SAND2007-2535P

VA Methodology and Demonstration

ASSESS & SAVI

Jim Lloyd
Security Analyst

Janice Leach
Security Analyst

Sandia National Labs
International Security Programs

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.

National Nuclear Security Administration

Sandia National Laboratories

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

Sandia National Laboratories

Evaluation of PPS Design

Step III
Evaluate the Design

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

Sandia National Laboratories

Risk Analysis

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

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

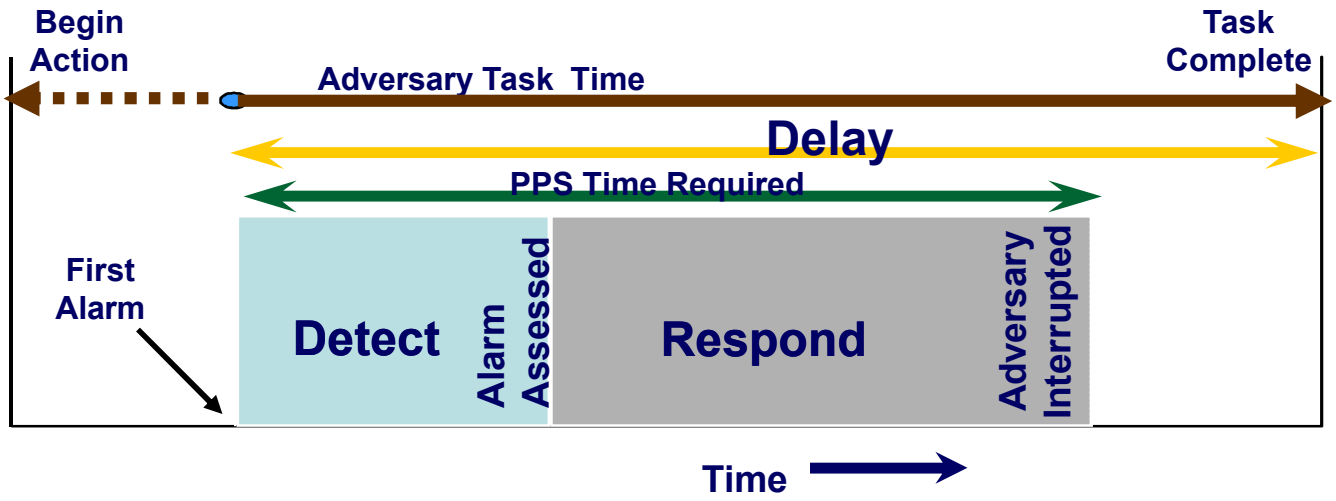
  - Probability of Interruption - P_I from ASSESS/SAVI
  - Probability of Neutralization - P_N from JCATS/STAGE
  - Consequence Value (C)
  - Probability of Adversary Attack P_A

