

VA Methodology and Demonstration

ASSESS & SAVI

Jim Lloyd
Security Analyst
Sandia National Labs
International Security Programs

Janice Leach
Security Analyst

April 24, 2007

SANDXXXXXX

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.



What is a VA?

- A systematic analysis that attempts to determine the effectiveness with which a “Petroleum Facility” is being protected against defined threats.
- Effectiveness is measured by Risk
- Based on the performance of a security system rather than a checklist or compliance approach.



Vulnerability Analysis

What is a VA?

- Design/Evaluation Process
- Path Analysis using ASSESS/SAVI
 - ASSESS software Overview
 - Path Analysis
 - Scenario Analysis



Evaluation of PPS Design

Step III Evaluate the Design

- EASI Model
- Table top
- SAVI
- ASSESS
- JCATS
- FOF



Risk Analysis

- How do we know if security measures are good enough?

$$\text{Risk (R)} = P_A * [1 - (P_I * P_N)] * C$$

- Probability of Interruption - P_I from ASSESS/SAVI
- Probability of Neutralization - P_N from JCATS/STAGE
- Consequence Value (C)
- Probability of Adversary Attack P_A

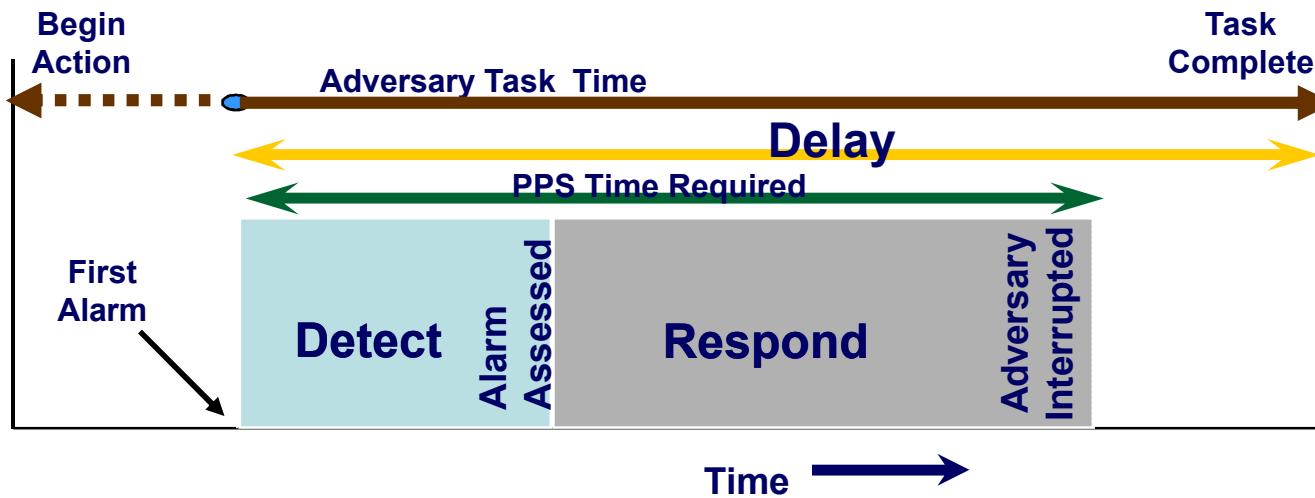


Sandia Security Methodology

- Detection
 - Assessment
- Delay
- Response



Sandia Security Methodology



Adversary Task Time
vs.
PPS Time Requirements



Path Analysis

- Describe Petroleum Facility by Adversary Sequence Diagram (ASD)
 - Concentric layers
 - Protection elements between layers
- ASSESS algorithm identifies paths with lowest Probability of Interruption



ASSESS

- ASSESS is a computerized tool for performing integrated safeguards evaluation
 - Considers nonviolent insiders, outsiders, and a special form of insider / outsider collusion
 - Focuses on theft and diversion of nuclear material
 - Provides a capability for “planning” and “managing” evaluation for many targets and facilities

