SAND2020-6884PE

Physical Security Modeling

Presented by Douglas M. Osborn, Sandia National Laboratories
MeV Summer Course
August 2020

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2020-XXXX

Overview

Methodology

- Design and Evaluation Process Outline (DEPO)
  - Basic Physical Protection System Functions (PPS)
- Analysis Metrics
  - Probabilities of Interruption, Neutralization, and System Effectiveness

Modelling and Simulation Tools

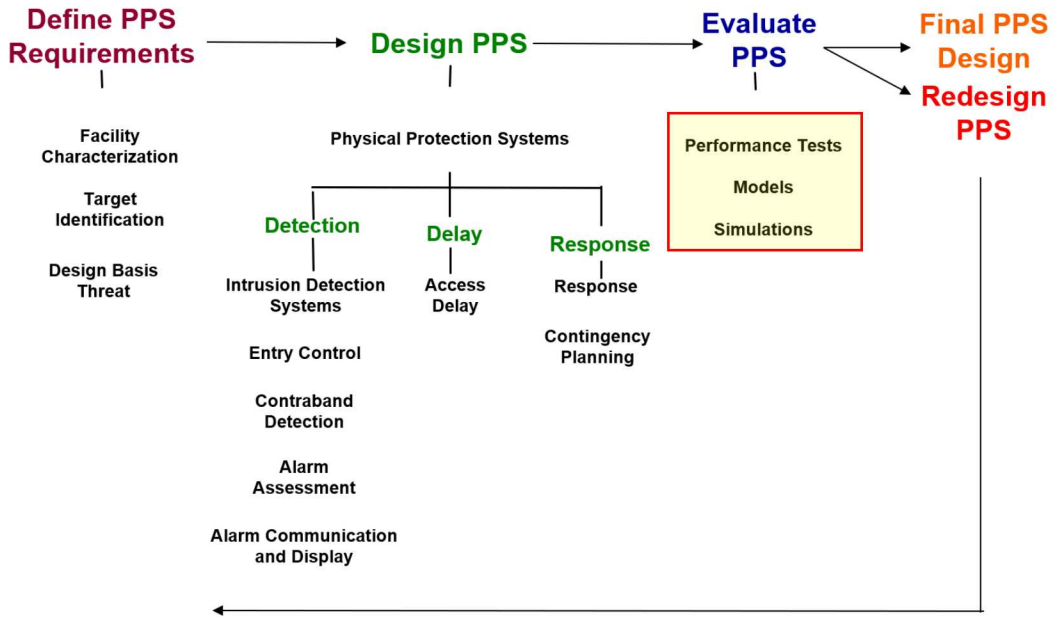
- Pathway Analysis
- Security Modeling Software
- Safety Analysis Modeling

Simulation Example

- Analysis Workflow
- Terrain/3D Modeling
- Safety/Security Integration

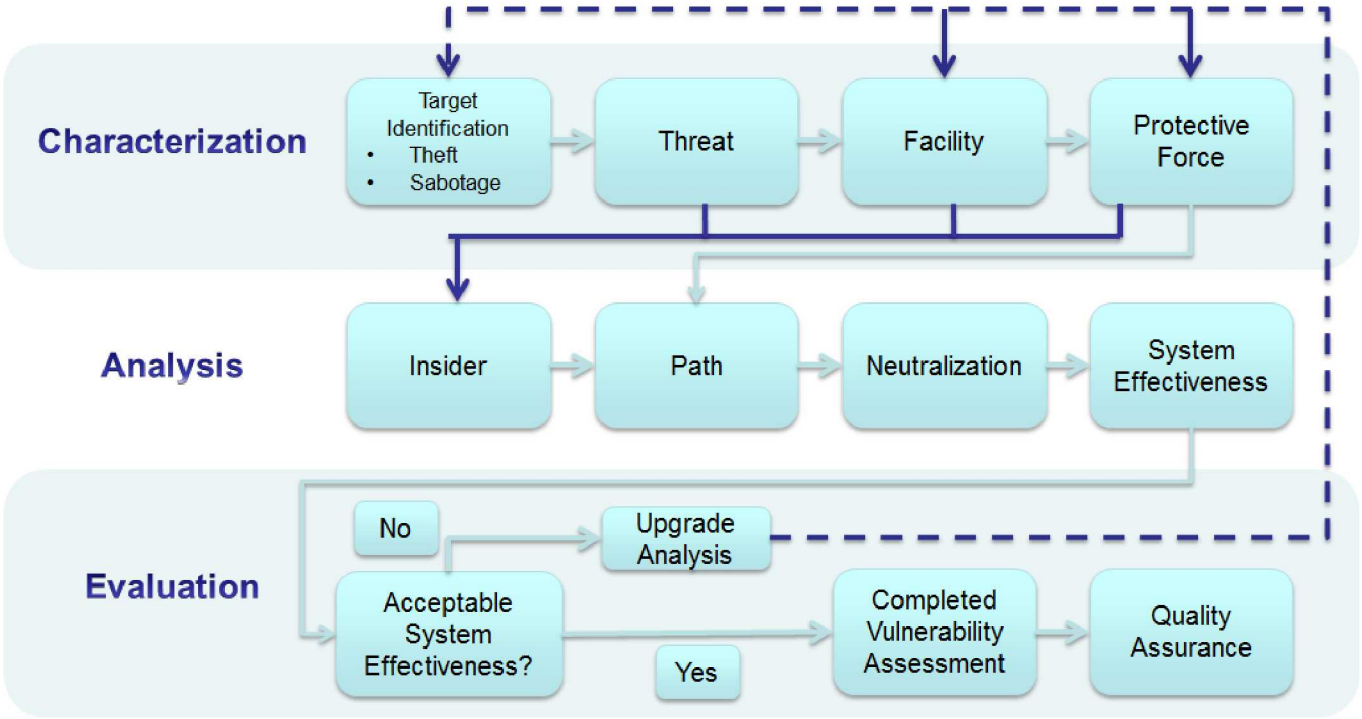
Methodology

Design and Evaluation Process Outline (DEPO)



