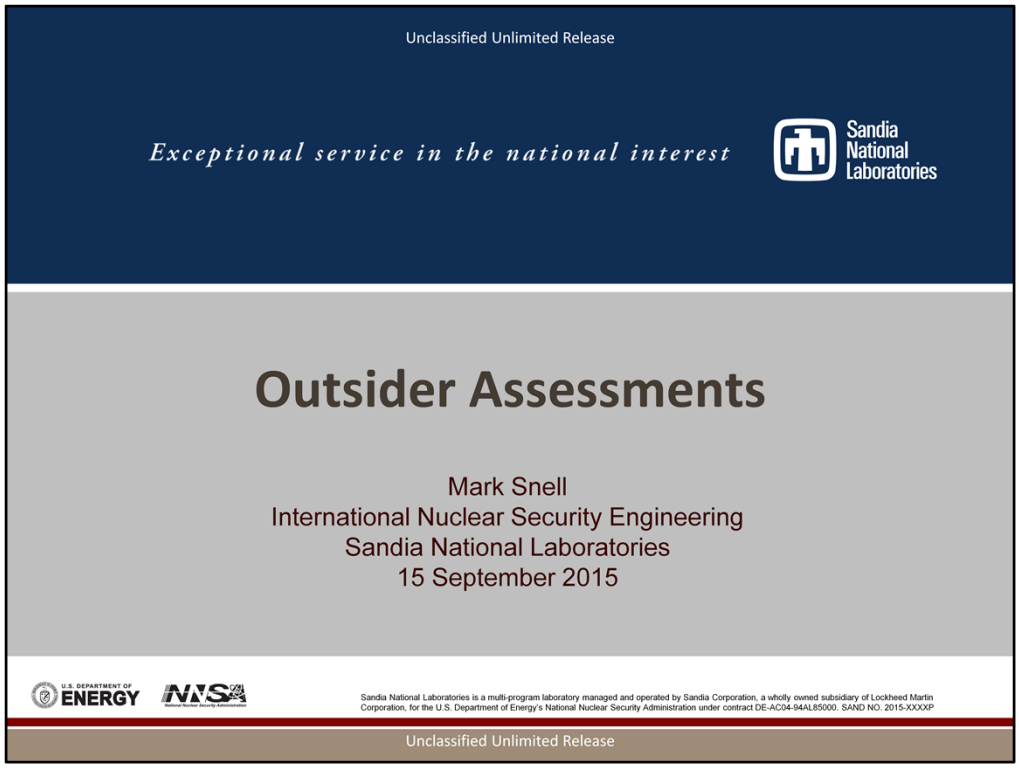
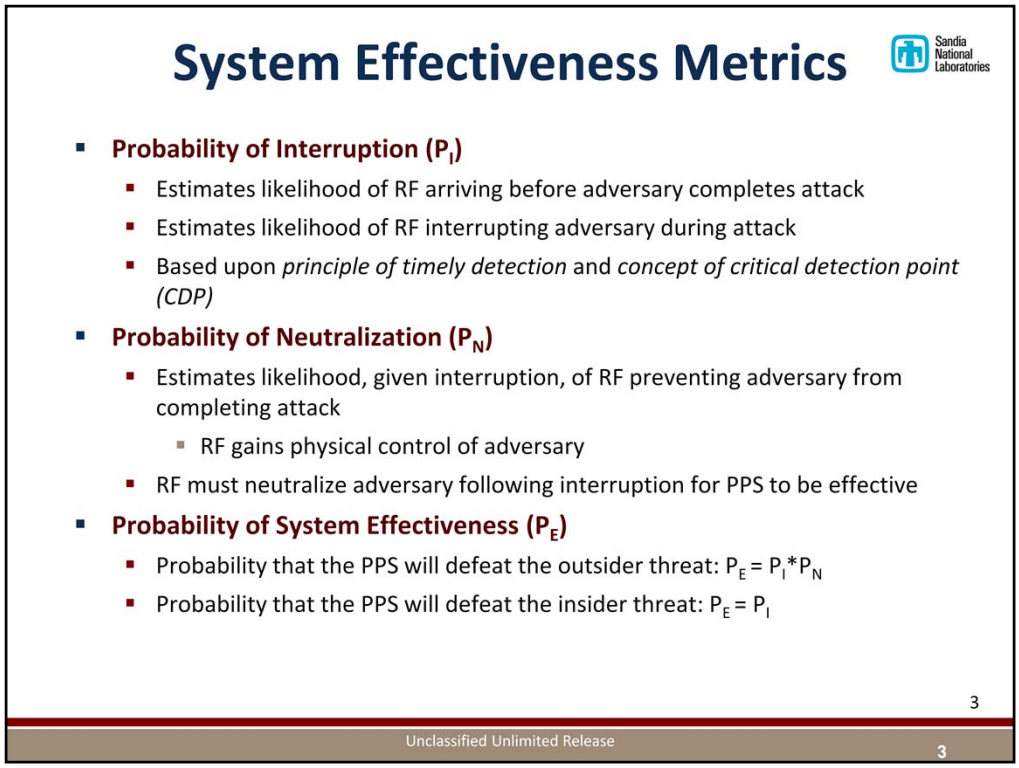


Slides 11-22 come from International Training Courses such as ITC 19 and ITC 25; Shelley could probably get the R&A references (SAND2015-1094 & SAND2006-1987C)

Outline

- Types of Outsider VA applications based on metrics
  - Determine Probability of Interruption for most-vulnerable paths
  - Determine Probability of Neutralization for adversary scenarios
  - Determine Probability of System Effectiveness for adversary scenarios
- Some description of processes to perform outsider evaluations
- History on VA tools to develop these metrics
- Discussion about SAVI as a Path Analysis Tool
- Conclusions



Metric for overall MPC&A System effectiveness is $P_E = P_I * P_N$

- System effectiveness (P_E)
- Probability of interruption (P_I)
- Probability of neutralization (P_N)

Probability of Interruption (P_I): The cumulative probability of detection along a path up to and including the Critical Detection Point (CDP)

Based on principle of Timely Detection and concept of Critical Detection Point (discussed in later slide)

