SAND2009-0024P

Introduction

Japan Vulnerability Assessment Seminar
January 20-21, 2009

Presentation Content

Seminar topics and format

Physical protection system effectiveness metrics based on risk of malicious acts

Vulnerability assessment overview

Seminar Topics

This seminar will provide participants with information on:

- **Methods used in the U.S. to assess physical protection system performance**
- **Tools used in vulnerability assessment and their strengths and weaknesses**
- **The relationship between prescriptive and performance-based requirements for physical protection systems**
- **Options for managing the risk of malicious attacks on nuclear facilities**

Seminar Format

Presentations by U.S. participants

Open discussion to address questions or alternative approaches

Day 1

- Introduction
- NRC approach
- DOE approach
- Comparison of NRC and DOE approaches (open discussion)

Day 2

- Analytical tools for vulnerability assessment
- Risk management, acceptable risk, and prescriptive versus performance-based approaches to regulation

General Definition: Security Risk

SECURITY RISK—exposure to the possibility of future harm or loss due to malicious actions of persons or groups of persons.

Security risk is a function of both:

- Frequency of loss describing how often successful malicious actions take place
- The consequences – a measure of harm or loss – that will occur if a successful malicious action takes place

For Nuclear Security, a Simple Risk Model Has Been Applied

Assumptions:

- Frequency of attack is relatively small (f < .1 attacks per year), so we can use probability or likelihood of attack, p, instead of frequency
- Risk, R, can be described adequately using a product model:

$$R = P * C, \text{ where:}$$

R = Risk
P = Likelihood or probability of an undesirable event
C = Consequences of an undesirable event

Likelihood of Undesired Event

The likelihood of an undesired event is dependent on two factors:

- The likelihood or probability of a malicious attack by an adversary
- The likelihood or probability that the malicious attack is successful

Thus the probability of an undesired event can be written as:

- $P = P_A * P_S$, where:

  P_A = Probability of attack
  P_S = Probability that attack is successful

System Effectiveness

A physical protection system is intended to reduce the adversary's probability of a successful attempt:

- Either the PPS is effective and the adversary is defeated, or the PPS is defeated and the adversary is successful
- Thus $P_E + P_S = 1$, where:

  P_E = physical protection system effectiveness

  P_S= probability that attack is successful

PE is represented as the product of two factors

- $P_E = P_I * P_N$
- P_I = Probability of Interruption

  P_I is the likelihood that the response arrives at the adversary location before the adversary completes malicious action
- P_N = Probability of Neutralization

  P_N is the likelihood that the response can defeat the adversary if the response arrives before the adversary completes malicious action

Security Risk Equation

Based on these concepts the classical security risk equation becomes:

- $R = P * C$
- $R = P_A * P_S * C$
- $R = P_A * (1 – P_E) * C$
- $R = P_A * (1 – P_I * P_N) * C$

Thus the more effective the physical protection system (the higher the value of P_E) then the lower the risk

Vulnerability assessment is used to estimate system effectiveness and ensure that it is adequate

Vulnerability Assessment

What is a vulnerability assessment (VA)?

- A systematic process used to determine whether a physical protection system meets established performance requirements.

Results of a VA may include:

- Estimate of overall system effectiveness
- Identification of system vulnerabilities
- Recommendations for upgrades to reduce identified vulnerabilities

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-benefit studies for system design alternatives

VA Process Phases

Planning Phase

Conduct Phase

- Defining system requirements
- Designing the system (or characterizing an existing system)
- Evaluating system performance

Closure Phase

- Upgrade analysis
- Report preparation

Planning Phase of a VA

Determine scope, goals, and requirements

Select VA team

Develop schedule

Gather preliminary data

Select analysis tools to be used

Prepare for site visit

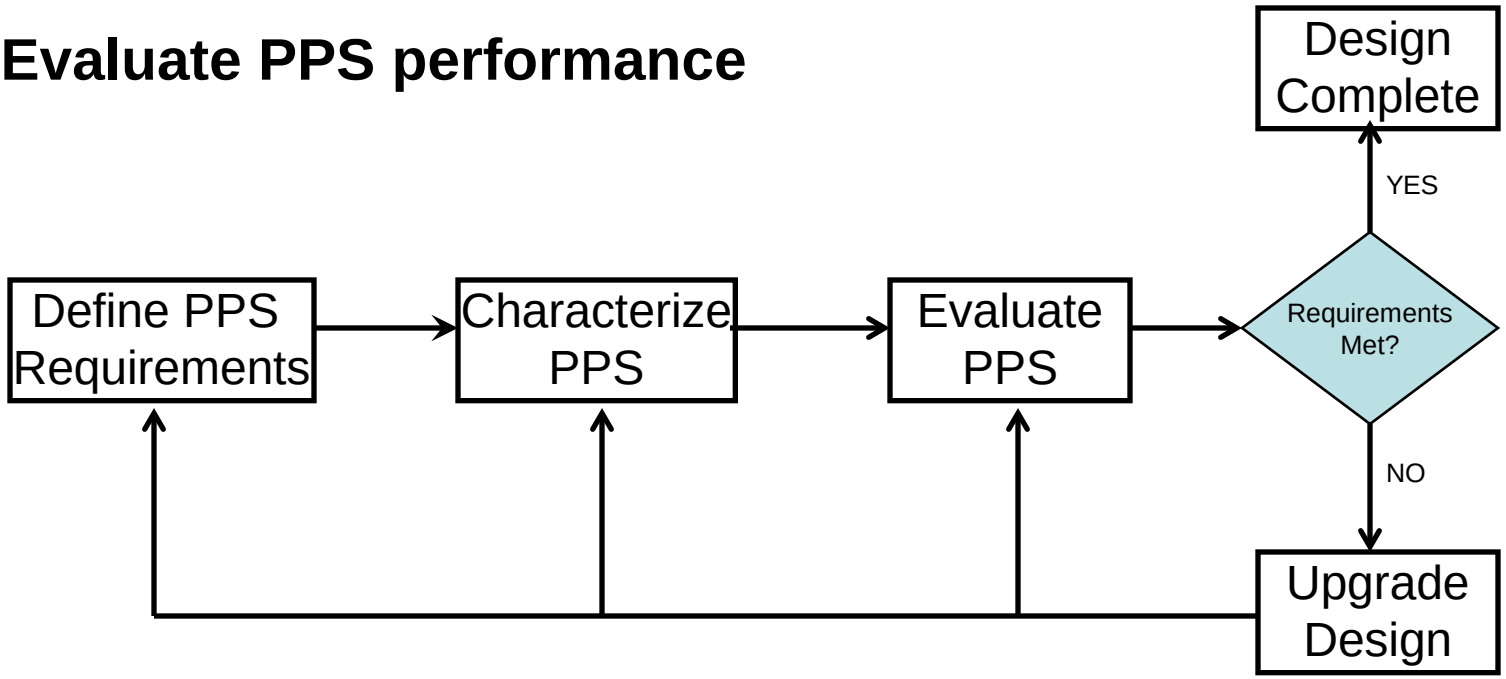
Establish document control and protection measures

Conduct Phase of VA

Define PPS requirements

Characterize PPS

Evaluate PPS performance



Define Requirements

Characterize facility

Identify targets

- Quantities and types of materials
- Vital areas

Determine design basis threat

Establish required system effectiveness level

Characterize PPS

Identify protection elements

- Detection
- Delay
- Response

Conduct site inspection

Review system design documentation

Conduct interviews of facility personnel

Validate data

Evaluate PPS Performance

Path analysis

- Facility model
- Protection element performance data
- Path analysis tools
- Most vulnerable paths

Neutralization analysis

- Expert judgment
- Computer simulation tools
- Force-on-force exercises
- Response force effectiveness

Scenario analysis

- Assess ways adversary could defeat protection elements
- Consider a variety of credible attack scenarios
- Tabletop analysis

Closure Phase of VA

Assess upgrade alternatives if required

Develop conclusions and recommendations

- Accept existing system
- Upgrade PPS
- Eliminate targets
- Mitigate consequences
- Accept risk

Prepare report

Summary

All nuclear programs are subject to the risk of malicious acts of theft and sabotage

Physical protection specialists focus on increasing system effectiveness to reduce risk

Vulnerability assessment is a structured process used to ensure that physical protection systems provide adequate protection

Path Analysis

Japan Vulnerability Assessment Seminar
January 20-21, 2009

Presentation Content

Adversary path definition

The principle of timely detection and the critical detection point

The use of the adversary sequence diagram in path analysis

Single-path and multipath methods for estimating probability of interruption

Adversary Path

An adversary path is a time-ordered sequence of physical areas and path elements the adversary must traverse to complete a theft or sabotage attack

Begins offsite

Ends when and where attack is successfully completed (Win Point)

- For sabotage attack, win point is when and where sabotage task is complete
- For theft attack, win point is when and where adversary exits the facility boundary

Timely Detection and Critical Detection Point

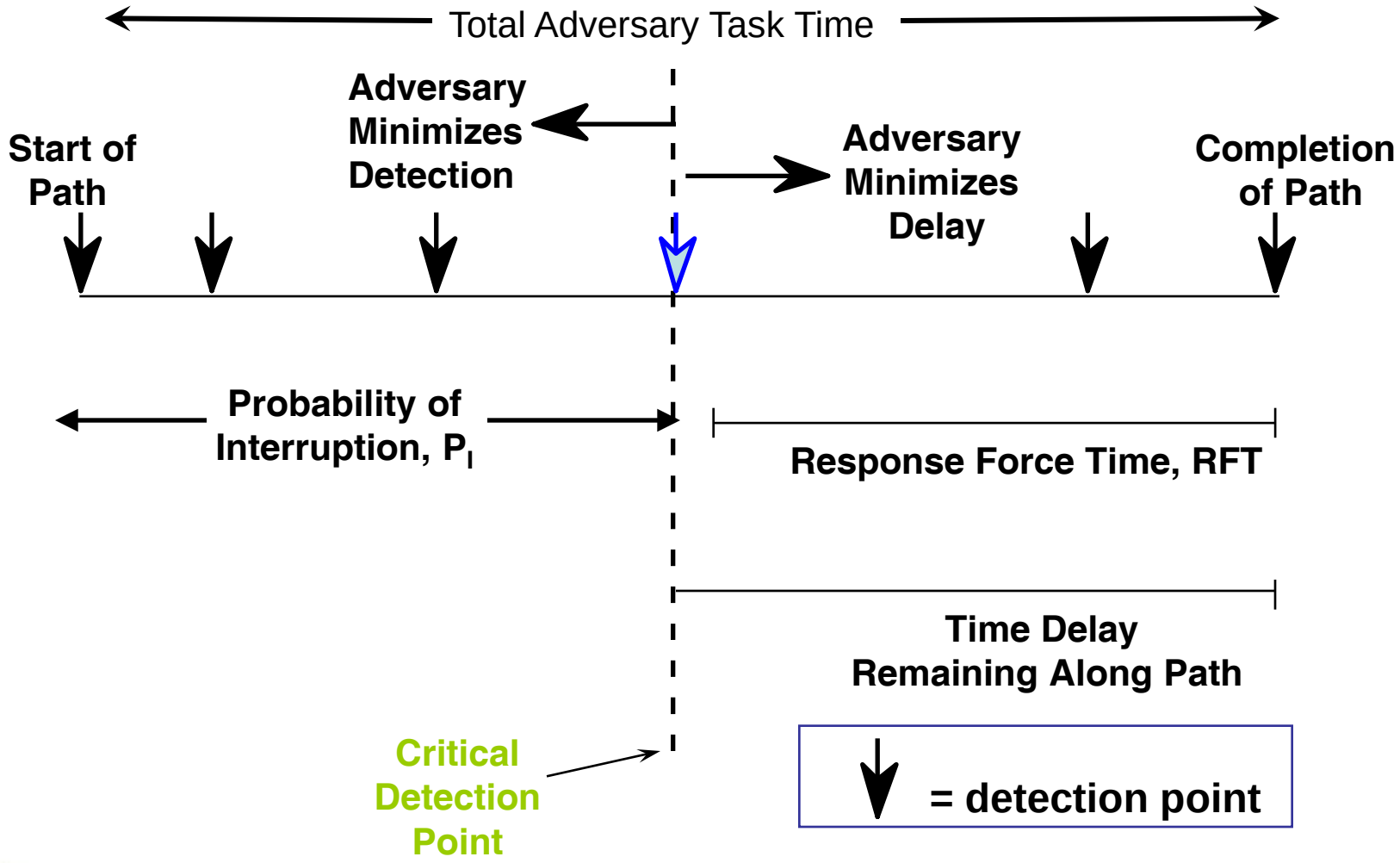
Timely Detection

- System response time must be less than system delay time after first alarm to achieve adversary interruption
  - For Design Basis Threat
  - Along all adversary paths

Critical Detection Point (CDP)

- Last detection point at which detection can occur in time for response force to interrupt adversary attack
- Last detection point at which task time remaining on adversary path is greater than response force time

Timely Detection and Critical Detection Point



Adversary Sequence Diagrams (ASDs)

ASD: *a graphical model used to help evaluate the effectiveness of the PPS at a facility*