Sandia Security Methodology

- Detection
  - Assessment
- Delay
- Response

Sandia National Laboratories

Sandia Security Methodology



Adversary Task Time
vs.
PPS Time Requirements

Sandia National Laboratories

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

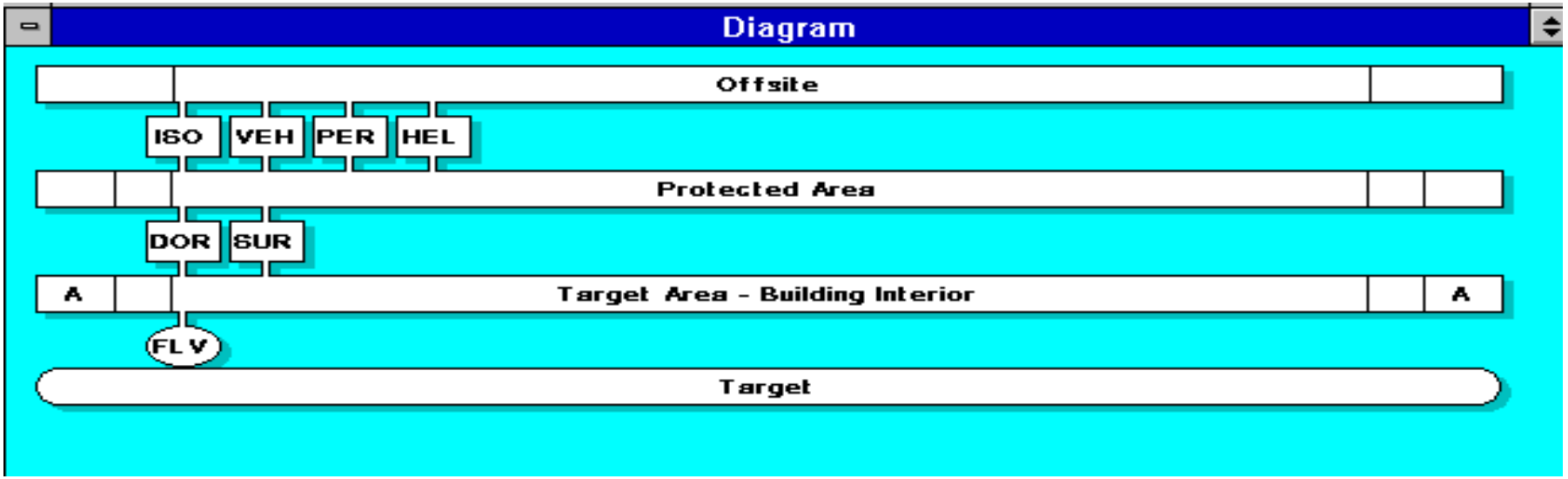
ASSESS

- 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



Sandia National Laboratories

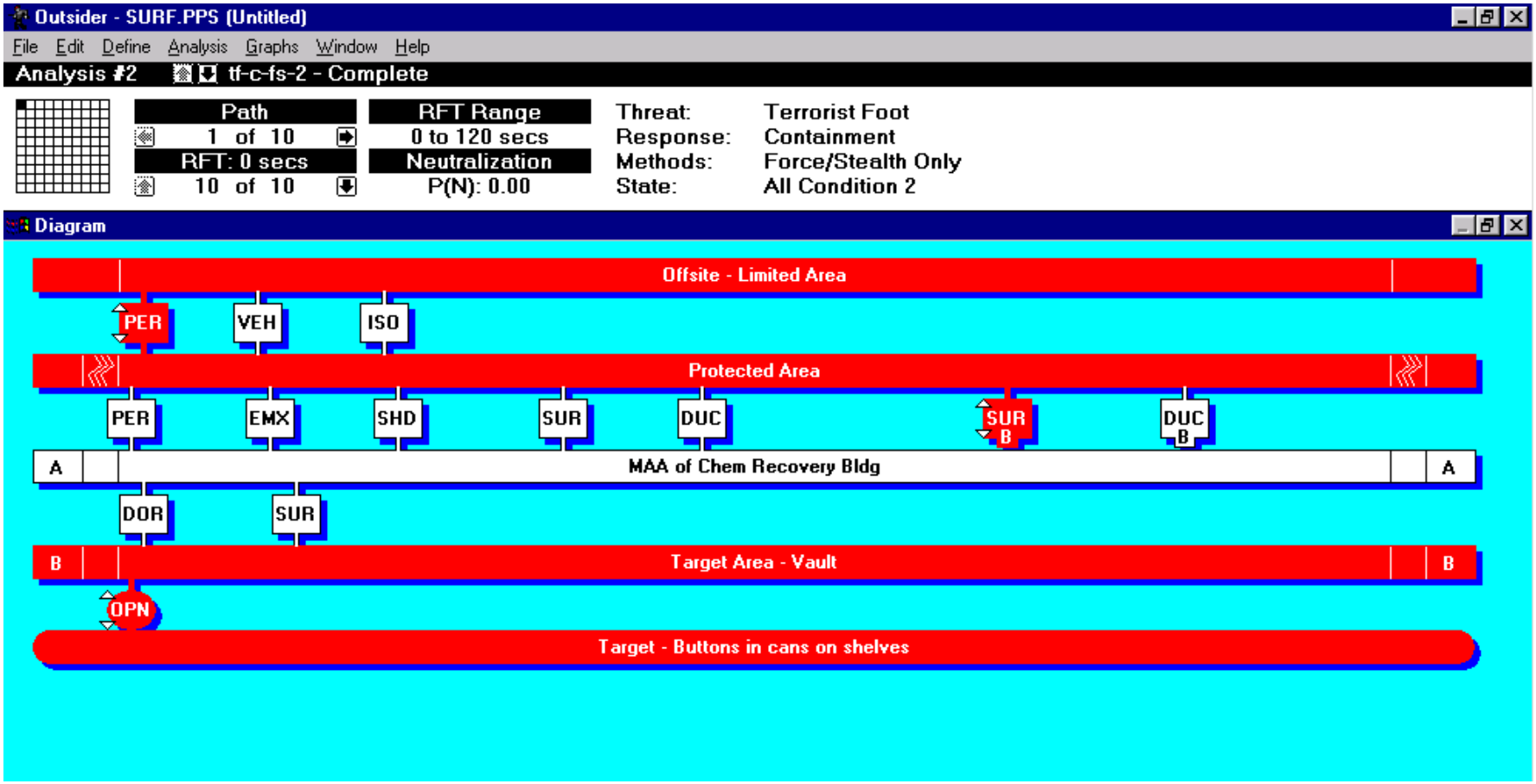
ASSESS Outsider

- 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



Sandia National Laboratories

ASSESS Insider

