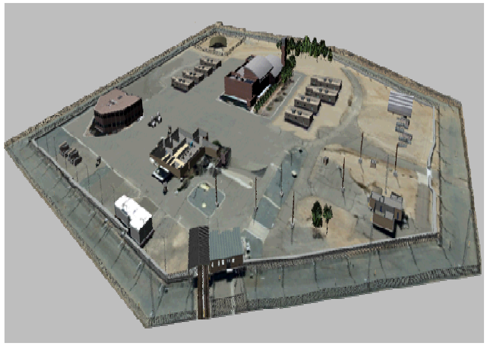
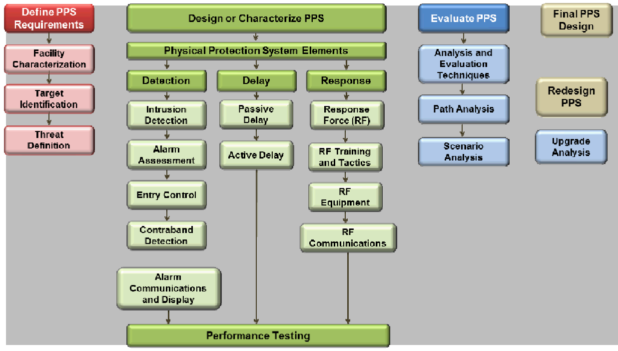
SAND2013-9779P

Sandia National Laboratories





Overview of Physical Protection System (PPS) Evaluation

Felicia A. Durán, Ph.D.
Security Systems Analysis

Korea Hydro Nuclear Power/Central Research Institute
Daejon, South Korea – November 18-22, 2013

U.S. DEPARTMENT OF ENERGY

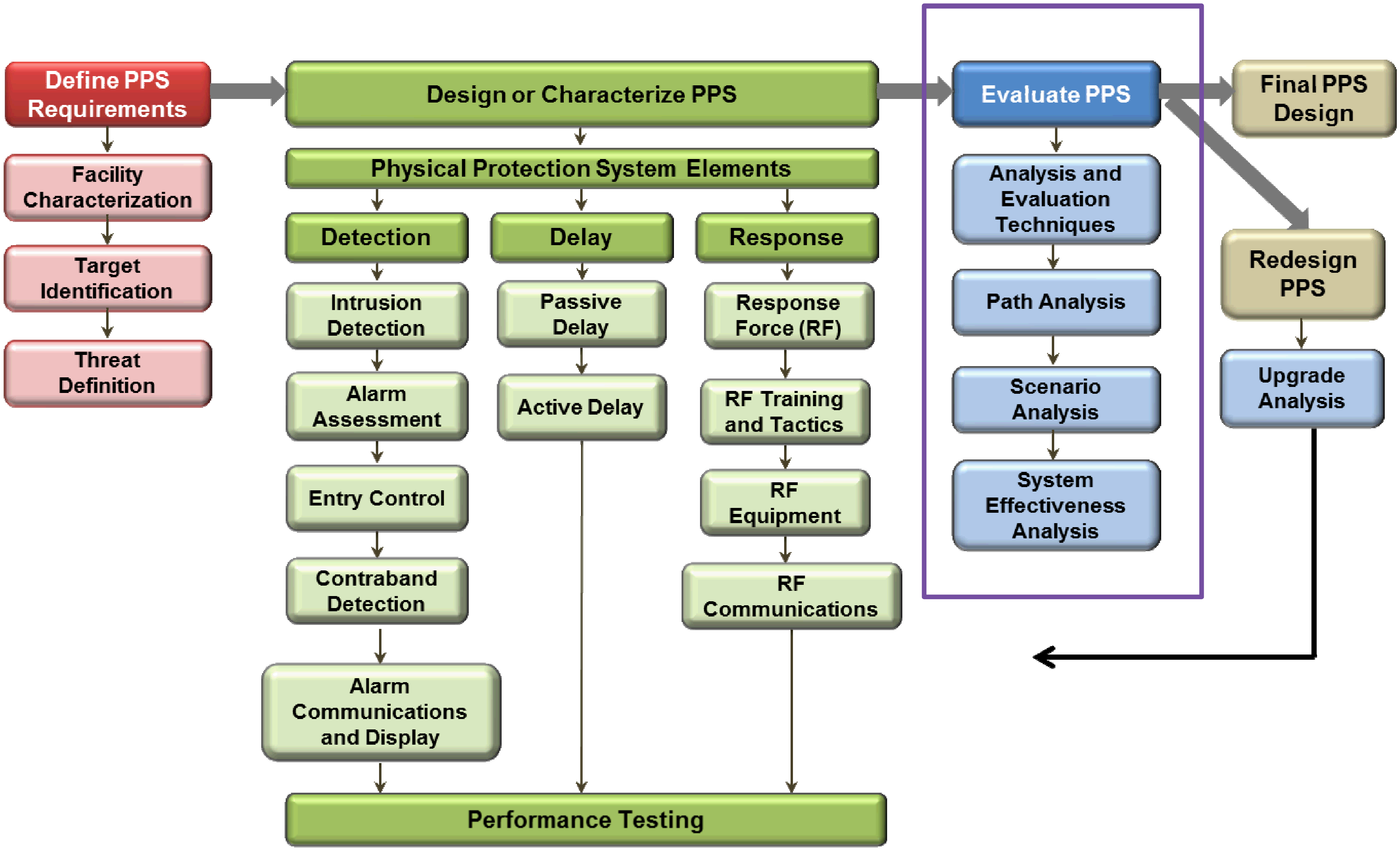
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2013-XXXX