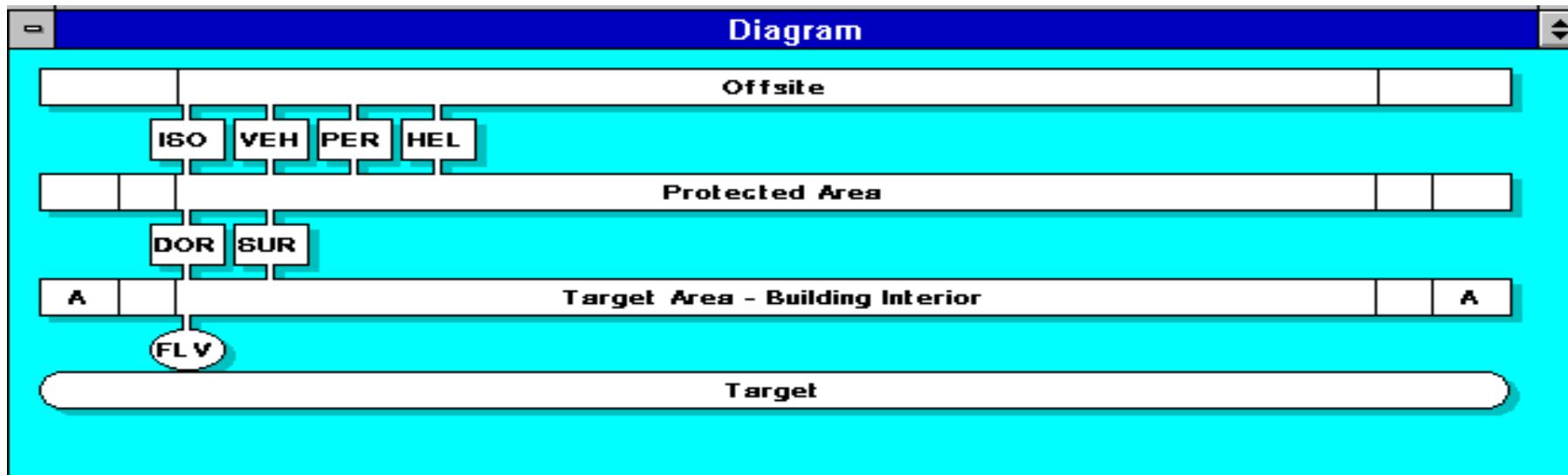


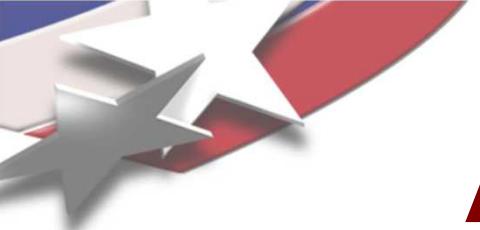
ASSESS Facility

- The Petroleum Facility Description Module is used for inputting common data for all the evaluation modules
 - Uses a graphical display (ASD) to depict facility layout
 - Contains extensive catalogs of safeguards hardware and procedures
 - Considers two states (e.g., open and secure)