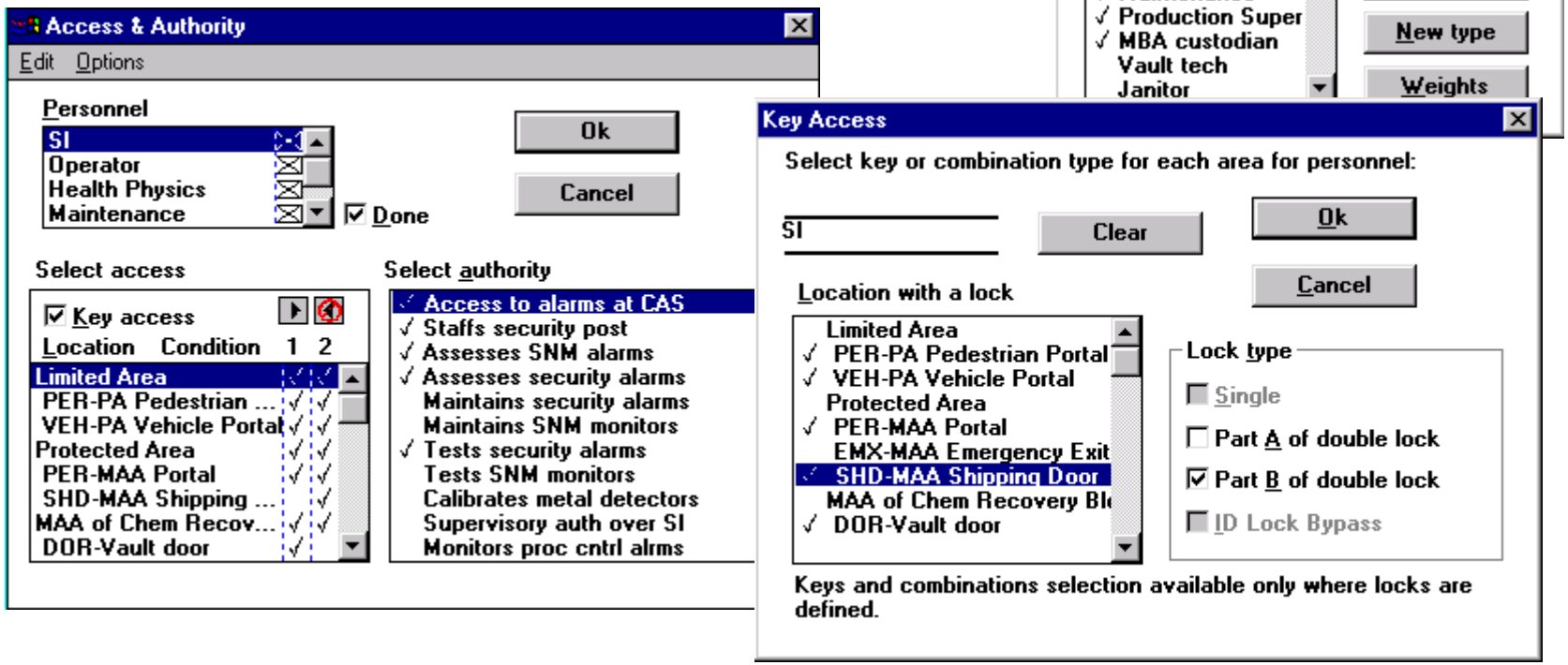
- The Insider module incorporates many features
  - Uses detailed facility data
  - Explicitly defines adversary access and authority attributes
  - Includes an extensive database
  - Predefined strategies based on facility-specific features