Presentation Outline

- System effectiveness measures
  - Probability of interruption (P_I)
  - Probability of neutralization (P_N)
  - System effectiveness (P_E)
- Physical protection system (PPS) evaluation approaches
  - Performance tests
  - Interruption analysis
    - Path analysis
  - Neutralization analysis
  - Scenario analysis

Design and Evaluation Process



Evaluation of PPS

- Evaluation of effectiveness of PPS should
  - Verify that PPS satisfies requirements
  - Identify system deficiencies
  - Analyze system upgrades
  - Compare cost versus performance
  - Be repeated periodically
    - Threat may change
    - Facility and/or operations may change

Evaluation Objectives

- Competent authority / government agency and operators have complementary objectives for PPS evaluation
  - Meet regulatory and operator requirements
    - Self-assessment by operators
    - Inspection by competent authority
    - Periodic revalidation
  - Verify and/or improve PPS performance
    - Verify PPS satisfies requirements
    - Identify system deficiencies
    - Analyze system upgrades
    - Compare cost versus performance
    - Select and implement overall best option

System Effectiveness

- Probability of interruption (P_I)
  - Estimates likelihood of response force arriving before adversary completes attack
  - Estimates likelihood of response force interrupting adversary during attack
  - Based on *principle of timely detection* and *concept of critical detection point (CDP)*
- Probability of neutralization (P_N)
  - Estimates likelihood, given interruption, of response force preventing adversary from completing attack
    - Response force gains control of adversary
    - Response force must neutralize adversary following interruption for PPS to be effective
- System effectiveness (P_E)
  - Probability that the PPS will defeat the outsider threat: $P_E = P_I * P_N$
  - Probability that the PPS will defeat the insider threat: $P_E = P_I$

