Conf 930749--22

VULNERABILITY ASSESSMENT USING TWO COMPLEMENTARY ANALYSIS TOOLS

William K. Paulus
Sandia National Laboratories
Org. 9545
Albuquerque, NM 87185 USA
505/844-9760

ABSTRACT

To analyze the vulnerability of nuclear materials to theft or sabotage, Department of Energy facilities have been using, since 1989, a computer program called ASSESS, Analytic System and Software for Evaluation of Safeguards and Security. During the past year Sandia National Laboratories has begun using an additional program, SEES, Security Exercise Evaluation Simulation, enhancing the picture of vulnerability beyond what either program achieves alone. ASSESS analyzes all possible paths of attack on a target and, assuming that an attack occurs, ranks them by the probability that a response force of adequate size can interrupt the attack before theft or sabotage is accomplished. A Neutralization module pits, collectively, a security force against the interrupted adversary force in a fire fight and calculates the probability that the adversaries are defeated. SEES examines a single scenario and simulates in detail the interactions among all combatants. Its output includes shots fired between shooter and target, and the hits and kills. Whereas ASSESS gives breadth of analysis, expressed statistically and performed relatively quickly, SEES adds depth of detail, modeling tactical behavior. ASSESS finds scenarios that exploit the greatest weaknesses of a facility. SEES explores these scenarios to demonstrate in detail how various tactics to nullify the attack might work out. Without ASSESS to find the facility weaknesses, it is difficult to focus SEES objectively on scenarios worth analyzing. Without SEES to simulate the details of response vs. adversary interaction, it is not possible to test tactical assumptions and hypotheses. Using both programs together, vulnerability analyses achieve both breadth and depth.

INTRODUCTION

To analyze the vulnerability of nuclear materials to theft or sabotage, Department of Energy facilities have been using, since 1989, a computer program called ASSESS. ASSESS was jointly developed by Sandia National Laboratories and Lawrence Livermore National Laboratory. It runs on a Personal Computer as a Microsoft Windows™ application.

During the past year Sandia National Laboratories has begun using an additional program, SEES, enhancing the picture of vulnerability beyond what either program achieves alone. SEES was developed by the Conflict Simulation Laboratory of Lawrence Livermore National Laboratory. It runs on a VAX computer in the VMS operating system.

These are not the only vulnerability analysis tools in use. A recent survey shows three additional models or modeling techniques have been used at various sites. Figure 1 summarizes these applications. Other models not listed, such as LAVA and THIEF, have properties that may be appropriate for particular applications. In general, no single model efficiently addresses all vulnerability analysis issues.

Site	ASSESS	SAVI	ALPHA	SEES	Table Top
RF	x				x
SRS	x	x			x
Y-12	x		x		x
ORNL	x				
LANL	x				
LLNL	x				
NTS	x			x	x
TSD	x			x	x
Mound			x		
SNL	x			x	x
Pantex	x				
Idaho	x				
Han-ford	x				x
Ports-mouth	x				

Figure 1. Model Utilization

TARGET AND THREAT

Analysis begins with a facility map showing the target to be protected. Figure 2 shows a hypothetical facility devised for ASSESS training classes. The target is in a vault in the Chemical Recovery Building.

Terrorists are a threat that might use violence in their attack. We assume their objective is theft from the vault. We further assume that their attack will minimize their probability of detection until such time that they can have possession of their target before a response force could interrupt them.

ASSESS takes a description of a layered system of physical protection, finds all the paths through the layers to a single theft or sabotage target, and ranks them according to the degree of vulnerability associated with each path. The analysis can be performed for several degrees of threat. The description of one of the most vulnerable paths is an attack scenario.

Figure 3 shows the most vulnerable path to the target in the hypothetical facility under specific conditions. The path is highlighted in black. The representation of the facility is called an Adversary Sequence Diagram (ASD). The long rectangles are areas that adversaries must cross to reach the target. The squares are protection elements that the adversary must defeat before crossing an area. The adversary starts his attack at the top of the diagram, and pursues a downward path to the target.