Response force interrupts before adversary completes task timeline

Models are used in path analysis codes to estimate P_I

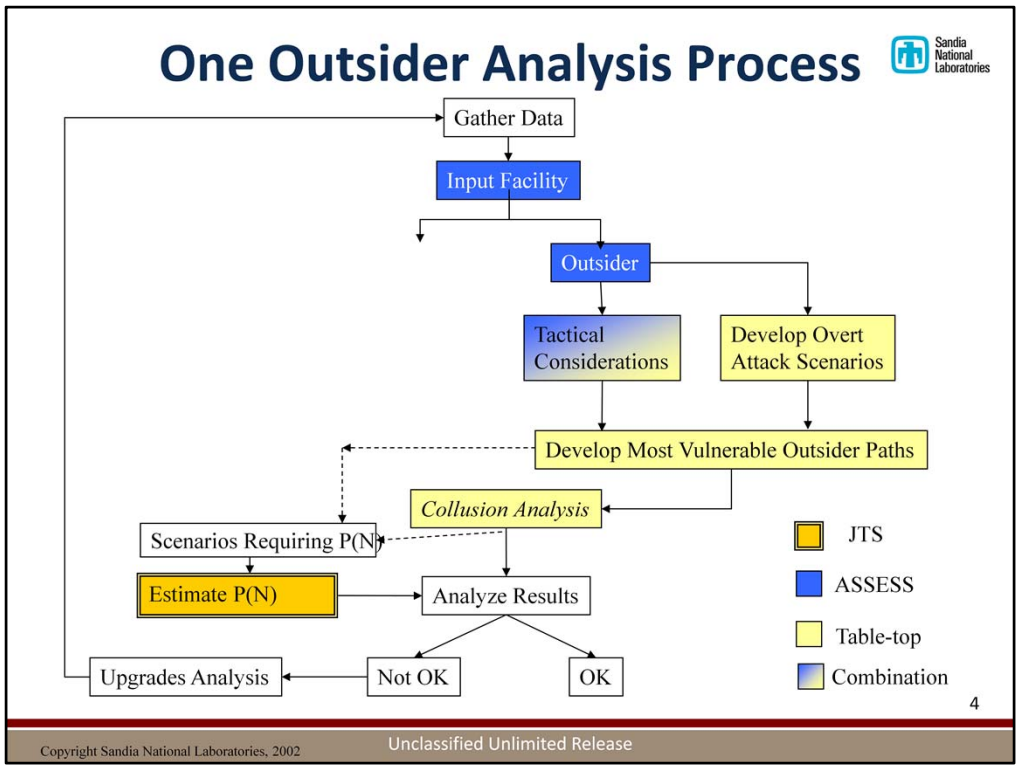
Q: An input into P_I estimates is P_D – how did we estimate P_D ? (through performance testing)

Probability of Neutralization (P_N): The probability, given interruption of the adversary by the response force, that the response force will gain physical control of the adversary

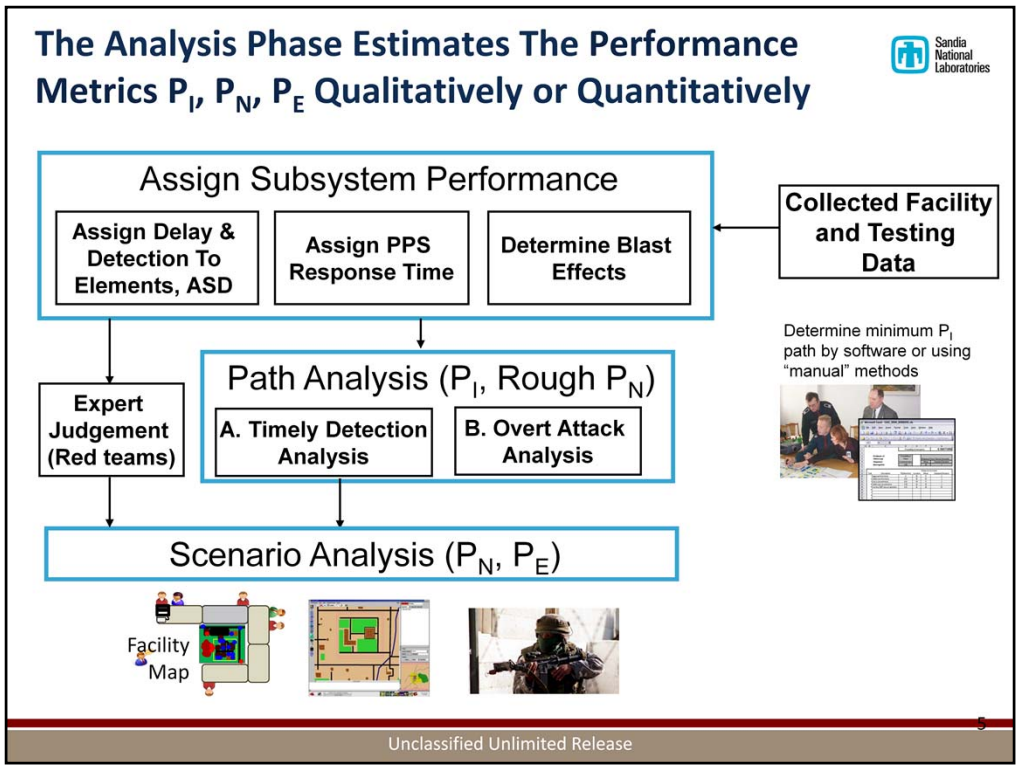
Response force must neutralize adversary following interruption

Neutralize means response force kills or captures adversary, or causes adversary to flee

Experts, calculations, simulations, or exercises are used to estimate P_N



Arrow left hanging is for insider analysis



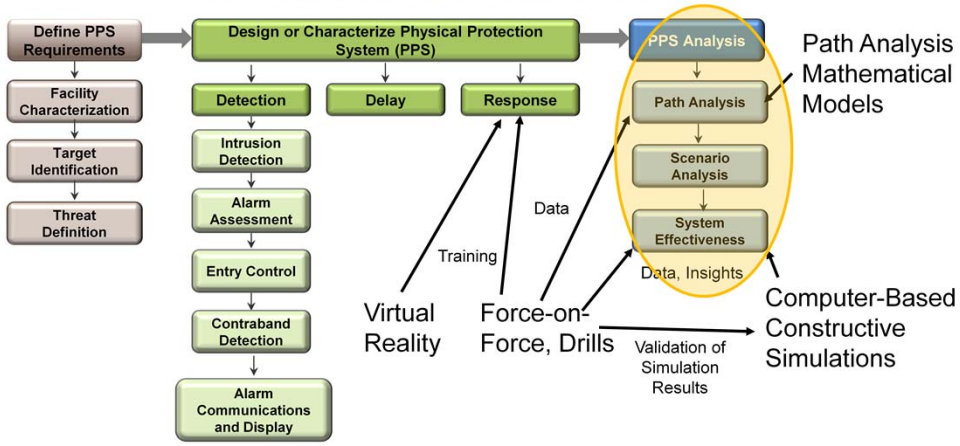
Path analysis and scenario analysis methodologies are complementary.

Scenario analysis typically involves performing one or more types of simulations: tabletop exercises, computer combat simulations, and/or Force-on-Force exercises

Assigning subsystem performance – to detection, delay, and response functions – is intimately connected to identifying vulnerabilities

Sandia National Laboratories

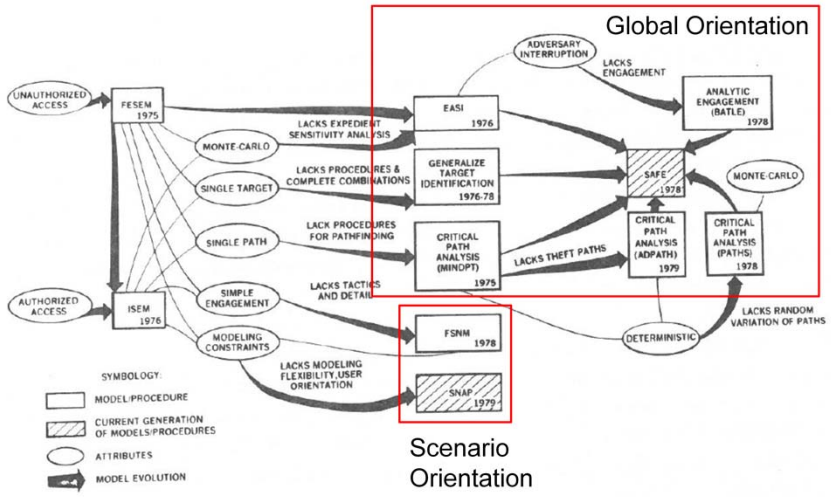
Types of Tools Used for Security Analysis and Design within the Context of DEPO



