility states included
 - System effectiveness for current system status
- Insider
 - Scenarios evaluated for each type of insider considered
 - System effectiveness for current system status
- Collusion
 - System effectiveness for current system status



Vulnerability Analysis Concerning Radiological Sabotage

- Confidence in data used
 - Data available
 - Testing done
 - Estimates and assumptions made
- May reference consequence analysis
- Systems and materials selected for sabotage scenarios
- Development of scenarios
- Threats relevant to sabotage, scenarios evaluated, and system effectiveness for current baseline system
 - Outsiders
 - Insiders
 - Collusion



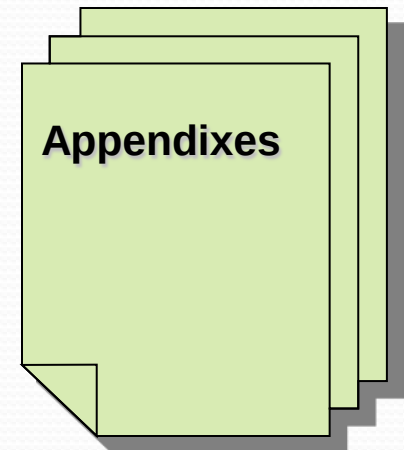
Conclusions and Recommendations

- VA findings and observations
 - Identification of weaknesses and strengths
- Insights of value for designers, such as root causes for vulnerabilities
 - Performance against changing threats
- Concise summary of what can reasonably be improved
 - Description of limitations under the current constraints
- VA team recommendations



Appendices

- Performance test plans and results
- References
- Detailed description of threat
- Descriptions and comparisons of upgrade options
- Additional analysis
- Detailed worksheets
- Etc.



Follow Information Security Requirements

- Determine security classification level
- Protect according to applicable state requirements
 - Document markings
 - Storage
 - Handling and destruction



Summary

- Organize a VA report
- Outline contents of each section
- Recognize the importance of protecting information





Subgroup Exercise:

Prepare VA Results Presentation

- Using the template provided, develop a presentation on the results of the VA you conducted during this course



VA Results for Site X

Team #

Vulnerability Analysis of Physical Protection Systems

Date:

Introduction

VA Team

-
-
-
-
-
-
-

Site Team

-
-
-
-
-
-
-

VA Methodology/Approach

- Describe the approach you used to generate the expected outcomes
- Expected outcomes
 - Determine the relative effectiveness of alternative protective strategies and systems
 - Ensure that systems provide balanced protection of assets
 - Identify strengths and weaknesses in existing or planned protection systems
 - Support cost-benefit studies for system design alternatives



Review of...

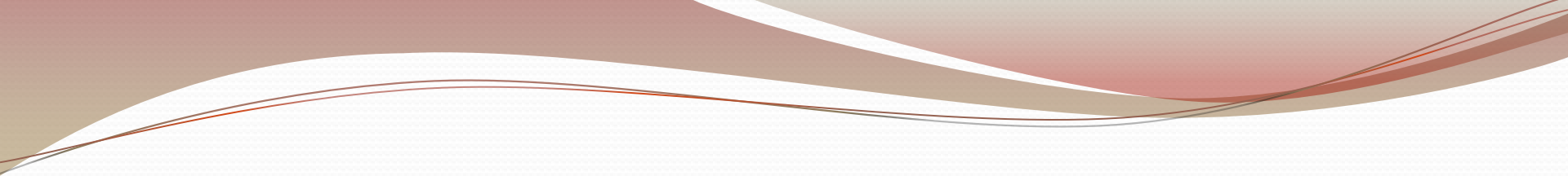
- PPS Objectives
- Design Basis Threat
- Materials and Targets
- Major Assumptions

Facility Characterization Data

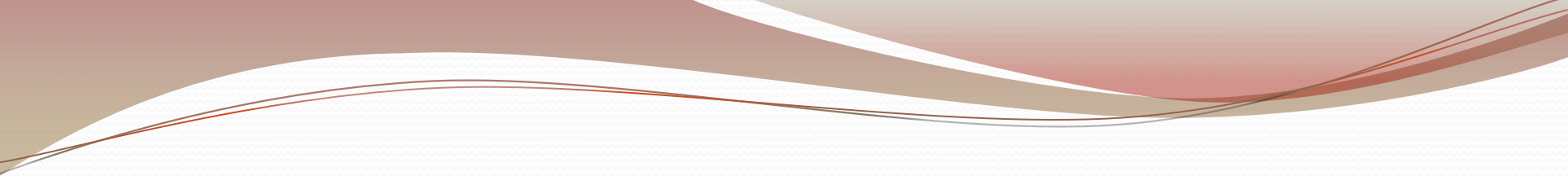
- Detection Subsystem Data
 - Notes and observations
 - Sensors
 - Video
 - Entry Control
 - AC&D
- Delay Subsystem Data
 - Notes and observations
 - Windows
 - Doors
 - Walls
 - Active/passive barriers

Facility Characterization Data

- Response Data
 - Notes and observations
 - Communication
 - Response time
 - Tactics
 - Procedures
 - Training