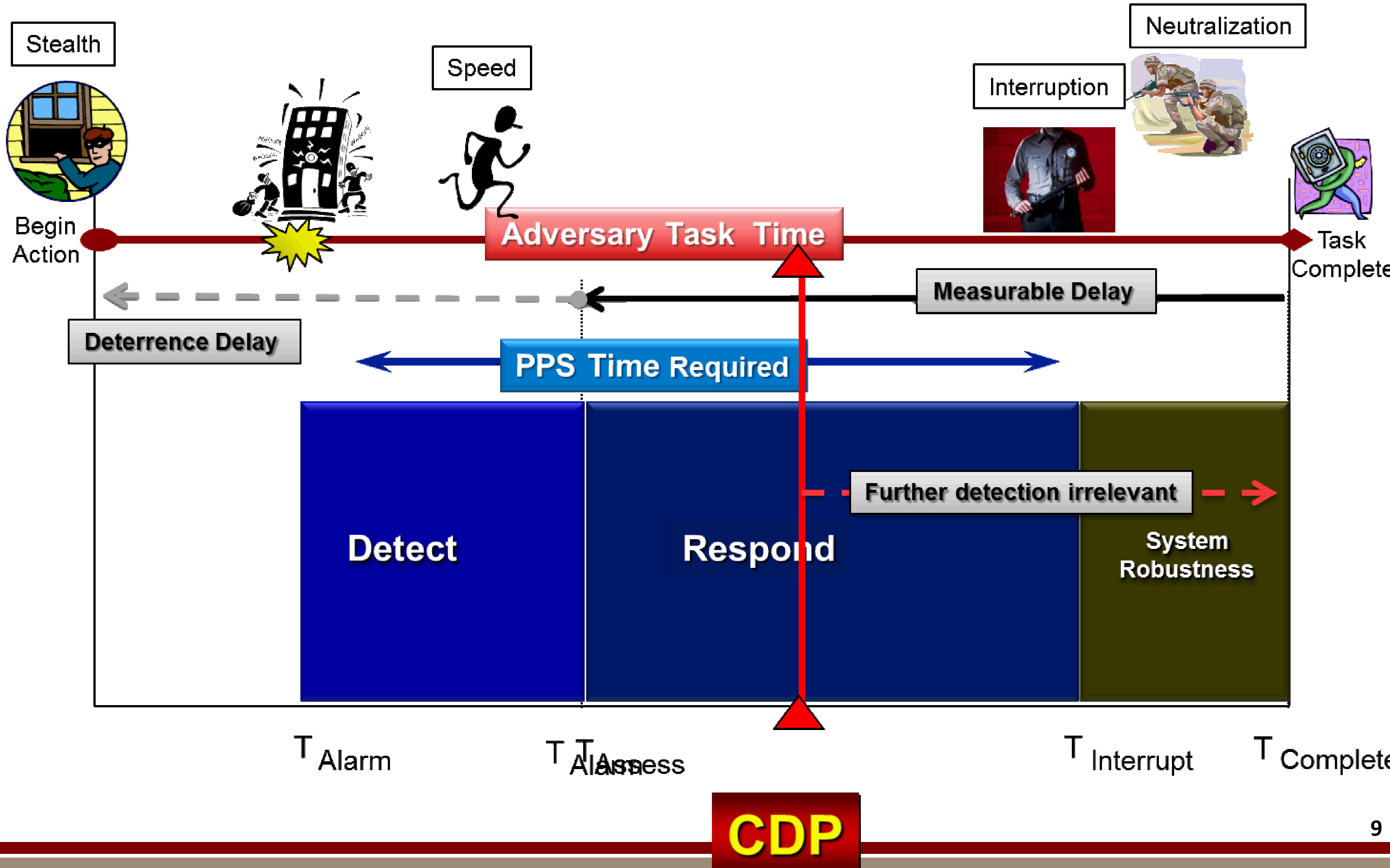
Performance Tests

- Objectives
  - Validate vulnerability analysis input data, assumptions, activities, results, and conclusions
  - Demonstrate protection capabilities
- Methodical means to
  - Establish or confirm performance level of PPS element
  - Test PPS elements over their planned range of operation
  - Provide statistical basis for calculation of P_E

Interruption Analysis: Terminology

- Principle of timely detection
  - Detection must occur early enough along the adversary path so that response force has time to interrupt adversary before task completion
- Critical detection point (CDP)
  - Last detection point along adversary path for which system response time is less than remaining adversary task time