"Second Generation" Outsider Analysis Tools

Sandia National Laboratories

- Path Analysis provides a global look across the PPS
- Scenario analysis provides a detailed look at a few scenarios

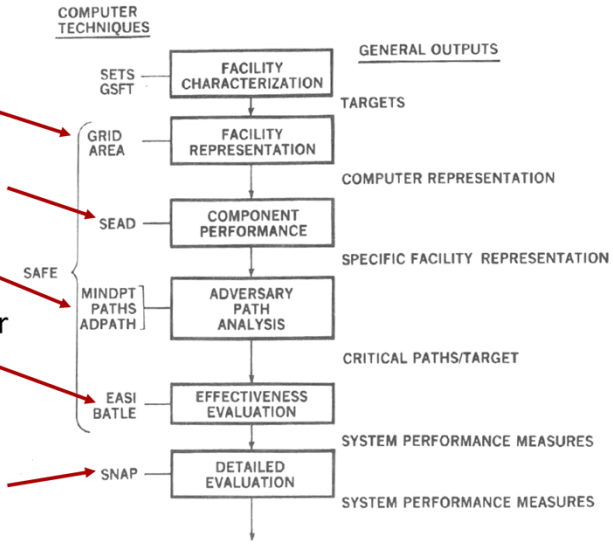


The Global Orientation

The SAFE/SNAP Approach had a Number of "Advanced" Features

Sandia National Laboratories

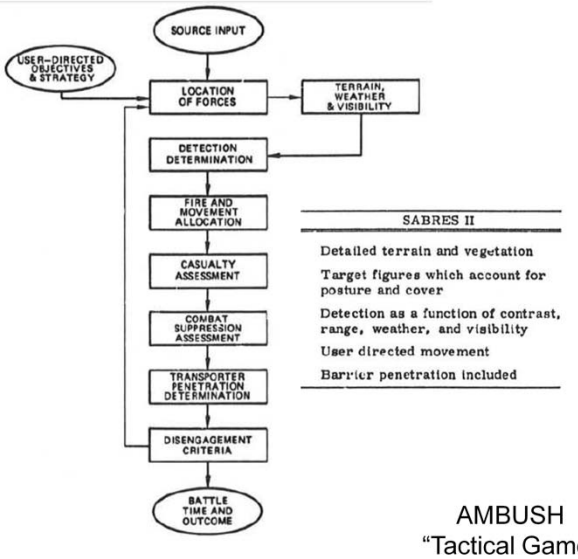
- Grid representation of facility layout
- Incorporated a Performance Database
- Multiple metrics for "most-vulnerable"
- Combination of EASI for P_I, BATLE for P_N
- Linkage between the path analysis and scenario analysis tools



Remark: This is the only diagram that refers to fault tree codes (such as SETS), but fault tree codes were used for vital area identification as well as enumerating ways to defeat complex technical systems.

P_I, P_N Simulations for Transportation Scenarios

Sandia National Laboratories



SABRES II
Detailed terrain and vegetation
Target figures which account for posture and cover
Detection as a function of contrast, range, weather, and visibility
User directed movement
Barrier penetration included

Figure 1. The SABRES Models

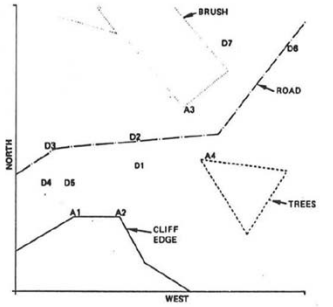


Figure 6. Vegetation, Obstacles, and Battle Participants AMBUSH Map 'A' Surface

AMBUSH
"Tactical Game"

9

Unclassified Unlimited Release

Note: The three top figures come from SAND 78-8650 = CONF 780506-29 available from the IAEA website: https://inis.iaea.org/search/search.aspx?orig_q=RN:10424053 as being presented at the 5th International Symposium on Packaging and Transportation of Radioactive Materials held May 7-12, 1978 in Las Vegas, Nevada. The Figure 6 from that same document shows terrain as shown in AMBUSH which apparently can be configured in a similar way in SABRES/SOURCE. The figure below shows folks performing the AMBUSH tabletop which came out of another document.

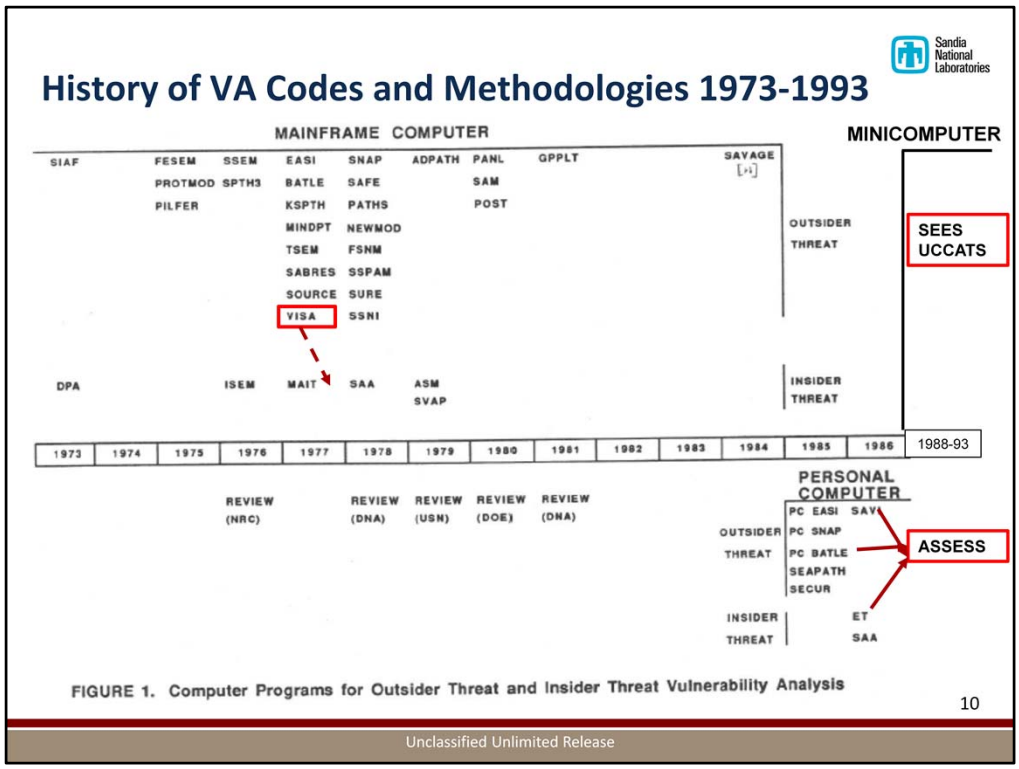
Speaker's notes:
At the same time SAFE and SNAP were being developed for fixed sites, there were quite detailed scenario analysis tools developed to look at scenarios against transportation systems.
Note the capabilities listed for terrain and vegetation, target figures (including posture and cover) as well as user directed movement. This is in a late 1970's software code. Note that SABRES/SOURCE was an "entity-level" simulation modeling each individual adversary and responder (just as SEES and UCCATS were based on JANUS which was also an entity-level simulation for military combat).

