

ICATS – FOF (P3) – July 24th thru July 26th 2013

Response Force:

Response force will use two pictures in time. The participants will be responsible for determining how to execute a contingency plan. They will use the lessons from the FOF to develop call signs, zone/sector assignments, responsibilities of entities, etc. Below is the force plan. Also, a “worksheet” will be available for each run to document how the response played out.

RF Deployment – Baseline Fixed Site				
Call Sign	Location – PIT 1	Location – PIT 2	Weapon	Muster
E1	ECP	ECP	Pistol (45 rnds)	0 sec
E2	ECP	ECP	Pistol (45)	0 s
E3*	ECP	ECP	5.56ass/Pistol(120/30)	0 s
E4*	ECP	ECP	5.56ass/Pistol(120/30)	0 s
H1	Bldg H – ECP Sentry	Bldg H – ECP Sentry	5.56 assault ball (150)	60 s
H2	Bldg H – ECP Sentry	Bldg H – ECP Sentry	5.56 assault ball (150)	60 s
H3	Vault	Bldg H – Vault door	5.56 assault ball (150)	60 s
R1	Rover	Rover	5.56 assault ball (210)	0 s
R2	Rover	Rover	5.56 assault ball (210)	0 s
F1	CAS – C2	CAS – C2	Pistol (45)	0 s
F2	CAS – Commander	CAS – Commander	Pistol (45)	0 s
F3	CAS – Reserve	CAS – Reserve	5.56 assault ball (210)	90 s
F4	CAS – Reserve	CAS – Reserve	5.56 assault ball (210)	90 s
SRT1	Bldg A	Bldg A	5.56 assault ball (210)	90 s
SRT2	Bldg A	Bldg A	5.56 assault ball (210)	90 s
SRT3	Bldg A	Bldg E	5.56 ass/M203 (120/6)	90 s
SRT4	Bldg A	Bldg E	5.56 assault ball (210)	90 s
SRT5	Bldg A	Bldg H – North Hall	5.56 assault ball (210)	90 s
SRT6	Bldg A	Bldg H – SW Corner	5.56 ass/M203 (120/6)	90 s

* Available to respond.

Topics for demonstration:

- CQB
- Containment
- Denial
- Assault
- VA: ASD, CDP, and performance metrics

What NTC will be teaching:

- They will establish protective strategy (participants will)
- Then step thru adv timeline, and they can see it
- Establish RF timeline: Comm, detection, assessment, gear up, muster, etc (~5min)

Opposition Force:

Opposition force will have one mission for the participants; theft, as that is reflective of international practices. The participants will be responsible for determining how to execute an attack plan. They will use the lessons from the FOF to develop call signs, zone/sector assignments, responsibilities of entities, breach locations, breach techniques, breach times, asset distribution, etc. Below is the force plan.

OpFor – Full Matrix Capability				
Call	Assignment	Weapon	Equipment/ Vehicles	Notes
Operator 1				
A1	Task/ Breach Team	7.62 assault AP (90)	5lb satchel (1), cutting charges (3),	Cannot carry large rifles and equipment
A2	Task/ Breach Team	7.62 ass AP/grenade (90/3)	cutting charges (3), ATV	Cannot carry large rifles and equipment
A3	Assault	7.62 assault AP (210)	LAV	A3 can be one of next 3 entities
A3	Assault	7.62 MG AP (300)		Cannot carry anything else
A3	Sniper	7.62 sniper AP (30)		
Operator 2				
A4	Assault	7.62 assault AP (210)		A4 can be one of next 3 entities
A4	Assault	7.62 MG AP (300)		
A4	Assault/RPG	7.62 ass AP/RPG (90/3)		
A5	Assault	7.62 assault AP (210)	VBIED (Soft) – low amount*	A5 can be one of next 2 entities
A5	Assault/M203	7.62 ass AP/M203 (90/6)		
A6	Assault	7.62 assault AP (210)	ATV (w/ IED) – low amount*	A5 can be one of next 2 entities
A6	Sniper	7.62 sniper AP (30)		

*Amount of explosives not important, just a low amount that would be reasonable in a generic DBT.

Scenario Template

Description:			
<p>The conditions of the facility represent a time when the adversary feels they would be most successful (ie, holiday, inclement weather). The adversary will use techniques available to a generic DBT that include breach capabilities, effective command and control, conservative insider “knowledge” of facility (ie, manning levels, and facility layouts), force multipliers, diversion techniques, and moderate to higher skilled marksmanship. The adversary intent will be theft of asset, and the response may employ a posture best suited for protection against theft.</p>			
Response Deployment:			
<p>The response can utilize two respective pictures in time (PIT). One PIT will represent a security response team (SRT) in a barracks, ready to muster/respond at alarm. The other PIT will represent the SRT in a “ready” mode, with pre-deployed positions throughout the facility. Participants will dictate response, but basic deployment locations can be pre-determined based on best practice.</p>			
Picture In Time: PIT 1 – SRT Barracks PIT 2 – SRT Deployed			
Unit:	At Alarm:	Building H Alarm:	Bldg H Vault Alarm:
ECP			
Rover			
Building H			
CAS Reserve			
SRT			
Upgrades:			
<p>Participants will utilize lessons learned from the baseline scenarios to devise ideas for implementation of upgrades. These ideas will be focused on detection, assessment, delay, or response.</p>			
Detection:			
Assessment:			
Delay:			
Response:			