ASD represents

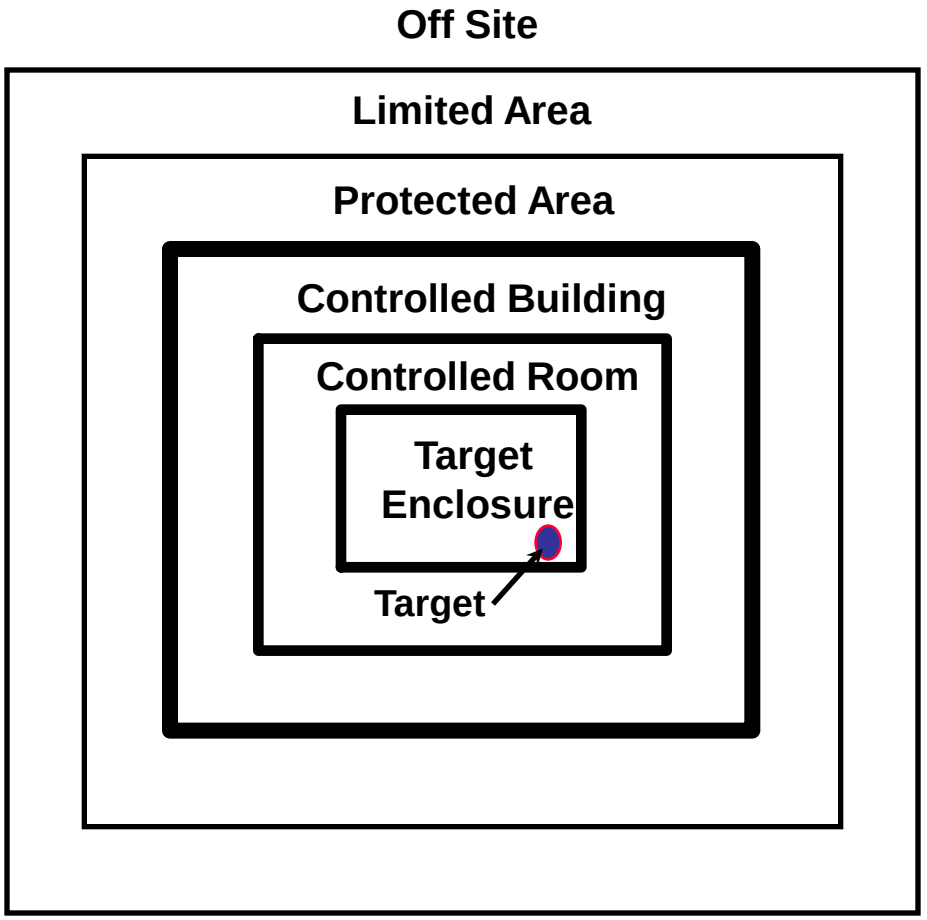
- Paths that adversaries can follow to accomplish sabotage or theft
- PPS elements along paths

ASD is used to determine the most vulnerable path for specific PPS and threat

Three Steps to Create an Adversary Sequence Diagram (ASD)

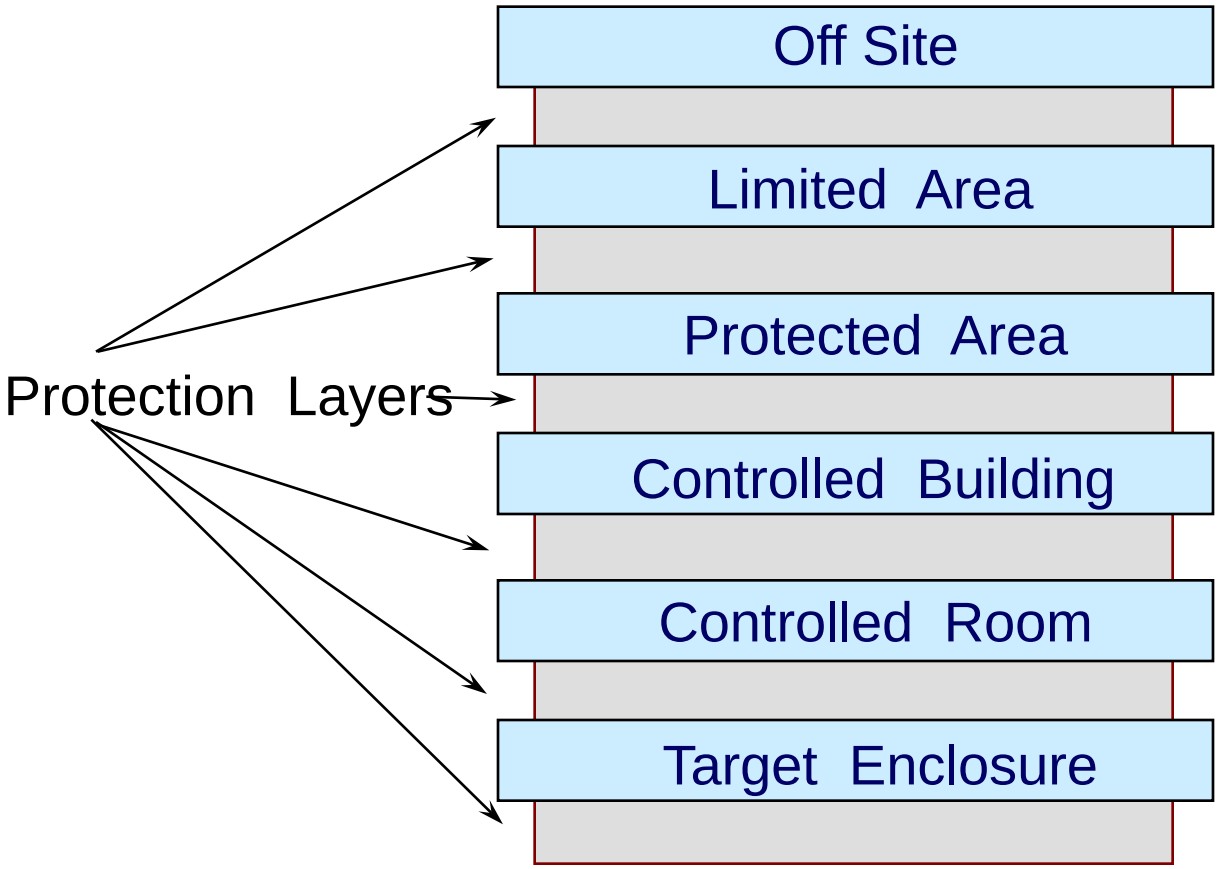
1. **Model the facility by separating it into adjacent physical areas**
2. **Define protection layers in terms of path elements between areas**
3. **Assign probability of detection (P_D) and delay time (T) for each path element and physical area**

Facility


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

Step 1: Identify Physical Areas of Facility

Step 2: Define Protection Layers of Facility

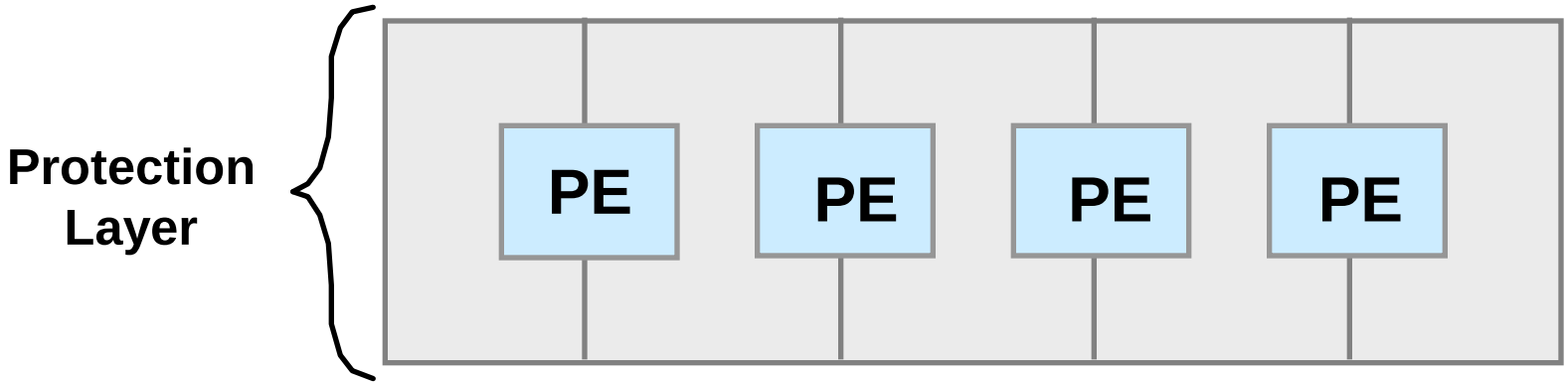


Step 2 (continued): Identify Path Elements (PEs)

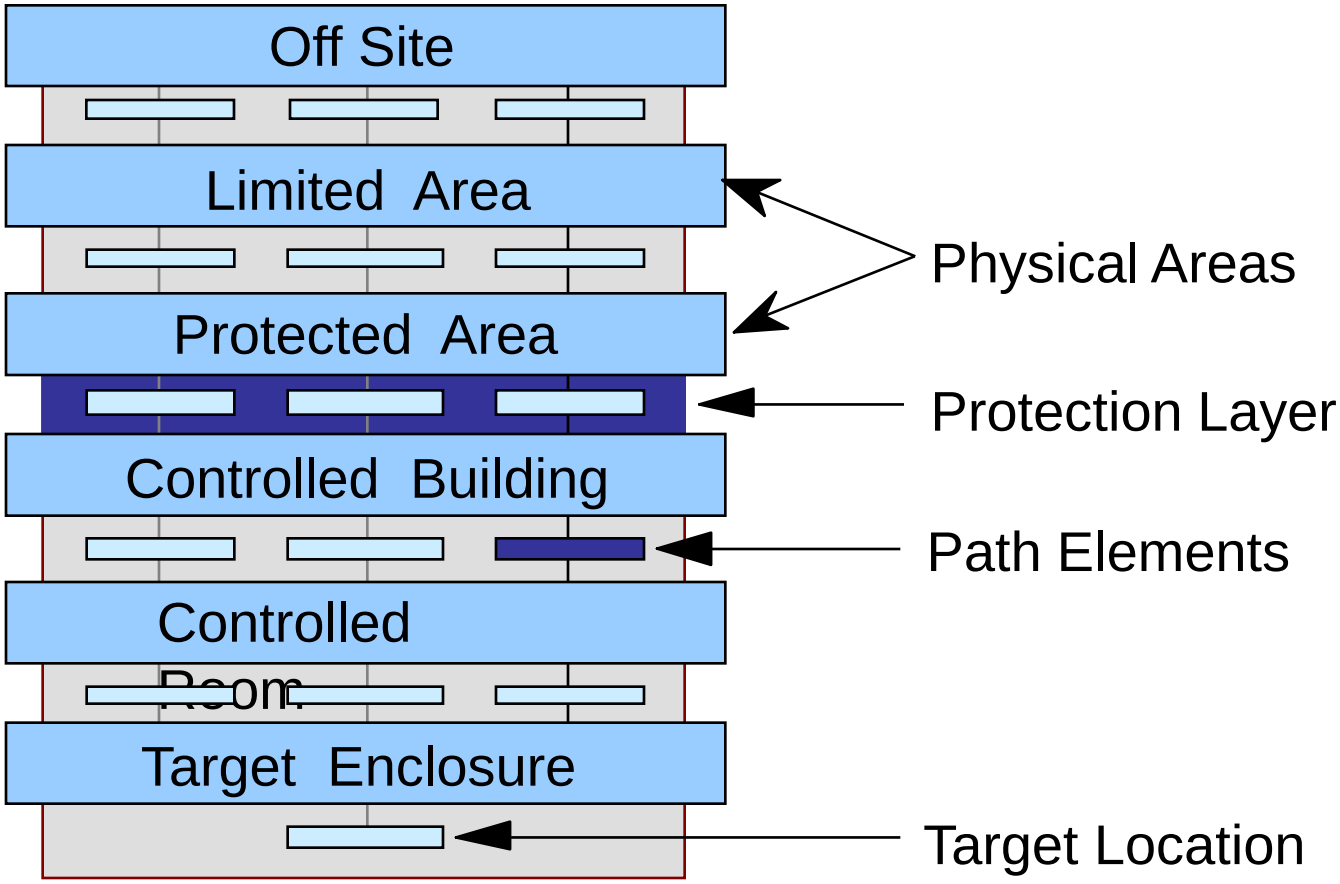
Each protection layer forms a security barrier that separates two physical areas

Path element: *any distinct part of the protection layer separating two physical areas*