Note that there was also a Table-top/Battle-board "game" called AMBUSH related to SABRES/SOURCE: Keeton, S.C., and gallagher, R.J. "A Tactical Game for Use in the Development and Evaluation of Road transit Physical Protection Systems." 5th International Symposium on Packaging and Transportation of Radioactive Materials held May 7-12, 1978 in Las Vegas, Nevada.
Information about this report from the IAEA website:

> "In order to gain insight into the various parts of the transportation physical protection system, a tactical board game, AMBUSH, was developed. The paper discusses the purpose and features of AMBUSH. AMBUSH can be used to help provide insight into the value of additional vehicles, guards, cargo barriers, equipment and alternative tactics. One value of using AMBUSH comes from the player participation in the events that take place. The tasks that are executed at any game turn are based on a human interpretation of the current overall situation and on which strategies appear to optimize the chance of success. Thus, this game may also be valuable as a training device for the transportation guard force. An advantage over computer-based combat simulation models is that AMBUSH is easily transportable and relatively inexpensive."

It is useful to note that the MILES laser engagement system was being developed at about the same time as these tools, meaning that **the three methods: computer simulation, tabletop exercises, and force-on-force exercises (with MILES gear) existed at a fairly advanced level by the early 1980's.**

.



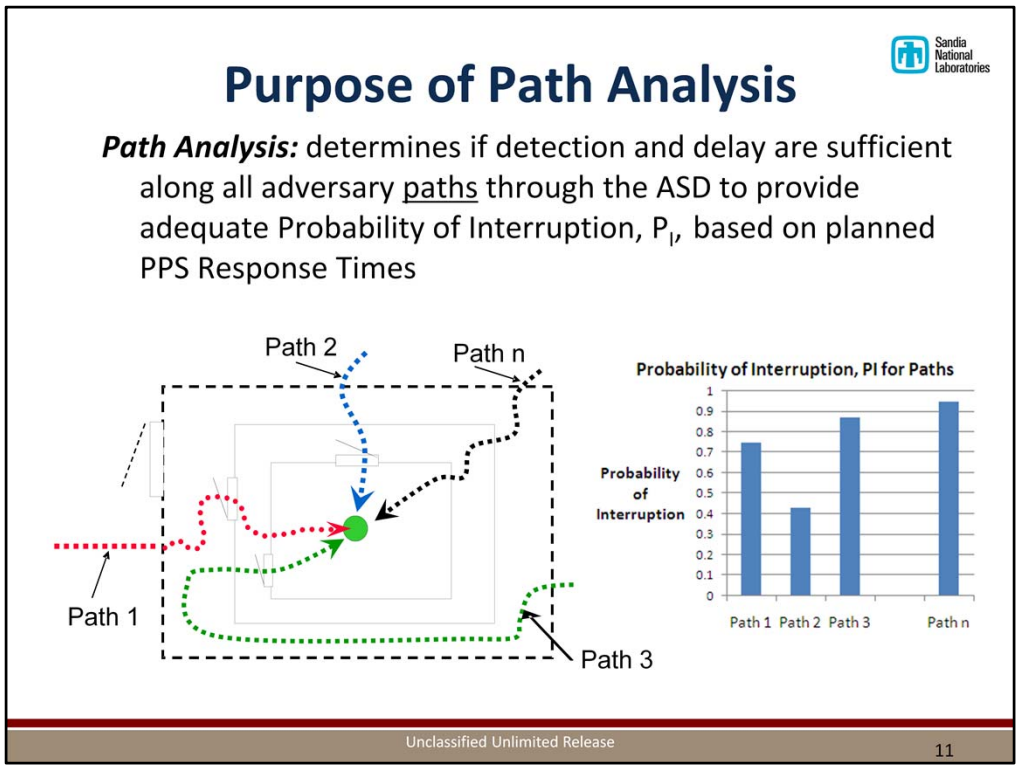
On the right side of this diagram I have added 7 more years, to include a code called ASSESS and two combat simulation codes, SEES and UCCATS; these latter codes were ancestors of JCATS, a modern-day combat simulation. Note: At that time, SEES and UCCATS ran on a VAX.

With this slide we can make a number of general observations:

- As one paper put it: "the principle observation to be made is there was great activity from 1975 to 1980 in the development of new computer programs for vulnerability analysis and then it ceased until 1985 when personal computer (PC) versions and variations of earlier programs began to appear."
- Except for VISA, the earlier main frame codes disappeared, with no linkage between SABRES and SEES/UCCATS for example.
- The Personal computer codes got incorporated into ASSESS which had Path Analysis codes to determine most-vulnerable Insider P_D paths (like ET) and outsider P_I paths (like SAVI), along with BATLE to determine P_N for most-vulnerable P_I paths.
- As SEES was a predecessor to UCCATS which was an ancestor to JCATS, by the early 1990's DOE's tools had, for the most part, dropped down to just 1) VISA, 2) UCCATS and later JTS, and 3) ASSESS. (Side note: a small number of sites used a tool called ALPHA, which is no longer being used.) This "down-selection" is directly related to the next section on Approaches: The insider assessment presentations will talk about manual approaches such as VISA; There will be a section on Outsider Assessments (discussing primarily ASSESS), and there will be a section on response and neutralization (linked backward in time to UCCATS/JTS).

- Remark: There was very little need for cyber-security assessments back in those days,

so this consideration is more recent (although vulnerabilities in computer-based alarm systems were already being considered in the early 1990's).



Slide Purpose: This definition for Path Interruption Analysis was presented in the evaluation section; here we will discuss it in more detail.

Instructor Notes: The measure or metric Probability of Interruption, P_I (pronounced "P sub I") is quite important for Path Interruption Analysis; as you will see, it measures the probability that the response force can arrive in time to interrupt the adversaries before they complete their mission. P_I combines information about Probabilities of Detection, Delay Times, and PPS Response Times.

Note that path analysis also identifies the Most-Vulnerable Path(s) having lowest P_I $_{\text{The purpose}}$ of path analysis is to determine which of the following two facts is true about my PPS:

- If this MV or worst-case Path has a high PI then we have achieved timely detection for all potential adversary paths. That is to say, our detection and delay is sufficient so that our response force has a high chance of arriving in time to interruption the adversary.
- If the MVP has a low PI, then there is some path where detection and delay is inadequate; in such a case, we will need to improve the PPS.

As was discussed earlier, we make a conservative assumption that the adversary can identify the path with the lowest, or least effective, P_I. As a result, we need to find a path with the lowest P_I; that lowest value is taken as the measure of how effective our PPS is in interrupting the threat. Note that the value of P_I will be influenced by the adversary threat capabilities as assumed in the Design Basis Threat (DBT); thus, Path Interruption Analysis demonstrates the adequacy of detection, delay, and response against the DBT.