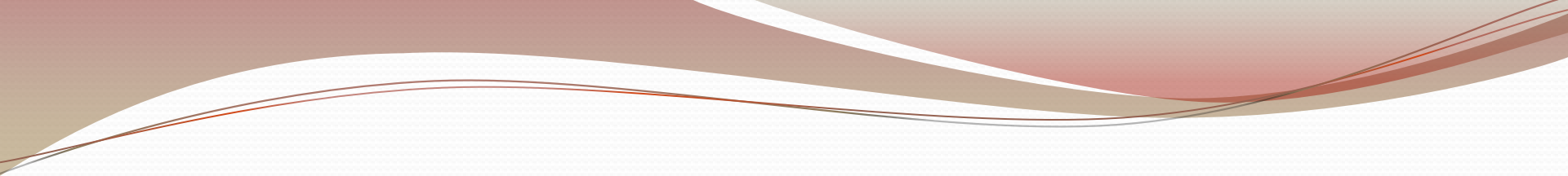
ASD Used for VA



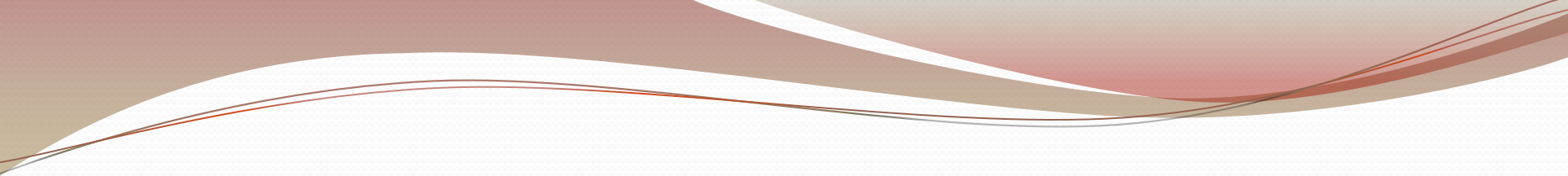
Results of Current System

Areas Identified for Improvement

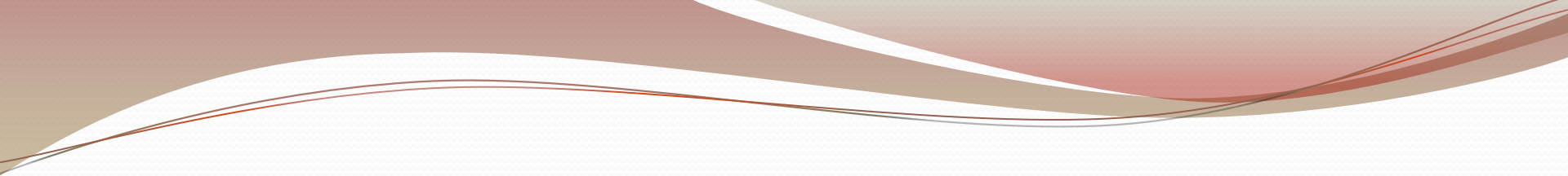
- Describe areas that need improvement.



Recommendations



Next Steps



Thank you!

Other Topics in VA

Module 12

Vulnerability Analysis Training Course
Date:

Student Learning Objectives

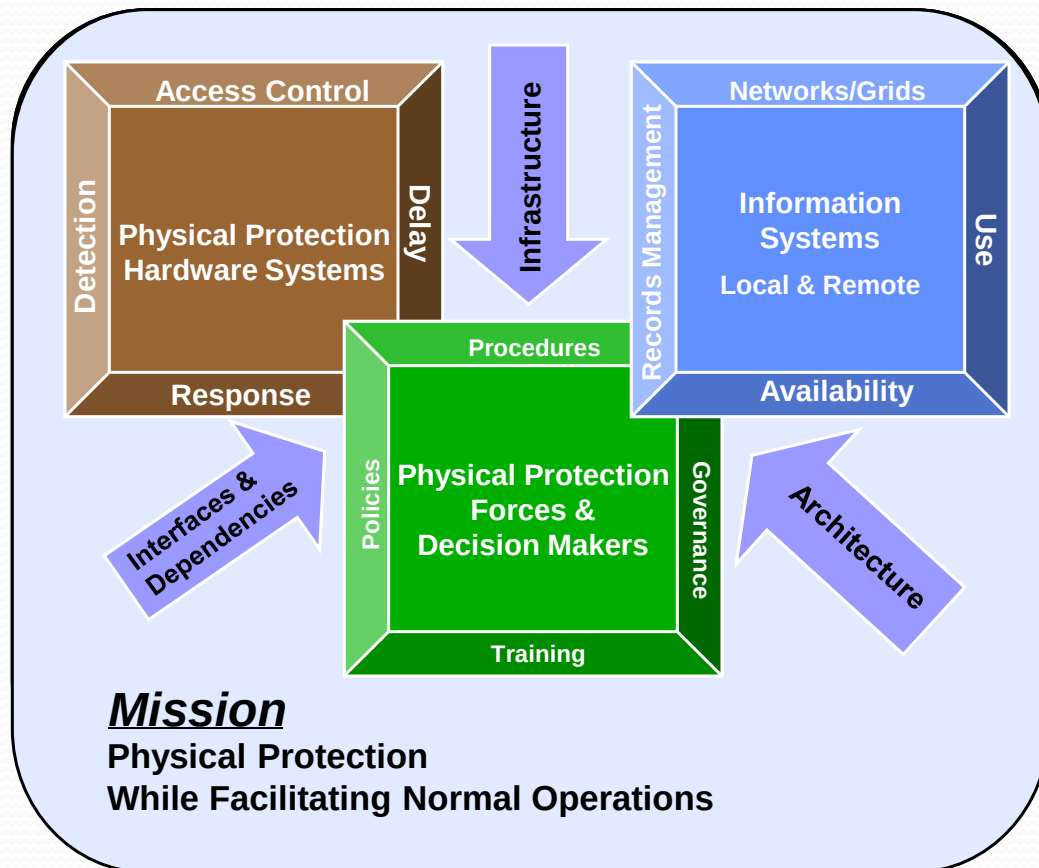
At the end of this module, you will be able to discuss:

- Other vulnerability assessment topics not covered elsewhere in this course
- Other vulnerability factors not considered
- Vulnerability topics covered by other IAEA guidance

Other Vulnerability Factors Not Considered

- System interdependencies within the PPS and between it and other systems
- People and the security culture
- Facility life cycle

PPS Systems Interdependencies

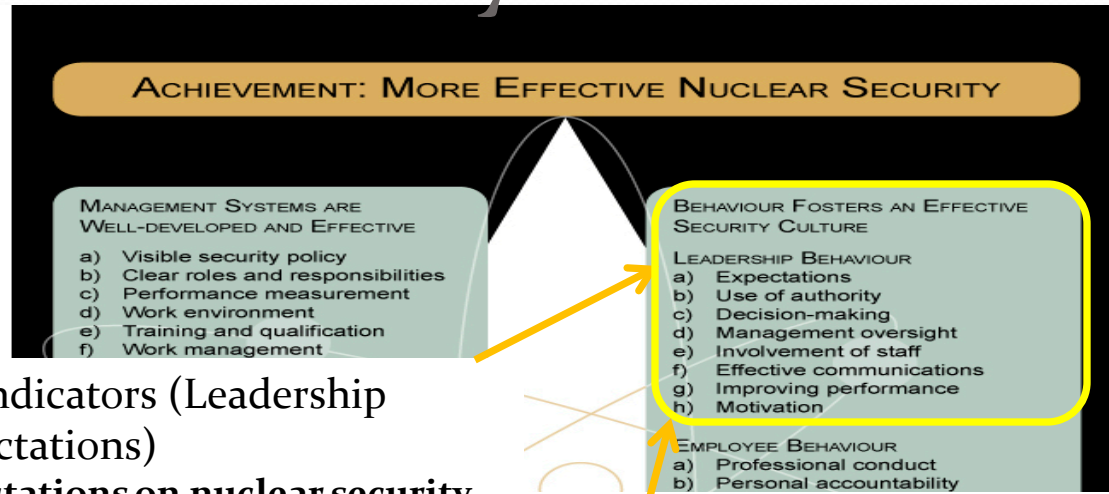


- Available infrastructure
- System architecture
- Interfaces
- Interdependencies

People

- Most security assumes that people follow the rules
- People tend to take the path of least resistance
- People can be your best detectors
- A positive security culture encourages participation in security

Nuclear Security Culture Model



❖ Security culture indicators (Leadership Behaviour - Expectations)