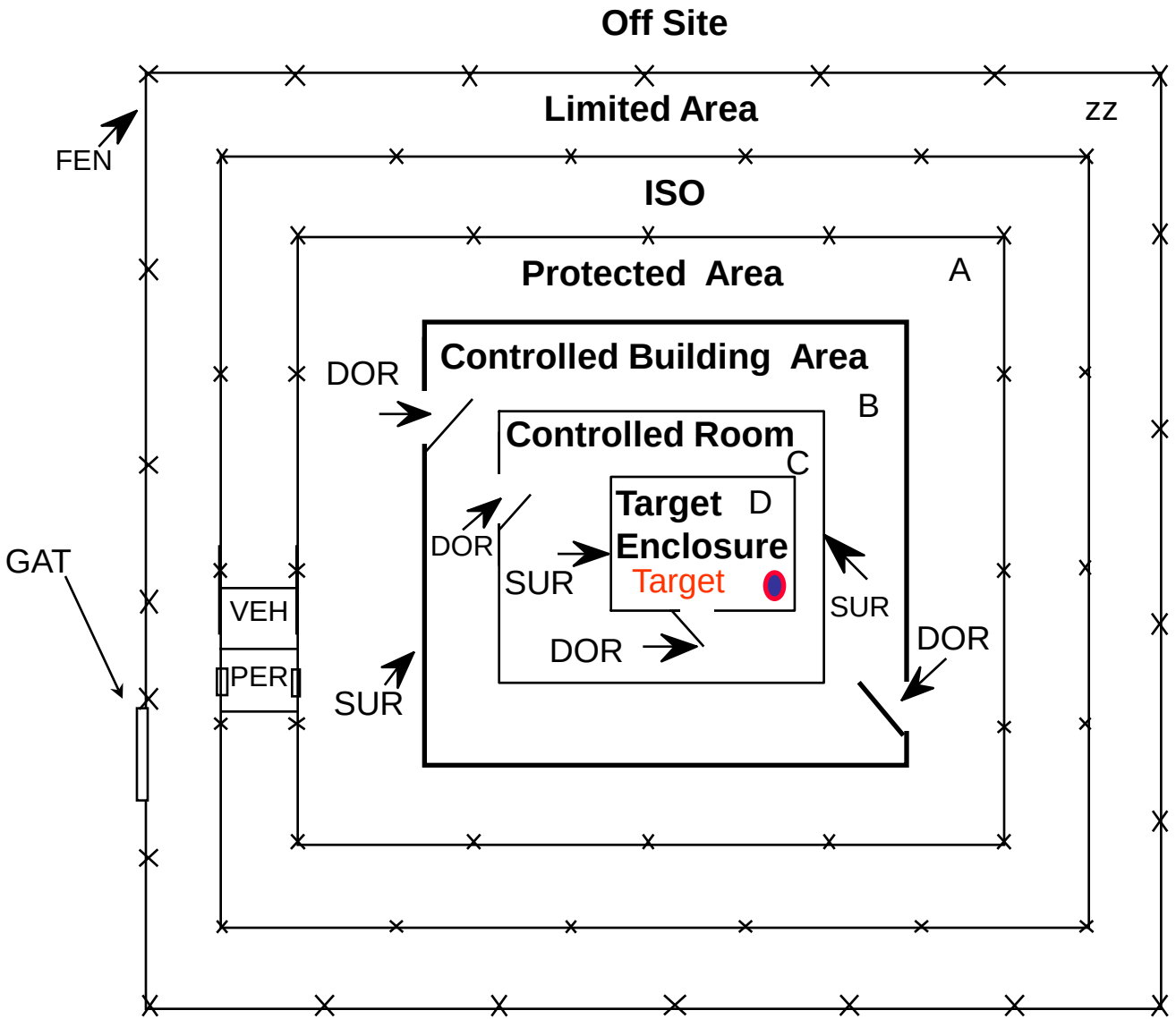
An adversary must pass over, under, around or through a PE to move between adjacent physical areas



Concept of Adversary Sequence Diagram

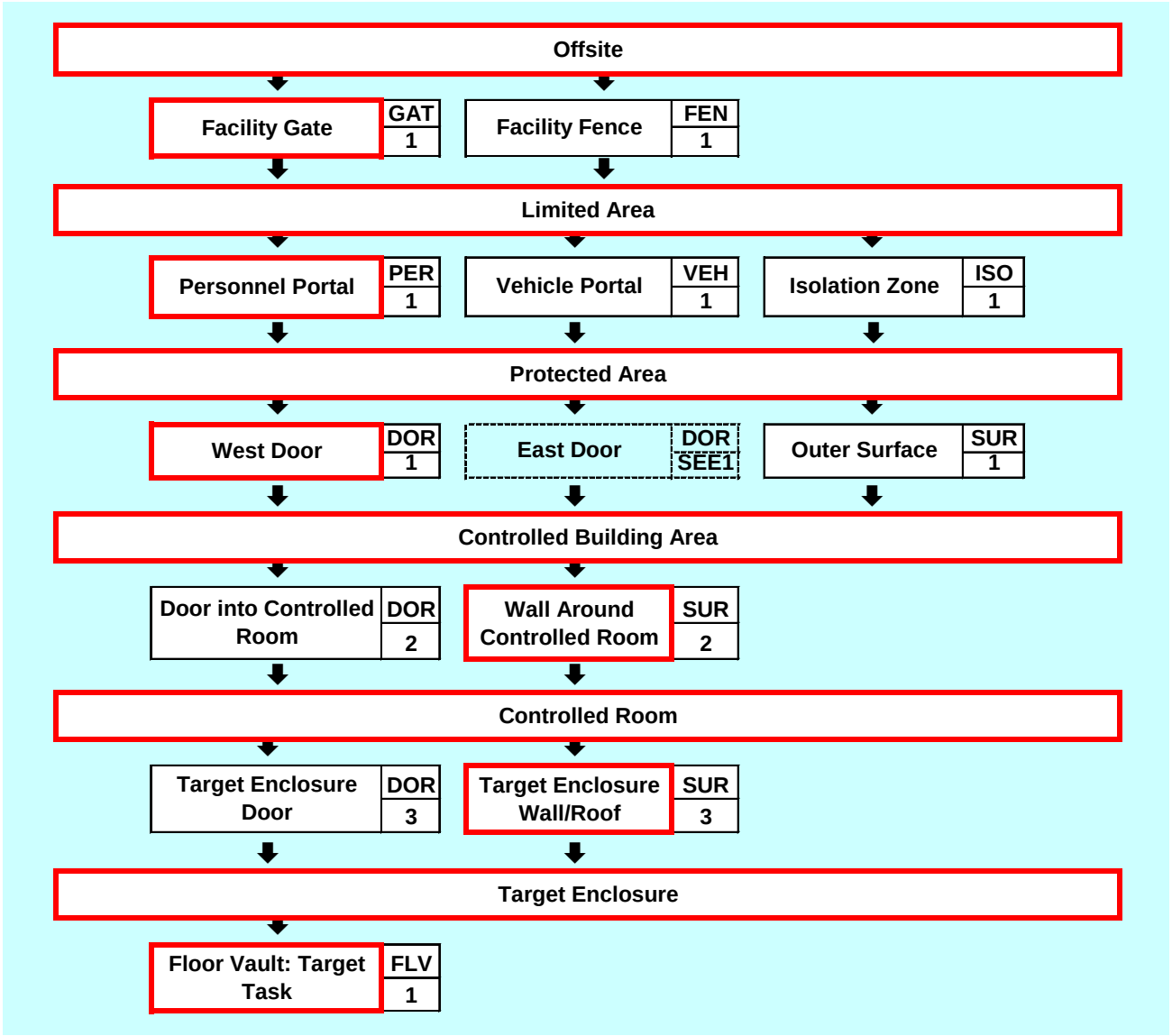


Sample Facility



Completed Site-Specific ASD for Sample Facility

Example Path



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 SNM Detection
- Determine minimum delay time
  - Barriers
  - Security Officers
  - Locks
  - Tasks

Physical areas

- Determine minimum P_D
  - Intrusion Detection
  - Human Surveillance
- Determine minimum delay time
  - Security Officers
  - Transit Time

Path Element Example

DOR 1 characteristics

- 10 cm wood door with metal sheeting
- Balanced magnetic switch position sensor

Attack scenario

- Force attack
- Power tools, explosives

Path Element Data

Door penetration time: 30 sec

Component Type	Component Description	No Equipment (sec)	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: 0.8

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

Physical Area Example

Protected Area Characteristics

- 30 meters minimum distance from isolation zone to building
- Random patrol by guards

Attack scenario

- Force attack
- Power tools, explosives

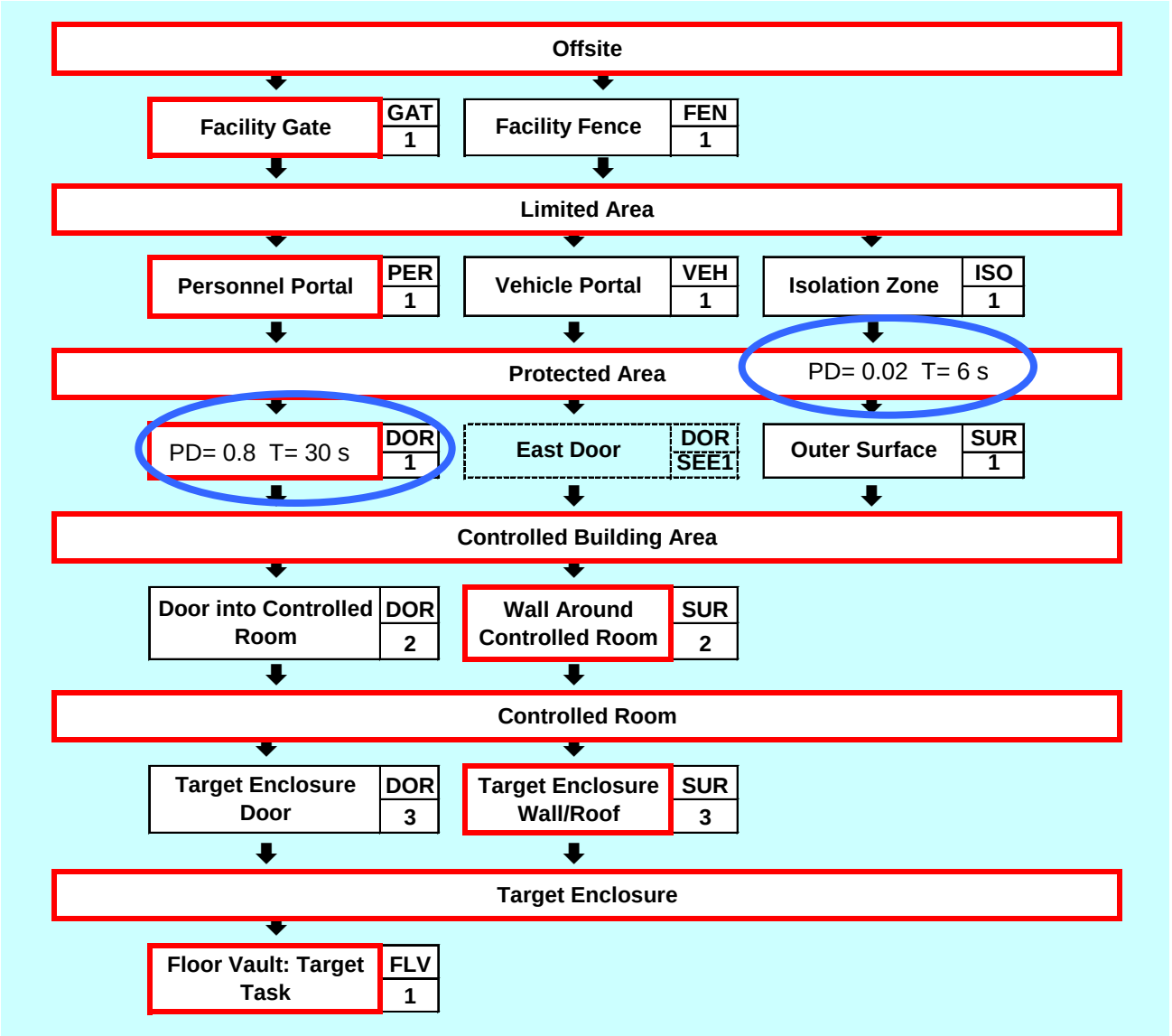
Physical Area Data

Transit time: 6 sec (5m/sec running)

Probability of detection: 0.02 (SO 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)
SO on Patrol	Random				2
	Scheduled				1

ASD with Example Data Added



Selecting the "Worst" Path and Computing P_I

Start at Win Point

Work backward through the ASD selecting the path element with the least delay time at each protection layer and adding the delay times

Once the total delay time is equal to or greater than the response force time (CDP), select the path element with the least detection probability at each protection layer out to the start of the path

The worst path traverses the minimum probability of detection path elements up to the CDP and the minimum delay path elements from the CDP to the Win Point

Accumulate (combine) probabilities of detection along this "worst path" up to, and including, the CDP to get the "probability of interruption" (P_I) along this path

$$P_I = 1 - (1-P_1)*(1-P_2)*\ldots(1-P_n)$$

Path Analysis Tools

Single Path Analysis

- Simple spreadsheet models available (EASI, VEASI)
- Provides quantitative estimate for overall system performance
- Analyst must specify adversary strategy for each path element and enter appropriate P_D and delay data
- Addresses only a single path

Multipath Analysis

- Multipath computer tools available (SAVI, ASSESS, MPVEASI)
- Finds the most vulnerable paths
- Determines best adversary strategy at each path element
- Provides efficient sensitivity analysis

Session Summary

An adversary path is a time-ordered sequence of physical areas and path elements the adversary must traverse to complete a theft or sabotage attack

CDP is the last detection point at which detection can occur in time for response force to interrupt adversary attack

ASD is a graphical model that represents all paths adversaries can follow to carry out attacks – used to find most vulnerable paths

Single-path and multi-path methods are used to quantitatively evaluate overall system performance

- Provide estimates of probability of interruption
- Address “worst” paths (smallest P_I)
- Computer models available

Scenario Analysis

Japan Vulnerability Assessment Seminar
January 20-21, 2009

Presentation Content

Definition of *scenario analysis* and *scenario* in the context of evaluating PPS performance

Steps in scenario analysis

Method for creating scenarios

Relationship of scenarios to paths from path analysis

What Scenario Analysis Is

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

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

Definition of Scenario

Scenario: A detailed description of the adversary attack that should include

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

For scenario analysis to be of maximum value, scenarios should be:

- Feasible
- Credibly generated and conducted by threats within the Design-Basis Threat
- Internally consistent
- Intellectually honest
- Well documented

Purposes of Scenario Analysis

To provide a basis for confidence about PPS performance

To help create "robust" security plans to match and fully use the capabilities of the PPS design

How?