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

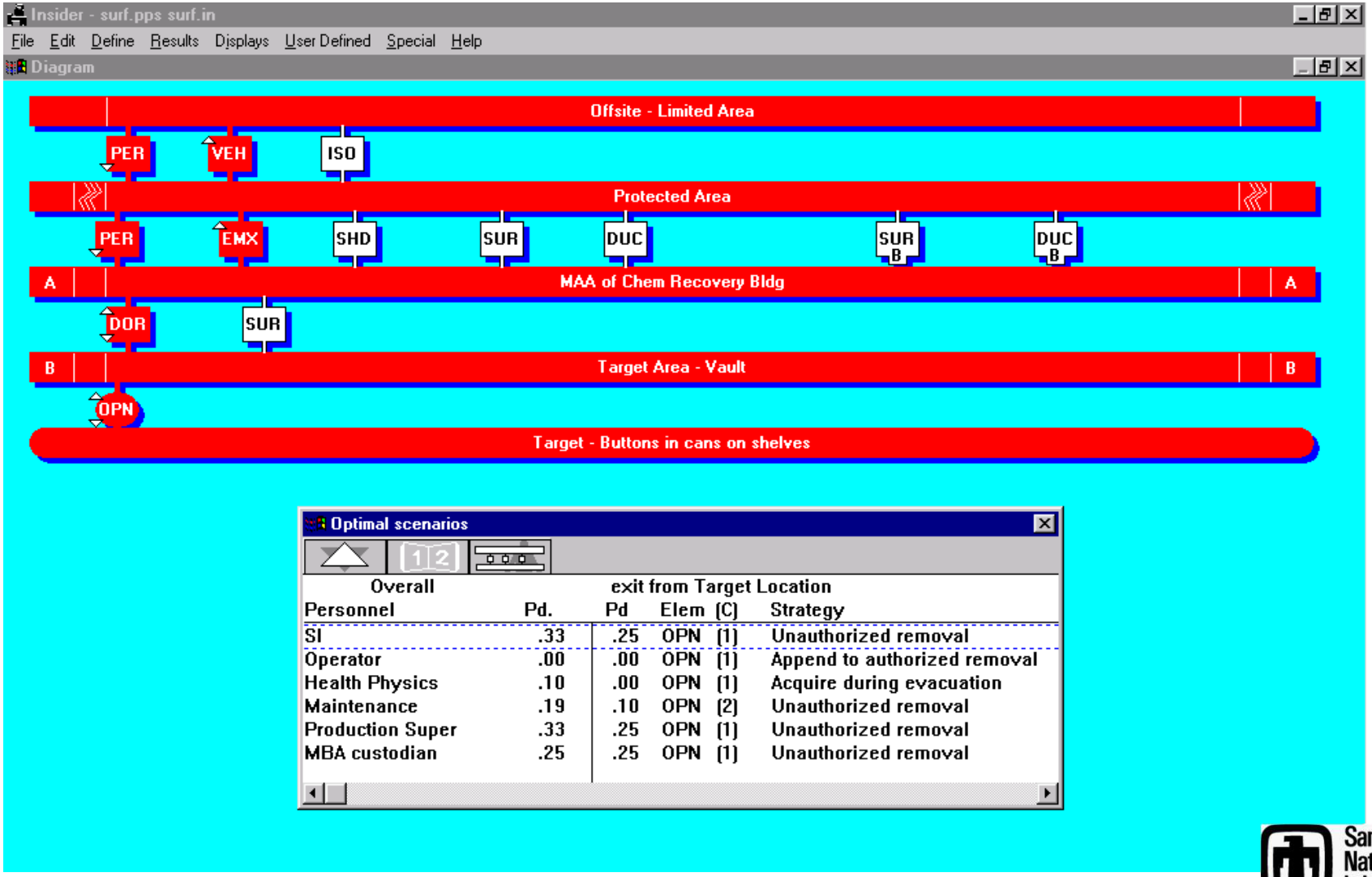
Insider Input

- Insider Types
- Access
- Authority
- Keys



Sandia National Laboratories

Insider Output

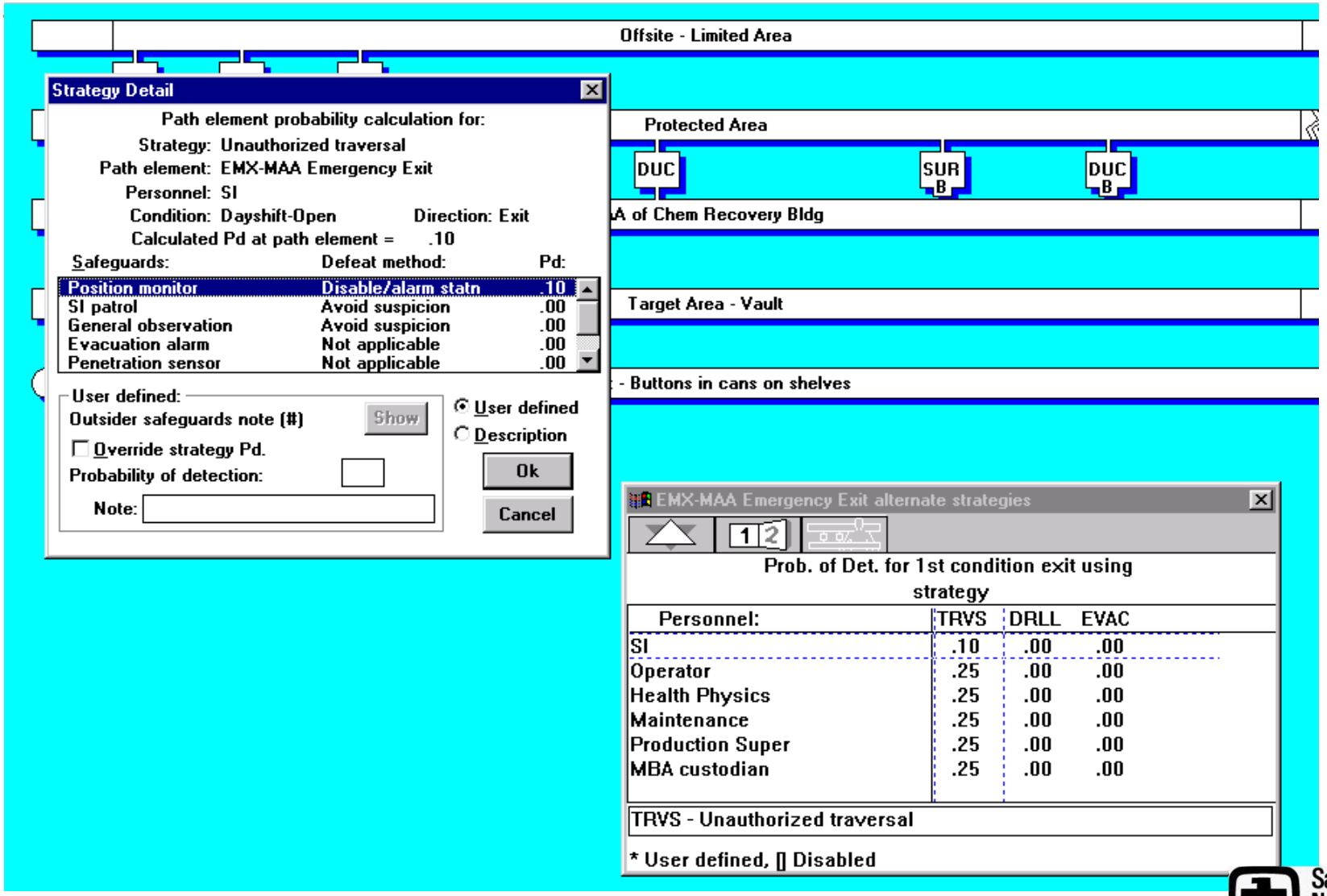


Optimal scenarios

Personnel	Overall 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

