SAND2007-3326C

Overview of Vulnerability Analysis Tools

International Best Practices in Nuclear Security Risk Management: Philosophy, Tools and Techniques

May 30-31, 2007

Manoj K Bhardwaj
Vulnerability Analysis Modeling and Simulation Department, Sandia National Labs

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.

Outline

- Brief Overview Of Risk Equation
- The “workhorse” tools
  - Adversary Time-Line Analysis System (ATLAS)
  - Joint Conflict And Tactical Simulation (JCATS)
- Future Directions

Acknowledgements

- Brady Pompei, Laura Whittet, James Rivera, Vernon Koonce, Rich Grochowski, Dean Dominguez…
- Mark Snell, Nate Roehrig, Brad Key, Jerry Karasz, Junko Mondragon, Trina Russ, James Garrison…
- Tommy Woodall, Dennis Miyoshi…
- DOE HSS – Carl Pocratksy, Sam Callahan, Bruce Campbell…

Brief Overview Of General Risk Equation

Risk Equation

$$\text{Risk} = P_A \times (1 - P_E) \times C$$

where

P_A = probability of attack (for a specified time frame)

P_E = probability that system will be effective against attack

C = Consequence of attack

Conditional Risk

$$R_C = (1 – P_E) = (1 – P_I \times P_N)$$

where

P_I = the probability that response force will interrupt adversary

P_N = the probability that response force will neutralize adversary

Sandia National Laboratories

“Workhorse” Tools

Vulnerability Analysis – Workhorse Tools

- ATLAS used for P_I
  - Calculates overall system effectiveness probability given neutralization probability
- JCATS used to help determine P_N

ATLAS

- Software program that analyzes the vulnerabilities in the physical protection systems
  - Discrete calculation that identifies most vulnerable paths for outsider, passive insider, and violent insider attacks
  - Models multiple security system states (normal operation, offshift, holiday, etc)
  - Identifies critical protection elements (potential single points of failure)
  - Contains extensive safeguard performance database
- Designed to provide the user with
  - A repository for Vulnerability Assessment (VA) documentation
  - An application for supporting decisions about site security

Physical Protection Systems
Performance Based Approach

- Definition: **Examines the detection, delay, and response elements of each facility to determine the overall system effectiveness, and helps customize the system at each facility to reduce risk to an acceptable level.**

Detection

Detect the Threat

- Intrusion Sensing
- Alarm Communication
- Alarm Assessment
- Entry Control
- Contraband Detection