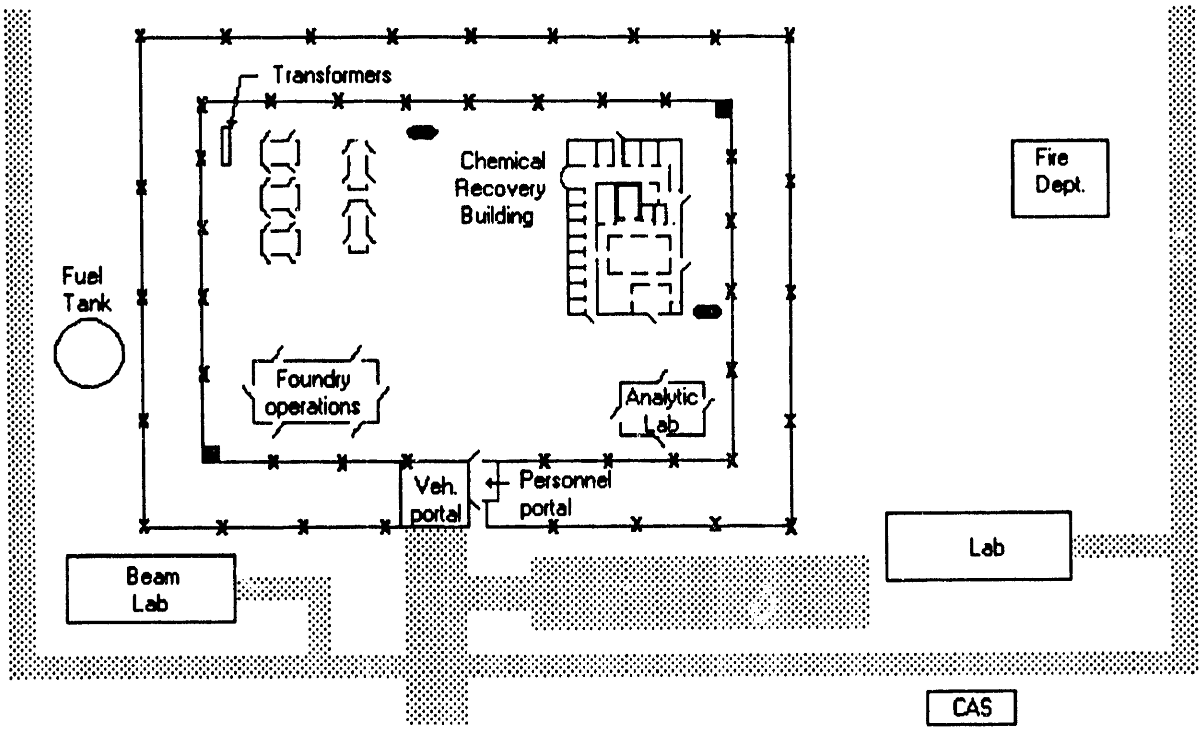

Figure 2. Hypothetical Facility

ASSESS

ASSESS is a <u>global</u> analytical tool in the sense that it analyzes <u>all</u> possible paths of attack on a target. Assuming that an attack occurs, it ranks the attacks by the probability that a response force of adequate size can interrupt the attack before theft or sabotage is accomplished. A Neutralization module pits, collectively, a security force against the interrupted adversary force in a fire fight and calculates the probability that the adversaries are defeated.

In this example, the attack penetrates into the Protected Area through a vehicle portal (VEH). Adversaries cross the Protected Area and enter the Material Access Area (MAA) of the Chemical Recovery Building by way of a wall, or surface, (SUR). Inside the building, the adversaries proceed to the Vault after defeating the vault door (DOR). They steal from the contents of the vault.

Figure 4 shows a summary portion of tabulated results of the path analysis. In the illustrated case, the response is almost immediate, requiring only 10 seconds from first detection of the attack (Response Force Time). The probability that this response can interrupt the attack before the adversaries can get their hands on their target is only moderate, 0.5. If it is important to prevent the adversaries from getting hands on their target, for example to prevent sabotage, improvements to the physical security of the hypothetical site are necessary.