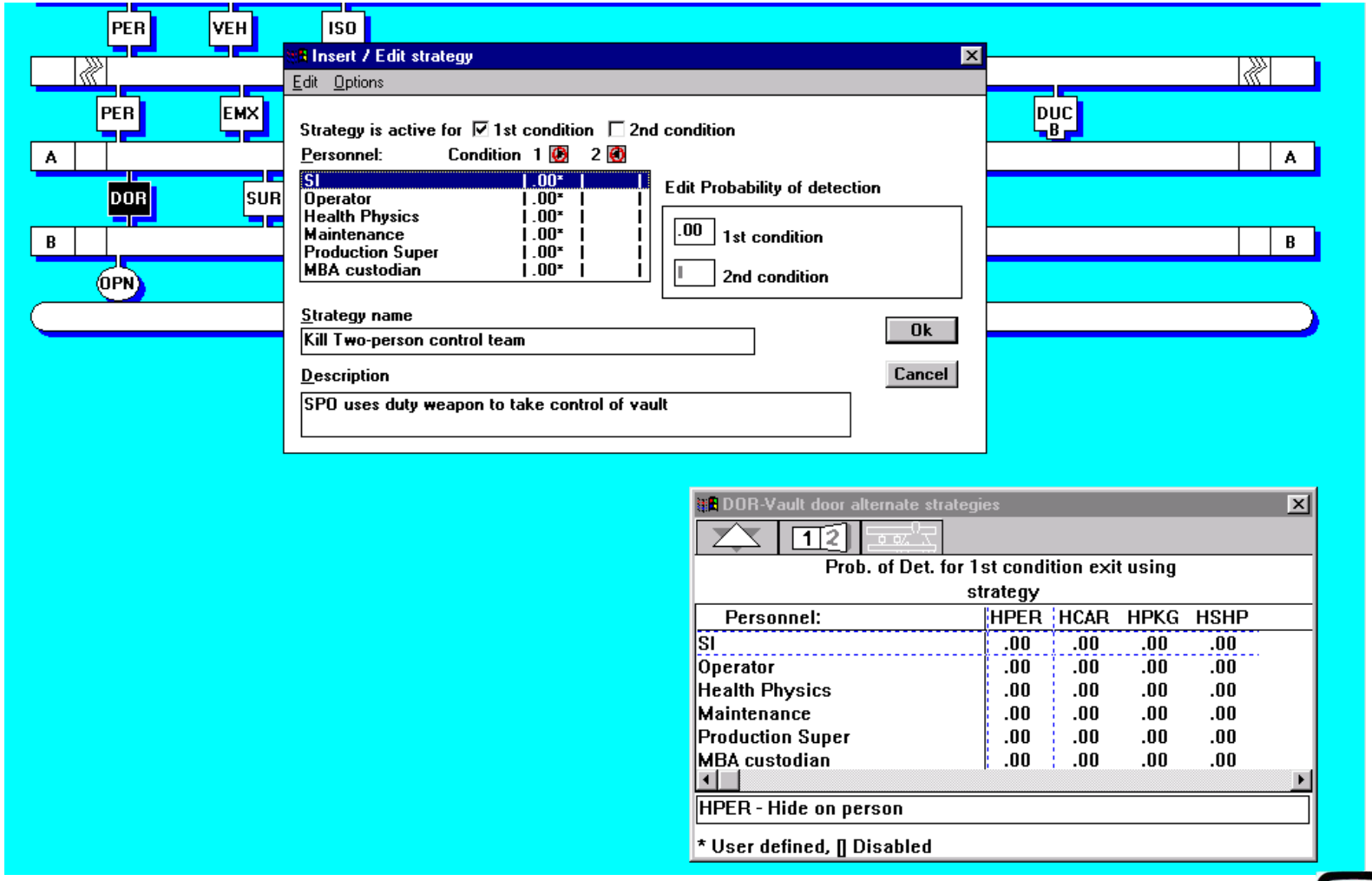
Sandia National Laboratories

Insider Output



Sandia National Laboratories

Active Violent Strategies



Sandia National Laboratories

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.

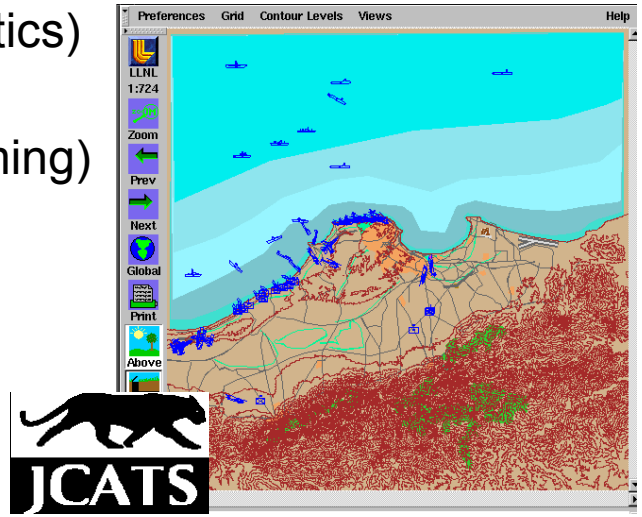
JCATS

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)



Sandia National Laboratories

JCATS

JCATS/Warrior Code Elements

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

Google Earth

JCATS Terrain Editor

Sandia National Laboratories

JCATS

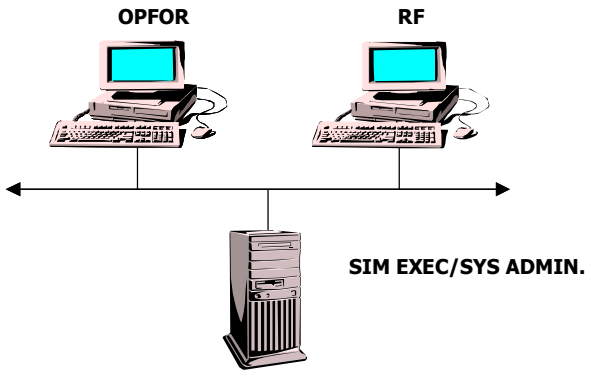
Protocol

- 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