- Develop details of realistic adversary attack plan
  - Specific, coordinated tasks and timeline for all attackers
- Develop detailed characterization of how PPS and response should behave, based on performance testing and site plans
- Simulate how PPS and response behave in face of attempted plan

IMPORTANT: *Overall physical protection system effectiveness is represented by physical protection effectiveness for a few specific scenarios*

- No attempt to determine worst-case scenario

Steps in Scenario Analysis Methodology

The methodology has the following general steps:

1. Identify the key questions
   - How effective is our PPS?
2. Identify major drivers – sort by controllable / uncontrollable
   - Numbers of adversaries, tactics, state of response force
   - State of PPS

- Collect necessary site data:
  - Performance test results
  - Detection and delay values developed for the path analysis
  - Detailed security plans and procedures

Steps in Scenario Analysis Methodology

The methodology has the following general steps: (Continued)

4. Follow a structured approach to create a range of scenarios
   - Formal: Use experts as attack planners (limit site knowledge)
   - Informal: Create internally when experts not available
5. Assess the system effectiveness, P_E, against the scenarios using
   - Subject Matter Experts (includes criteria-based assessments)
   - Simulations
     - Tabletop analysis
     - Computer simulations
     - Force-on-Force exercises and performance tests
6. Document results and conclusions along with scenario descriptions

This presentation focuses on step 4 while a later one explains how to perform tabletop exercises

A Structured Approach to Creating Scenarios

Identify site vulnerabilities across various operational conditions and states

Determine how an adversary would exploit promising vulnerabilities – Build scenarios

Review and select final plans/scenarios based on criteria

Identify site vulnerabilities across various operational conditions and states

Consider different

- Operational conditions (operational versus non-operational)
- Target material configurations (reactor load-out versus operations)
- Response force alert levels and personnel “crews”
- Different upgrades

Sources of vulnerabilities

- Experts
- Path analysis
- Previous vulnerability studies and performance tests

Develop how an adversary would exploit promising vulnerabilities

Create a list of essential tasks that have to be accomplished for the attack to succeed

1: Enter building XYZ

2: Collect 20 Kg of U235 in storage containers

3: Leave site with material without pursuit by response forces

4: Arrive undetected at safe house in city ABC

5: Hold off responding units so that steps 1-3 are accomplished

Create a sub-plan describing how a team of attackers can perform each task within resource constraints

- Who is involved?
- What are they doing as a function of time?
- How are they performing each step?
- What equipment are they using?
- How are they transporting the equipment?

For promising vulnerabilities (continued):

Combine sub-plans into a master attack plan/scenario description, adjusting sub-plans to

- Meet overall DBT and other constraints
- Achieve synchronization between teams

Achieving synchronization requires planning so

- Teams can coordinate their progress at key steps (e.g., the point of detection)
- Task time estimates are reliable
- Surprises (e.g., chance encounters with security or site personnel) are limited

Lack of synchronization can result in failure of the attack

Review and select final plans/scenarios based on criteria

Are analysis objectives covered that we want covered?

- Are conditions and states covered adequately?
- Have we addressed several means of adversary approach from the set {on foot, in land vehicles, on water, or by air} that apply, based on the Design-Basis Threat (DBT)?

Are paths credible, credibly generated and conducted by threats within the DBT, etc.?

Relationship to Paths from Path Analysis

Path Analysis can suggest sub-plans that serve as the main or "direct" part of the attack (direct in the sense of going to the target)

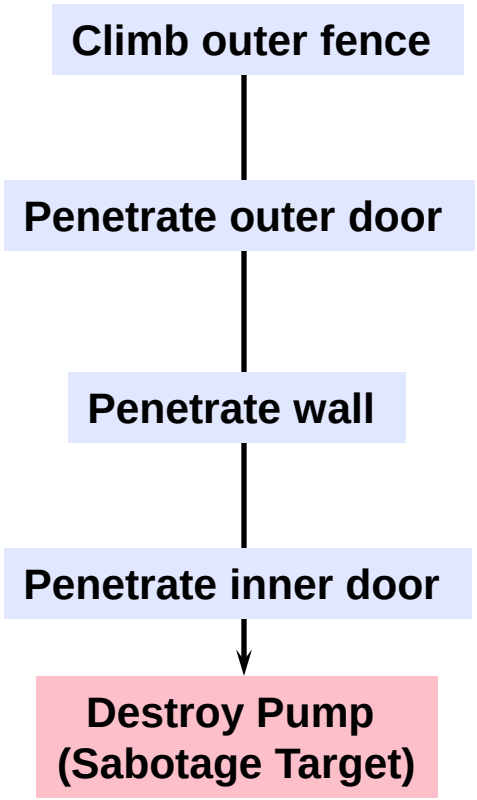
- Start with minimum delay, minimum P_I, or minimum P_I*P_N paths
- Add scenario details to these paths
- Add supporting team plans to assist these attackers

Be aware, though, the most-vulnerable path (MVP) from Path Analysis may not be the best basis for a scenario

- Low P_I paths should be corrected with upgrades during path analysis
- After such upgrades, the MVP should now have a high P_I rendering that path less desirable
- At this stage scenario analysis can consider factors not found in path analysis: preventing neutralization and employing other teams to prevent interruption

Building a Scenario Around a Path Description

Path Description



Scenario details (Adversary)

Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during storm, last adversary monitors radio traffic
Two adversaries penetrate door using burn bar, avoid sensor activation.
Two adversaries penetrate wall using linear shaped charge at night during storm.
Two adversaries penetrate door by manually removing hinges to inhibit sensor activation
Two adversaries destroy pump with linear shaped charge. All adversaries retreat.

Adding Supporting Team Sub-Plans to Scenarios

Employ other support teams to complete other essential tasks or to aid the main team

- Often, the remaining tasks look like: “Hold off responding units so ...” or “Neutralize offsite response...”

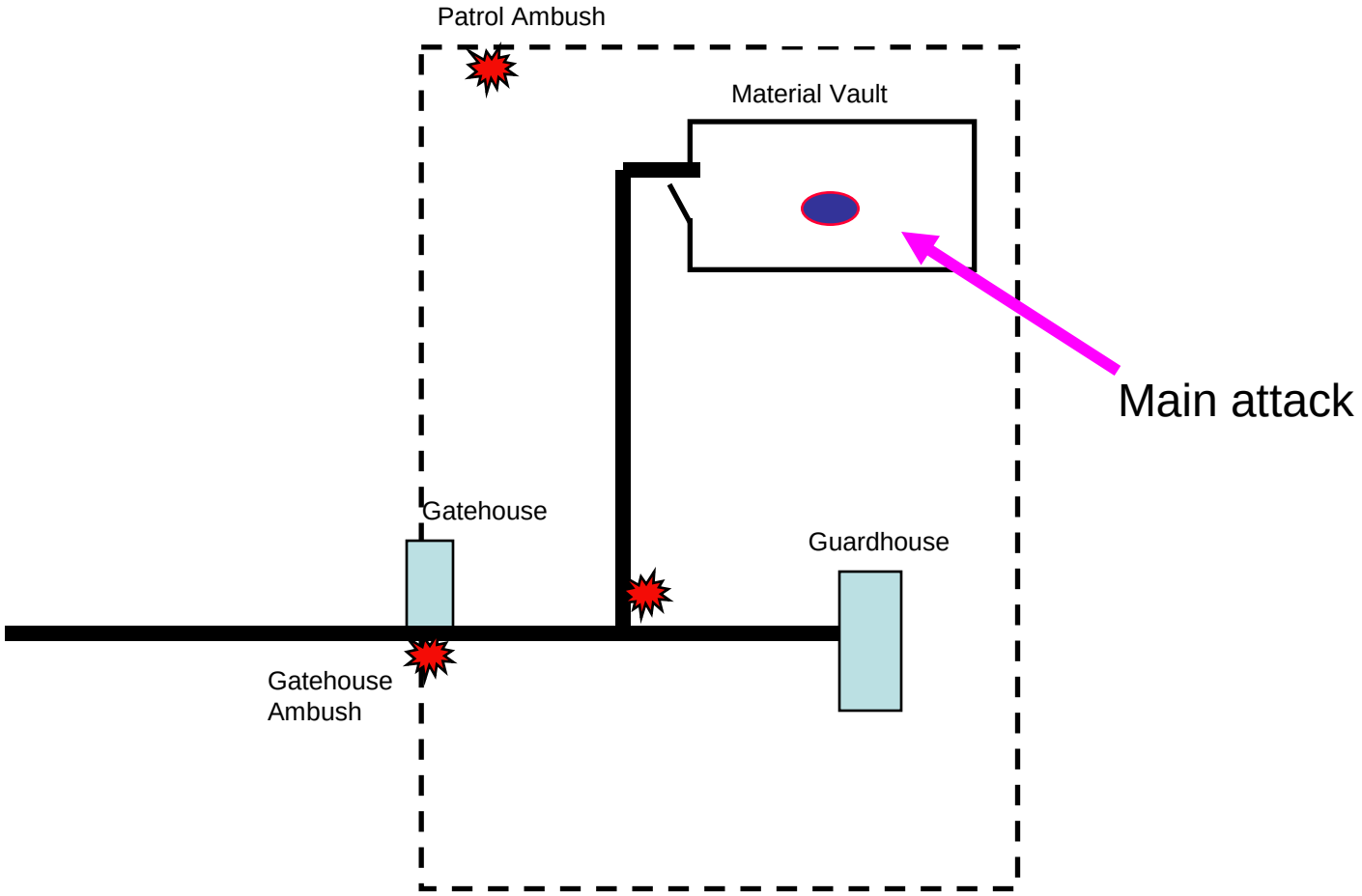
Use support teams to delay or incapacitate response