JCATS SIMULATION RUN DATA COLLECTION SHEET

Neutralization Number: _____

General Information

Date:		Run No.:	Run Time =
Site/Target:	<input type="checkbox"/> Day <input type="checkbox"/> Night		
Scenario:	Site Configuration: Baseline / Upgraded		
If upgraded, description of upgrade(s):			
Target Configuration:	closed/open		
Attack vector - land, air, multiple, other (specify):			
Threat Support Equipment (size, location)			

Results

Blue Total:	Blue Loss:	Details:	
Red Total:	Red Loss:	OPFOR Plan:	
Time Assault begins:	Shots Fired At:		
When detected:	How / Where detected:		
Time Red Breach Perimeter:			Red on foot / in vehicle:
Time Red Reach Building:			Red begin Breach:
Time Enter Building:			No. Red Enter Building:
No. Red able to Reach Target/Target Location:			Task Time Begins:
Uninterrupted Time on Target/Location:			
		Neutralization or Task Completion Time:	
First RF Engagement:			
Blue interrupt Red? Time:	Where:		
Time:	Where:		
Time:	Where:		
Time:	Where:		
OTHER:			

Location Primary Target(s): _____ (be specific) **Valid Run** **Invalid Run**

Location Secondary Target(s): _____ (be specific) **Blue Win** **Red Win**

Robustness Sensitivity Rating: VH, H, M, L, VL

Notes:

Exceptional service in the national interest



Application of Modeling and Simulation for Training and Analysis

SNL – Global Security Programs

Joe Sandoval



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. SAND2013-5879.

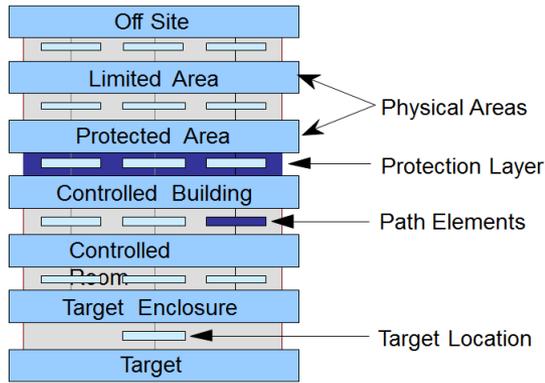
Application of and Benefits in Security

- Modeling and Simulation is used in security to support:
 - Leadership decision making and planning
 - Design of security systems
 - Training of security personnel
- Use of models and simulations has led to improvements in:
 - Decision making and security plans
 - Efficiency
 - Quality
 - Preparedness of responders

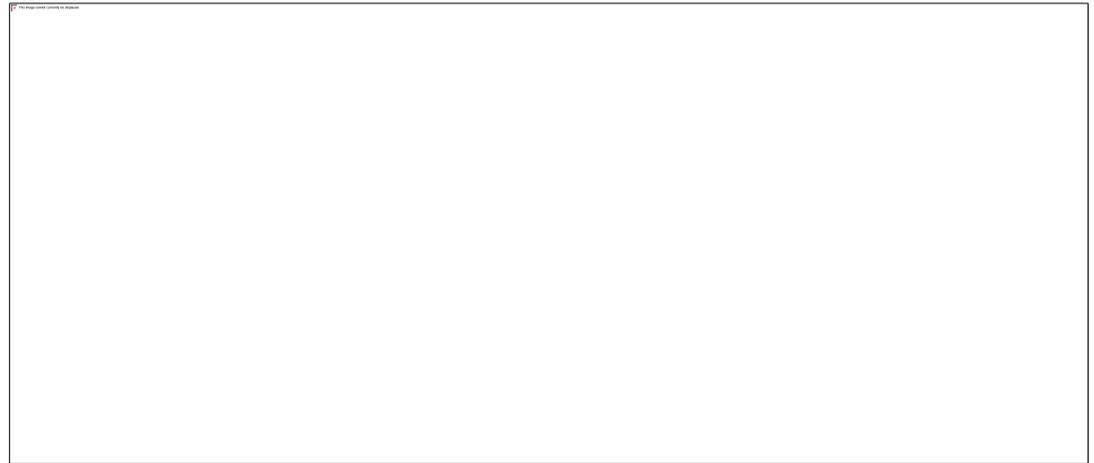
Types

- The types of models and simulations used in security include:
 - Models
 - Models representing real systems for use in simulations
 - Mathematical models used to determine quantitatively the consequence of an event, cumulative barrier delay times, cumulative detection probabilities, etc.
 - Simulations – A method for implementing a model over time to replicate potential real world events. Simulations used in security include:
 - Computer Simulations
 - Force on Force Exercises
 - Drills
 - Tabletop Exercises