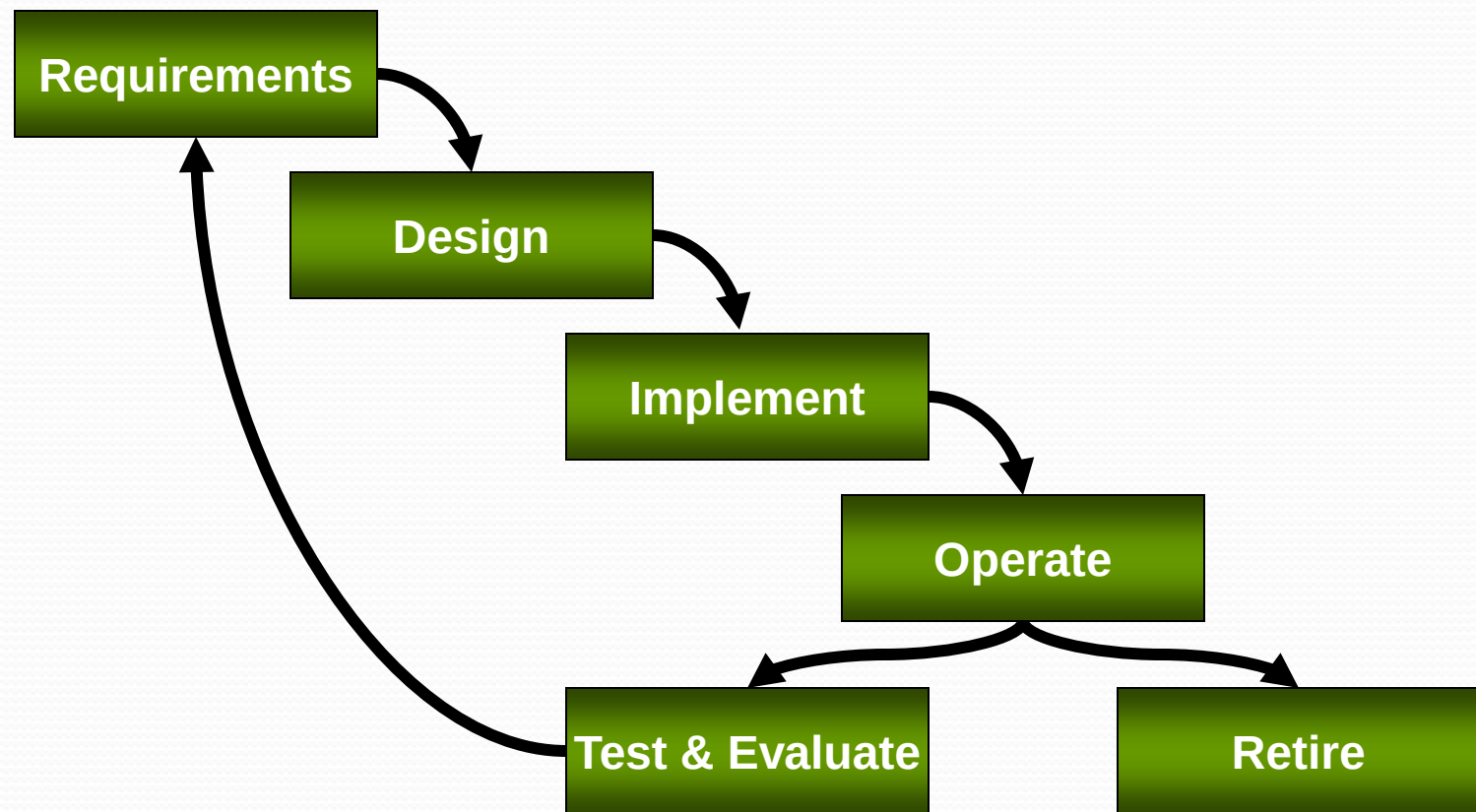
- **Specific expectations on nuclear security explicitly communicated by leadership**
- **Leading by example**
- **Recognize degraded conditions and effect corrections**
- **Personally inspect performance (walking, looking, listening)**
- **Demonstrate sense of urgency for corrections**
- **Ensure resources are available for effective nuclear security**

❖ Security culture indicators (Leadership Behaviour – Use of Authority)

- **Designated managers recognize and take charge when there are changes to vulnerability, security or threat**
- **Managers are approachable, encourage communication and encourage reporting concern or suspicions**
- **Leaders do not circumvent security by their authority**

NUCLEAR SECURITY CULTURE

Facility Life Cycle Considerations



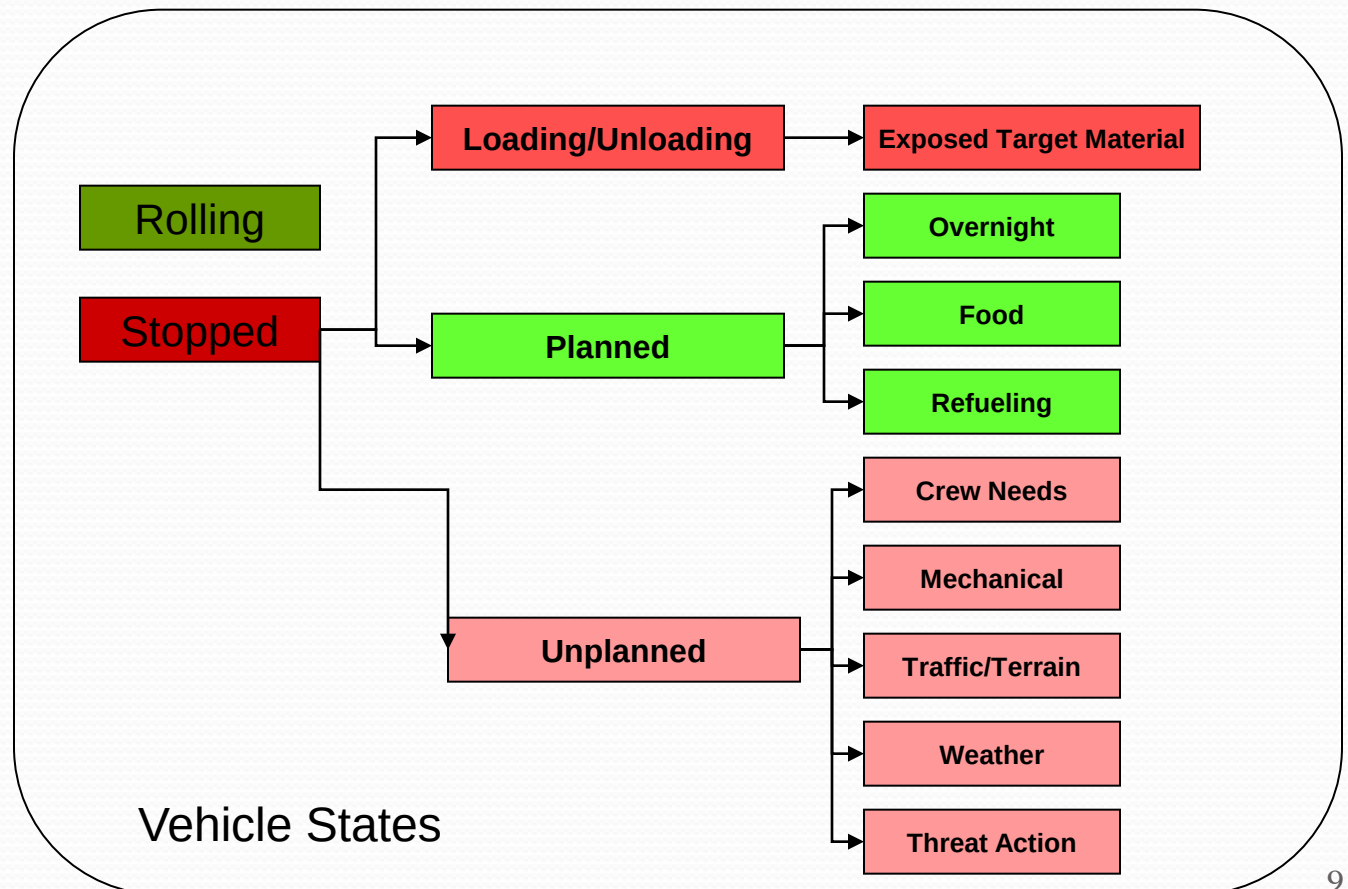
Vulnerabilities can be introduced or exist at any stage