- Ambush
- Diversion, confusion

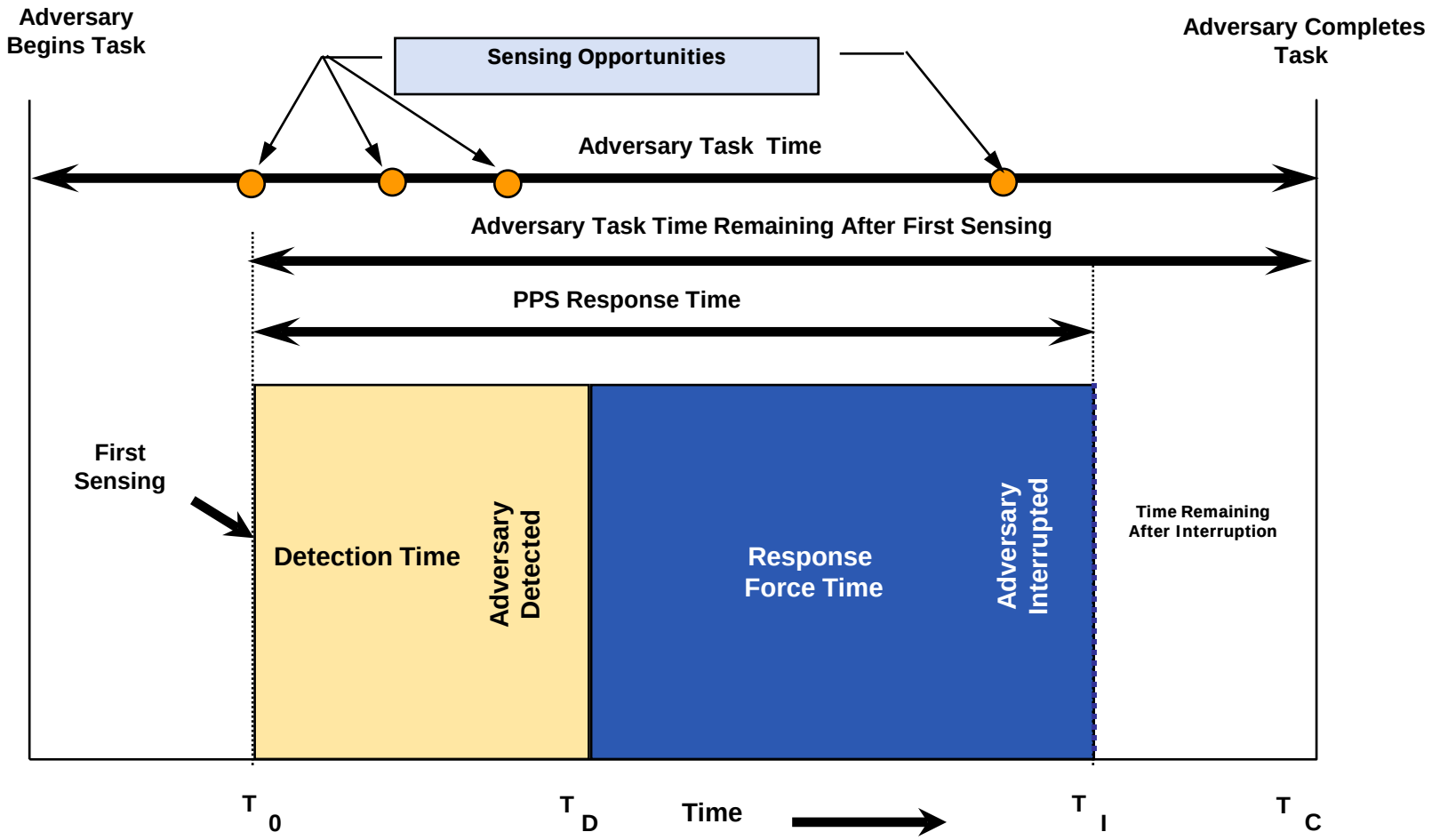
Inside colluders allow other options

Expert opinion is used to develop these scenarios

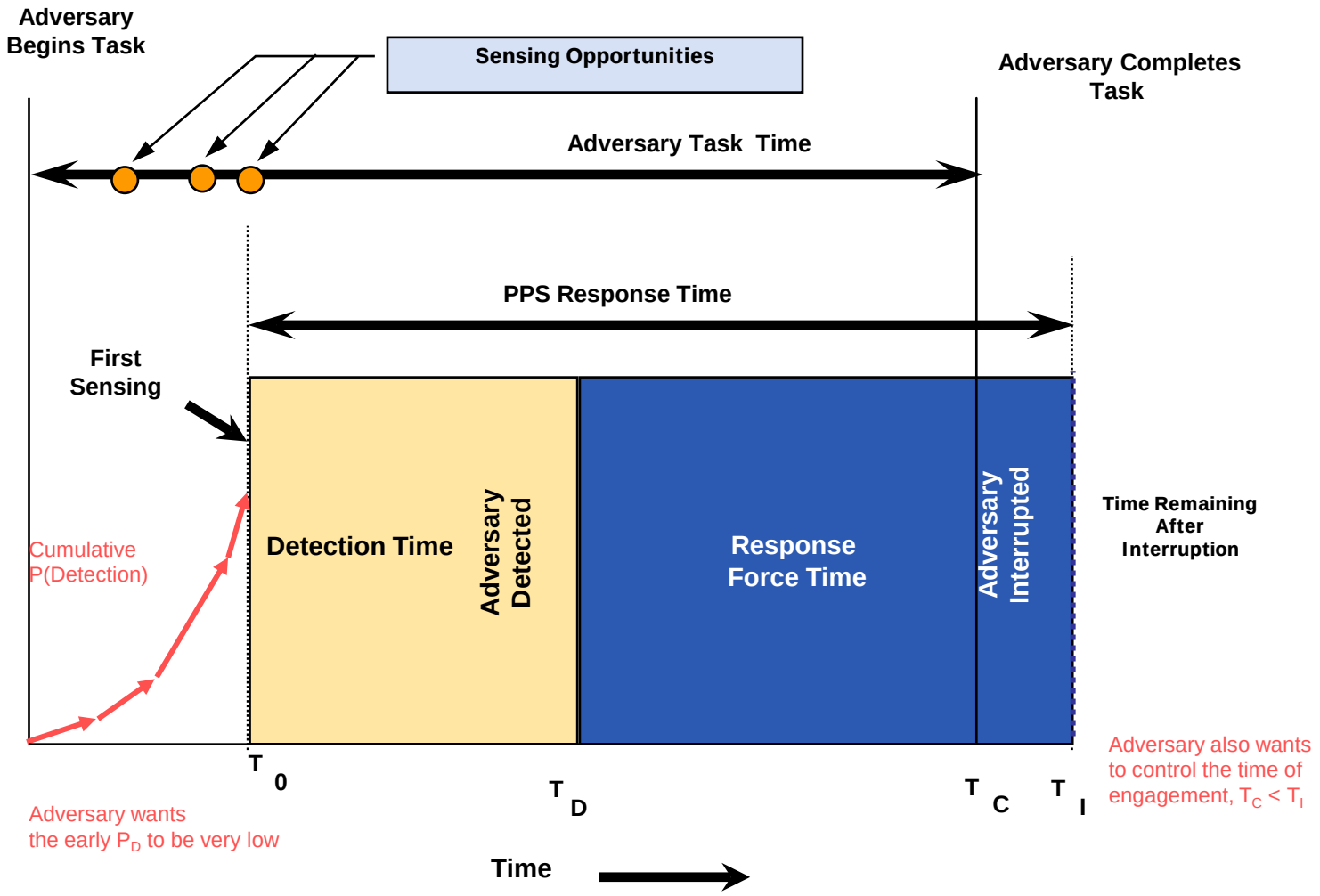
Example of Supporting Team Attacks



Adversary and PPS Timelines



Here is How You can Use the Timeline From the Adversary's Perspective for Main *and* Supporting Teams



Consider Impact of Colluding Insiders

Modify appropriate detection, delay, response force time, or response force numbers to reflect what insider can accomplish

Examples of collusion scenarios

- Detection
  - Insider tampers with alarm communication lines
- Delay
  - Insider opens vault door at time of attack
- Response
  - Insider activates an emergency alarm in a different location to divert response force
  - Insider detonates explosive at armory

Planning and Complexity Factors in Generating Scenarios

The best scenario for the adversary does not always use *all* of the equipment allowed within the design basis threat

- Not all of the equipment may provide an advantage to the attackers once training and the need to hide the attack from intelligence services is factored in
- Adding equipment may increase the complexity of the scenario

Keep this in mind when reviewing scenarios

Reasons Why Adversary Attack Plans May Fail

Early detection (before point in plan adversaries expect to be detected)

- Detection by intelligence organizations directly or by populace
- Lead-up to the attack

Non-combat failures (typically due to failure to plan and stock for contingencies)

- Logistic failures (inability to get weapons, etc.)
- Breakdowns of vehicles, communications equipment
- Exhaustion of team-members during the attack
- Tool/explosive failure to breach
- Timing and synchronization failures
- Wrong plan due to bad information

Inadequate training and rehearsal

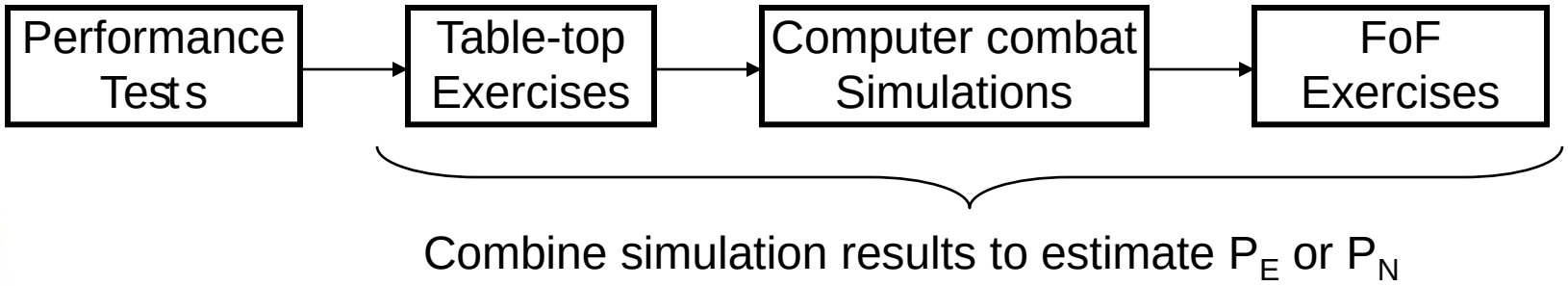
Even if adversary is not detected early *AND* there are no non-combat failures AND there is adequate training and rehearsal, the response force can also win

Performing Simulations to Determine System Effectiveness Against Scenarios

Table top exercises can be used as the simulation technique to determine P_E (qualitatively)

When have a choice of simulations, the best sequence of use is shown below

- Performance tests provide necessary input to Table-tops
- Table-top exercises can often foresee the analysis and logistic issues that will arise in computer simulations and FoF exercises
  - In some cases, issues are identified in table-tops that have to be addressed before other simulations can be performed



Summary

Scenario analysis is used to assess PPS performance against a variety of adversary attacks

Scenario is a detailed description of an adversary scenario (feasible, credible, internally consistent)

A structured process should be followed to develop scenarios that address potential PPS vulnerabilities

Path analysis results can be used to identify good scenario attack paths

Computer Simulation Tools

Japan Vulnerability Assessment Seminar
January 20-21, 2009

Performance-based approach to the design and evaluation of physical protection systems

Reference INFCIRC/225/Rev.4:

- *4.4.1. To ensure that physical protection measures are maintained in a condition capable of meeting the State's regulations and of effectively responding to the design basis threat, the State's competent authority should ensure that evaluations are conducted by operators at nuclear facilities and for transport. Such evaluations, which should be reviewed by the State's competent authority, should include administrative and technical measures, such as testing of detection, assessment and communications systems and reviews of the implementation of physical protection procedures. Such evaluations should also include exercises to test the training and readiness of guards and/or response forces. When deficiencies are identified, the State should ensure that corrective actions are taken by the operator.*

Performance Evaluation Metrics

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)

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

- Based on principle of Timely Detection and concept of Critical Detection Point
- Response force interrupts adversary task timeline

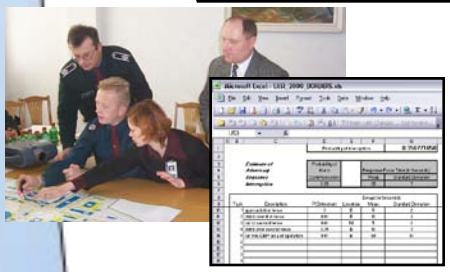
Probability of Neutralization (P_N)

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

General Evaluation Process

Timeline Analysis

Determine minimum P_I path by software or using "manual" method



Minimum P_N scenario

Overt Attack Analysis

Minimum P_E scenario

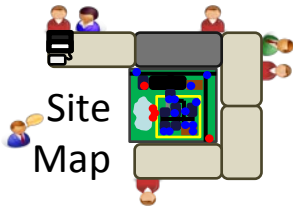
Red-Team Analysis

Manual methods

Scenarios Requiring P_N, P_E Evaluation

Scenario Analysis

- Tabletop Exercises
- Computer Combat Simulations
- Force-on-Force (FoF) Exercises



Path Analysis Computer Tools

NEED SLIDES TO BRIEFLY DESCRIBE PATH ANALYSIS TOOLS

Small force engagement computer simulation methodology

Description**: computer simulation that models entities, acquisition, targeting, and weapons' effects**

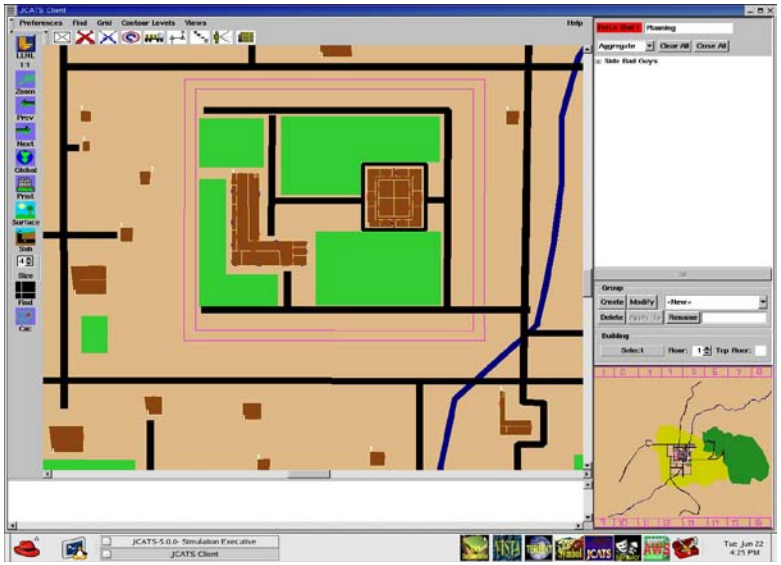
Results**: Win/loss, statistics (deaths, times of events, shots fired)**

Strengths**:**

- Well-developed methodology with established protocols
- Cheaper than Force-on-Force, without the safety and operational limitations:

Required resources**:**

- Software, classified weapons data, significant training on software
- Human in the loop: computer network with multiple workstations (~3-5 entities per workstation), 2-3 full time staff + 1=2 week runs



Tabletop exercise methodology

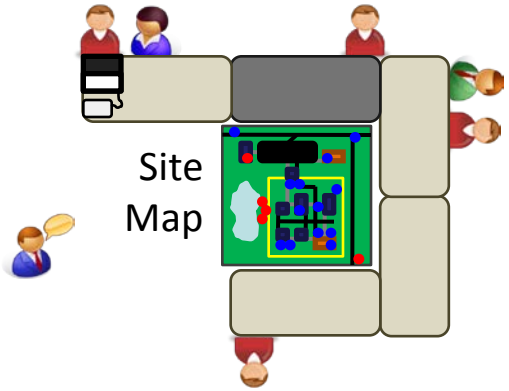
Description**: A collaborative simulation performed on a "sand-table" of a security response to an adversary attack**

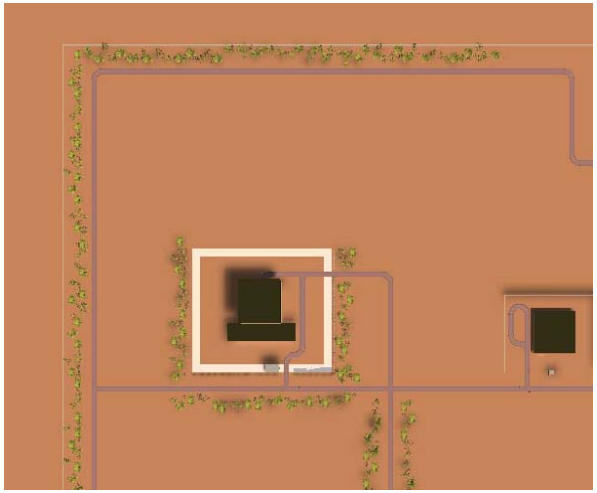
Results**: Qualitative results on outcomes, along with insight about how an attack will proceed (win/lose, casualties, timeframes)**

Strengths**: Can cover same ground as other simulations (engagement/FoF) but with less cost**

Required resources:

- Expert(s) to design attack and conduct tabletop
- Organization Representatives
- Several weeks to build scenarios, 1-3 days to run tabletop exercise





Force-on-Force (FoF) exercise methodology

Description**: Actual simulation of an attack in the field using response force, simulated adversaries, and weapon simulators**