Delay

Delay the Threat

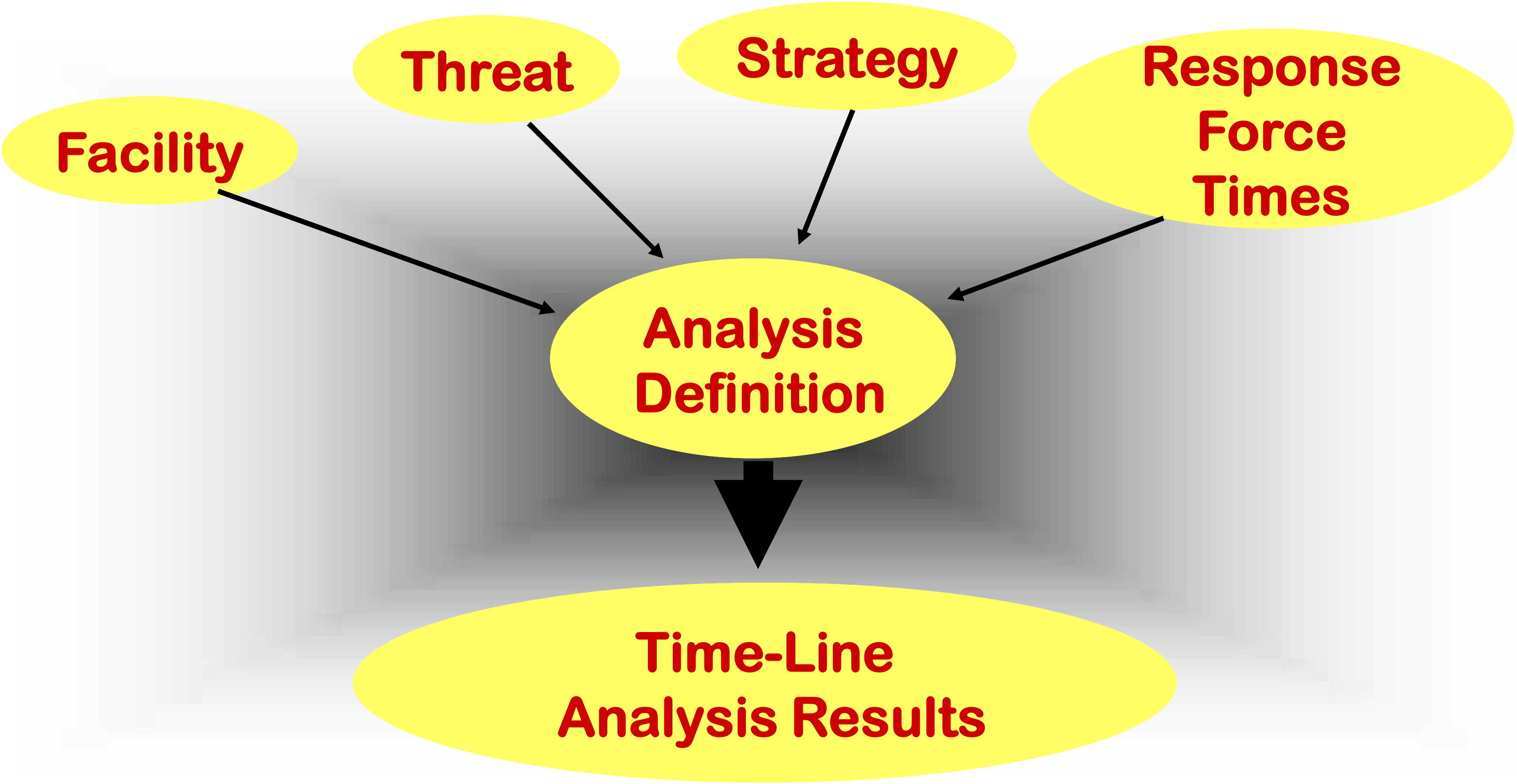
- Passive Barriers
- Active Barriers

Respons
e

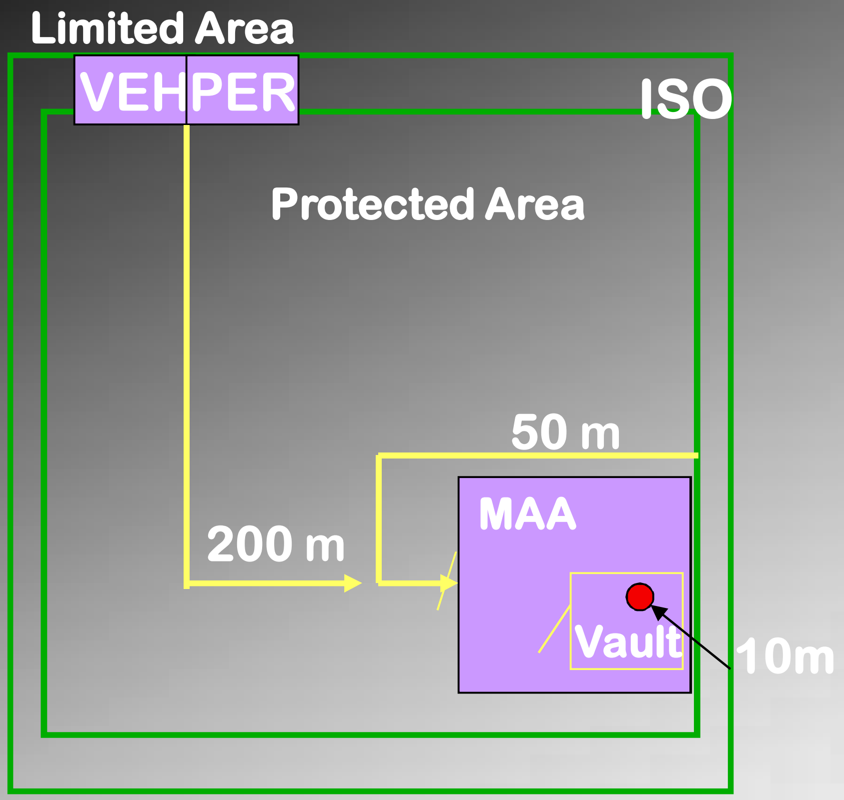
Interrupt and Neutralize the Threat

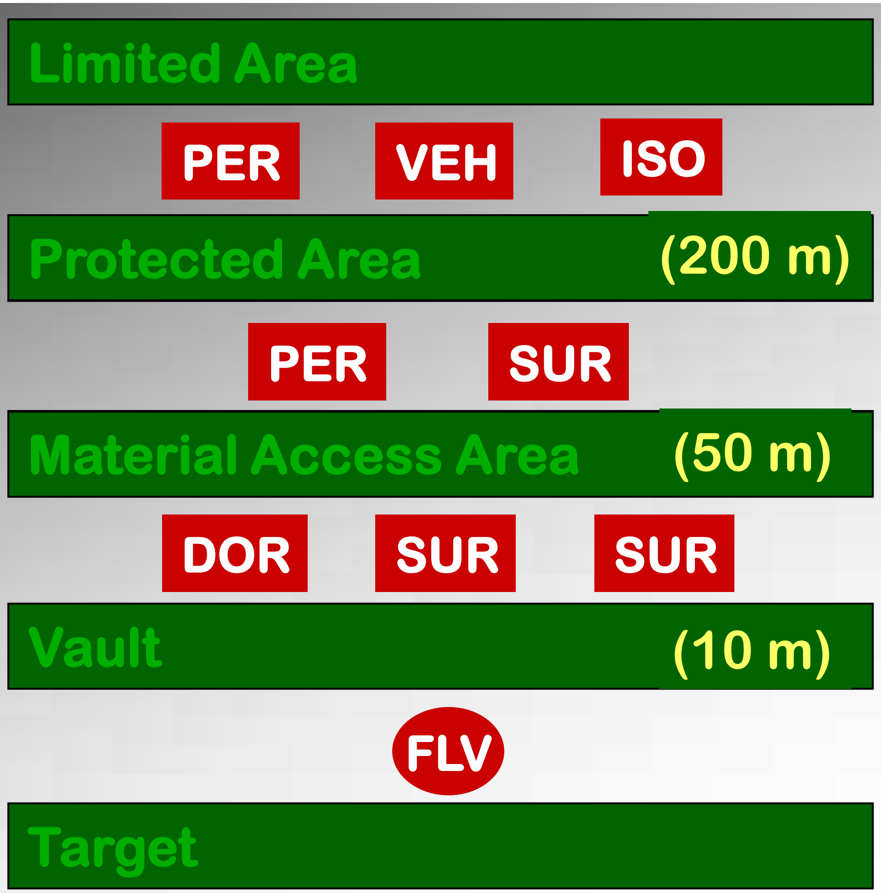
- Interruption- Deployment of the response force
- Neutralization

ATLAS System Overview



Facility Map to Adversary Sequence Diagram (ASD)





Limited Area

PER VEH ISO

Protected Area (200 m)

PER SUR

Material Access Area (50 m)

DOR SUR SUR

Vault (10 m)

FLV

Target

Threat

- **Outsider: Distinguished by equipment set and transportation**
  - **Equipment – Hand tool, power tool, etc..**
  - **Transportation – Land Vehicle, Helicopter**

- **Violent Insider: Distinguished by access and authorities, equipment set and transportation**
  - **Access and Authorities – Perform searches, access to badges, etc.**