Vulnerability Topics Covered by Other IAEA Guidance

- Transportation security
- Insider protection
- Information security
- Sabotage analysis
- Recovery of missing or stolen nuclear material

Transportation Elements

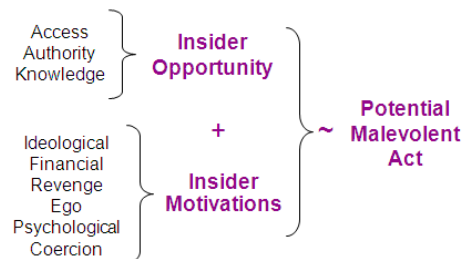
- Material movement within a site
- Material movement to and from a site



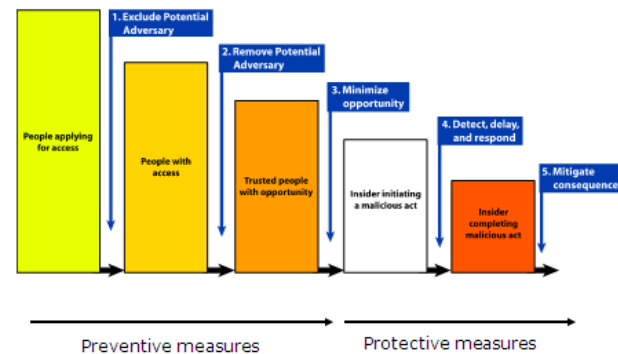
Insider Protection: Preventive and Protective Measures

- Covered in an IAEA workshop
- Reflects IAEA Implementing Guide on *Preventive and Protective Measures Against Threats by Insiders*

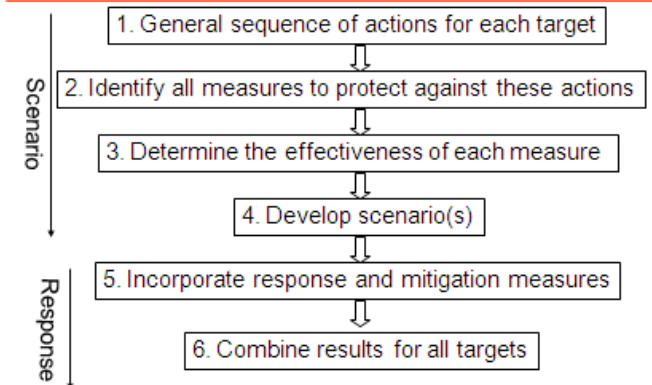
Potential for Malevolent Act

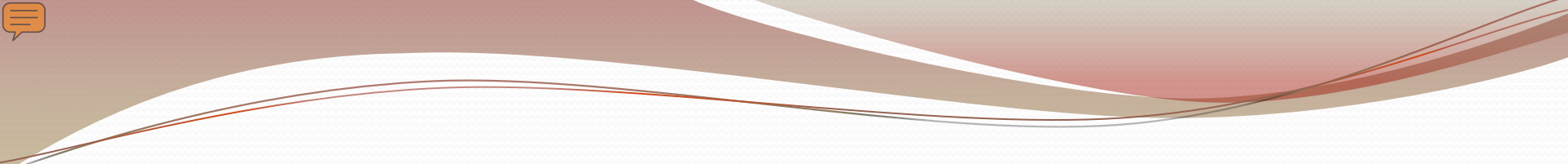


Measures against Insiders



Performance-Based Approach





Information Systems

- Physical Protection Systems may depend upon one or more information systems
- Information systems may contain their own vulnerabilities
- Note that such issues have not been addressed in this course
- Example considerations
 - Isolation of the information system from outside networks
 - Configuration management to track modifications
 - Need to redo VA anytime there is a significant change to an information system