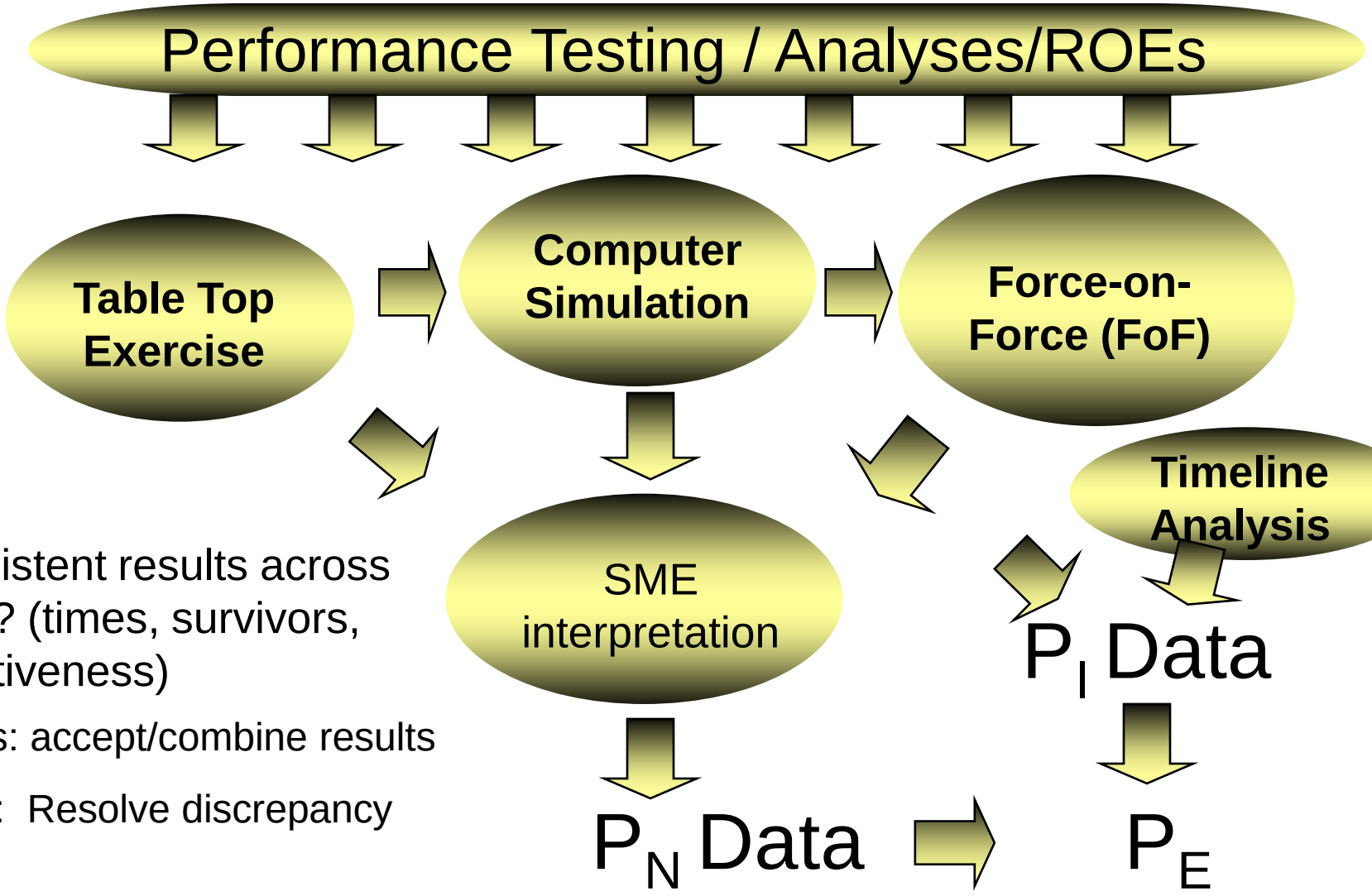
Results**: Win/loss, engagement statistics (deaths, times of events, shots fired)**

Strengths:

- Evaluates the response force's actual, not perceived, capability under stressful, realistic conditions against a DBT-based adversary
- Provides training

Required resources**: Engagement Simulation Systems (ESS), controllers, shadow-force, simulated adversary force**

Representative Process for Combining Results



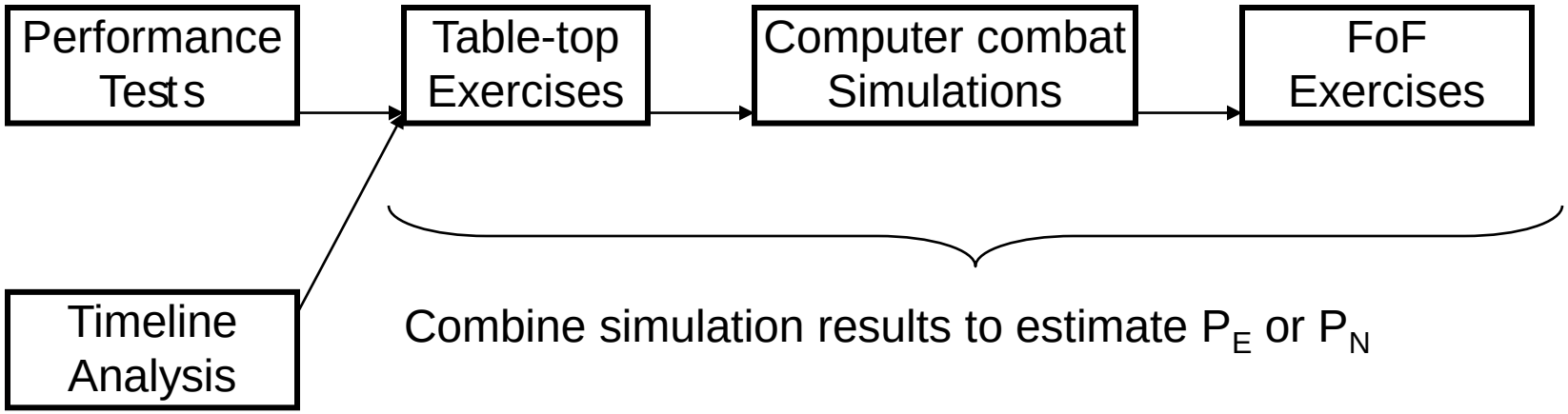
Consistent results across tools? (times, survivors, effectiveness)

- Yes: accept/combine results
- No: Resolve discrepancy

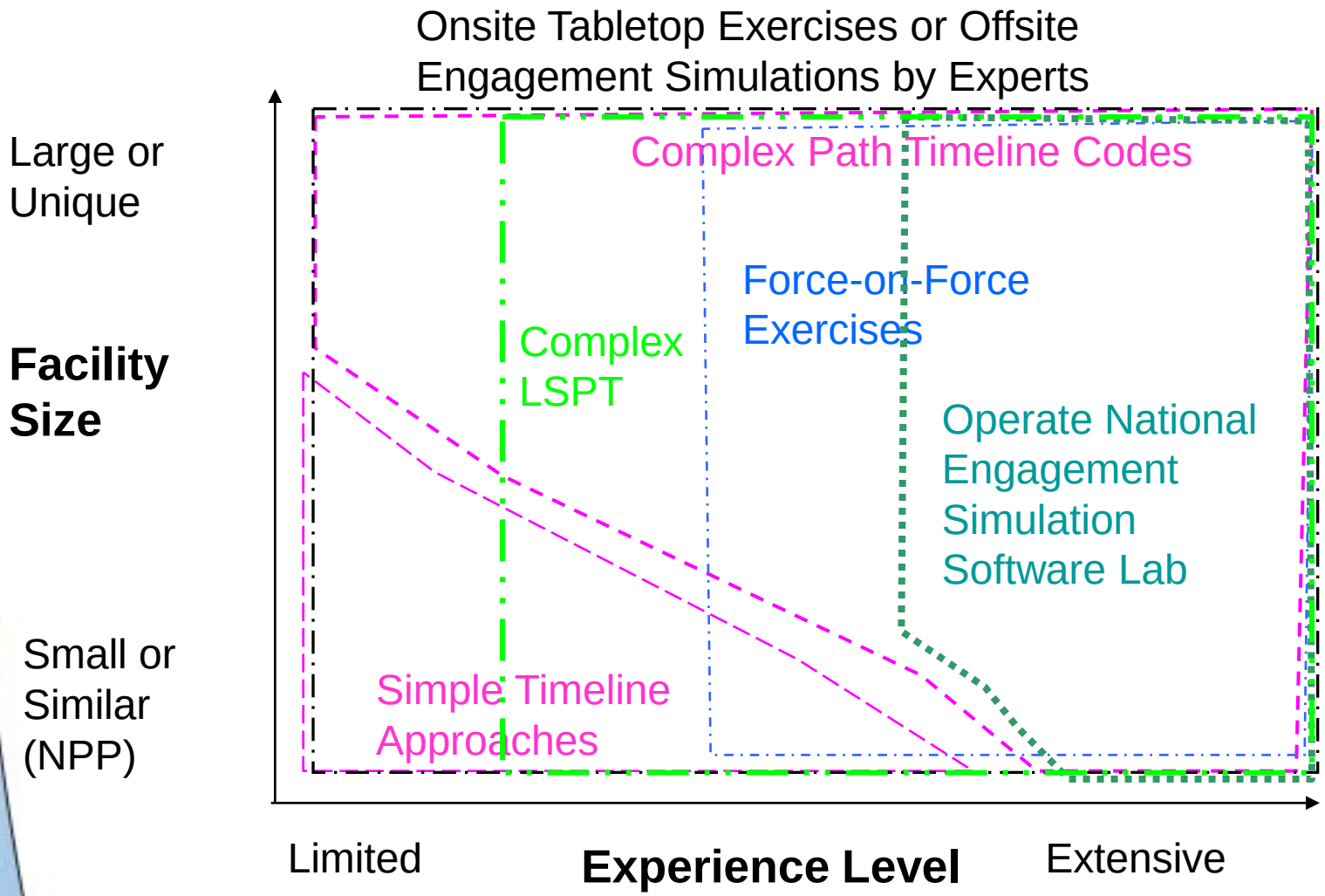
Performing Simulations to Determine System Effectiveness

When a choice of simulations is possible, the best sequence of use is shown below

- Performance tests provide necessary input to Table-tops
- Table-top exercises can often foresee the analysis and logistic issues that will arise in computer simulations and FoF exercises
  - In some cases, issues are identified in table-tops that have to be addressed before other simulations can be performed



Methodologies to use depends upon size of facility and national experience



PPS Evaluation Tools

Methodology	Source	Restrictions
Timeline Analysis		
SAVI (PI)	SNL	Take training
ASSESS (PI - Insider; PI - Outsider)	DOE	DOE Approval
VISA (PI, Expert-Assigned PN,PE)	SAIC Originally	Open Source
Tabletop methodology used in DOE/NTC	SNL	Take training
Computer Engagement Simulations		
ACATS	LLNL	Exportable; issue is data
JCATS	LLNL	Not exportable; military data
STAGE	Presagis (Canada)	Presagis software; SNL supporting files
Simajin	RhinoCorps	Code exportable; issue is data
Tabletop Exercise Simulations		
Defense Effectiveness Evaluations	SNL	US training
Transportation Tabletop Methodology	SNL	US training
Force-on-Force Exercises		
Engagement Simulation System (ESS)	Unitech	Has been exported, maybe some restrictions

Workshops and Training Courses

General Vulnerability Assessment

- Basic VA Fundamentals (how to calculate P_I, P_E)
- Performing an effectiveness evaluation (field aspects of evaluation)

Examples of More Advanced Courses

- Specialized software tools (e.g., path codes, blast effects)
- Insider protection/analysis
- Engagement simulation courses (system administration, operator)
- Performance testing, operating FoF-related equipment
- Neutralization (tabletops, engagement simulations, FoF)

Summary

INFCIRC/225 calls for PPS evaluations and performance testing

A variety of methodologies and tools are available for application

Use of a complementary set of tools is a good practice

Topical workshops and training courses are available

Tabletop Analysis

Japan Vulnerability Assessment Seminar
January 20-21, 2009

Presentation Content

Definition of tabletop exercise

- Phases of the tabletop exercise process
- Benefits and limitations of a tabletop exercise
- Other tools used in conjunction with tabletop exercises

What is a Table-Top Exercise?

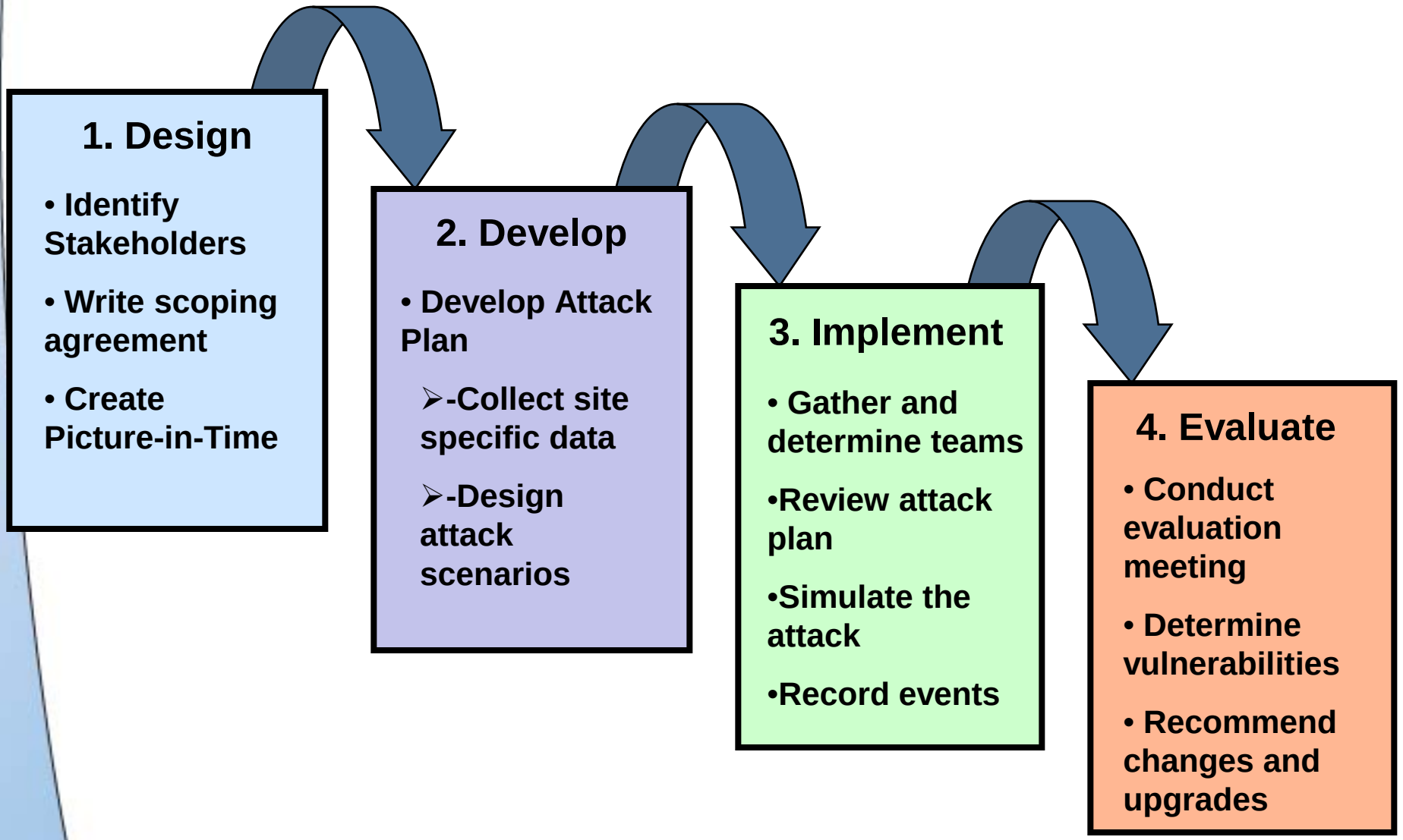
- **Tabletop exercise:** A method to simulate an adversary attack on a site's existing or proposed Physical Protection System (PPS).
- **Analyzes PPS elements:**
  - Detection
  - Delay
  - Response
- **Yields QUALITATIVE data that can stand alone or be used in other analysis tools.**
- **Results can 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 physical protection systems
  - Current and increased (postulated) threats