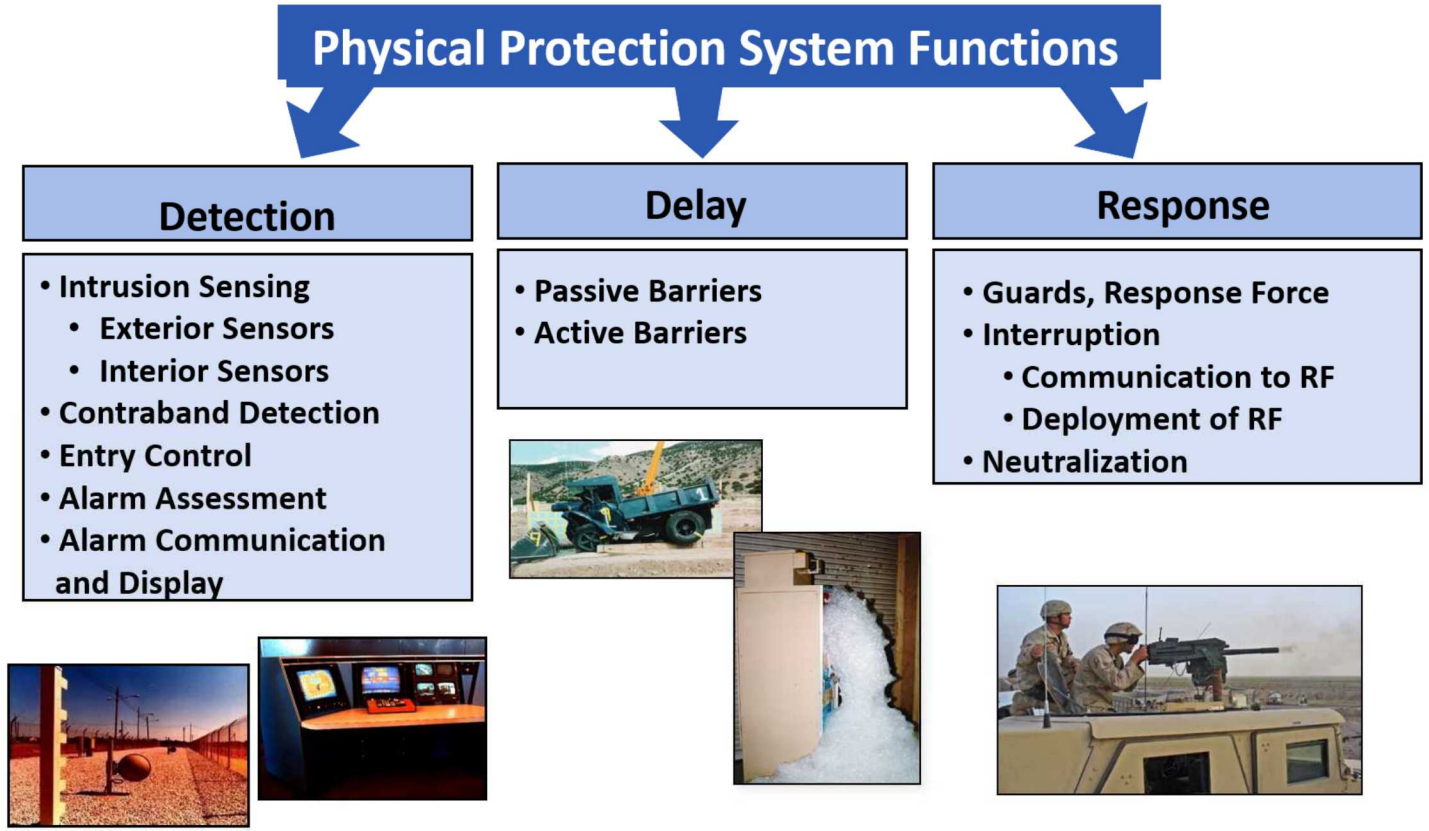
- Forms both the basis for the PPS design process and the evaluation process