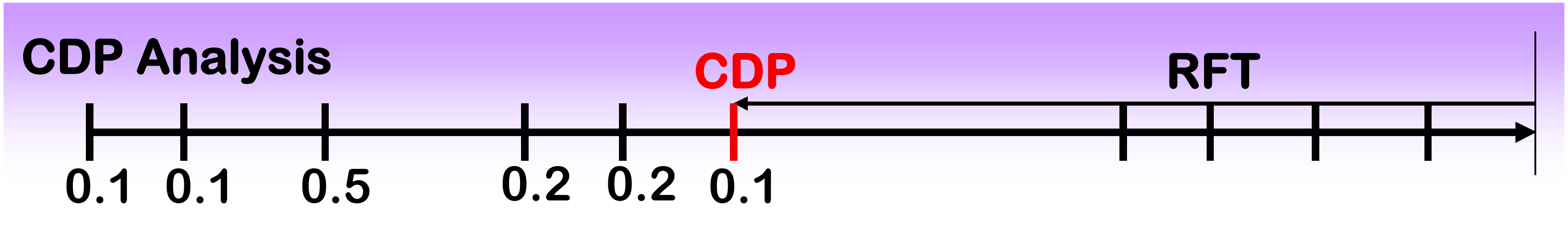
Response Strategy

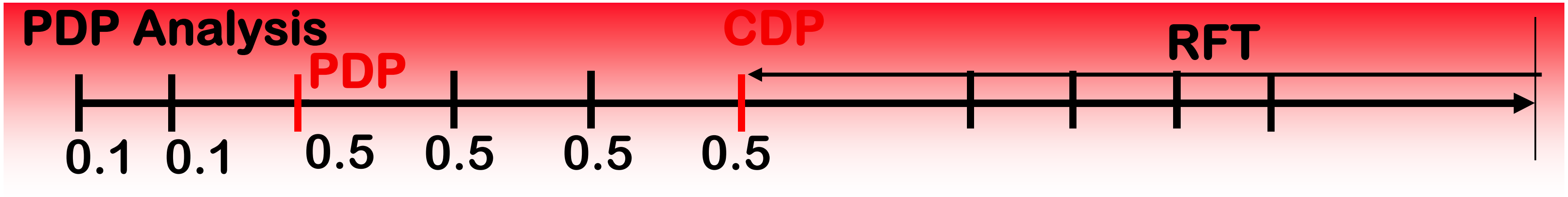
- Denial: Preventing the intruder/s (either Outsider or Insider) from getting to the target to perform threat action
  - Scenario – sabotage
- Containment: Preventing the intruder/s from accessing the target and taking it out of the facility
  - Scenario - theft

Time-Line Analysis Methods

- **CDP Analysis**
  - Minimize PD before CDP
  - Minimize Delay after CDP

- **PDP Analysis**
  - Motivation – may not be practical to continue minimizing detection when near CDP if avoided detection is small Minimize P_D until Cum. P_D would exceed user-defined PDP Threshold (this is PDP location)
  - Switch over to minimizing delay immediately