Independently, the likelihood of neutralizing the attackers if they are interrupted can be investigated. This scenario can be analyzed with the Neutralization module to obtain an estimate of the probability that the attackers can be defeated by a security response force in a fire fight. The statistically expressed result is backed up by capability to quickly produce graphs of the variation of the result as a function of one variable. The variables include number of combatants on one side, average exposure to incoming fire, weaponry, accuracy of fire, and others.

Most Vulnerable Path
RFT - Response Force Time #1: 10 seconds
P(I) - Interruption Probability: 0.5061

Figure 4. Results

Figure 5 shows how probability of neutralization depends upon the size of the security force.

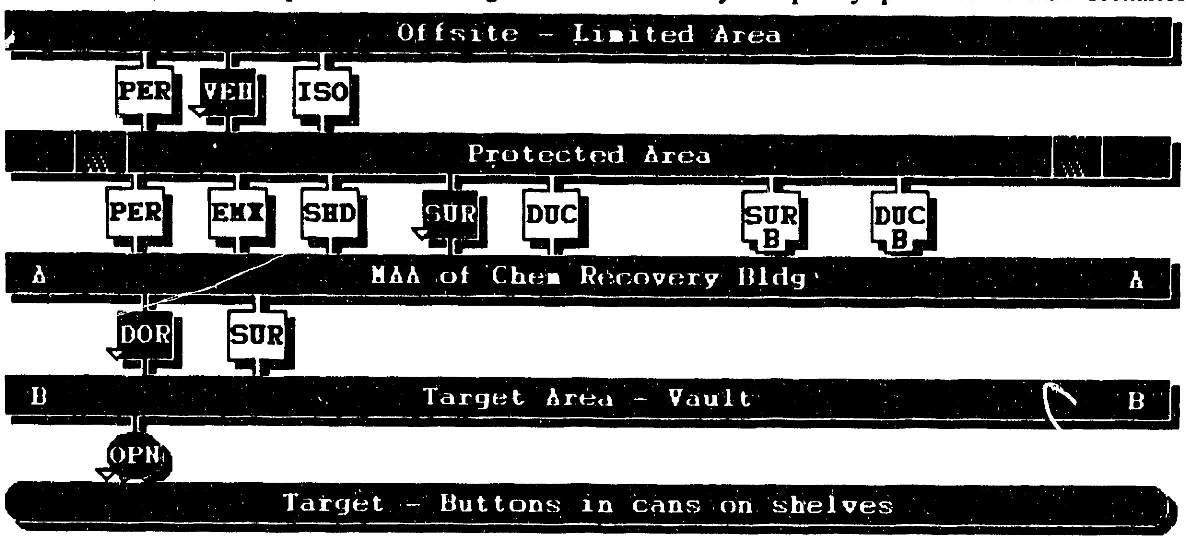

Figure 3. Most Vulnerable Path, Shown on ASD

To calculate these results quickly, the model is kept simple. Each side has the average of the combatant characteristics defined for each combatant. Casualties are generated by applying a rate of attrition based on the average characteristics for a side of the fire fight. There is no way to explicitly model continual movement of combatants, or which individuals target whom. Much desirable detail is sacrificed to achieve a quickly calculated statistical estimate of the overall outcome of the fire fight.

The usefulness of ASSESS/Neutralization is its ability to quickly point out which scenarios are weakest with respect to likely success of the neutralizing security force. When this is known, a tool is needed to simulate the scenarios in detail, discover the tactical weaknesses, and try possible remedies.

<u>SEES</u>

SEES examines a single scenario and simulates in detail the interactions among all combatants. Among other data, its output includes acquisition of target, shots fired between shooter and target, and the hits and kills. The time when each action occurs is reported. The simulation is displayed on a video screen. Icons representing combatants move on a two dimensional map. A line between two combatant icons indicates that a shot is fired.