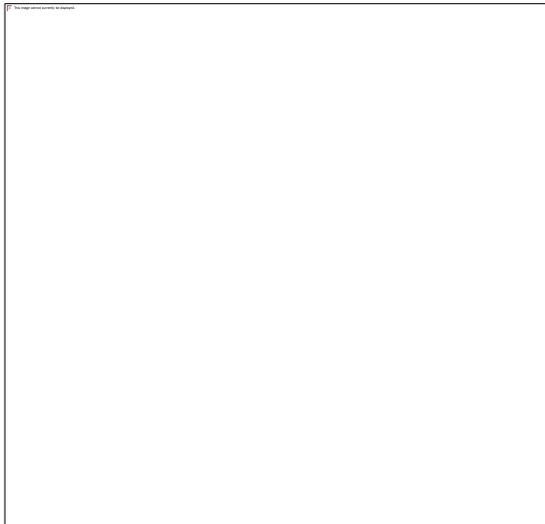
Examples of Mathematical Models



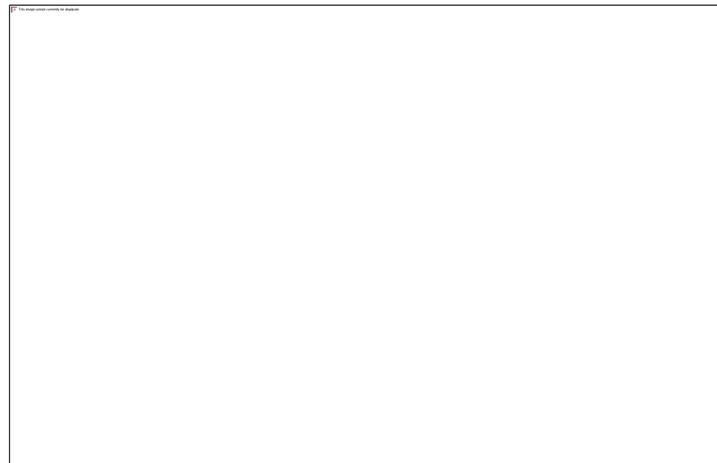
Adversary Sequence Diagram of a Physical Protection System