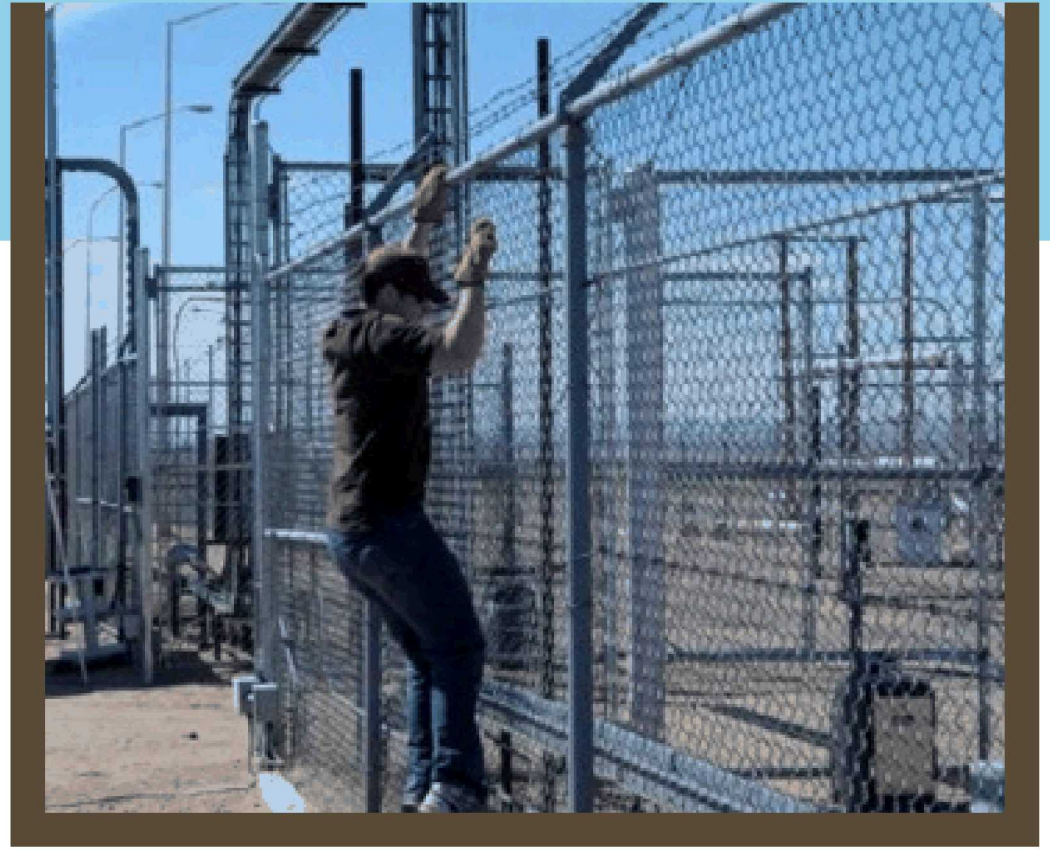
Vulnerability Analysis Process

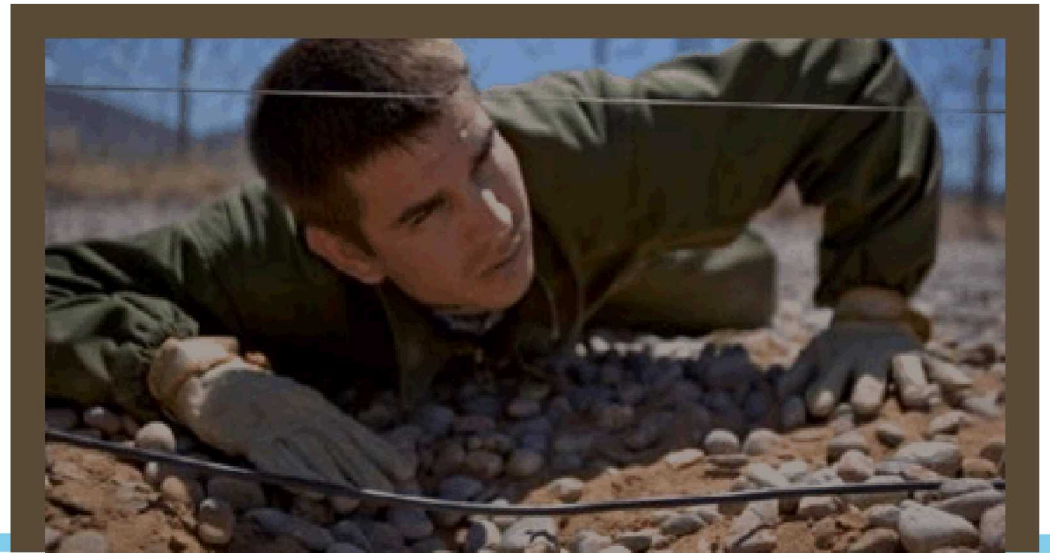


Basic PPS Functions

- Essential to the design and evaluation process
- Must be modelled correctly
- Assumptions must be made explicit







Performance Evaluation Metrics

- Three metrics are commonly used for evaluating the performance of PPS:
  - System Effectiveness (P_E)
    - Probability that the PPS will prevent the adversary from completing the undesired event
    - $P_E = P_I * P_N$
  - Probability of Interruption (P_I)
    - Probability that the response force arrives in time to stop the adversary
  - Probability of Neutralization (P_N)
    - Probability, given interruption of the adversary, that the response force kills or captures the adversary or causes the adversary to flee

Path Analysis: P_I

- Does the PPS design adequately provide:
  - Timely detection?
  - Defense in depth?
  - Balanced protection?

Scenario Analysis: P_N and P_E

- Does the PPS design provide the required level of protection against an adversary attack (scenario) consistent with the Design Basis Threat?

Regulator Thresholds

- Often, protection requirements are in terms of P_E being above a threshold, such as 85%
- That is, $P_E = P_I \times P_N > 0.85$
- Competent Authority specifies required performance against DBT

How Metrics relate to Design

Uses for Modeling and Simulation

Conduct performance and risk assessment studies of current security operations, plans and security systems

- Personnel allocation
- Response plans, response force tactics, techniques, and procedures
- Process monitoring
- Contingency planning

Evaluate and validate candidate changes

- Impact of new sensors, vehicles and weapons
- Changes to facility operations and/or processes
- Improvements to process efficiency for better material control
- Locations of key measurement points

Uses for Modeling and Simulation (continued)

Enhance

- Augment existing exercises
  - Multiple data points versus single data point
  - No restrictions due to safety of facility operations

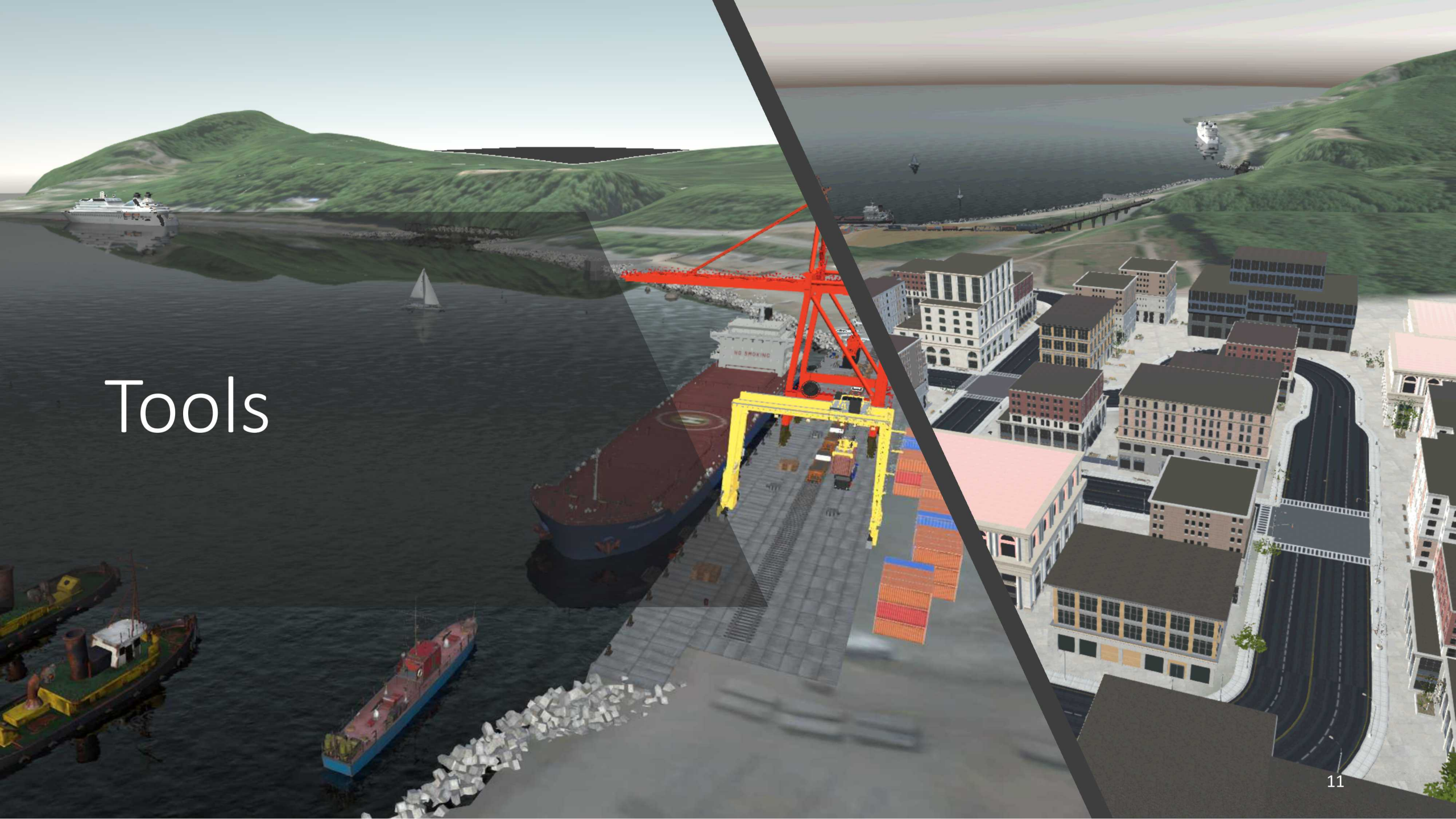
Reduce

- Reduce costs
  - Typically uses less resources than large scale live exercise
  - Once developed, model can be reused for future simulations