The two diagrams at the bottom illustrate conceptually how Path Interruption Analysis works:
• The diagram on the left shows different paths to a target; these might represent paths an adversary takes to sabotage a target.
• The diagram on the right is conceptually a graph of Probability of Interruption along all the n paths that the adversary might use.

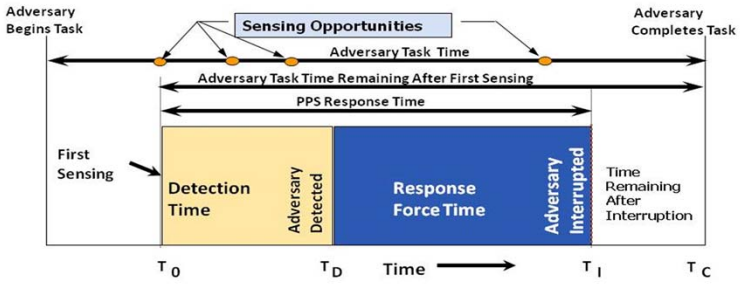
In the rightmost diagram, Path 2 seems to have the lowest Probability of Interruption among all of the paths shown; if this is also the path with the lowest Probability of Interruption among all the paths not shown, then Path 2 would be a most-vulnerable path (note that there might be other paths with the same lowest value).

For you to do PI Analysis, then, you need to know how to do three things:
1. How to calculate P_I for a single adversary path; that topic is covered in this presentation.

2. How to represent all the paths that the adversary might take; that topic is covered in the next presentation on the Adversary Sequence Diagram.
3. How to find a path with the lowest P_I; that topic is discussed in the later presentation on MultiPath Interruption Analysis.

Interruption Analysis: Terminology

- **Principle of timely detection**
  - Detection must occur early enough along the adversary path so that RF has time to interrupt adversary before task completion
- **Critical detection point (CDP)**
  - Last detection point along adversary path for which system response time is less than remaining adversary task time



12

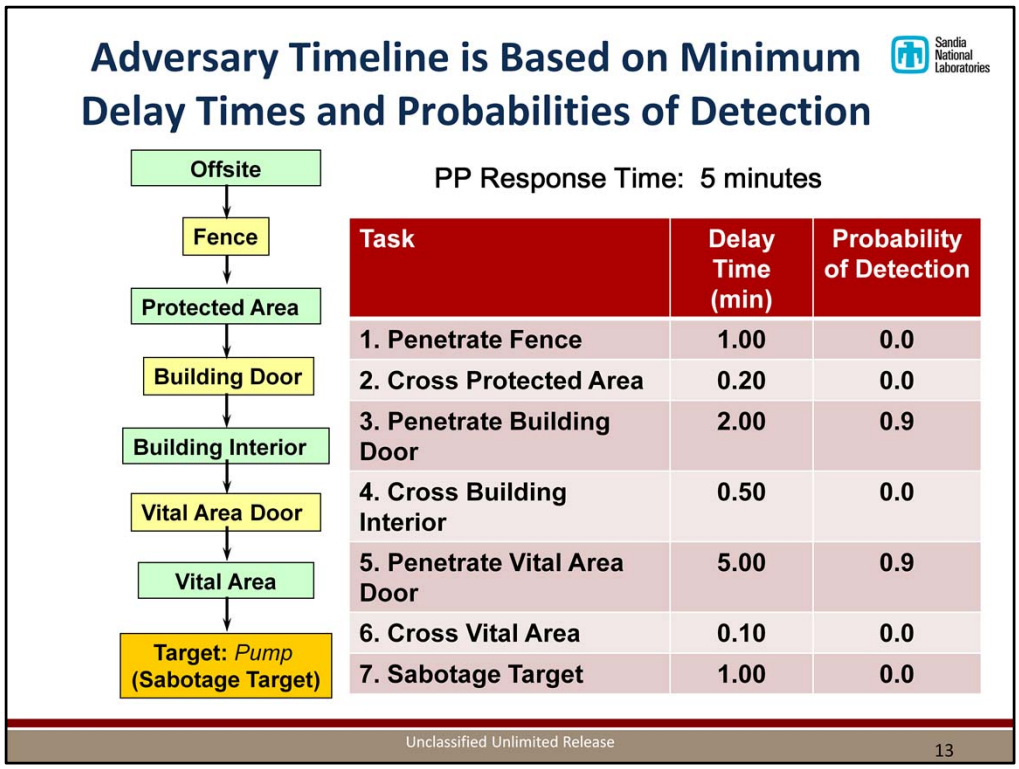
Unclassified Unlimited Release

12

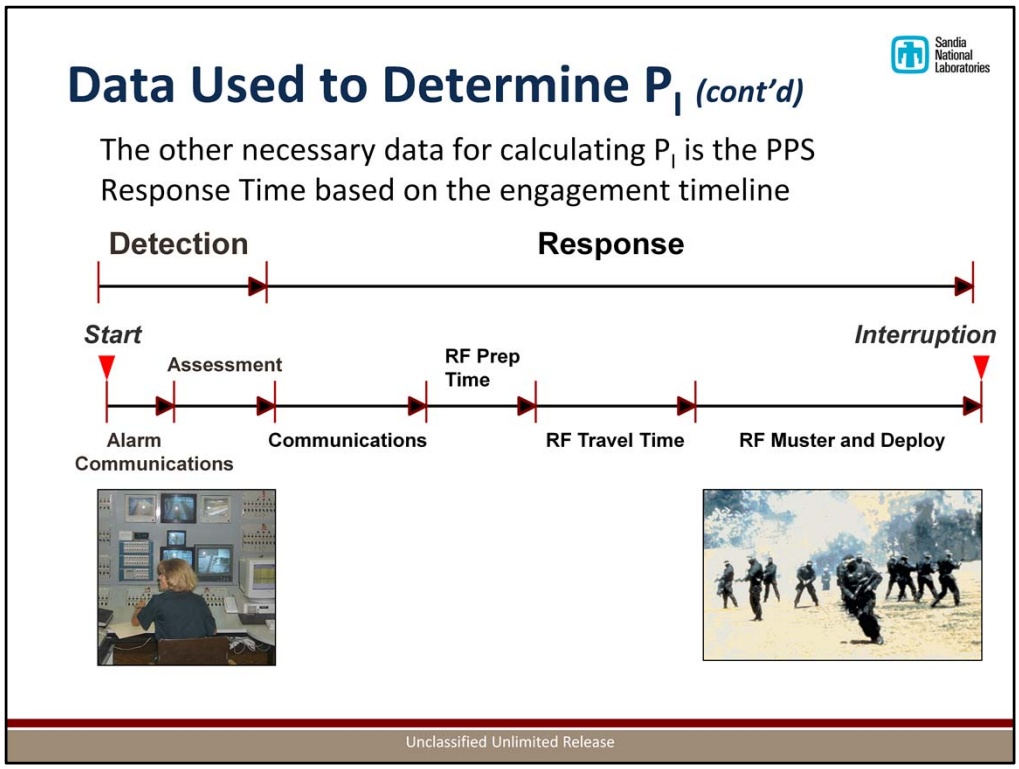
Goal: Response Force Time (RFT) should be < adversary task time
Adversary has path and task timeline

P_I depends on relationship of two timelines
- Adversary path and task timeline
- PPS timeline in response to adversary

Calculating P_I
- At each element along the adversary pathway, there is a probability of detection (P_D) as well as a probability of non-detection (P_{ND})
- P_{ND} of each detection point before the CDP is used to calculate the probability that the adversary will not be detected along each step along path



Slide Purpose: Continue to explain how to create the data to determine PI for an adversary path (continued from previous slide).
Instructor Notes: The second step is to assign minimum delay times and detection probabilities based on those components,
for each Area and Element and to collect the PRT. Note all times are in minutes.