Cumulative Barrier Delay Timeline



Plume Model

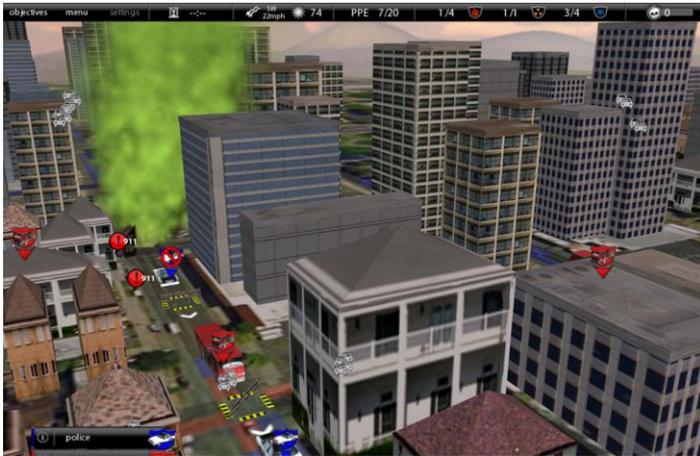


Pressure-time curve for a free air blast wave

$$P_E = P_I * P_N$$

System Effectiveness Equation

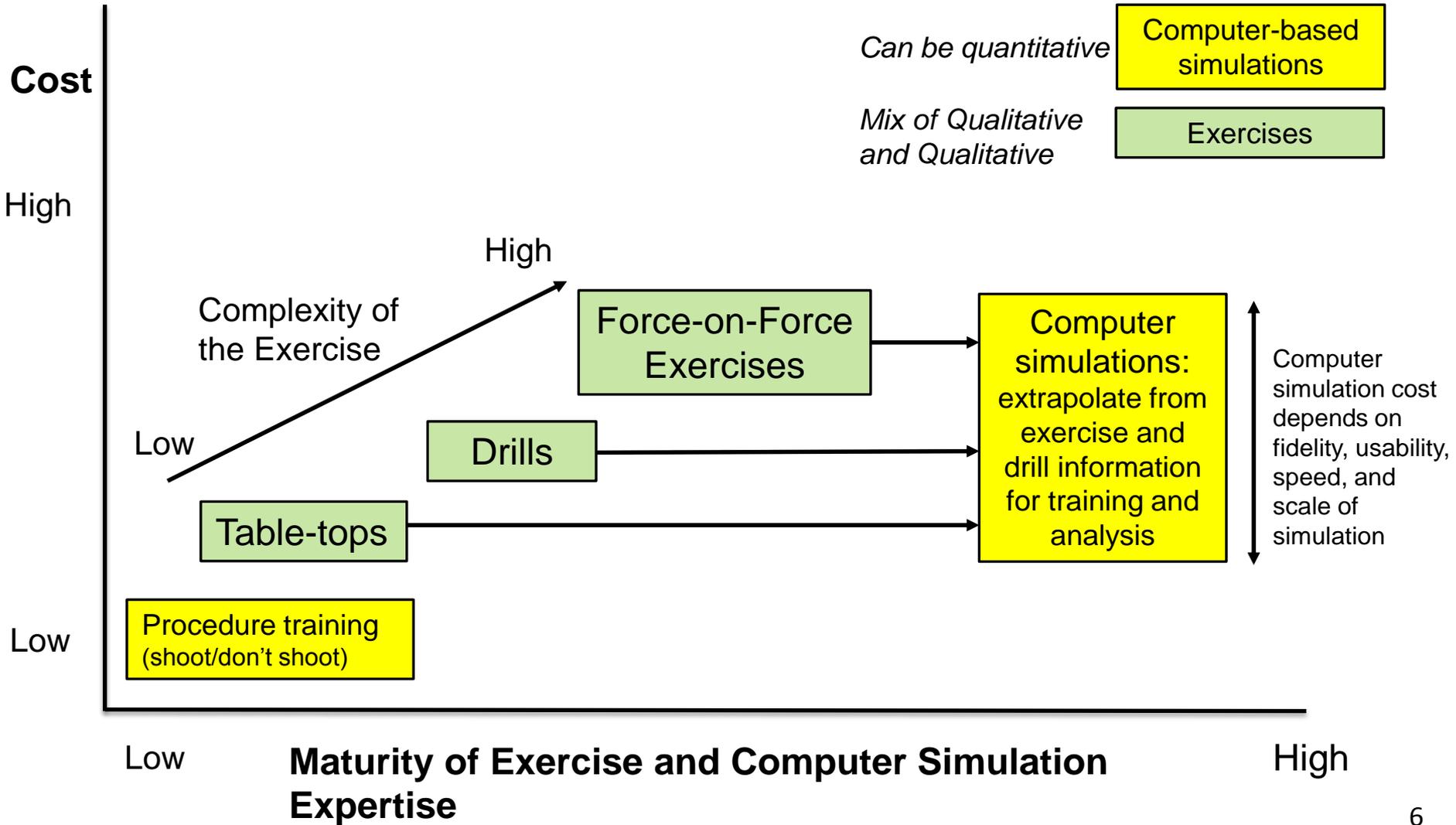
Types of Simulations



Computer Simulation – uses a “virtual” model of the city



Relationship Between Exercises and Computer Based Simulations



Simulation Strengths and Weaknesses

	Computer-Based	Force-on-Force	Drills	Table-Tops
Strengths	<ul style="list-style-type: none"> • Good at simulating some events: <ul style="list-style-type: none"> ○ Explosives ○ Munitions effects ○ Complex Systems • Detailed record of events • Minimal impact on operations • Flexible application <ul style="list-style-type: none"> • Can evaluate many different facility configurations • Can evaluate infinite number of variables 	<ul style="list-style-type: none"> • Better at simulating human behavior: <ul style="list-style-type: none"> ○ Individual ○ Team tactics ○ Real time decision making • Evaluates system as a whole • Controlled environment • Good training method • Greater fidelity in terrain and facility layout 	<ul style="list-style-type: none"> • Better at simulating human behavior: <ul style="list-style-type: none"> ○ Individual decisions ○ Team tactics ○ Real time decision making • Specific conditions can be evaluated • Controlled environment • Good training method 	<ul style="list-style-type: none"> • Better at simulating: <ul style="list-style-type: none"> ○ Leadership decision making ○ Plans and procedures
Weaknesses	<ul style="list-style-type: none"> • Does not simulate human behavior well • Requires many assumptions <ul style="list-style-type: none"> ○ Accuracy of assumptions may affect outcome • Computer operator skill may affect outcome 	<ul style="list-style-type: none"> • Difficult to simulate: <ul style="list-style-type: none"> ○ Violent acts such as explosions ○ High risk operations ○ Some weapons effects 	<ul style="list-style-type: none"> • Better at simulating human behavior: <ul style="list-style-type: none"> ○ Individual decisions ○ Team tactics ○ Real time decision making • Does not evaluate system as a whole 	<ul style="list-style-type: none"> • Does not simulate human behavior well • Requires many assumptions <ul style="list-style-type: none"> ○ Accuracy of assumptions may affect outcome • Requires skilled moderators

Application of Models in Security

- Path analysis tools are used to:
 - Evaluate the balance of detection, delay, and response in a physical protection system
 - Determine probability of interruption - Used as a measure of the effectiveness of the physical protection system
- Results of other models are used to determine protection requirements
 - As an example, radiological dispersal models are used to meet international guidelines
 - *“...the State should establish its threshold(s) of unacceptable radiological consequences in order to determine appropriate levels of physical protection.”*

IAEA Nuclear Series No. 13

Application of Simulations in Security

- Drills, Tabletops, Force on Force Exercises, and Computer Simulations are used to:
 - Train personnel
 - Evaluate command, control, and communications
 - Evaluate operational and contingency plans
 - Determine probability of neutralization - Used as a measure of the effectiveness of the physical protection system

Summary

- Models and simulations can be used to support
 - Leadership decision making and planning
 - Design of and evaluation of security systems
 - Training of security personnel
- They can improve
 - Decision making
 - Efficiency
 - Quality
 - Preparedness of responders
- They are not absolute reflections of real life, and should be used carefully and validated

Exceptional service in the national interest



History of Modeling and Simulation for Training and Analysis

SNL – Global Security Programs

Mark Snell



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. SAND2013-5879.