Critical Detection Point



Interruption Analysis: Calculation

- P_I is the first factor in system effectiveness (P_E)
- P_I depends on relationship of two timelines
  - Adversary path and task timeline
  - PPS timeline in response to adversary
- Calculating P_I
  - At each element along the adversary pathway, there is a probability of detection (P_D) as well as a probability of non-detection (P_{ND})
  - P_{ND} of each detection point before the CDP is used to calculate the probability that the adversary will not be detected along each step along the path

Calculating P_I – Example

Adversary Task	Task Time (s)	Time Delay Remaining (s)	P_D
Penetrate fence	10	284	0.4
Run to outer door	25	274	0.02
Penetrate outer door	36	249	0.5
Run to wall	8	213	0.02
Penetrate wall	100	205	0.75
Run to inner door	6	105	0.02
Penetrate inner door	60	99	0.9
Run to target	4	39	0.0
Sabotage target	35	35	1.0

Total task time = 284 s

Response Force Time (RFT) = 200 s

Where is the CDP?

Calculating P_I – Example (cont.)

Adversary Task	Task Time (s)	Time Delay Remaining (s)	P_D
Penetrate fence	10	284	0.4
Run to outer door	25	274	0.02
Penetrate outer door	36	249	0.5
Run to wall	8	213	0.02
Penetrate wall	100	205	0.75
Run to inner door	6	105	0.02
Penetrate inner door	60	99	0.9
Run to target	4	39	0.0
Sabotage target	35	35	1.0

P_{ND}= (0.6) (0.098) (0.5) (0.98) = 0.29

$P_I = 1 - P_{ND} = 1 – 0.29 = 0.71$

Path Analysis

- Evaluation of P_I uses the concept of an adversary path for a defined threat against a security system
  - Adversary must traverse a path from starting point to target
    - Path is composed of a series of actions
      - Each action has a delay time based upon DBT capabilities
    - Detection may occur at various points along the path
      - Detection may be minimized or defeated based on DBT capabilities
    - Response Force may interrupt the adversary along the path
- Focus of path analysis is on most vulnerable paths – those with minimum P_I