RFT includes detection time, yes? That's what the slide seems to indicate.

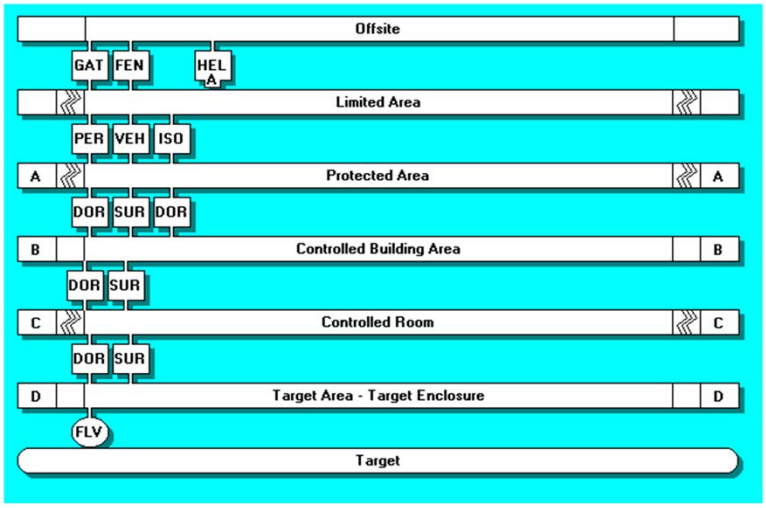
We've just discussed detection and delay – here is a timeline that helps you see the series of events involved in the PPS Response Time (PRT). The detection portion includes the sensor sensing, the alarm being sent to the CAS, and the CAS operator assessing the alarm.

The communications portion of the Response timeline includes the communications time from the CAS as well as communicating to all appropriate RF personnel. Other activities in the Response portion include prep time, travel time, and muster/deploy time. You'll recall that when we were discussing the Response portion of the PPS, we ran exercises to determine RFT time to kit-up, and then included modeling information to determine the complete the response portion of the PRT. In the field, this response portion would be determined using either or both of those methods – LSPTs, to gather data about actual times, as well as modeling and simulation runs.

SAVI is a Path Analysis Tool Used Internationally

Sandia National Laboratories

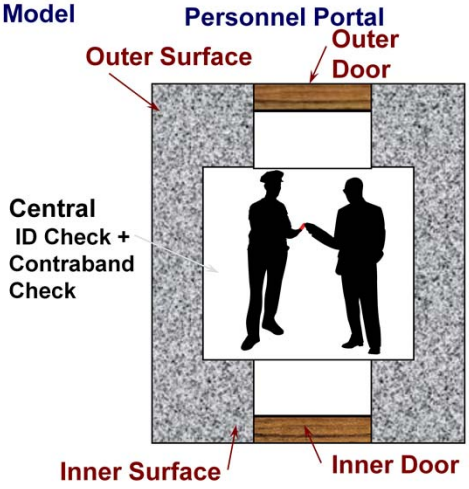
Represents Facilities as Adversary Sequence Diagrams (ASD's)

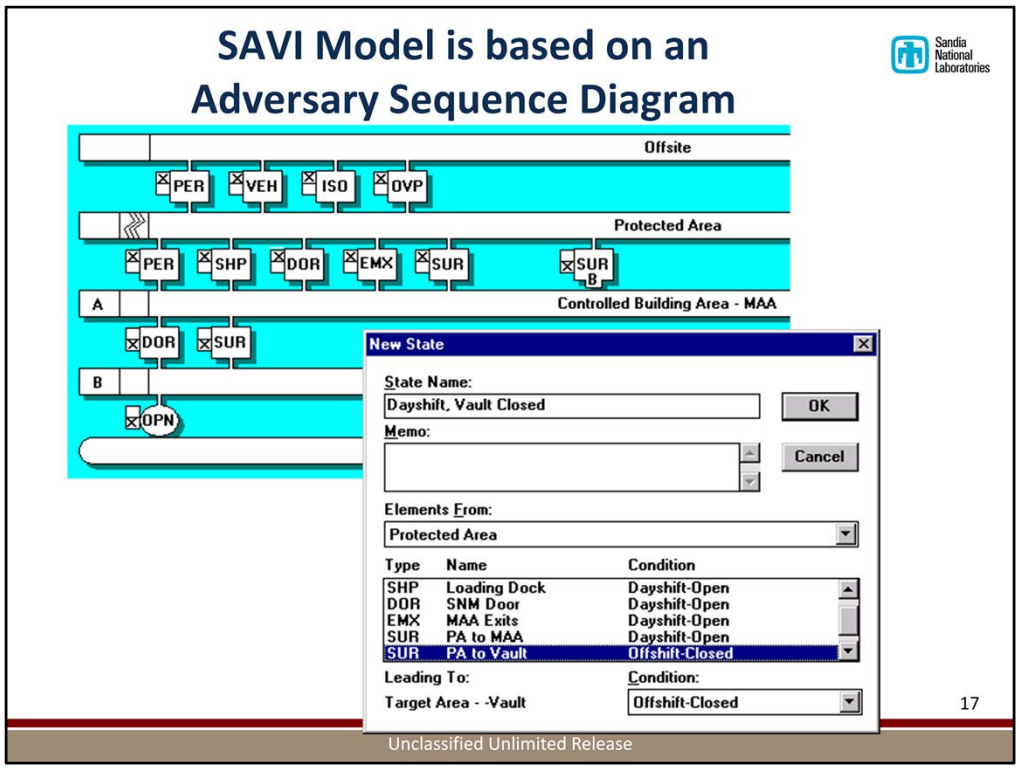


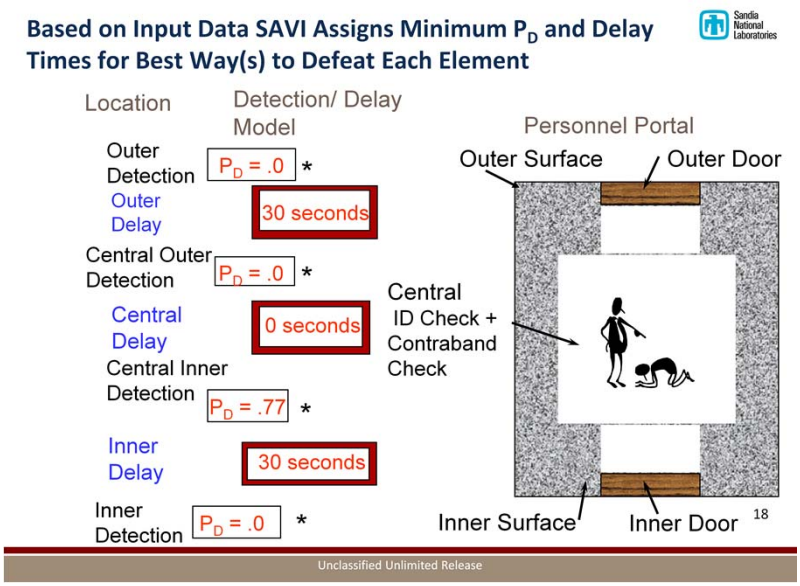
SAVI Define Components at Each Path Element in the ASD