The facility layout shown in Figure 1 becomes the field of action for a SEES engagement after the analyst turns it into a Terrain File. The description of the most vulnerable path provided by ASSESS should somewhat restrict the movement of adversary combatants in SEES. Penetration of the Chemical Recovery Building should be through the wall into the Material Access Area. As shown in Figure 6, this is possible on only two sides of the building. The doors should not be used if the simulation is to follow the ASSESS most vulnerable path scenario.

To achieve this amount of detail in the output information, the input must include similar detail. Defining a scenario for SEES to simulate, running the simulation, getting printouts of the results, and analyzing them requires time. Ability to select worthwhile scenarios for simulation keeps the expenditure of time as small as possible.

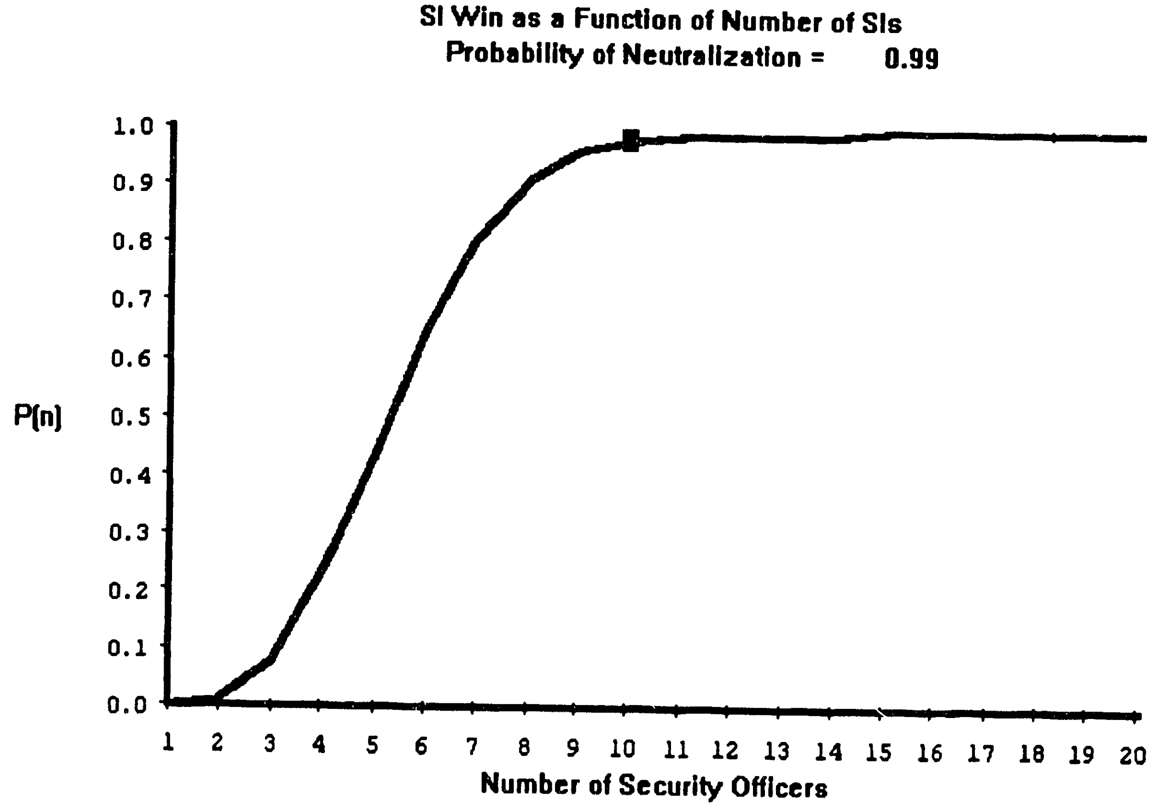

Figure 5. Variation of Probability of Neutralization with Security Force Size

Because of the detail presented, winning an engagement can depend on more complex criteria in SEES than in ASSESS/Neutralization. A win in ASSESS means that one side is reduced to zero combatants (or some other specific number). SEES does not declare the winner of an engagement. In SEES, win criteria are judged by the analyst, so they can be any logical combination of actions that can be observed on the screen and read from a printout. For example, a particular combatant reaching a particular location, perhaps carrying a stolen item, can be a win criterion. The win could be contingent upon another particular combatant remaining alive to perform a critical operation before a deadline. Scenarios can reflect realistic dependencies that are beyond the scope of the simpler ASSESS/Neutralization model.