Outline

- Terminology for modeling and simulation
- General overview of modeling and simulation history for the military
- Security design and evaluation process (DEPO) for security
- Use of security modeling and simulation tools as part of the Design Evaluation Process Outline (DEPO)

Definitions

■ Model

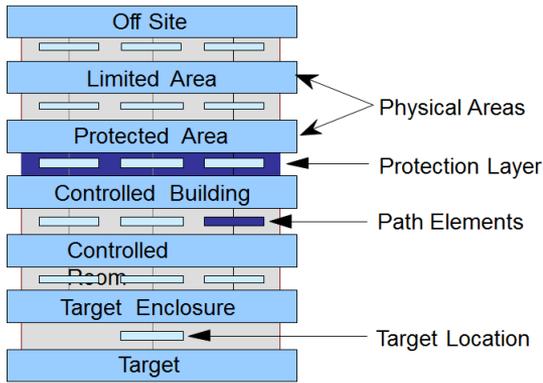
- A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process
 - Mathematical model: A symbolic model whose properties are expressed in mathematical symbols and relationships

■ Simulation

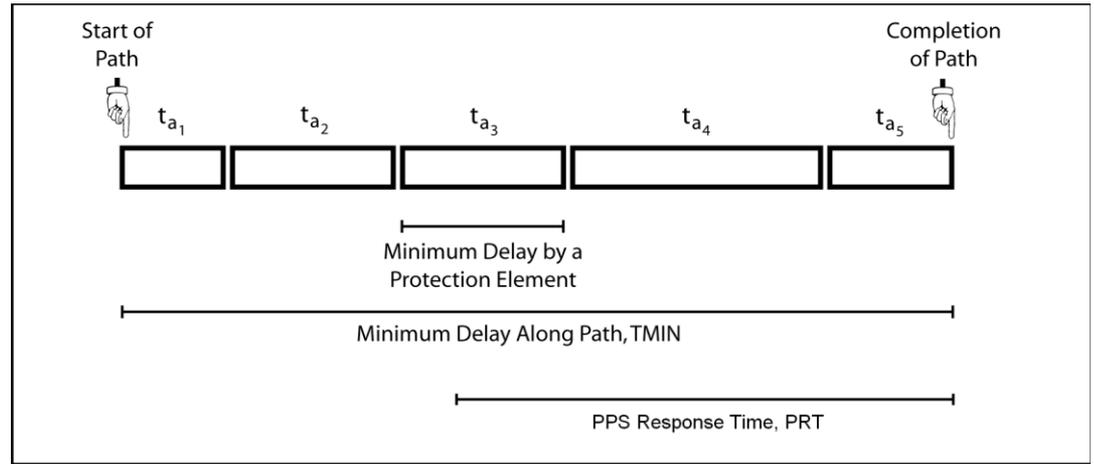
- A method for implementing a model over time
 - Includes live simulations like drills and exercises as well as computer-based simulations

Definitions excerpted from the DoD Modeling and Simulation Glossary

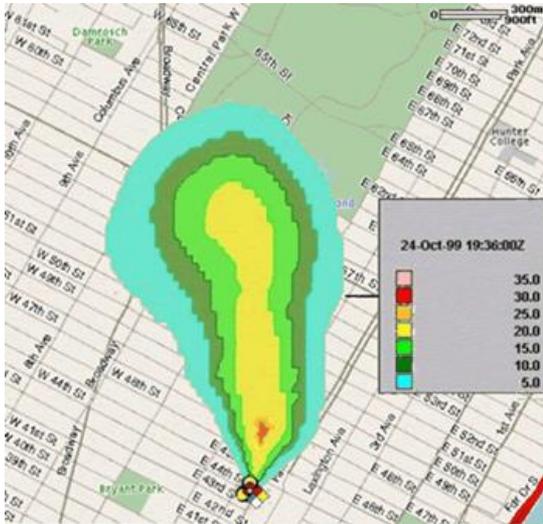
Examples of Mathematical Models



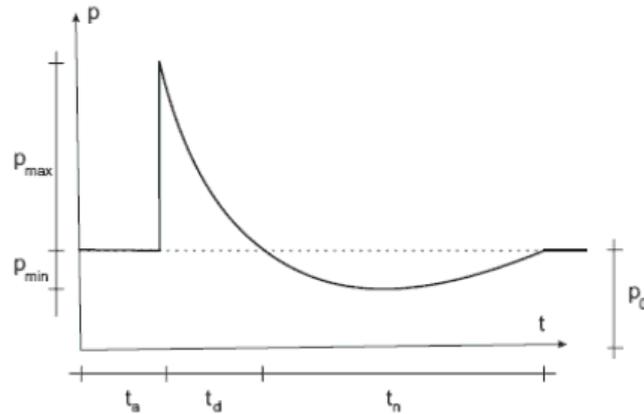
Adversary Sequence Diagram of a Physical Protection System



Cumulative Barrier Delay Timeline



Plume Model



Pressure-time curve for a free air blast wave

$$P_E = P_I * P_N$$

System Effectiveness Equation

Types of Simulations

- Real Simulations (Exercises): Real humans, real systems and environments



- Virtual Simulations: Real humans, *simulated* systems and environments

- Real decision-making and responses

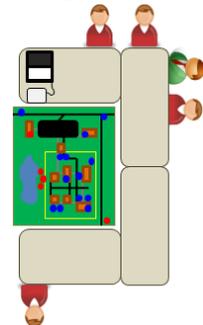


- Constructive Simulations: Real people providing input but simulated people, simulated systems and environments