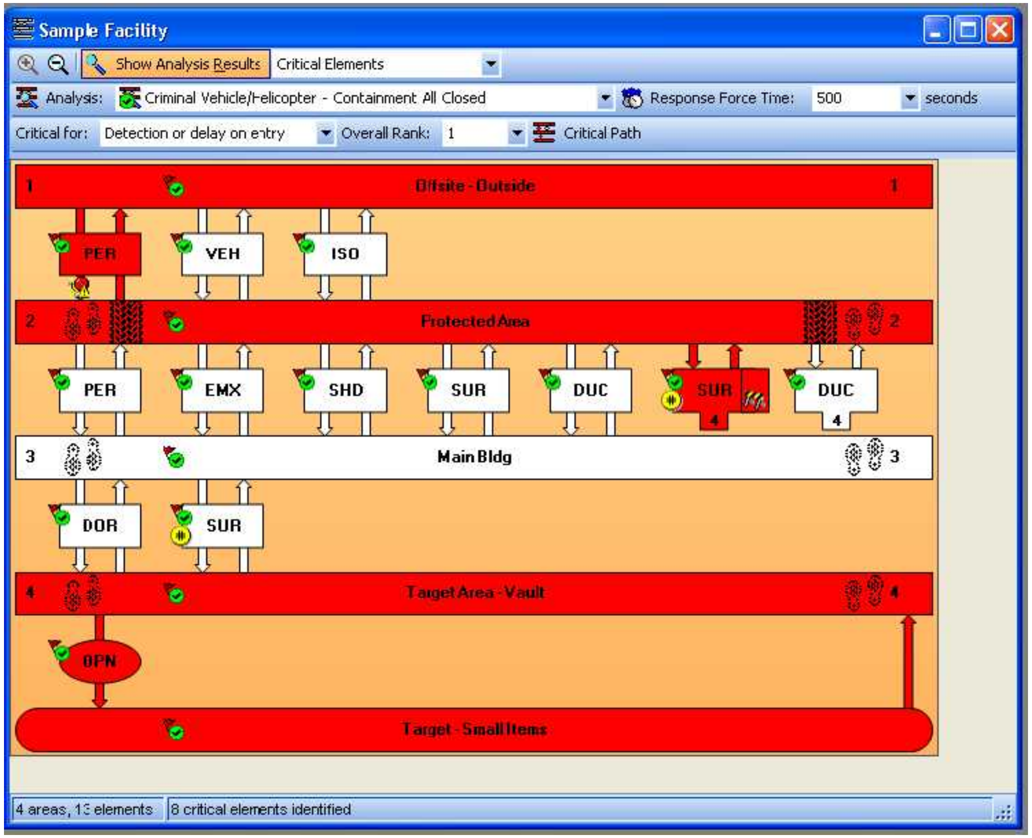


Critical Element Analysis

Definition: **determines elements that if singularly degraded would reduce the system effectiveness below the user specified critical system effectiveness level (P_E*).**

Attributes

- **Critical elements are determined for detection and delay**
- **The path on which element e is critical is displayed**
- **Critical elements are ranked by minimum percent degradation required to make the element critical**
- **Methodology is currently implemented for Outsider and Violent Insider CDP analyses.**



Sample Facility

Show Analysis Results: Critical Elements

Analysis: Criminal Vehicle/Helicopter - Containment All Closed

Response Force Time: 500 seconds

Critical for: Detection or delay on entry

Overall Rank: 1

Critical Path

4 areas, 13 elements

8 critical elements identified

Sandia National Laboratories

ATLAS Summary

- **ATLAS analysis methodology has been used throughout DOE for over 15 years**
  - **Discrete analysis tool to calculate most vulnerable paths (not a simulation)**
  - **Excellent tool for evaluating potential upgrade cost/benefit**
- **Leverages Sandia National Laboratories (SNL) Vulnerability Assessment (VA) expertise**
  - **Subject Matter Expert for Design Evaluation Process Outline (DEPO)**
  - **Extensive VA experience at both DOE and DOD sites**

Joint Conflict And Tactical Simulation (JCATS)

What is JCATS?

- **Joint Conflict and Tactical Simulation**
- **A multi-sided, interactive, entity level conflict simulation used by the military and government security agencies for:**
  - Training (individuals, staffs, command elements, JOINT)
  - Analysis (weapons, tactics, PPS effectiveness)
  - Planning (course of action analysis)
  - Mission rehearsal (coordination and timing)
  - Experimentation (force size, delay options, weapons)
- **Characteristics:**
  - A real-time, stochastic, human-operated simulation modeled at the entity-level