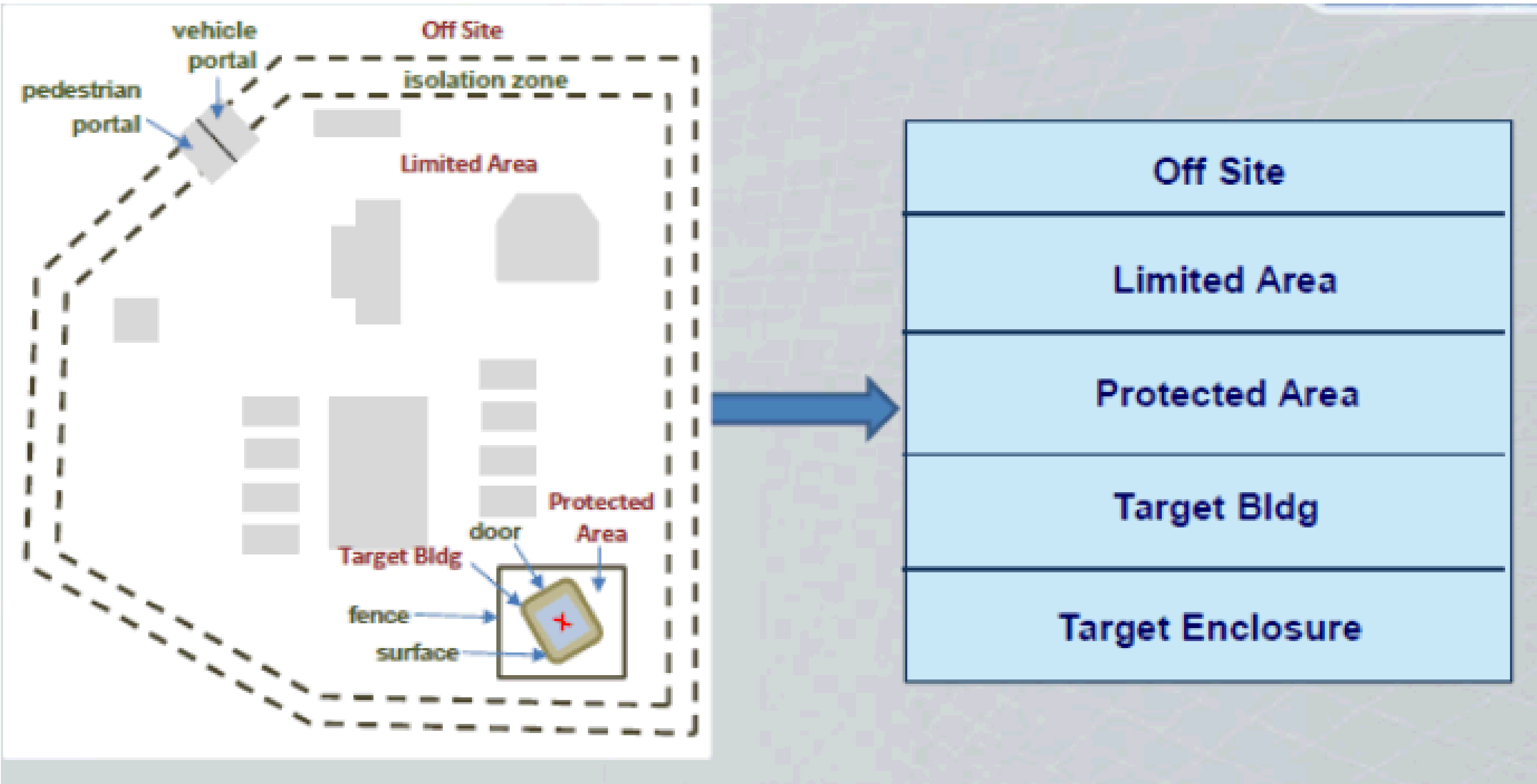
Path Analysis

- Variety of tools available to estimate P_I
  - Single path models
    - Calculate P_I based on principle of timely detection and CDP
    - Single pathway analysis techniques are basis for multiple pathway analyses
  - Multipath tools
    - Calculate PI for most vulnerable paths and generic scenarios of force, stealth, and deceit