Uses a computer model of the site



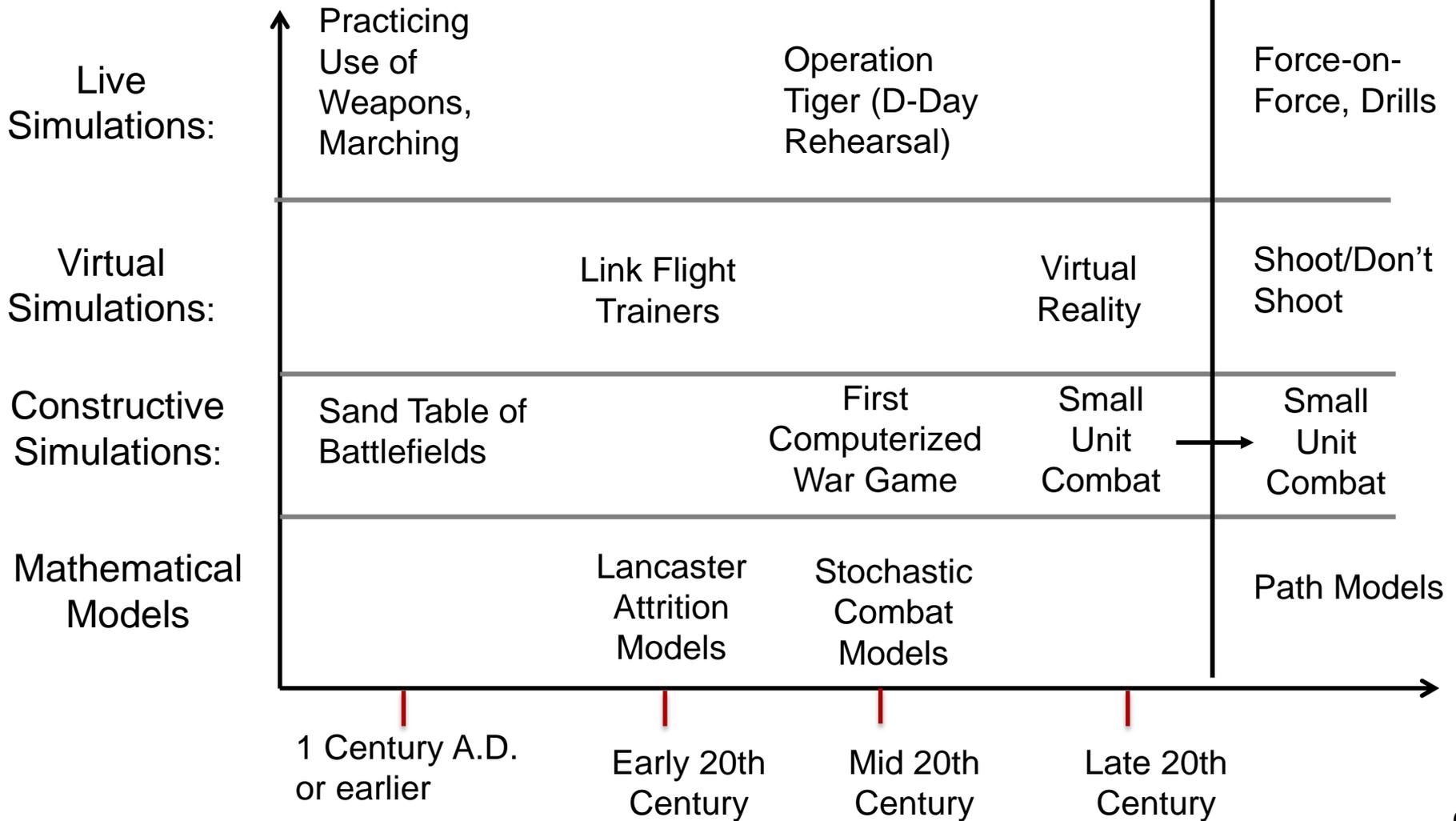
Map Exercise:
Sand Table



Use of Modeling and Simulation

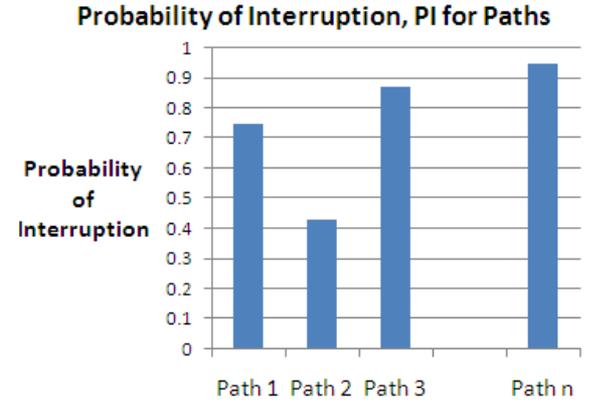
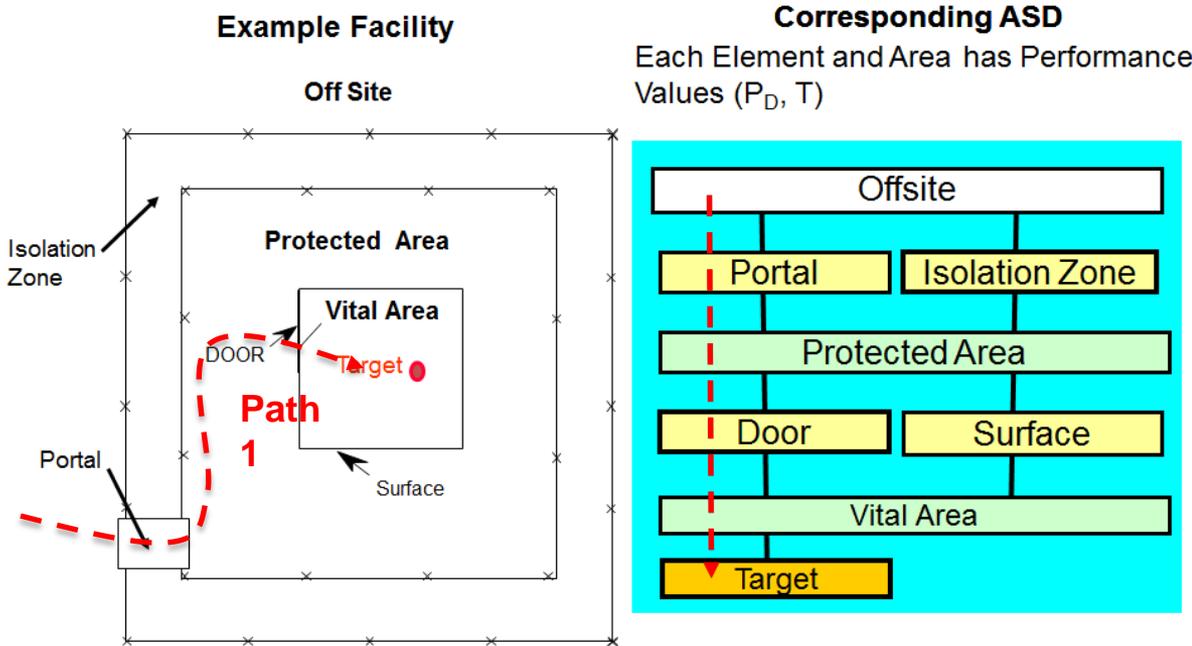
For Security Use