- **As a training tool:**
  - Identifies inconstancies in responses and site procedures
  - Maintains response force proficiency

Tabletop Exercise Process



Identify Stakeholders

- 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 amongst appropriate stakeholders that identifies the parameters of the tabletop exercise.

Define requirements

Threat Statement (DBT, ACL)

Facility Characterization

Target ID (type of targets)

Identify credible SME's for attack planning

Types of attacks & numbers of scenarios

- Sabotage/ theft

Identify & agree to assumptions

Evaluate effectiveness of site's PPS

Determine Type of Insider (Passive/Active, etc.)

MOU w/ LLEA or government

Review security posture

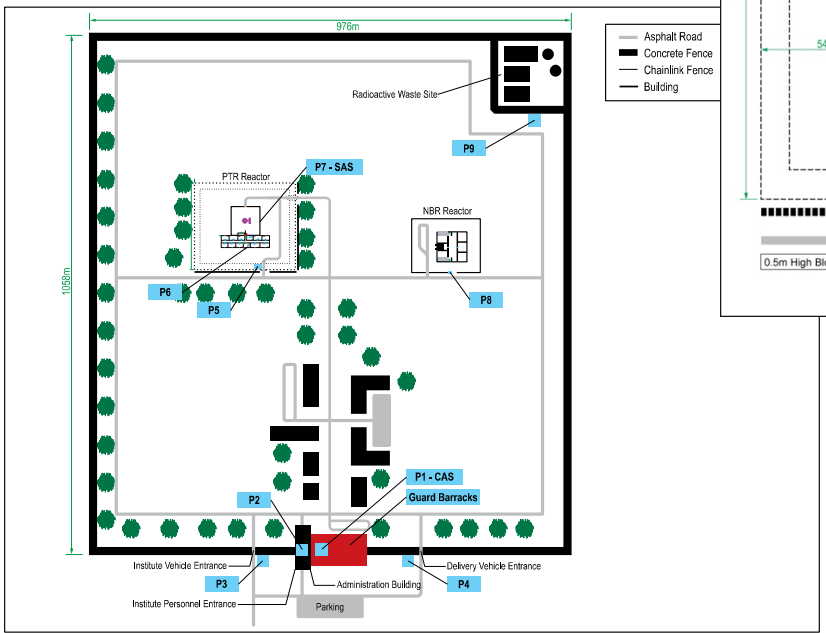
Determine PIT (PF)

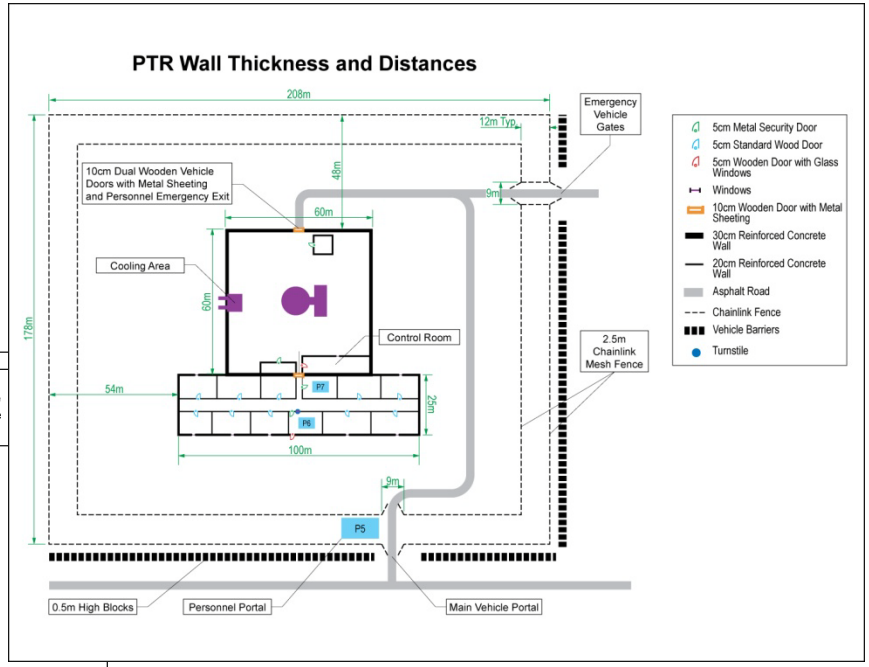
1. Design

Security Force Picture-in-Time

Picture-in-Time provides the team with:

- Security Emergency Response Plan
- Post and Patrol
  - Locations
  - Activities
  - Equipment Status
  - Numbers





1. Design

Attack Planning

A. Collect site specific PPS Data

- Passive Insider Information.
- Site Surveillance
- Outside Sources (Internet, Libraries, etc.)

2. Develop

Attack Planning

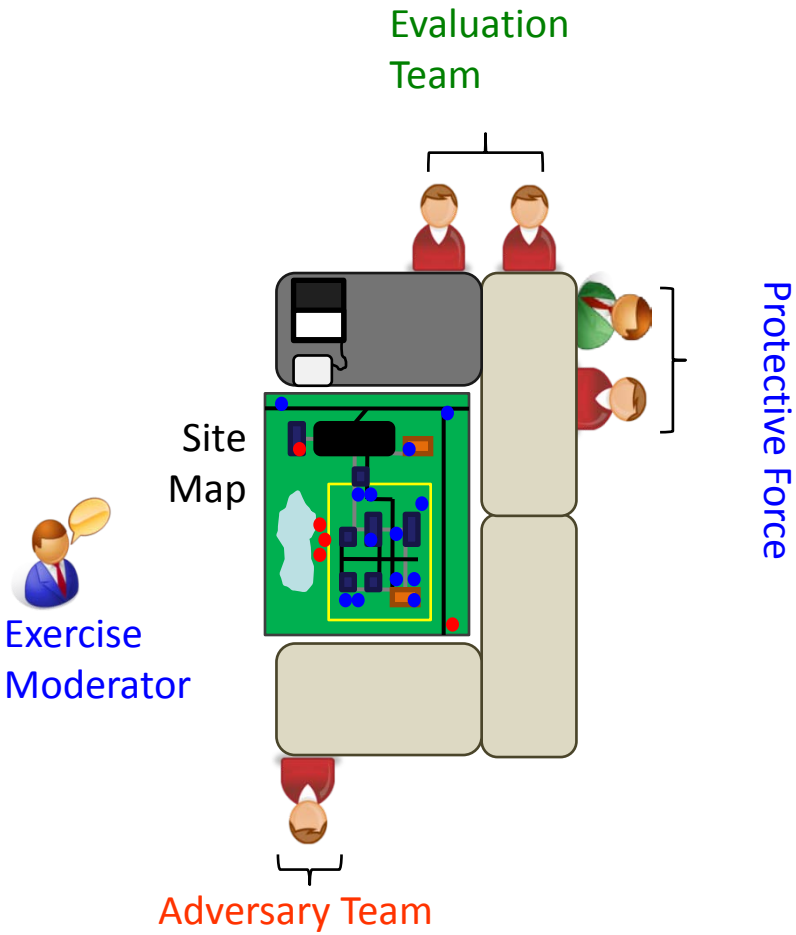
B. Design attack scenarios

- Utilize DBT
- Determine how to get adversary team from offsite to the target
- Identify least path of resistance, least detection/delay
- Identify inclement weather
- Identify time of adversary attack (day or night)
- Identify state of facility (operational/non-operational hours)
- Identify target selection
- Identify breaching techniques

2. Develop

Implement Tabletop

- **Gather all necessary participants**
- **Determine teams**
  - Blue = Protective Force
  - Red = Adversaries
  - Green = Evaluation team and Exercise Moderator
- **Review necessary information including:**
  - Facility and PPS
  - Types of attacks, # of scenarios
  - Attack plan steps and timeline
  - Adversary team briefs the attack plan



3. Implement

Implement Tabletop

- **Critical Event:** Any event that requires attention and resources to overcome (detection, delay, critical engagement).
- **Critical Engagement:** An engagement that occurs between the protective force and the adversary along the adversary attack path.
- **Simulate the attack against PPS**
  - Identify each critical engagement using Picture-In-Time
  - Determine outcome of each critical engagement
  - Document engagements, vulnerabilities, outcomes, performance test issues, etc.

3. Implement

Simulate the Attack

- **Begin at the start of the timeline, before the initial point of detection or engagement**
- **Work through the timeline until the first point where detection, contact, or engagement may occur**
  - The Adversary timeline and Security Force PIT are overlaid and any potential detection, contact, or engagement are played through
  - Determine chance-based outcomes with random number generator (dice, pull number out of hat)
- **Assess and record the critical event (who, what, when, where)**
- **Adjust the timeline and participant status and move forward to the next step in time**
- **Continue simulation until the critical event**

NOTE: **Find and Fix**. It is encouraged to stress the PPS as long as the attack plans are reasonably credible.

3. Implement

Evaluation Meeting (1 of 2)

- **Evaluation meetings are held with appropriate stakeholders and participants after the exercise has been completed.**
- **Evaluate and determine:**
  - response force casualties
  - access to target
  - duration of engagement
  - mitigation measures
  - performance testing concerns
  - response discrepancies
  - vulnerabilities, where exploited

4. Evaluate

Evaluation Meeting (2 of 2)

Possible discussion points are:

- key attack points, scenarios considered but not used
- system changes that would have affected the attack scenarios
- ranking of vulnerabilities
- possible upgrades, acceptance, and downgrade options

Output of the evaluation meeting:

- Vulnerabilities identified and documented
- Recommendations for changes and upgrades

4. Evaluate

Benefits

Tabletop exercises are beneficial because they:

Are Simple

Are Cost effective

Require minimal resources (unlike force on force and computer simulations)

Focus on scenarios that are most attractive to adversaries.

- Incredible, relatively risky, and unproductive adversary strategies are weeded out by experienced Adversary Team and Exercise Moderator

Readily handle difficult-to-simulate technologies and tactics

Analyze small system changes more effectively

- No time spent rebuilding computer models or resetting people

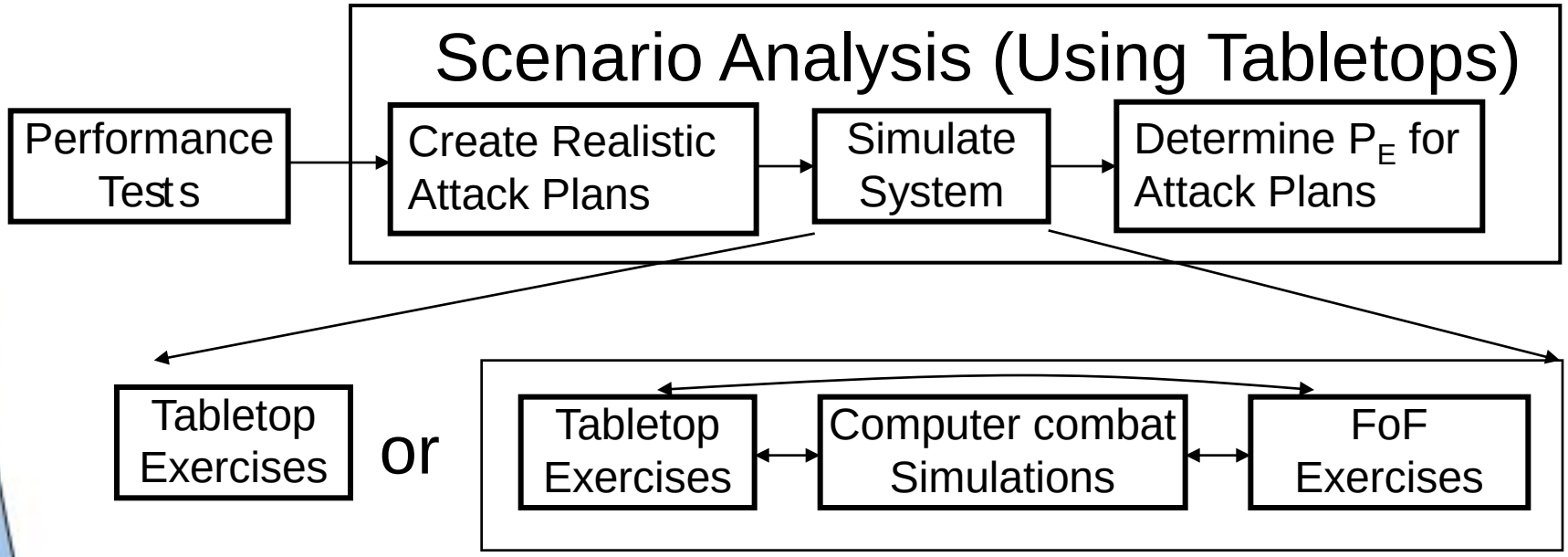
Produce results that stand-alone or can be used with other tools