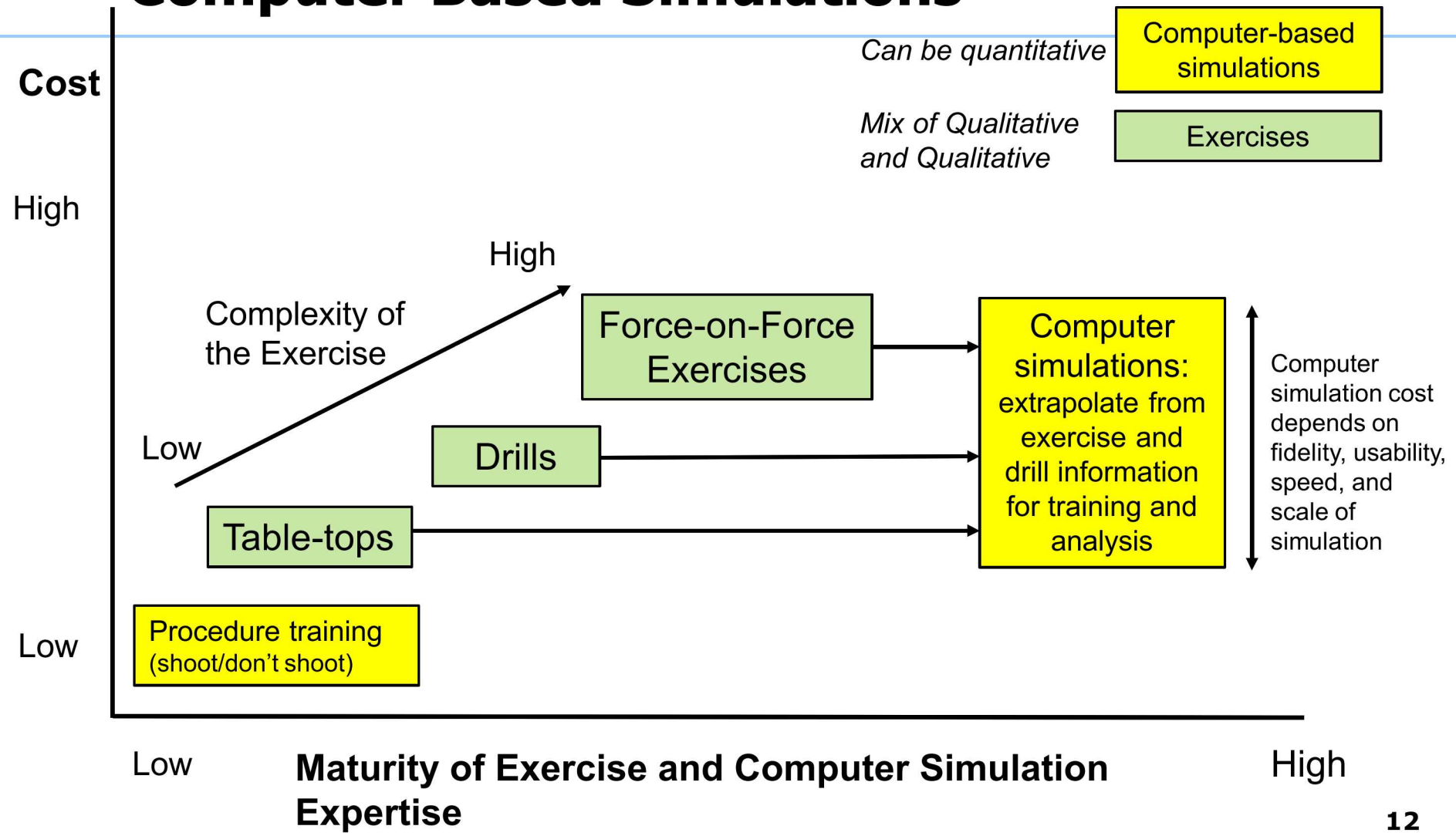
Train

- Augment security training
  - Visualize the outcome of an attack scenario
  - Role-play to interact with adversaries in a dynamic threat environment

Tools



Relationship Between Exercises and Computer Based Simulations



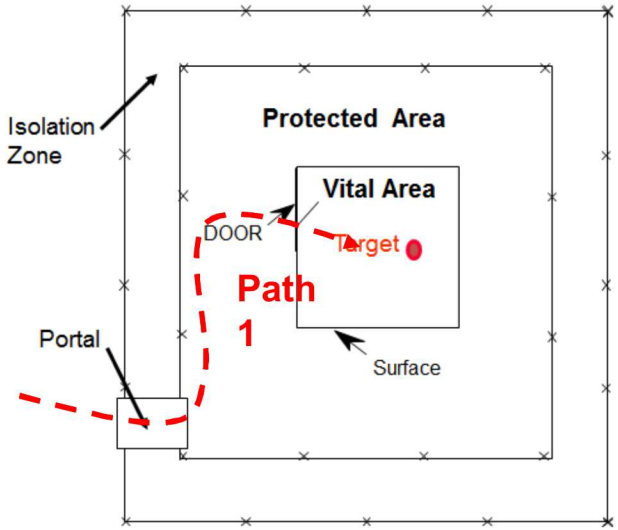
12

Path Analysis Tools

- **Path Analysis is a process to determine whether detection and delay are sufficient along all adversary paths to provide an adequate level of Timely Detection (Probability of Interruption)**