Sabotage Analysis

- Sabotage can be the result of a direct or indirect attack
 - Direct Attack Example: Explosion to disperse material
 - Indirect Attack Example: Pouring salt into a primary cooling system allowing material to overheat
- To protect against sabotage, it is essential to identify and protect vital areas that contain:
 - Nuclear/other radioactive material that could be dispersed
 - Safety/process equipment needed to prevent indirect attacks
- Vital Area Identification (VAI) is a technique to analyze and identify areas that need to be protected



Recovery of Missing or Stolen Nuclear Material (INFCIRC/225 Revision 5 recommendations)

- Establish a coordinated rapid response for the location and recovery of missing or stolen nuclear material
- Operators are required to develop a process
 - Detection and confirmation
 - Contingency plans (requires regularly testing and evaluation)
 - Actions to locate, secure, and return
 - Recovery needs to be included during transport

Summary

- Other vulnerability factors not considered may influence the performance of the security system
 - System interdependencies within the Physical Protection System and between it and other systems
 - Security culture/people
 - Facility life-cycle elements
- Vulnerability Topics Covered by Other IAEA Guidance
 - Transportation security
 - Insider protection
 - Information security
 - Sabotage analysis

Summary and Review

Module 16

Vulnerability Analysis Training Course

Date:

Learning Objectives

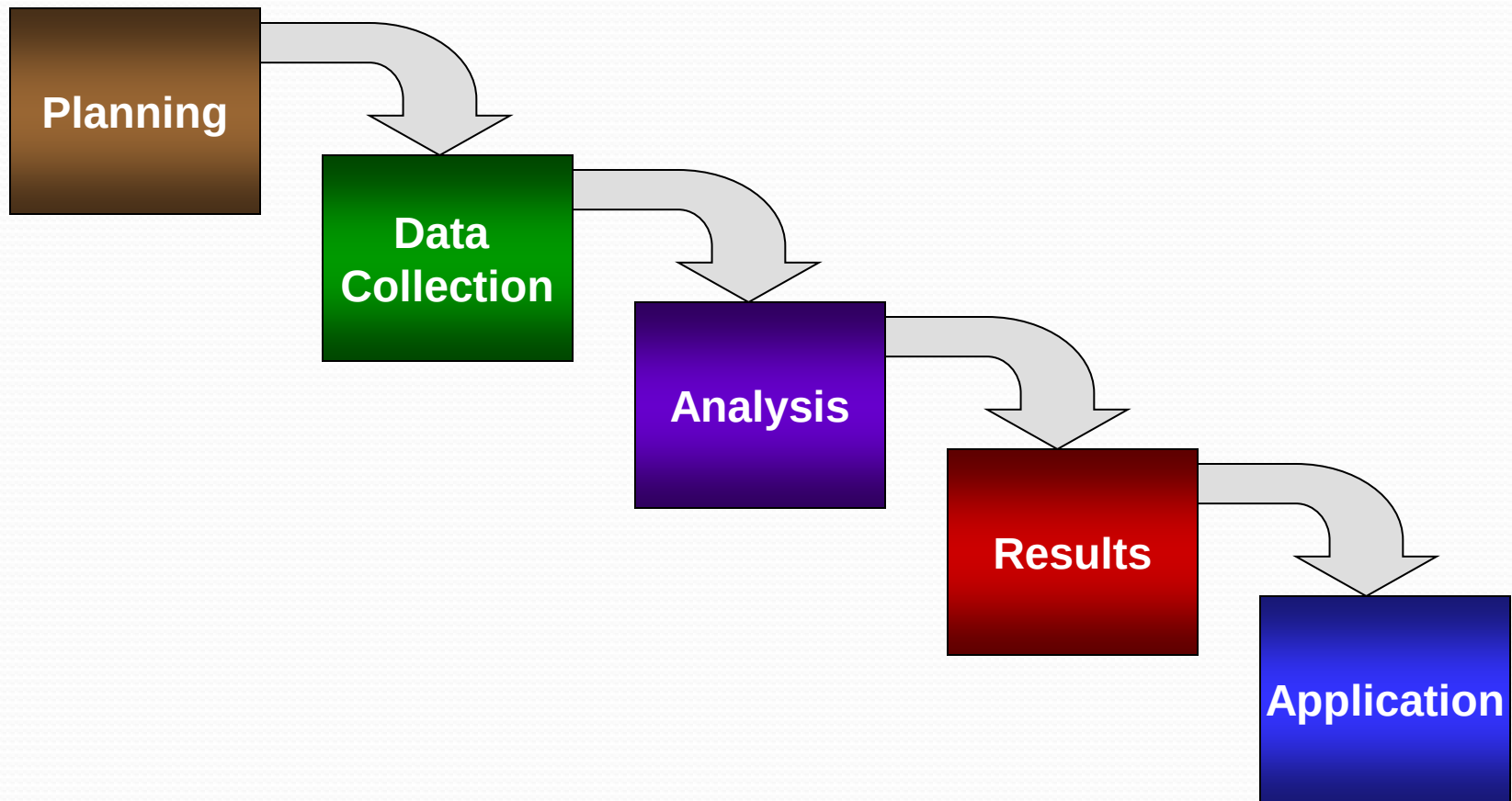
- Review the VA methodology
- Review the content of the VA overview course
- Define what we will do next



What Is a Vulnerability Analysis (VA)?