Adversary Sequence Diagram





ASSESS Outsider

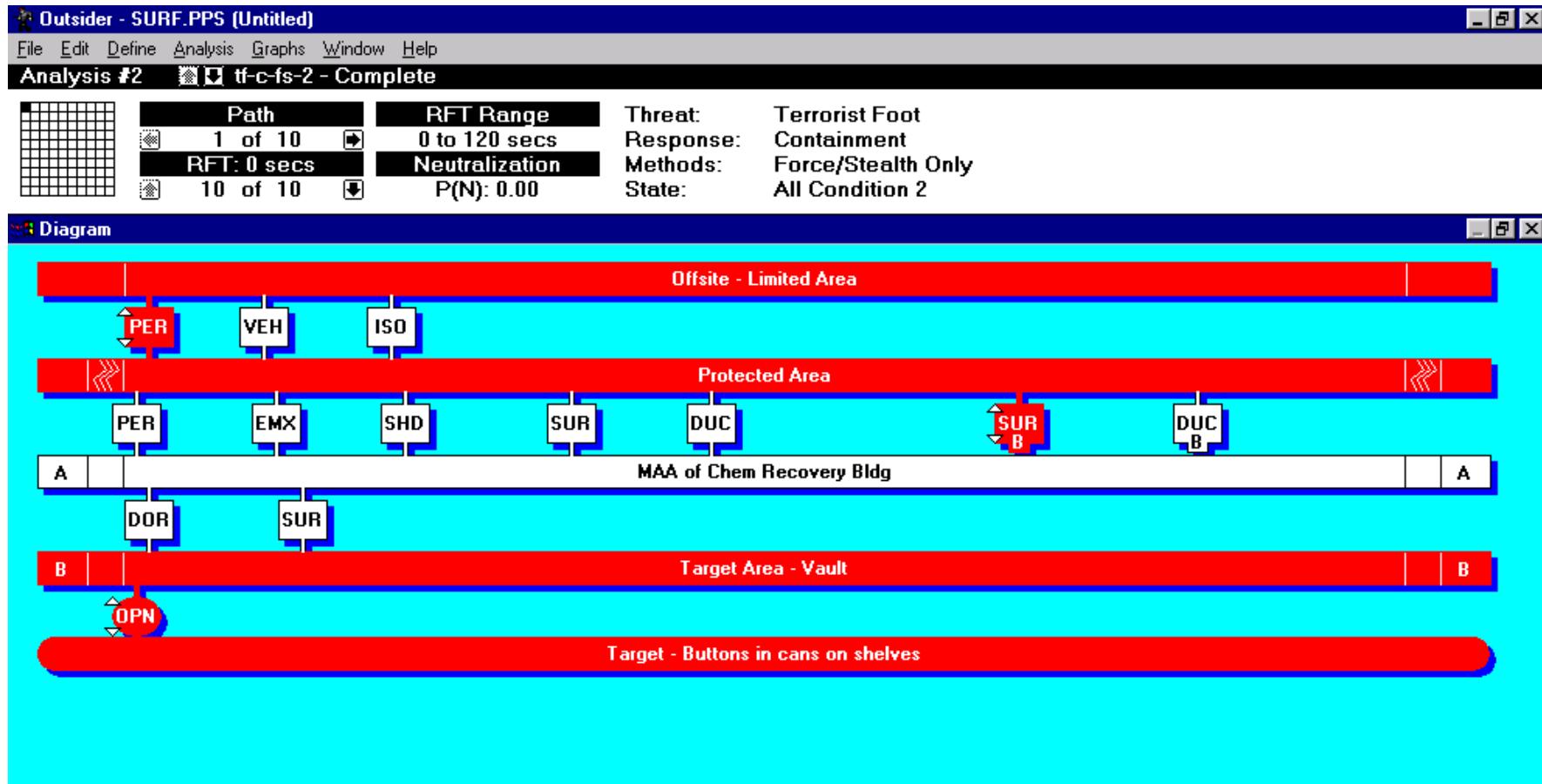
- The Outsider module calculates the “most vulnerable paths” for a spectrum of outsiders
 - Considers terrorists, criminals, psychotics, and antinuclear extremists
 - Analyze both the detection and delay components of a facility’s safeguards system
 - Incorporates a fast algorithm for path calculations

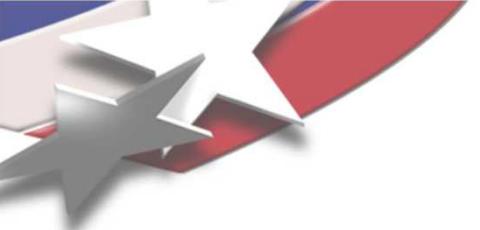


Outsider Input

- Facility State Information
- Defensive Strategy (Containment / Denial)
- Threat Capabilities
- Threat Tactics
- Protective Force Response Times

Outsider Output





ASSESS Insider

- The Insider module incorporates many features
 - Uses detailed facility data
 - Explicitly defines adversary access and authority attributes
 - Includes an extensive database
 - Predefined strategies based on facility-specific features



ASSESS Insider

- The Insider module incorporates many features
 - Probabilities of detection based on safeguards and target characteristics, strategies, and adversary attributes
 - Provides for summary and detailed graphical and tabular results
 - The Insider Module combines data gathered in the Facility module and insider-specific information