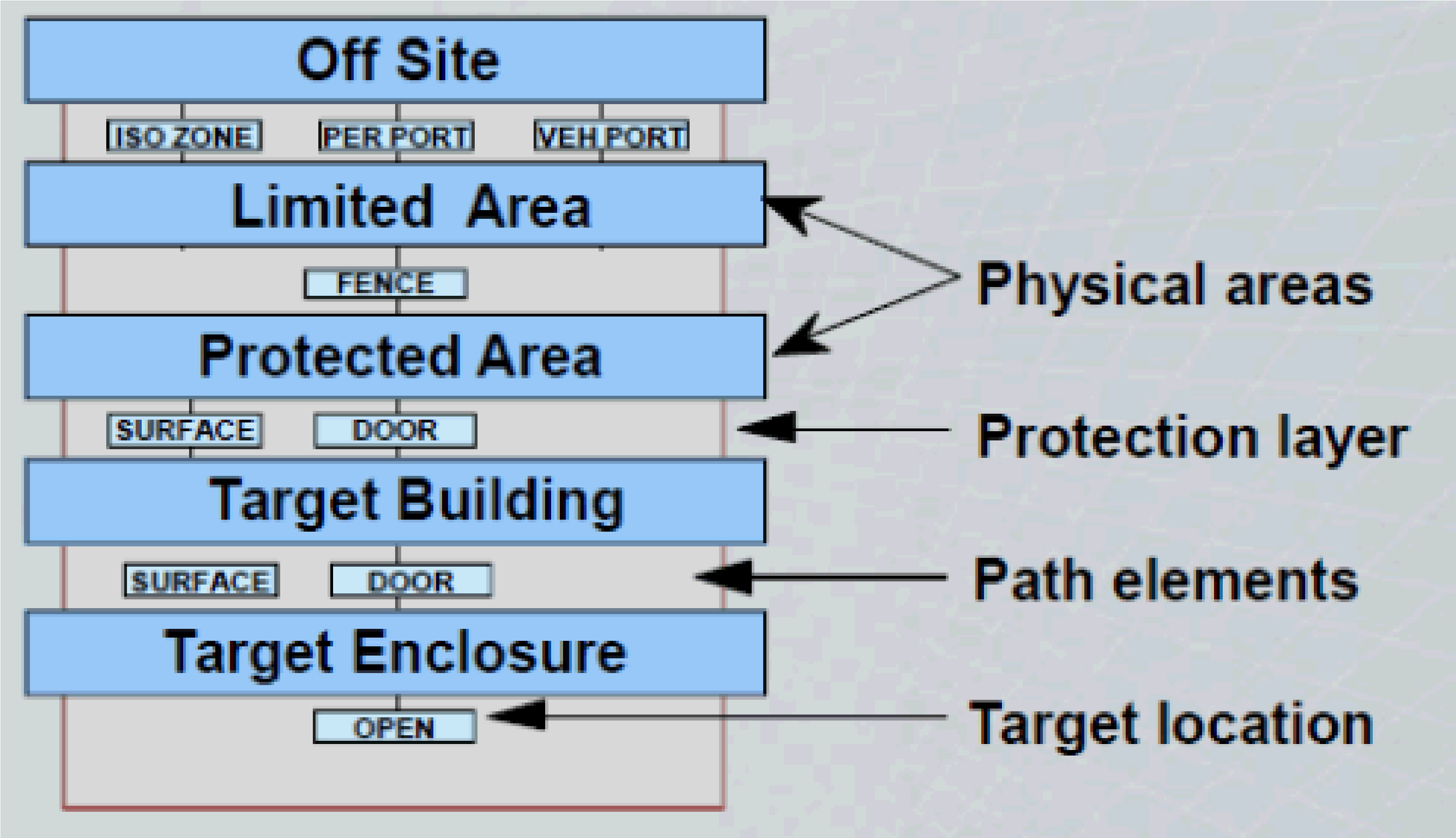
Adversary Sequence Diagram

- Adversary sequence diagram (ASD) is a graphical representation of
  - Facility PPS
  - All adversary path
- PPS is modeled as concentric layers around adversary target
  - Each layer composed of PPS path elements
  - Each path element has associated detection and delay characteristics
    - Designed performance for initial path analysis
    - Degraded performance, if appropriate, for scenario analysis
  - Each adversary path traverses single path element in each protection layer