JCATS History

Campaign (Tactical) Models

1974	JANUS
1992	Joint Conflict Model

Urban Combat Models

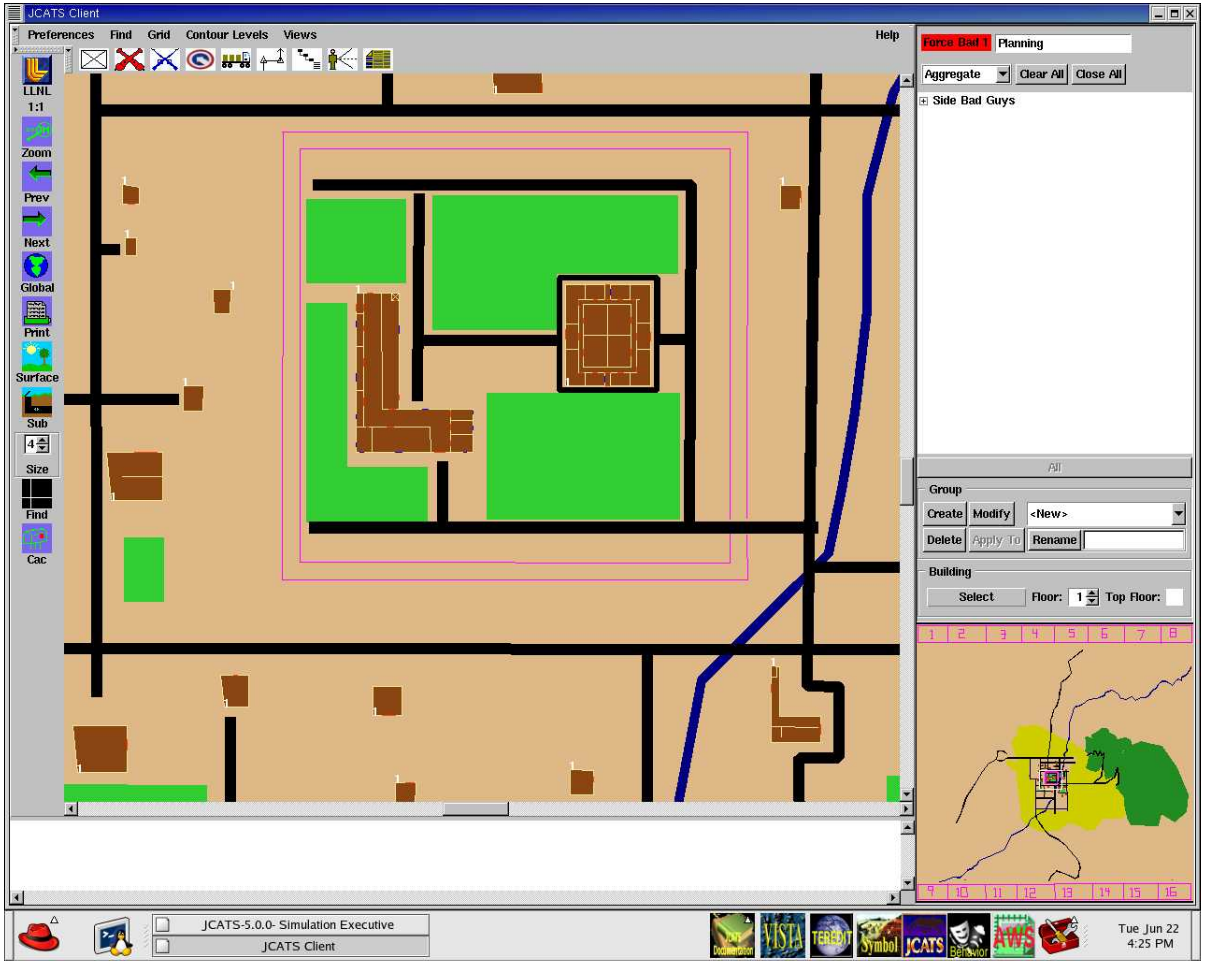
1989	Security Ex Eval System
1991	Urban Combat Trng System
1995	JOINT Tactical System

- **Theater-Level and Small-Force simulations were combined to create JCATS**
- **Latest Version is 7.1**
- **Runs on Desktop or Laptop PCs**
- **Small scale simulations can be run on very modest computers**
- **Uses Red Hat Enterprise Linux**

JCATS Capabilities

- Entity Level
  - Troops, ground vehicles, aircraft and watercraft
    - Weapon and munitions, size, speed, vulnerability, etc.
- 3D terrain model with a 2D user interface
  - Satellite imagery – topography
  - Shape files – buildings, roads, fences
- Interactive display
  - Operators control movement, engagement, etc.
  - Report capabilities – ammo count, terrain, energy levels, etc.
- Human operators emulating human responses
  - Not a computer making human decisions