Insider Input

- Insider Types
- Access
- Authority
- Keys

Access & Authority

Edit Options

Personnel

SI	Manager
Operator	SI supervisor
Health Physics	✓ SI
Maintenance	✓ Operator
	✓ Health Physics
	✓ Maintenance
	✓ Production Super
	✓ MBA custodian
	Vault tech
	Janitor

Select access

Key access

Location	Condition	1	2
Limited Area		✓	✓
PER-PA Pedestrian ...		✓	✓
VEH-PA Vehicle Portal		✓	✓
Protected Area		✓	✓
PER-MAA Portal		✓	✓
SHD-MAA Shipping ...		✓	✓
MAA of Chem Recov...		✓	✓
DOR-Vault door		✓	✓

Select authority

Access to alarms at CAS

✓ Staffs security post
✓ Assesses SNM alarms
✓ Assesses security alarms
Maintains security alarms
Maintains SNM monitors
✓ Tests security alarms
Tests SNM monitors
Calibrates metal detectors
Supervisory auth over SI
Monitors proc cntrl alrms

Select personnel types

Personnel

Manager	Ok
SI supervisor	Cancel
✓ SI	Rename
✓ Operator	New type
✓ Health Physics	Weights
✓ Maintenance	
✓ Production Super	
✓ MBA custodian	
Vault tech	
Janitor	

Key Access

Select key or combination type for each area for personnel:

SI

Location with a lock

Limited Area

✓ PER-PA Pedestrian Portal
✓ VEH-PA Vehicle Portal
Protected Area
✓ PER-MAA Portal
EMX-MAA Emergency Exit
✓ SHD-MAA Shipping Door
MAA of Chem Recovery Bl
✓ DOR-Vault door

Lock type

Single
 Part A of double lock
 Part B of double lock
 ID Lock Bypass

Keys and combinations selection available only where locks are defined.



Insider Output

Insider - surf.pps surf.in

File Edit Define Results Displays User Defined Special Help

Diagram

Offsite - Limited Area

Protected Area

MAA of Chem Recovery Bldg

Target Area - Vault

Target - Buttons in cans on shelves

Optimal scenarios

Overall Personnel	Pd.	exit from Target Location		
		Pd	Elem (C)	Strategy
SI	.33	.25	OPN (1)	Unauthorized removal
Operator	.00	.00	OPN (1)	Append to authorized removal
Health Physics	.10	.00	OPN (1)	Acquire during evacuation
Maintenance	.19	.10	OPN (2)	Unauthorized removal
Production Super	.33	.25	OPN (1)	Unauthorized removal
MBA custodian	.25	.25	OPN (1)	Unauthorized removal

Sandia National Laboratories

Insider Output

Offsite - Limited Area

Strategy Detail

Path element probability calculation for:

Strategy: Unauthorized traversal

Path element: EMX-MAA Emergency Exit

Personnel: SI

Condition: Dayshift-Open Direction: Exit

Calculated Pd at path element = .10

Safeguards: Defeat method: Pd:

Position monitor	Disable/alarm statn	.10
SI patrol	Avoid suspicion	.00
General observation	Avoid suspicion	.00
Evacuation alarm	Not applicable	.00
Penetration sensor	Not applicable	.00

User defined: _____

Outsider safeguards note (#)

User defined Description

Override strategy Pd.

Probability of detection:

Note:

Protected Area

DUC SUR B DUC B

A of Chem Recovery Bldg

Target Area - Vault

- Buttons in cans on shelves

EMX-MAA Emergency Exit alternate strategies

1 2

Prob. of Det. for 1st condition exit using strategy

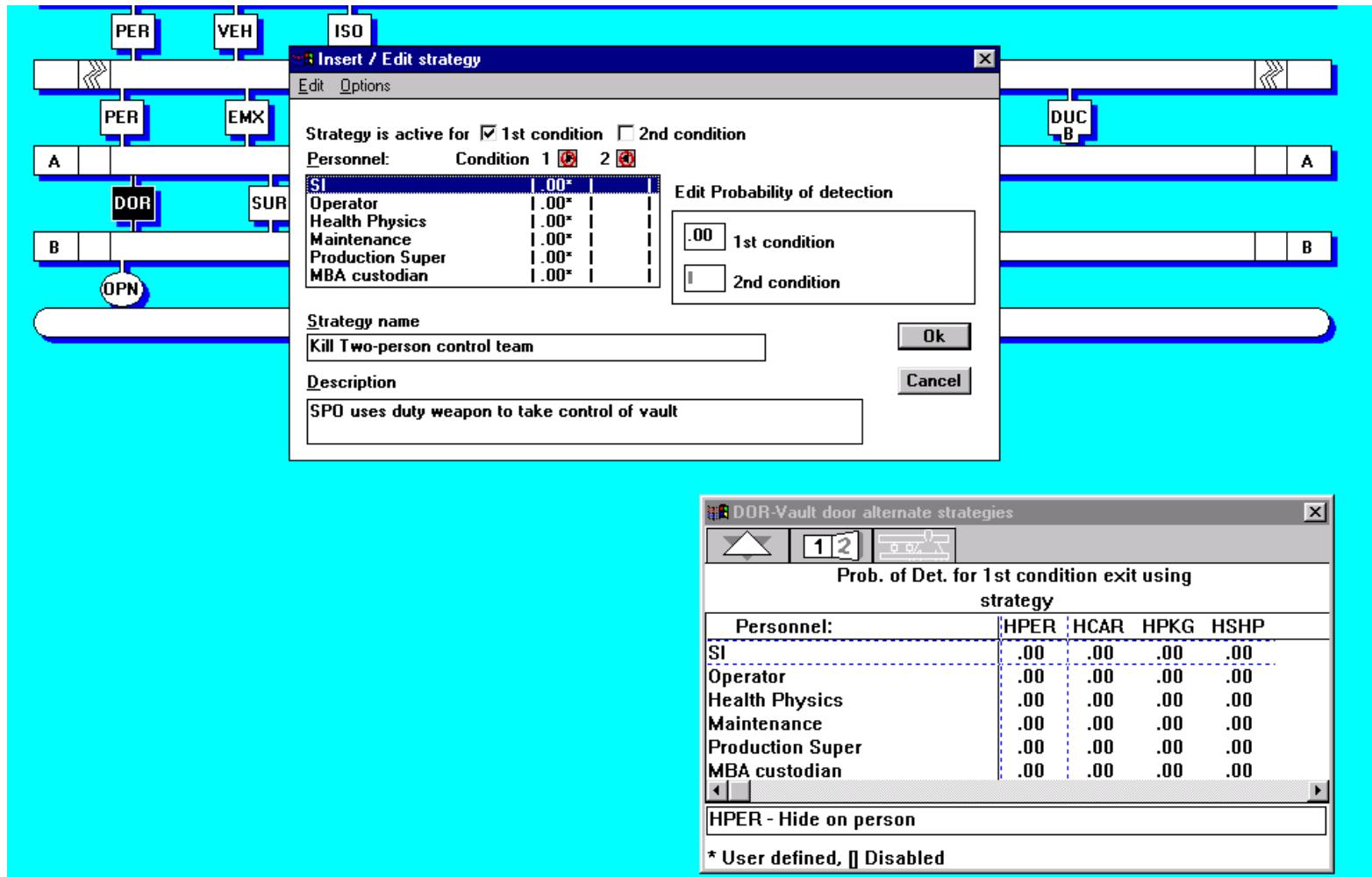
Personnel:	TRVS	DRLL	EVAC
SI	.10	.00	.00
Operator	.25	.00	.00
Health Physics	.25	.00	.00
Maintenance	.25	.00	.00
Production Super	.25	.00	.00
MBA custodian	.25	.00	.00

TRVS - Unauthorized traversal

* User defined, [] Disabled



Active Violent Strategies





Collusion

- Insiders Assisting Outsiders
 - Change Protection Effectiveness against Outsiders
 - Insiders Open Vaults, disable alarms, impede response, etc.
- Outsiders Assisting Insiders
 - Change Protection Effectiveness against Insiders
 - Outsiders engage responders, facilitate facility exit, etc.