Adversary Sequence Diagram: Facility Model

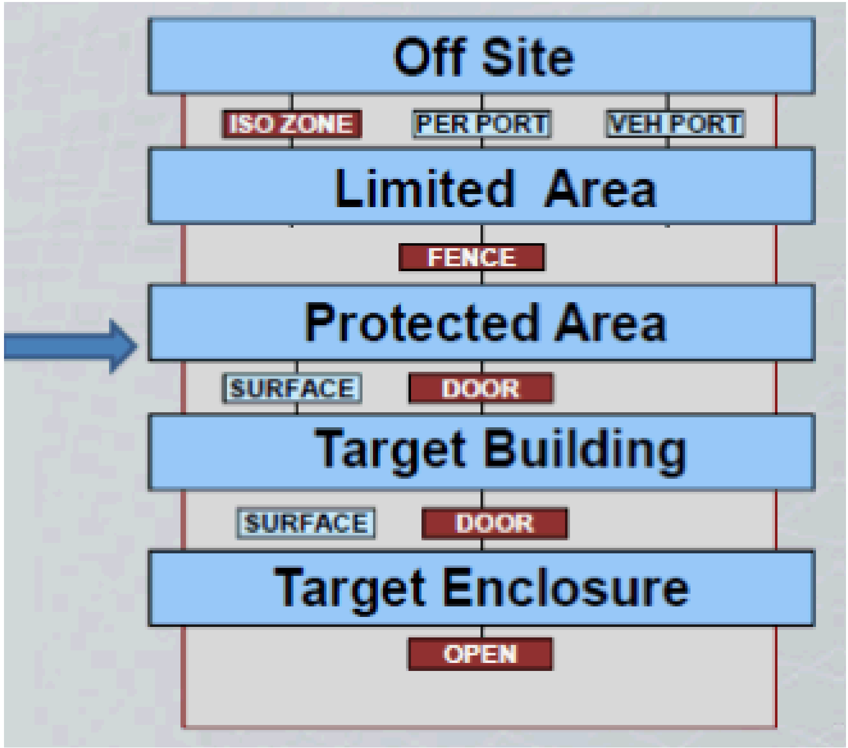


Adversary Sequence Diagram: Facility Model



ASD Pathway

Off Site
Limited Area
Protected
Area
Target Bldg



Off Site
ISO ZONE
PER PORT
VEH PORT
Limited Area
FENCE
Protected Area
SURFACE
DOOR
Target Building
SURFACE
DOOR
Target Enclosure
OPEN

Path Analysis Tools

- Single path tools
  - Estimate of Adversary Sequence Interruption (EASI)
  - Very Simplified Estimate of Adversary Sequence Interruption (VEASI)
- Multipath tools
  - Analytic System and Software for Evaluating Safeguards and Security (ASSESS)
  - System Analysis of Vulnerability to Intrusion (SAVI)
  - Multipath VEASI

Neutralization Analysis

- P_N is second factor in system effectiveness (P_E)
- Definition of P_N
  - Probability, given interruption of the adversary by the response force, that the response force will gain physical control of the adversary
- Calculation
  - $P_N = N_{wins}/N_{engagements}$
    - $N_{engagements}$ is a statistically significant number of engagements
    - All engagements have the same initial conditions
    - Two possible outcomes per engagement: win or loss

Neutralization Analysis (cont.)

- Terminology and Definitions
  - Probability: Chance that a given event will occur; ration of number of events with a specified outcome to total events in set
  - Deterministic process: Outcomes are caused by preceding events or natural laws
  - Stochastic process: Random process with various outcomes involving probability
  - Engagements: Stochastic process in which two opposing forces use weapons and tactics to achieve a goal
  - Win: Response force captures adversary or causes adversary to flee

Neutralization Analysis Tools

- Neutralization analysis requirements
  - Threat data
  - Response force data
  - Neutralization analysis
    - Scenarios of concern
    - Analysis methodology
- Wide range of methods to determine neutralization (PN)
  - Expert opinion
  - Simple calculations
  - Tabletop exercises
  - Complex simulations (STAGE)
  - Force-on-Force exercises
- Tradeoff between different methods is accuracy vs cost

Neutralization Analysis Tools (cont.)

- Examples of simple numerical methods
  - Data tables
  - Tabletop path analysis
  - Markov chains
  - Monte Carlo simulation
- Simulations
  - Tabletop exercises
  - Complex computer simulations
  - Force-on-Force exercises
- Actual engagements

Neutralization Accuracy

- Difficult to assess accuracy because rarely have actual battles to compare results
- Each neutralization methodology has strengths and weaknesses
- Use of several methods is better than use of any one alone