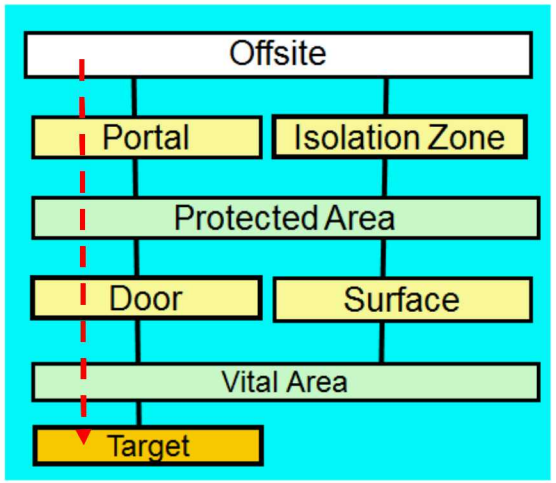
Example Facility

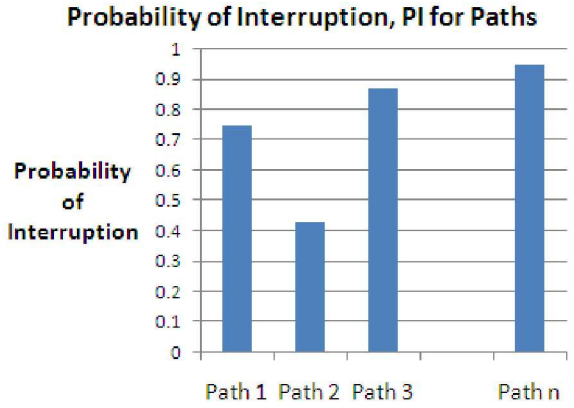
Off Site



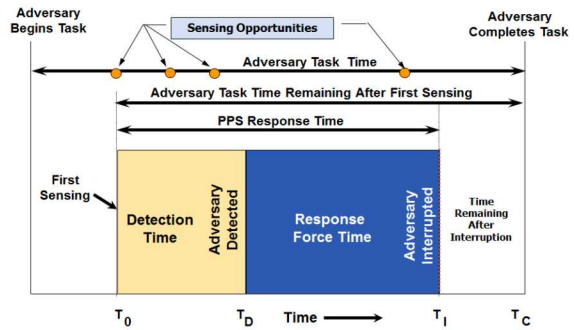
Corresponding ASD

Each Element and Area has Performance Values (P_D, T)





Timeline Models for Calculating Probability of Interruption



Examples
1970's: PANL
1980's: SAVI
1990's: ASSESS

Tabletops / Scribe3D©

- Why we use tabletops
  - Find the scenarios of interest
  - Quick and inexpensive
  - Widely available

Traditional tabletop gaps

- Difficult to record all movements and information
- 2D maps lead to incorrect assumptions
- Measuring distances and speeds is time consuming

SCRIBE3D© Tabletop Centric Approach

- Scirbe3D© is a simulation framework for automating a tabletop excercise
  - Provides flexibility
  - Can be used in multiple contexts
  - Training, Analysis, Demonstration
- The Analyst creates the VA simulation
  - Decisions are made by the analyst, not at the entity level
  - Behavior is limited to what is defined in the tabletop
  - Creates a simplified, streamlined analysis framework with (limited) dynamic behavior when necessary
  - Highly traceable
- Does not replace typical neutralization tools, rather augments tabletop excercises

Force-on-Force Simulation Codes

Several codes are used for evaluating force-on-force and tabletop development scenarios

- JCATS
  - Lawrence Livermore National Laboratory
- STAGE
  - Presagis International
- AVERT
  - Ares Security Corporation
- Dante/Umbra
  - Joint codes, produced by Sandia National Laboratories
- Simajin/VANGUARD
  - Rhinocorps Ltd.
- Scribe-3D
  - Sandia National Laboratories

Safety Simulations

High fidelity modeling captures the effects to the reactor of losing combinations of systems

Dynamic analysis – timing and order are captured

Can be headless or human-in-the-loop

- Headless can run many times to capture uncertainties
- Human-in-the-loop integrates operator actions with the system response

Common codes:

- MELCOR
- MAAP
- RELAP5-3D
- ADS

Fukushima Daiichi Unit 1-4
Courtesy of TEPCO

Integrating Security with Safety

Security and safety models each model part of the problem

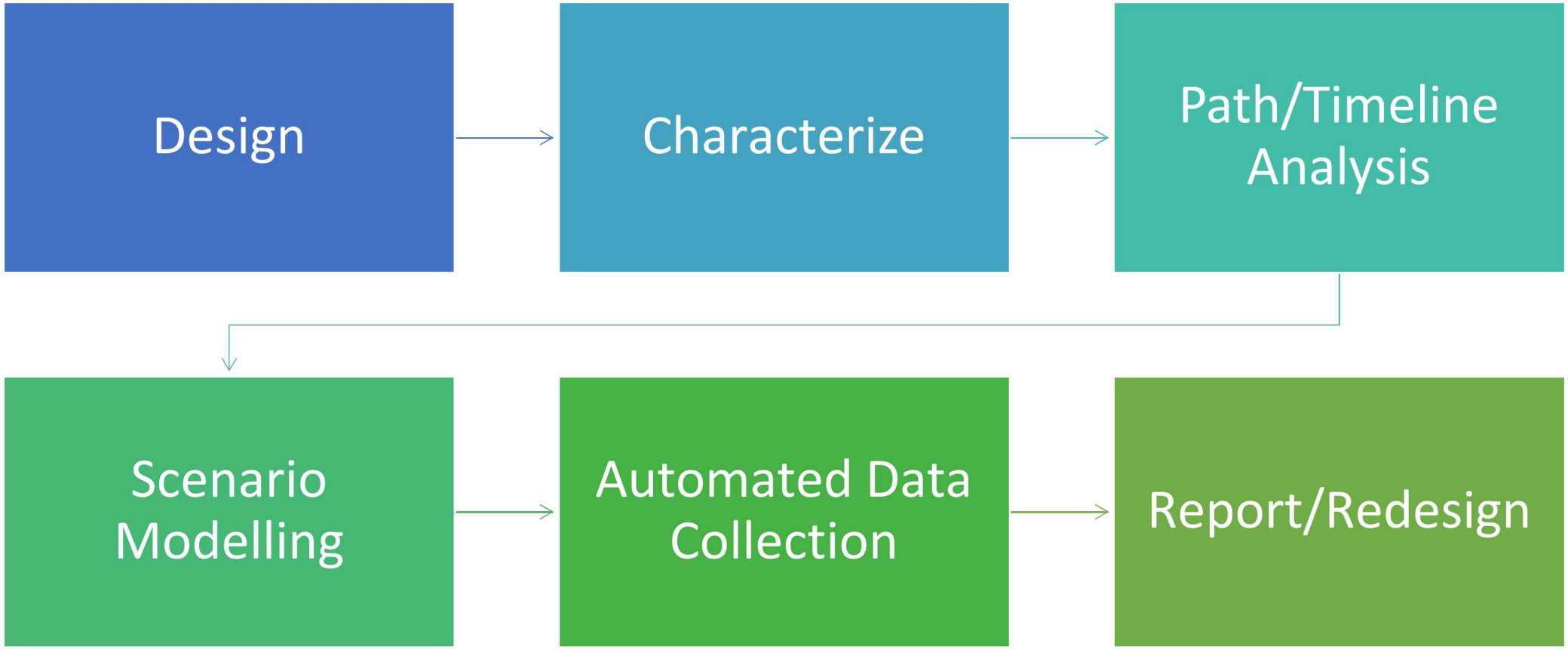
- Security models determine which systems are lost and when
- Safety models predict the effects of those system losses