JCATS Client



Force Bad 1 Planning

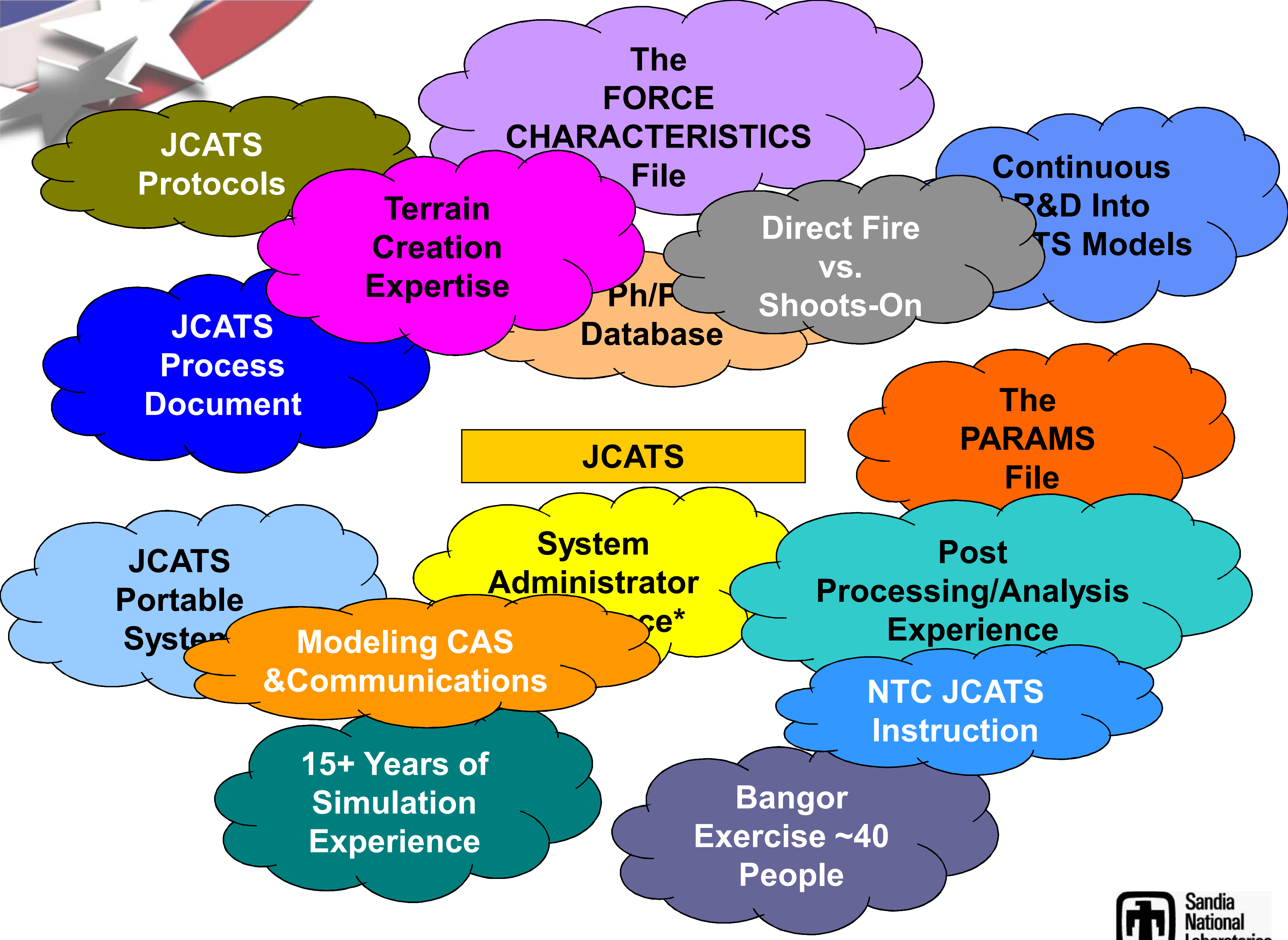
Aggregate

4

<New>

Floor: 1

Operating The JCATS System



The FORCE CHARACTERISTICS File

JCATS Protocols

Terrain Creation Expertise

Continuous R&D Into TS Models

Direct Fire vs. Shoots-On

Ph/F Database

JCATS Process Document

JCATS

The PARAMS File

System Administrator ce*

Post Processing/Analysis Experience

JCATS Portable Syste

Modeling CAS &Communications

NTC JCATS Instruction