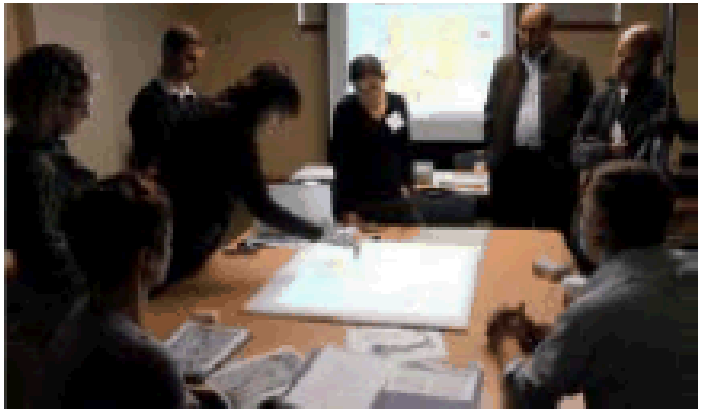
	Accuracy	Cost
Expert judgment	L – M	L
Simple numerical	M – H	L
Tabletop	L – M	L - M
Computer simulations	?	L – M
Force on Force (FOF)	L – M	?
Actual engagements	H	H

Scenario Analysis

- Methodology for analyzing system effectiveness, PE, by considering several alternative, possible, adversary attacks (scenarios)
  - Allows more detailed analysis of attack, defense, and results than path analysis
  - Focus is on identifying gaps in planning and vulnerabilities
- Purpose
  - Provides basis for confident evaluation of PPS performance
  - Helps create robust security plans to math and fully use capabilities of the PPS design

Scenario Analysis (cont.)

- Characteristics of a good scenario analysis
  - Credible
  - Internally consistent
  - Intellectually honest
  - Conservative
  - Transparent
  - Well documented
  - Vetted among stakeholders
  - Useful (i.e., provides useful results)



Scenario Analysis Methodology

1. Identify key objectives
   - Determine PPS system effectiveness
   - Determine response force effectiveness
2. Identify major drivers
   - Numbers of adversaries, tactics, state of response force
   - Facility state / PPS state
3. Collect necessary site data
   - Detailed security plans and procedures
   - Performance test results
   - Detection and delay values developed for path analysis

Scenario Analysis Methodology (cont.)

4. Create a set of valid scenarios
5. Determine PE for each scenario using
   - Subject matter experts
   - Tabletops or simulations
6. Document scenario descriptions, results, conclusions

Quantitative vs Qualitative Analysis

Sandia National Laboratories
KHNP Central Research Institute

- Qualitative Analysis
  - Uses subjective judgment based on non-quantifiable information
    - Assigns metric for system performance based on high, medium, or low performance
  - Typically involves subject matter expertise to assign a categorical description (acceptable/unacceptable)
- Quantitative Analysis
  - More rigorous method of analysis, typically used to assess facilities that protect very valuable assets
  - Uses numerical estimates of delay and/or response times
- Approach is more objective, not mathematically rigorous
  - Characterizing technology by testing is still the best technique to objectively assess security elements and systems

Potential Analysis Issues

- At some facilities, the number of individual targets may be too large to allow all to be analyzed
- Ways to reduce number of targets for analysis
  - Combine targets by type, protection, and location
  - Prioritize targets and analyze highest priority
    - Example: Based on adversary attractiveness or categorization

Conservative Estimate

- To avoid overestimating system effectiveness, we use two conservative yet credible assumptions
  - Assume adversary attacks most vulnerable path for operator (best path for the adversary)
    - For sabotage, entry path with lowest PI
    - For theft, combined entry/exit paths with lowest PI
  - Assume adversary defeat strategy for each path element is based on CDP
    - Prior to CDP, adversary uses stealth and/or deceit strategy
    - After CDP, adversary uses force strategy

Summary

- System effectiveness measures
  - Probability of interruption (P_I)
  - Probability of neutralization (P_N)
  - System effectiveness (P_E)
    - Outsider $P_E=P_I*P_N$
    - Insider $P_E=P_I$
- PPS evaluation approaches
  - Performance tests
  - Path analysis
  - Neutralization analysis
  - Scenario analysis