Integrated safety-security analysis may capture events from initial intrusion through radionuclide release

Requires combining safety analysis with security analysis

- Helps promote communication between otherwise separate departments

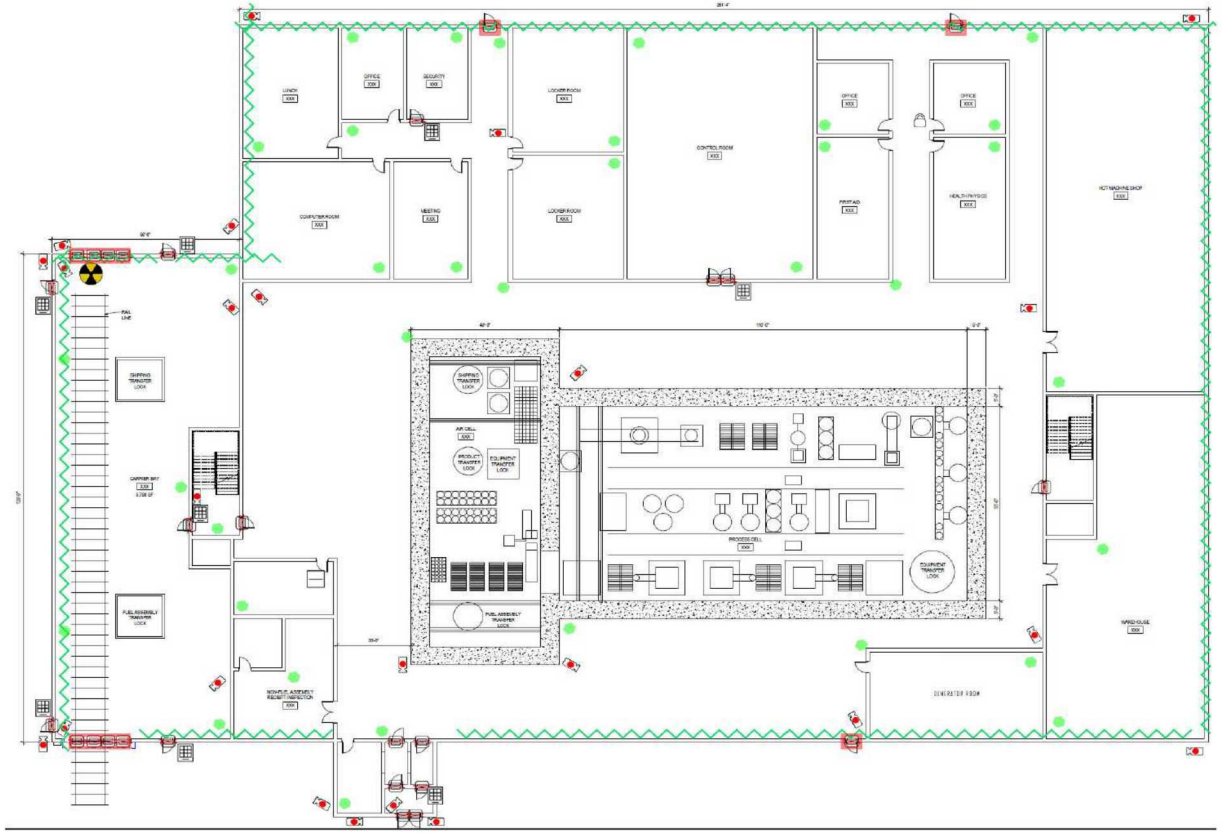
Analysis Example

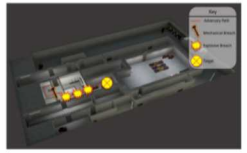


Process Workflow

Design/Characterize

- Larger dictated by the facility purpose
- Process specific SMEs
- Integrating security into the design process reduces cost and improves future security