Limitations

- **Tabletop exercises are interactive but not real-time simulations.**
- **It is typically difficult to obtain a credible and experienced individual to represent the adversary force planner.**
- **The quality of the tabletop depends upon both the professional judgment of those that participate, and upon Subject Matter Experts (SMEs) in a variety of fields.**
- **There is presently no official published protocol document to describe rigor and utilization of a tabletop.**

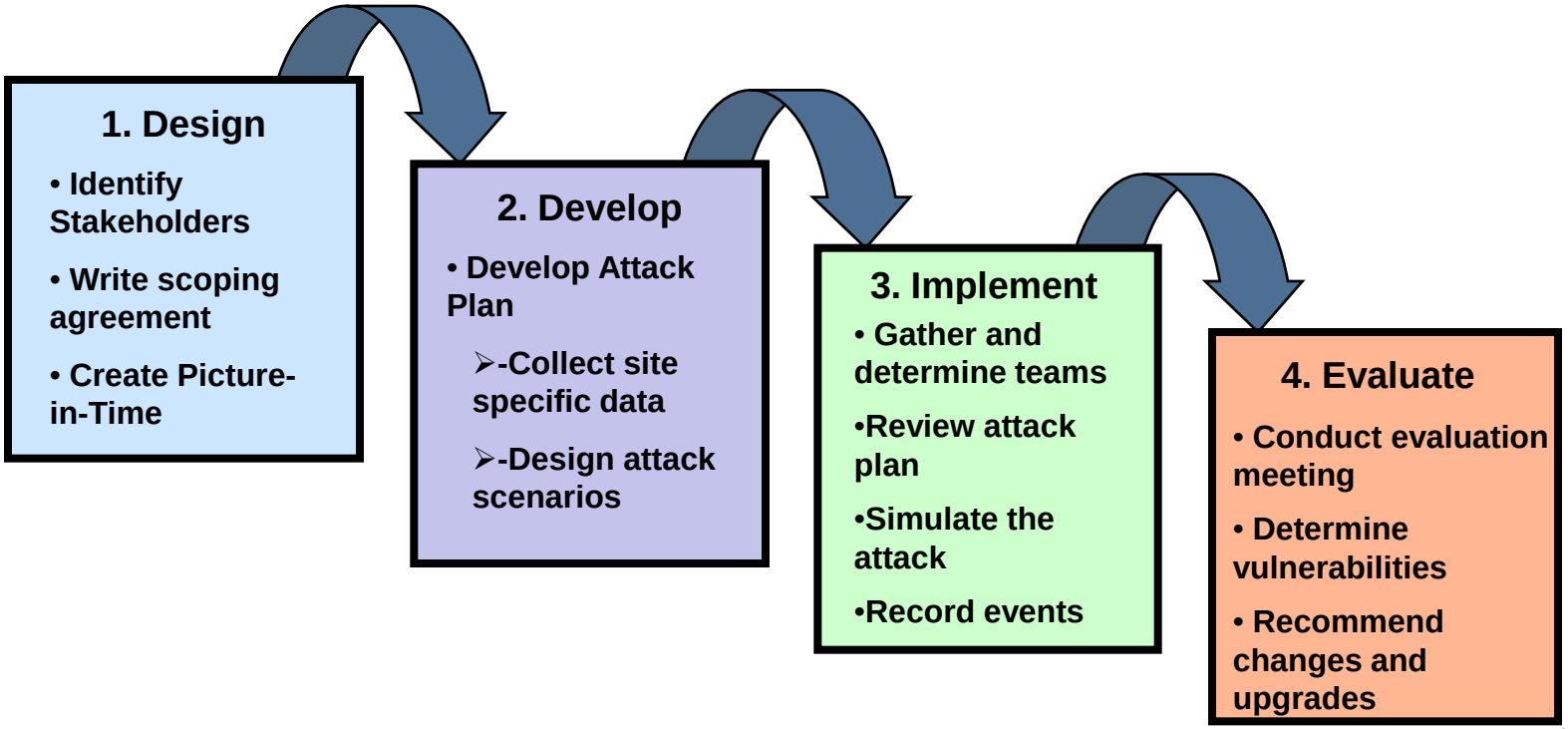
Other Tools

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



Summary

- A tabletop exercise is a method to simulate an adversary attack on a site's existing or proposed PPS that yields qualitative data, measures and improves security system effectiveness, and establishes a rationale for risk-acceptance.
- Tabletops are beneficial because they are simple, cost effective and require minimal resources.



Regulatory Approaches

Japan Vulnerability Assessment Seminar
January 20-21, 2009

Presentation Content

- **Risk management concepts**
- **Acceptable risk determination**
- **Performance-based and prescriptive physical protection system requirements**

Security Risk Equation

Based on these concepts the classical security risk equation becomes:

- $R = P * C$
- $R = P_A * P_S * C$
- $R = P_A * (1 – P_E) * C$
- $R = P_A * (1 – P_I * P_N) * C$

Thus the more effective the physical protection system (the higher the value of P_E) then the lower the risk

Vulnerability assessment is used to estimate system effectiveness and ensure that it is adequate

Risk Management

Risk management is the process of identifying and applying measures that reduce or mitigate the risk of an undesired event

- Physical protection is an element of risk management
- Physical protection systems are intended to reduce the risk of theft or sabotage

Security Risk Management

According to the security risk equation, security risk management or risk reduction can be accomplished in three ways:

- Reduce the likelihood of an adversary attack, P_A
- Increase the effectiveness of the physical protection system, P_E
- Reduce the severity of the consequences should an attack succeed, C

$$R = P_A * (1 - P_E) * C$$

Reduce P_A

The only direct way to reduce P_A is to detect and stop the adversary prior to an attack:

- Improve threat assessment

The three risk factors probably have some interdependence:

- An adversary may seek a softer target if the physical protection system is overtly robust (deterrence)
- An adversary may seek an alternate target if the material is not attractive for theft or sabotage

This factor is difficult to quantify

Increase P_E

Physical protection measures can be enhanced to increase P_E

- Increased effectiveness against a high level threat is expensive
- State and regulator must determine how much can be spent on security vs. how much risk can be accepted

P_E can be estimated and quantified

- Focus of this seminar is on methods used to estimate physical protection system effectiveness

Reduce C

Potential adverse consequences are related to:

- For theft, material attractiveness
- For sabotage, material attractiveness and facility design

There are some options for control and modification of the material attractiveness and facility design factors to reduce potential consequences

Mitigation can reduce real consequences if the adversary attack is successful

Material Attractiveness

Material attractiveness is based on how easily the material can be used for the adversary's malicious intent, including:

- Weight, size, and packaging
- Physical and chemical form
- Processing required to make a weapon
- Ease of dispersal

To reduce C, select least attractive material for use, storage, and transport

Facility Design

Facility design factors can significantly affect obstacles for adversary's malicious acts and affect attractiveness, including:

- Location of vital equipment
- Redundant safety systems

To reduce C design facilities to reduce the accessibility of vital equipment and to increase the effectiveness of safety systems

Mitigation

In the case of adversary success, there is the remaining possibility of reducing the consequences via mitigation, including:

- For theft, locate and recover the missing material before the adversary uses the material in a malicious act
- For sabotage, emergency management can reduce the radiation exposure and radioactive contamination or their effects

Risk Reduction Strategies

There are a number of options for risk reduction in a State's nuclear program:

- Consolidation to fewer locations
- Conversion to less attractive materials
- Final disposition of excess materials
- Cost effective physical protection systems

Acceptable Risk

Objective: reduce the risk of theft or sabotage of nuclear materials or facilities to an acceptable level

Must strike a balance between physical protection and beneficial use

The level of security should reflect the potential consequences of malicious acts: higher potential consequences imply higher levels of security

Risk-Based PPS Performance Requirements

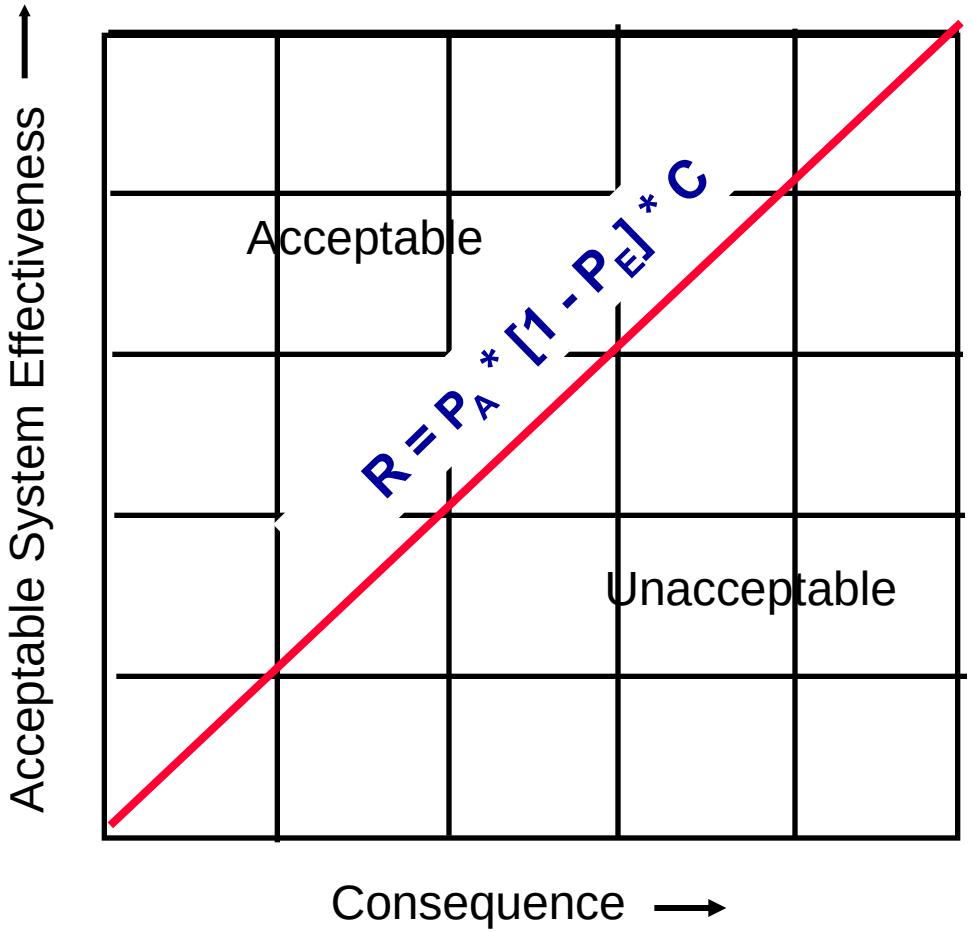
There is some level of risk that society will accept

PPS performance requirement (P_E) should be related to potential consequences of an attack to maintain risk at an acceptable level

As potential consequences increase, P_E must increase to keep risk at or below acceptable level

Competent authority may establish a minimum P_E for different types of facilities (Graded Approach)

System Effectiveness Requirements



Regulatory Requirements

The State and its Competent Authority are responsible for establishing, implementing, and maintaining the State's physical protection regime, including:

- Risk management
- Physical protection requirements
- System effectiveness, P_E
- Emergency Management

Regulatory Approaches

The State's Competent Authority has two general approaches to establishing requirements for the Licensees and verifying their compliance:

- Prescriptive approach
- Performance approach

In practice, many states use a combination of performance and prescriptive requirements

Prescriptive Approach

In the prescriptive approach, the Competent Authority specifies for the Operators what protection measures must be implemented

- Compliance by the Operator consists of implementing the required protection measures
- The Competent Authority is responsible for assuring that the required protection measures are adequate to prevent the malicious acts that are unacceptable

Performance Approach

In the performance approach, the Competent Authority specifies for the Operators the required level of system effectiveness, P_E, against a specified adversary

- Compliance by Operator consists of designing and evaluating its physical protection system to achieve this P_E
- The Competent Authority is responsible for verifying that the Operator's system satisfies the required performance against the potential adversary

Combined Approach

A combined prescriptive/performance approach might include:

Some prescriptive requirements such as:

- At least two barriers surrounding Category 1 materials
- Specified number and location of alarm systems
- Specified types of locks or other security equipment

Subsystem performance requirements such as:

- Required probability of detection for alarm systems
- Required delay for entry into vital or material access areas
- Maximum value for response force time

Overall system performance requirement

- Minimum acceptable P_E
- Approved tools and analysis methods

Summary

Security risk management can be accomplished by:

- Reducing the likelihood of malicious acts
- Increasing the effectiveness of physical protection systems
- Reducing the consequences of successful attacks

Acceptable risk

- Level of risk that is acceptable must be determined by the Competent Authority
- To maintain risk at acceptable levels, P_E must increase as potential consequences increase

Regulatory requirements generally will include a combination of prescriptive and performance measures