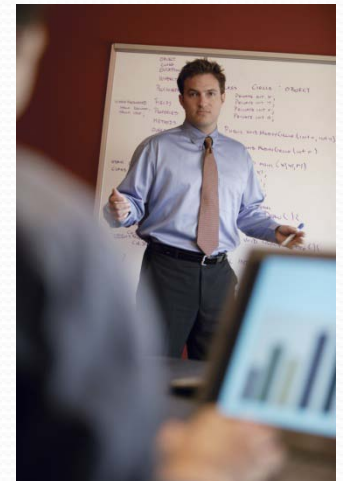
- A systematic, performance-based process that is used to evaluate the ability of a physical security system to meet performance requirements
- The results of a VA usually include:
 - System effectiveness
 - Risk assessments
 - Upgrade recommendations to reduce vulnerabilities

Phases of Vulnerability Analysis



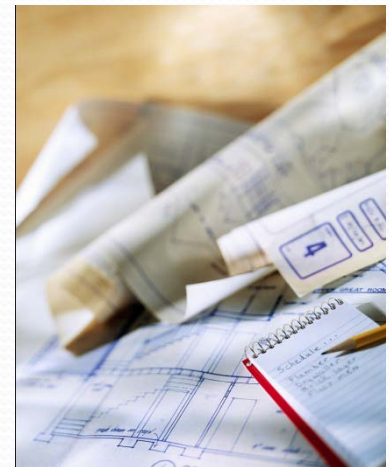
Planning Phase of a VA

- Initiate the analysis
- Determine requirements, goals, and scope
- Form a VA team
- Develop schedule
 - Milestones, dates, deliverables, etc.
- Gather preliminary site data
- Produce “VA Team Guide”



Preparing for the Site Visit

- Gather as much information as possible for the analysis
- Identify the additional information to be gathered during the site visit
- Develop methods to organize this information
 - Data sheets
 - Logs
 - Drawings
 - ASDs
- Prepare for the site visit
 - Scheduling
 - Logistics



Conducting the Site Visit

- Tour site and facilities
 - Take pictures, notes, mark drawings, etc.
- Gain an in-depth knowledge of pertinent features and operations
- Develop visit format
 - Conduct an in-briefing
 - Develop procedures for both planned and ad-hoc activities
 - Verify/gather information from site
 - Provide frequent updates to site
 - Conduct an out-briefing



Target Characterization and Prioritization

- Identify the targets and locations of targets for theft and sabotage at the facility
- Characterize the targets by:
 - Type and amount
 - Theft or sabotage
 - Potential consequences
 - Attractiveness
- Prioritize the targets to be considered in the VA



Facility Characterization

- Identify the pertinent characteristics of the protection features at the facility
- Investigate anything that impacts performance of the protection system
- Get detailed data on all protection elements
- Update drawing notations and ASDs



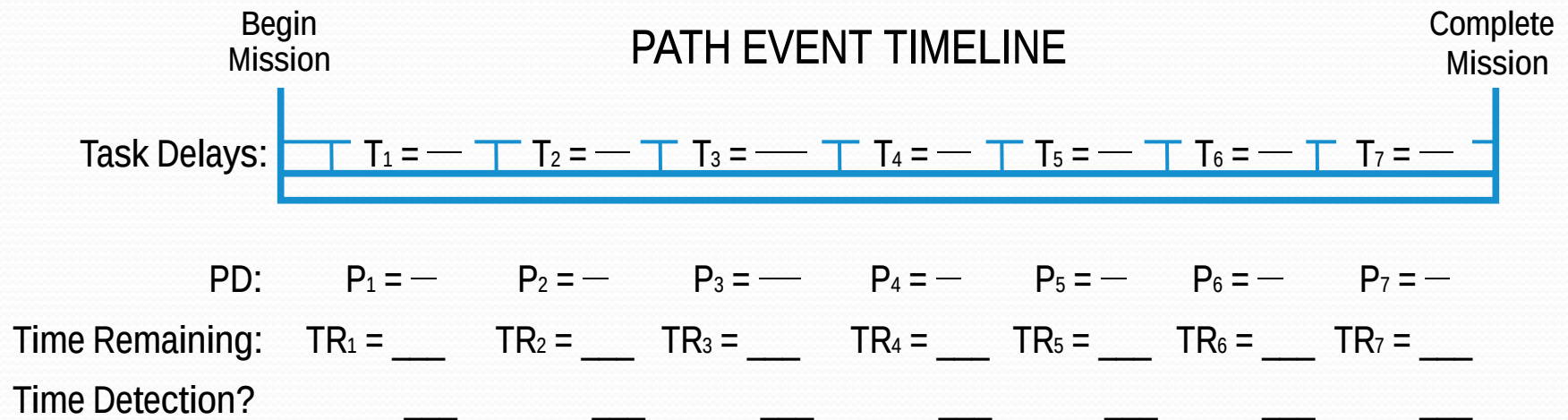
Outsider Threat

- Review the national DBT for threat guidance
- Define an outsider threat spectrum for use in the VA