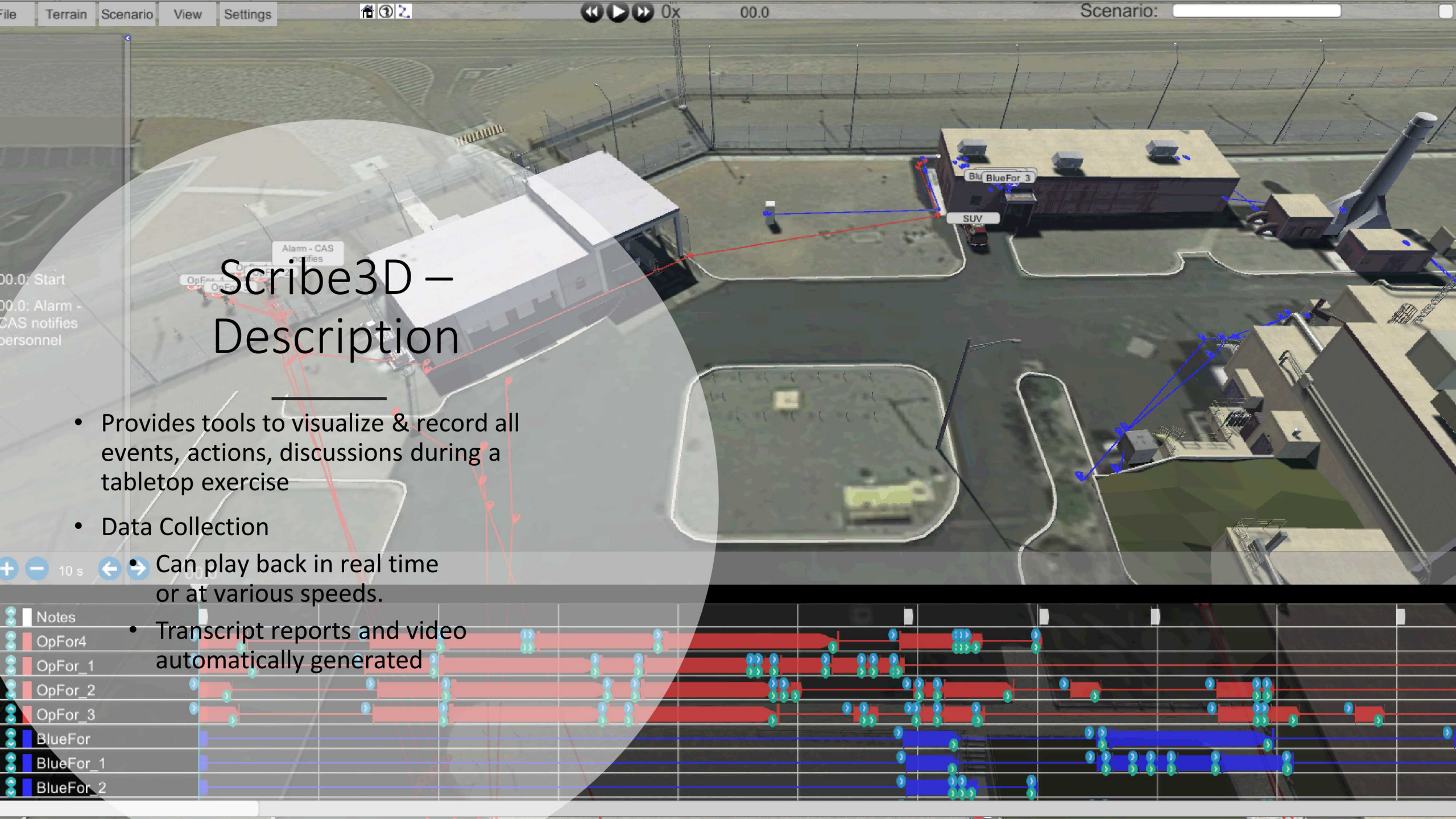
Path/Timeline Analysis

- Multiple software options
- Identify most vulnerable path
- Detection/delay options along that path
- Identify delay/detection deficiencies
- Identify delay/detection surpluses

				Del Sec
Task	Description	P(Detection)	Location	N
1	Breach outer passive fence	0.02	M	
2	Engage foot patrol	0.10	M	
3	Move to building exterior (50m)	0.02	M	
4	Breach Emergency Exit Door	0.95	E	
5	Move to Stairwell Door	0.80	M	
6	Breach Upper Stairwell	0.80	E	
7	Move down to Lower Stairwell door	0.02	M	
8	Breach Lower Stairwell Door	0.80	E	
9	Move to Basement Hall Door	0.02	M	
10	Breach Basement Hall Door	0.80	E	
11	Move to Vault Door at TRU Vault Control Room	0.02	M	
12	Breach Vault Door	0.80	E	
13	Move to Shield Wall at TRU Vault	0.02	M	
14	Breach Shield Wall at TRU Vault	0.80	E	
15	Move to inner Shield Wall	0.02	M	
16	Breach Inner Shield Wall	0.80	E	
17	Set up and Climb step latter into TRU Vault	0.02	M	
18	Retrieve target material	0.02	M	
19	Exit Site	0.02	M	
	Probability of Interruption:	.99		
	^Denotes values that a sums of the steps preceding which have "--" for their delay value			

Scribe3D – Maps/Terrain

- 2D/3D maps
- Terrain derived from
  - Maps
  - Imagery
  - GIS
  - High-fidelity laser scan models
- Notional facilities



Scribe3D – Description

- Provides tools to visualize & record all events, actions, discussions during a tabletop exercise
- Data Collection
  - Can play back in real time or at various speeds.
  - Transcript reports and video automatically generated

Integrated Safety and Security

- Dynamic Probabilistic Risk Assessment (DPRA) analyzes the evolution of various scenario paths between initiating events & possible end states
  - A 'bottom-up' technique that statistically evaluates simulation run-based data from deterministic approaches
  - Better accounts for both epistemic (e.g., arising from the model) and aleatory (e.g., stochasticity in the system) uncertainties → higher fidelity analytical conclusions for complex system analysis

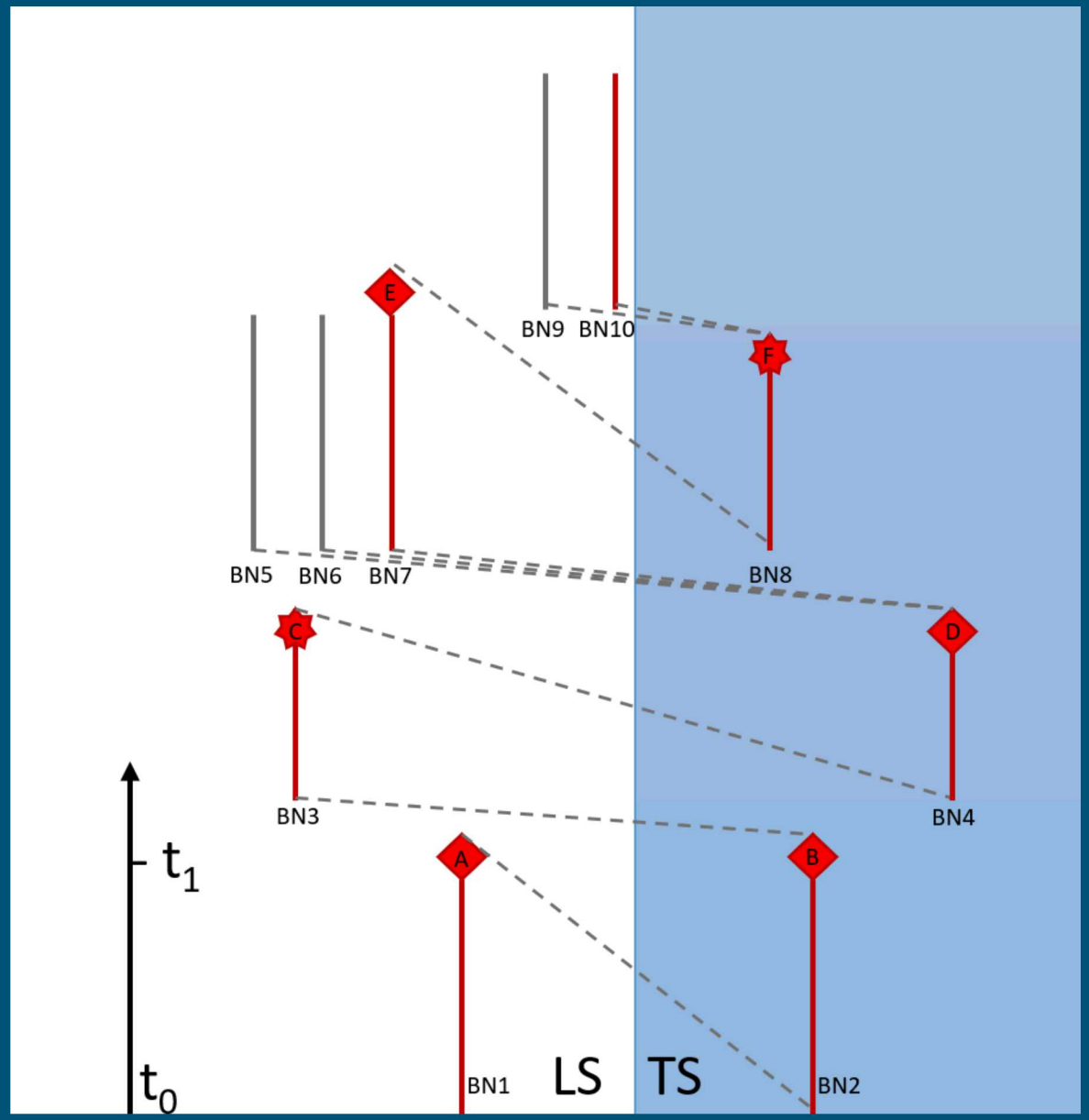
- ADAPT serves as the scenario coordinator and scheduler for the system codes
  - Security Force-on-Force simulation to model damage to and availability of plant safety systems
  - Safety model to determine accident progression and recovery options given sabotage of safety systems