For Military Use

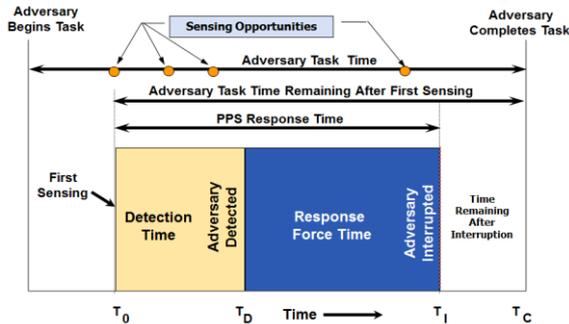


Path Analysis Mathematical Models

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

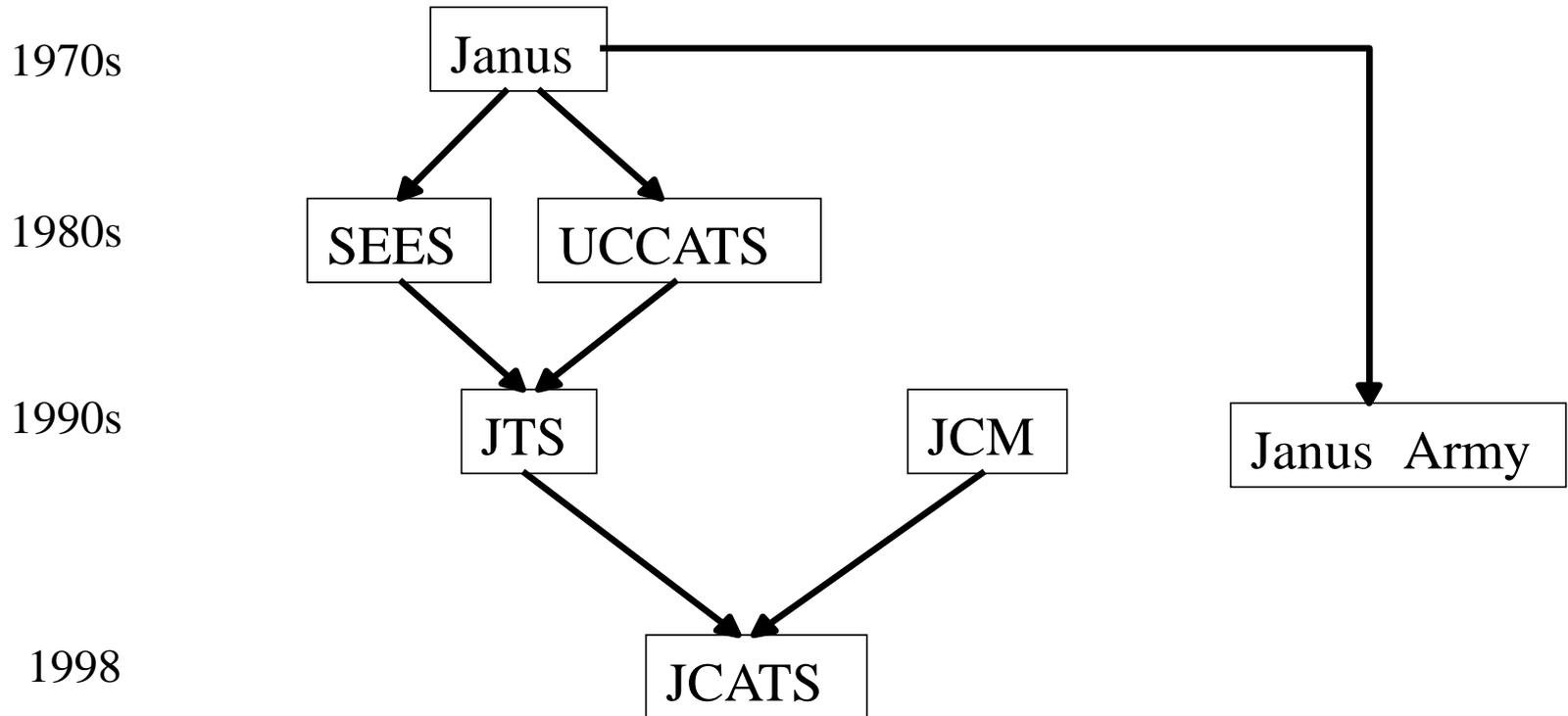


Timeline Models for Calculating Probability of Interruption

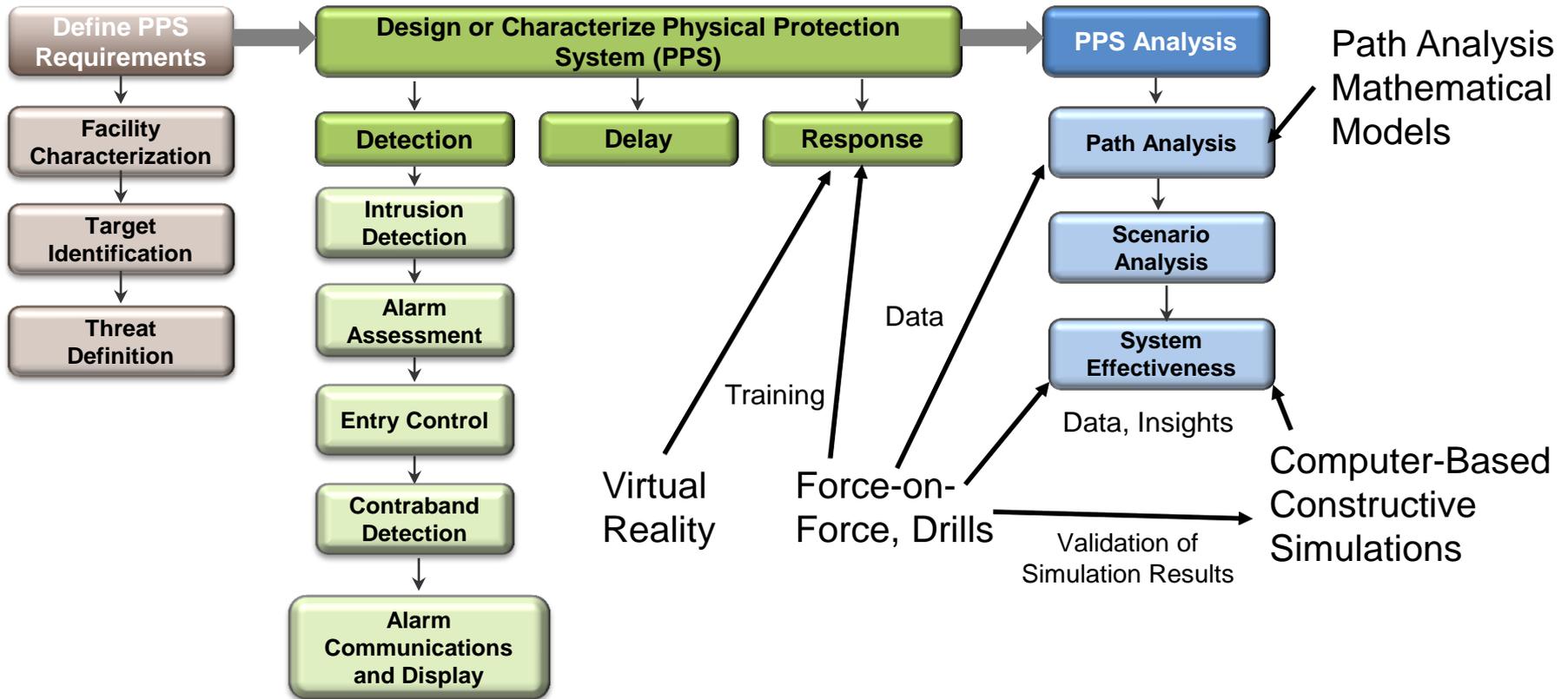


Examples
 1970's: PANL
 1980's: SAVI
 1990's: ASSESS

Small Unit Combat Simulation Timeline



Design Evaluation Process Outline Used for Security Analysis and Design



Considerations for Use

- No security model or simulation is completely accurate
 - Decision should not be based solely on the results of models and simulations
- Controls should be established to get the best results
 - Assumptions should be supported when practical
 - Databases should be controlled
- Validation of model or simulation
 - First collect evidence from exercises and testing before running model or simulation
 - Then evaluate evidence to see if model/ simulation results are close enough to exercises/tests results to be useful
 - Finally if useful, extrapolate to other training or analysis cases

Summary

- Specific terminology associated with modeling and simulation
 - Mathematical models
 - Virtual, real, and constructive simulations
- Modeling and simulation for military use has an long and extensive history
- Security modeling and simulation tools are used as part of the Design Evaluation Process Outline (DEPO) and for training