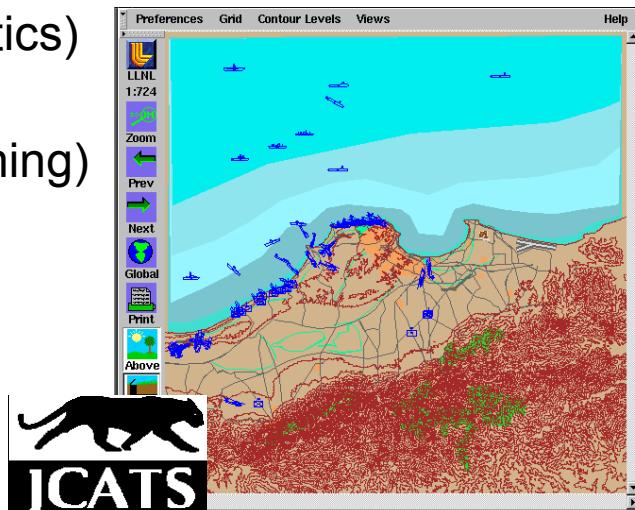
JCATS

What is JCATS?

JCATS is a cost effective method for modeling small force engagements in both rural or urban settings.

JCATS is a computer-based conflict simulation used by a number of government agencies for:

- training (individuals, staffs, command elements)
- analysis (weapons, force structure, tactics)
- planning (course of action analysis)
- mission rehearsal (coordination and timing)





JCATS

JCATS/Warrior Code Elements

- Terrain Map
 - DTEDS
- Force Plan
 - (ALPHA Files)
 - Adversary Composition
 - Response Force Composition



Google Earth



JCATS Terrain Editor



JCATS

Protocol

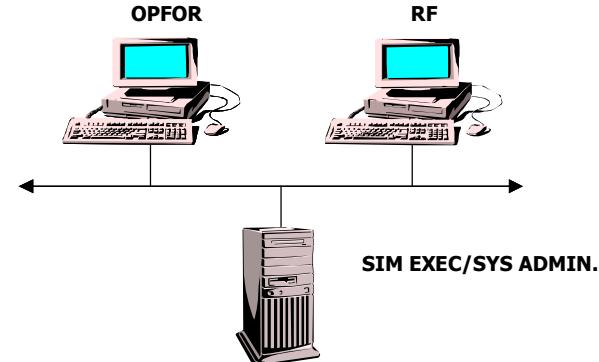
- ASSESS/ATLAS Path & Thieves scenario
- SME round table creates overall scenario
 - Delay Expert
 - Physical Security Experts
 - Pro Force and Military Tacticians
- BATLE P_N / Order of battle
- Setup JCATS scenario, test, & run
 - One Time Set-up (Baseline & Upgrade)
 - Time / Run starts @ 0:00
 - Pause @ after target task time (Data collection point)
 - 3-5X speed during certain activities

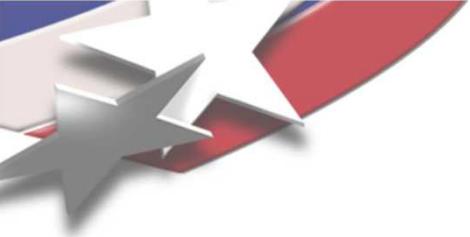


JCATS

Warrior Code Methodology

- Two operators
 - Response Force
 - OPFOR
- Limited number of systems available (predefined)
- Pre-node and lengthy setup
 - Nodes inclusive of delay and task times
- Shoots On
- Short run times





JCATS

What JCATS Can Model

- Optical and thermal sensors
- Explosives
 - Bombs
 - IED
 - Claymores
- Entity level movement, acquisition, and targeting
- Movement and engagement in rural and urban areas
- ChemBio Effects
 - ChemBio agents affect the health of systems
 - Effects are modeled in two ways:
 - Red-Blood Cell Acetylcholinesterase (RBC-A ChE) depression model
 - » Relates cumulative ingested dose of nerve agents to the % inhibition of RBC-A ChE activity
 - LD50
 - » Expressed as mg-min/m³