Sandia National Laboratories

Location	Detection/Delay Model
Outer Detection	*
Outer Delay	
Central Outer Detection	*
Central Delay	
Central Inner Detection	*
Inner Delay	
Inner Detection	*




SAVI Model is based on an Adversary Sequence Diagram
Sandia National Laboratories
Offsite
PER
VEH
ISO
OVP
Protected Area
PER
SHP
DOR
EMX
SUR
SUR
B
A
Controlled Building Area - MAA
DOR
SUR
B
OPN
New State
State Name:
Dayshift, Vault Closed
OK
Memo:
Cancel
Elements From:
Protected Area
Type Name Condition
SHP Loading Dock Dayshift-Open
DOR SNM Door Dayshift-Open
EMX MAA Exits Dayshift-Open
SUR PA to MAA Dayshift-Open
SUR PA to Vault Offshift-Closed
Leading To:
Condition:
Target Area - -Vault
Offshift-Closed
17
Unclassified Unlimited Release



It actually uses internal fault trees (or booleans

The SAVI Results Report Shows P_I for the Most-Vulnerable Path

Sandia National Laboratories

Most Vulnerable Path
RFT - Response Force Time #1 (seconds): 25

P(I) - Interruption Probability: 0.5061
P(N) - Neutralization Probability: 0.4500
P(W) - System Win Probability: 0.2278

P_I, P_E

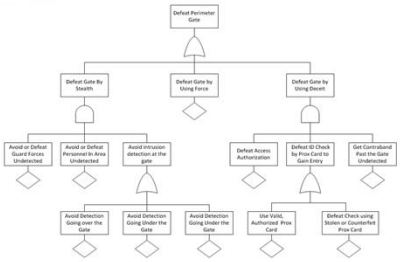
Detection Potential (points) : 5
TRI - Time Remaining after Interruption (seconds): 79

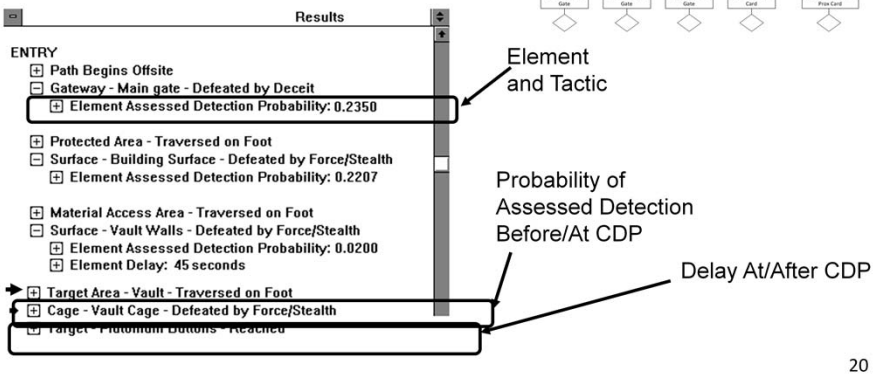
CDP - Critical Detection Point at Surface - MAA Surface on Entry
Leading from Protected Area to MAA of Chem Recovery Bldg

Cumulative Path Delay after CDP (seconds):104

CDP

Path Results - Overview





Sensitivity Graph Shows the Tradeoff Between Worst Case P_I and RFT

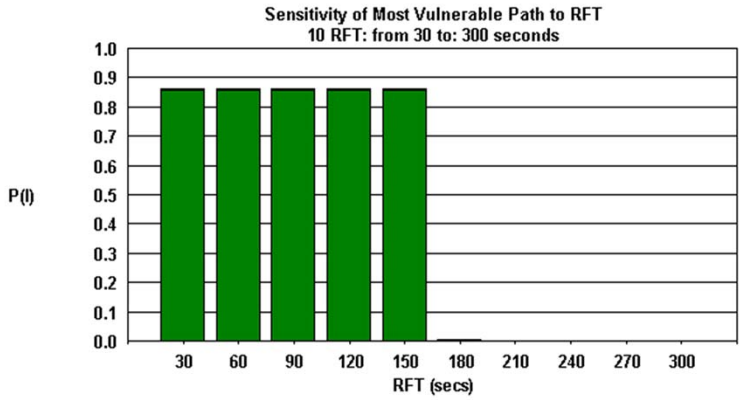
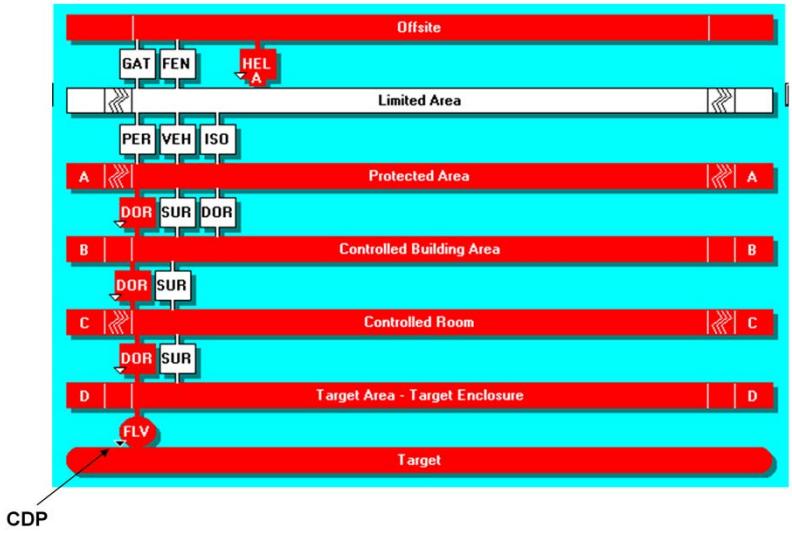


Diagram Window Displays the Path

Sandia National Laboratories



Common Types of Issues with Path Codes Such as SAVI

Sandia National Laboratories

- Silly Paths
  - Paths based on incorrect transit distances
  - Reappearing vehicle
    - Adversary passes through Personnel portal then drives a vehicle across an area
  - Use of deceit just after force/stealth
    - Adversary breaches a 12” wall then uses deceit at next portal
  - Practical Detection Point problem: may not want to minimize detection to CDP
    - Happens if CDP is past high-P_D layer
- At some facilities, the number of individual targets may be too large to allow all to be analyzed

Conclusion

Sandia National Laboratories

- There are a range of approaches to performing outsider analyses but typically path analysis is performed before scenario analysis
- During the period 1973-1980, all major types of Outsider-related VA tools were developed at a fairly advanced level
- One VA tool that has been used internationally is SAVI