Outsider Threat Protection Analysis

- Scope an outsider threat protection analysis
- Develop methods for defeating the protection system
- Characterize protection elements
- Develop scenarios
- Determine both element and system effectiveness



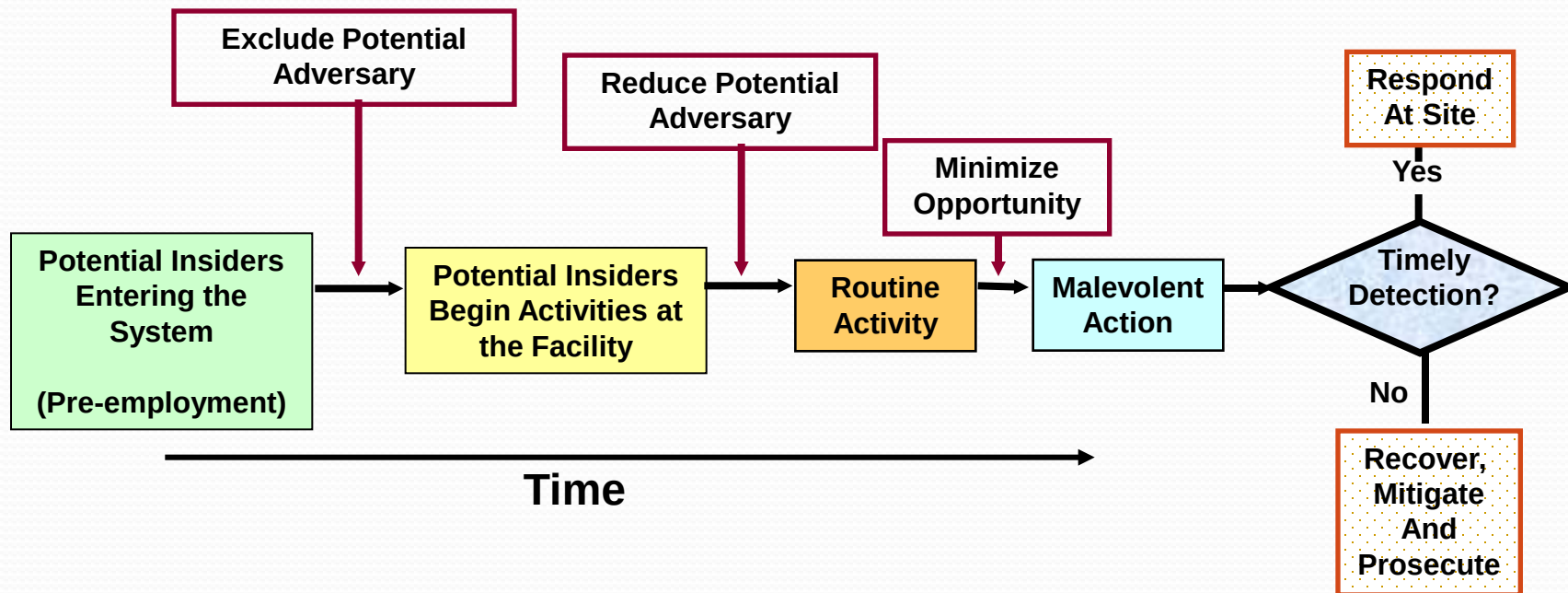
Insider Threat

- Review the national DBT for threat guidance
- Define an insider threat for use in the VA
 - Usually not well-defined in the national DBT
 - Develop potential insider threat groups by categorizing personnel with access to the facility
 - Group by targets

Job Position	Routine Access	Routine Authority / Responsibility	Knowledge
Health Physics Technician	M	L	M
Operations Support	M	L	M

Insider Threat Protection Analysis

- Very similar process to that for outsider analysis
 - More qualitative than outsider analysis
- Difference is that each threat group will have different capabilities for different targets



Collusion Analysis

- Essentially the same as outsider analysis except the insider can modify some characteristics of the protection system
 - Select potential insiders who can significantly enhance outsider attack success
 - Define the effects of insider collusion
 - Modify collusion scenario timelines
- Re-analyze the system with the changes caused by the insider
- The scenarios in this situation may be the very worst case

Upgrade Analysis

- Consider detection, delay, and response in developing upgrades
 - System upgrade
- Identify risk reduction due to proposed upgrades
- Identify cost-effective upgrades for the protection system
- Clearly define the upgrade options for subsequent review
- Include operational and MC&A upgrades and impacts
- Develop approaches for presenting upgrade options

VA Report

- Outline the contents of each section for the report early on in the process
- Document throughout the process
 - If it isn't documented – it didn't happen
- The work isn't done until the paperwork is completed!!
- Recognize the importance of protecting information



Summary

- Review the VA methodology
- Review the content of the VA overview course
- Define what we will do next

Questions or Comments??