15+ Years of Simulation Experience

Bangor Exercise ~40 People

Future Directions

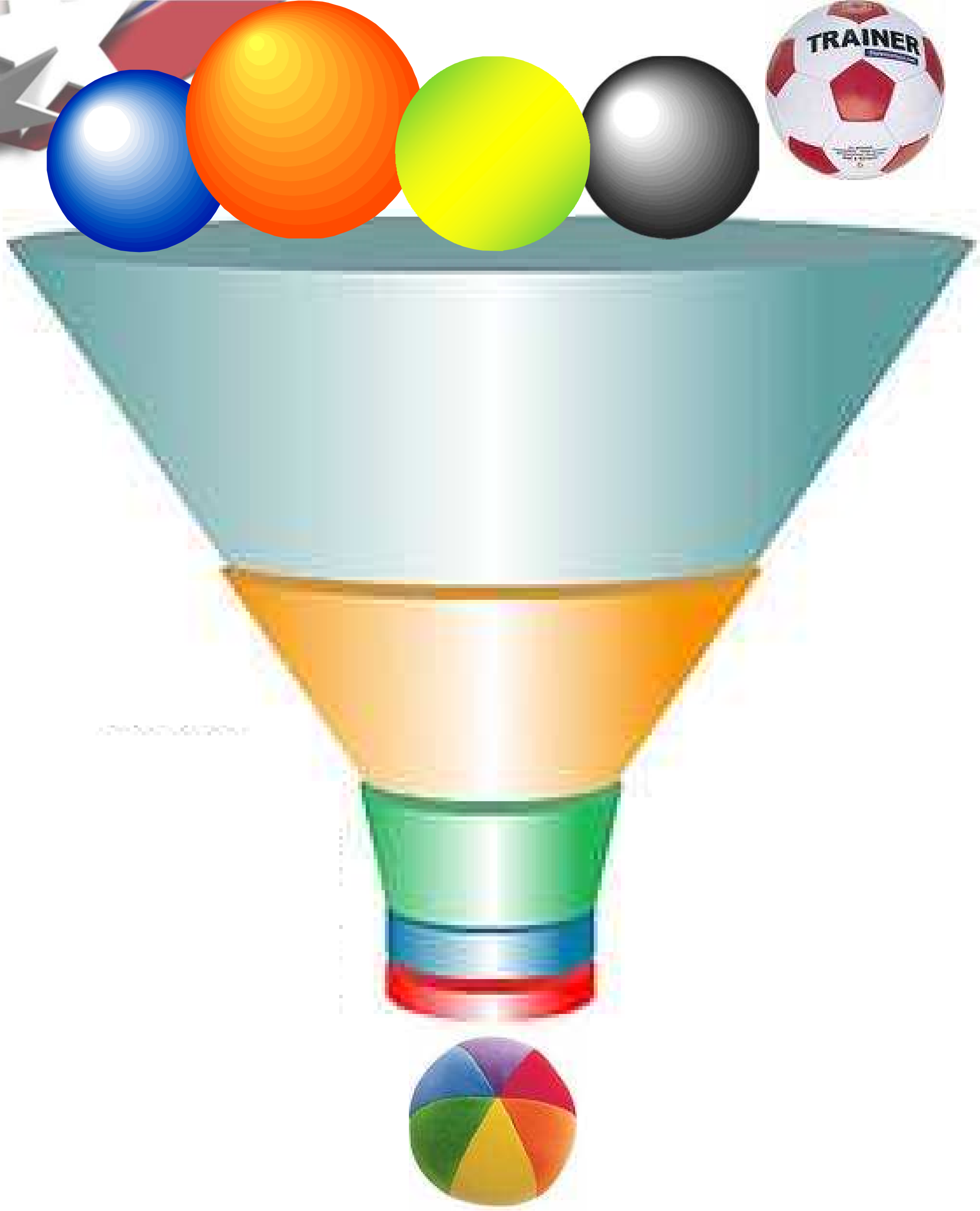
Risk Equation

$$\text{Risk} = P_A \times (1 - P_E) \times C$$

Expansion of the first and last terms in this equation (reference other work here? Merkle, Snell, Darby, Wyss)

Improved our most vulnerable scenario selection by investigating more integrated solutions

SCENARIO FUNNEL



ATLAS

JCATS

Tabletops

FoF

Sandia National Laboratories

Summary

- ATLAS, JCATS
- Questions?