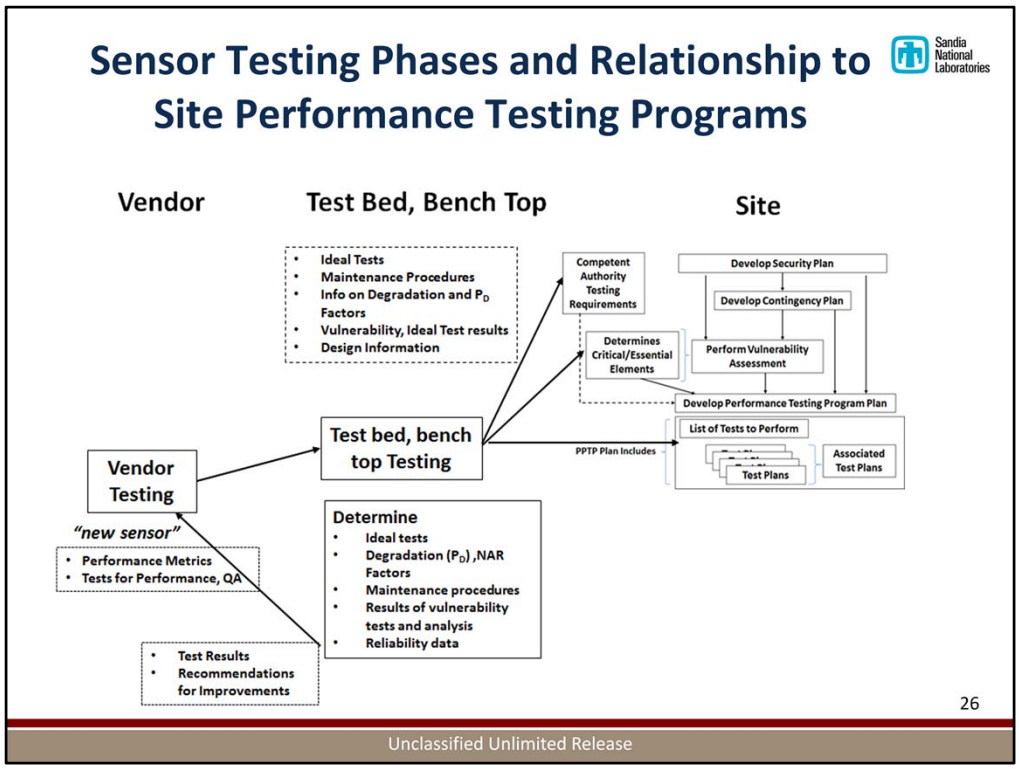
Notes:

1) The issue of modeling adversary and response force decision-making and its effects on planning was recognized as both an important and a hard problem but tool developers didn't know how to address it at the time. Approaches to human decision-making and planning tended to be fairly basic based on user-defined scenario tasks and user-specified response logic (if alarm X do Y).

2) 2) Regarding VV&A: Both the Conflict Simulation Lab at LLNL which developed SEES and UCCATS and the LLNL/SNL team that developed ASSESS took great pains to make sure that their algorithms worked properly. However, accreditation for physical protection application was not recognized as an issue, yet.

Backup Slides

Sandia National Laboratories



Also called performance assurance programs.

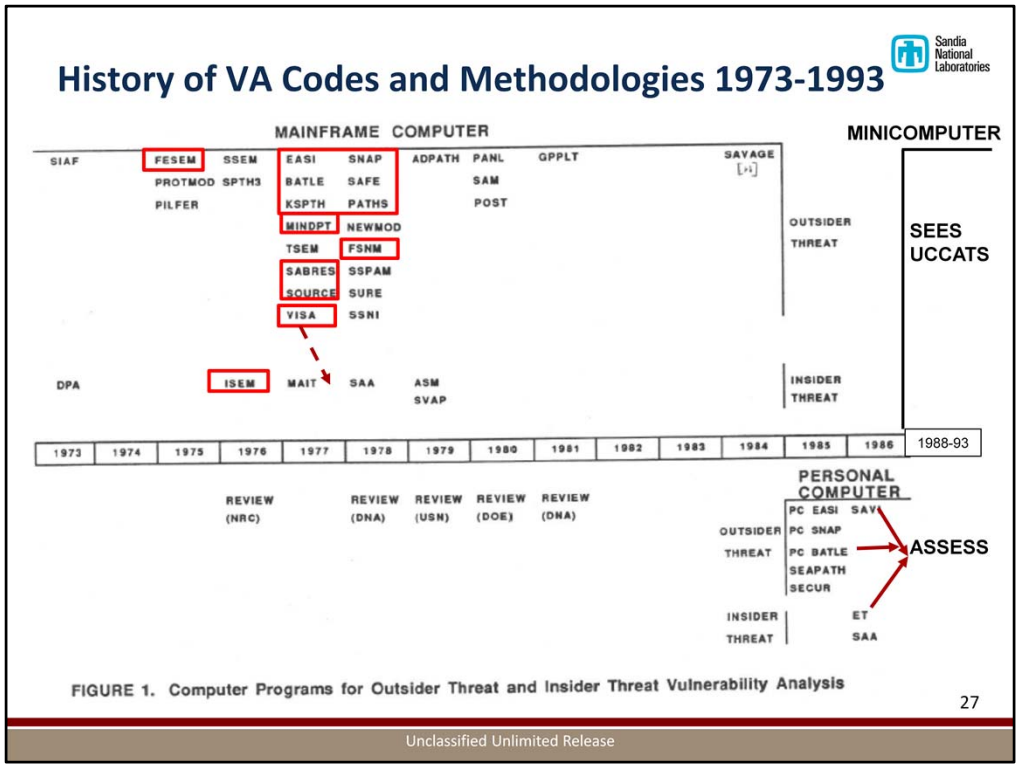


FIGURE 1. Computer Programs for Outsider Threat and Insider Threat Vulnerability Analysis

This figure is taken from an INMM Paper: USE OF COMPUTER PROGRAMS TO EVALUATE EFFECTIVENESS OF SECURITY SYSTEMS, Harris, Goldman, and McDaniel; James, and Rajczak. The figure in the paper only covers 1973-1986.
Note that this diagram differentiates between insider and outsider threat tools; generally, a tool/method only covers one and not the other.

VISA: There is one exception here, a manual approach called VISA. This is shown in the diagram as an outsider tool but you will hear today about how VISA can be used as an insider analysis approach; long after this diagram was created in 1988, the IAEA adopted a version of VISA as the basis of its insider analysis approach.

The first insider and outsider computer-based tools used at Sandia were ISEM and FESEM, respectively, which were simulations. These were considered to be “first-generation” models/procedures.
The second generation of the outsider analysis approaches is included in the next set of boxes: EASI, BATLE, and as we will see are centered around SAFE which was a path analysis tool and SNAP which was a scenario analysis tool

We have also included SABRES and SOURCE which were used for transport security. These made up a set of simulations for scenario analysis

Note that it is not shown on this diagram but
I have added 7 more years, to include a code called ASSESS and two combat simulation codes, SEES and UCCATS; these latter codes were ancestors of JCATS, a modern-day combat simulation. Note: At that time, SEES and UCCATS ran on a VAX.