ADAPT

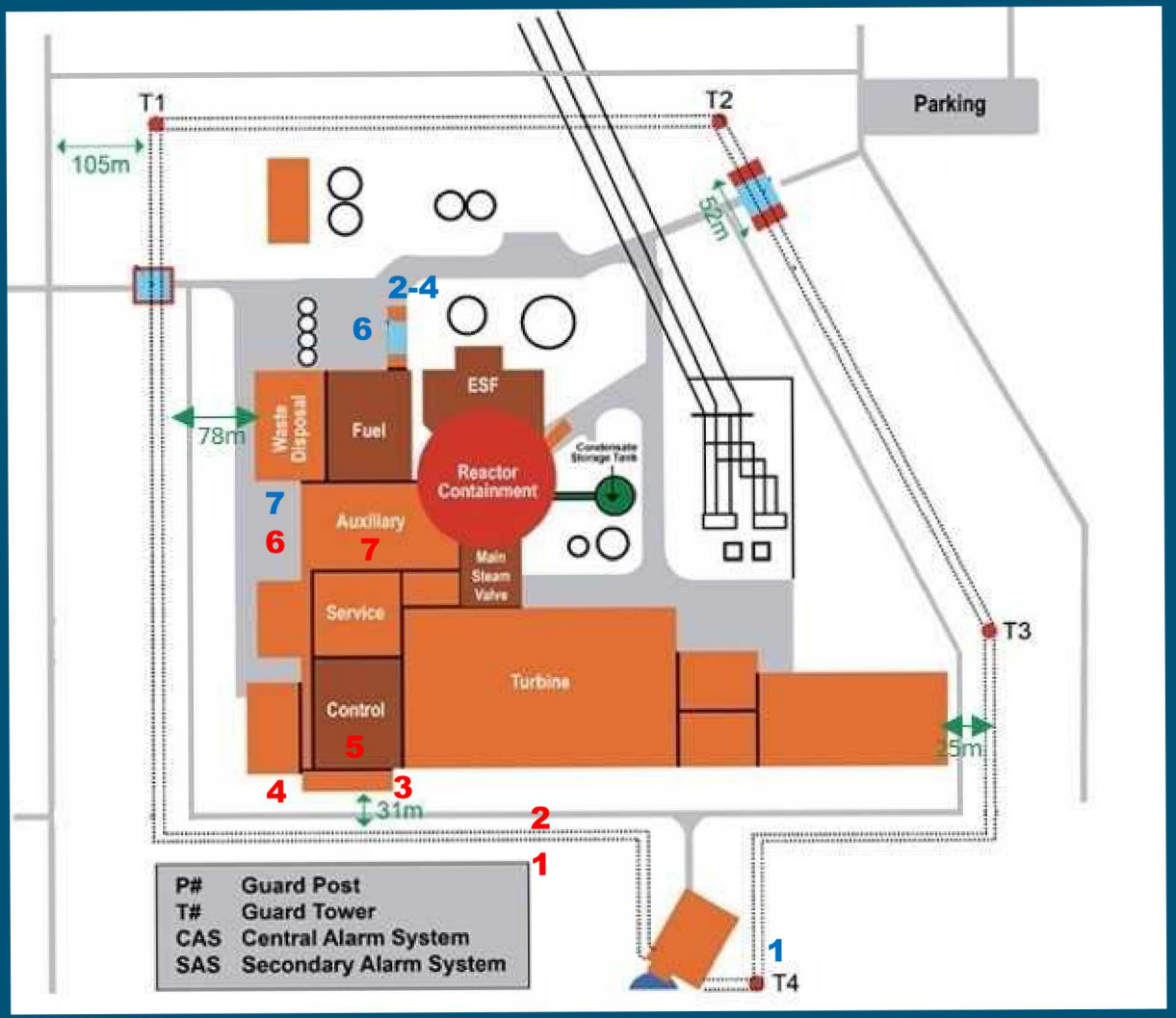
- ADAPT performs Dynamic Event Tree (DET) analysis
- Code agnostic
  - Requires connected system models to:
    - Stop on a preset condition
    - Report stopping condition
    - Save the current system state in a text file
    - Restart on loading a modified save file
- Analysis begins with one instance and splits into daughter branches at points of uncertainty
- Branches based on analyst selected condition
  - Can explicitly include time element
- Recently modified to allow for multiple simulators
  - Cannot currently accommodate two simulators branching at unknown times

Leading Simulator/Trailing Simulator Approach

- Will use a hybrid approach inspired by ADS-IDAC
  - Construct time blocks of approximately 10 minutes
  - Leading Simulator (LS) executes for one time block
    - Include occasional saves during time block
  - Trailing Simulator (TS) executes for the same time block
- If LS identifies a branching point, TS executes until branching time
- If TS identifies branching point, branching occurs immediately
- Create new time block and begin execution with LS



Hypothetical Lone Pine Plant for Case Study



Step	Time [s]	Adversary Task	Timely Response Task
1	5	Truck crosses PIDAS fence	First detection of adversaries
2	125	Adversary cuts aircraft cable	Notification sent to response forces
3	133	Truck approaches control room wall	--
4	203	Adversaries exit blast radius	Response forces complete preparations
5	204	Bomb detonation	--
6	274	Adversaries enter auxiliary building	Response forces begin driving to adversary location
7	284	Adversaries breach auxiliary control room	Response forces arrive
8	285	Sabotage	--


Thanks!
Questions?