ASSESS AND SEES ARE COMPLEMENTARY

Whereas ASSESS gives breadth of analysis, expressed statistically and performed relatively quickly, SEES adds depth of detail, modeling tactical behavior. ASSESS finds scenarios that exploit the greatest weaknesses of a facility. SEES explores these scenarios to demonstrate in detail how various tactics to nullify the attack might work out. Without ASSESS to find the facility weaknesses, it is difficult to focus SEES objectively on scenarios worth analyzing. Without SEES to simulate the details of response vs. adversary interaction, it is not possible to test tactical assumptions and hypotheses. Using both programs together, vulnerability analyses achieve both breadth and depth.

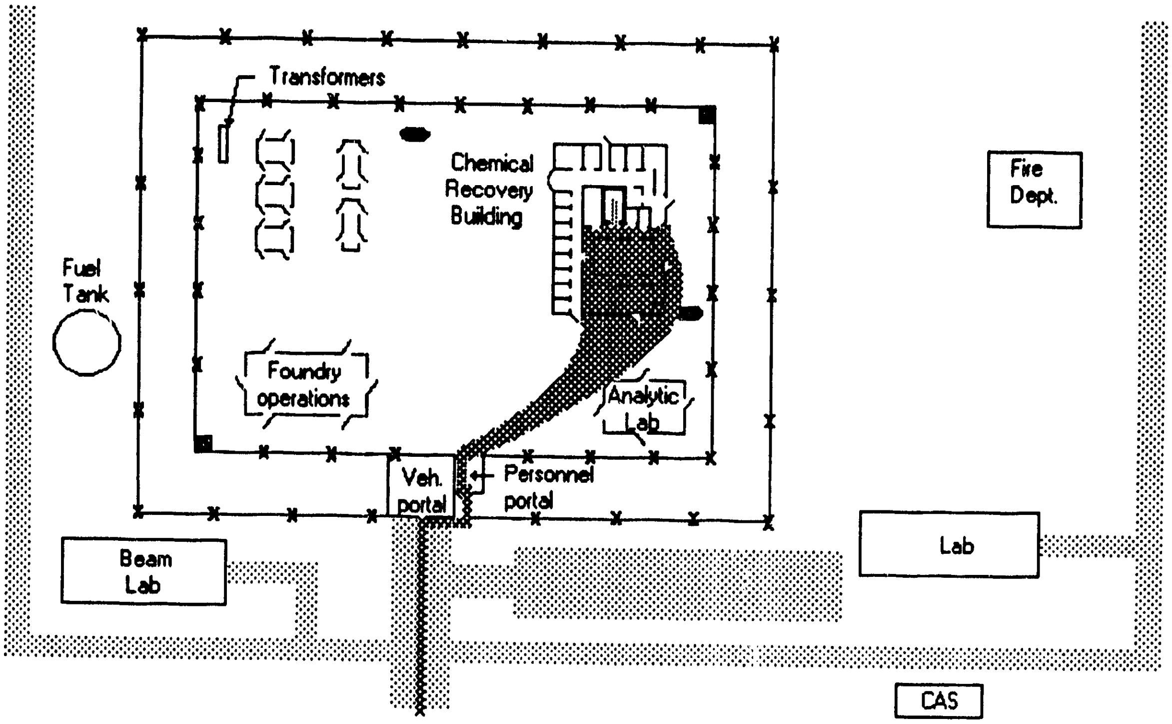

Figure 6 Most Vulnerable Path

Another way to look at the complementarity of models is shown in Figure 7. Cost of modeling increases as the realism of the model increases. Cost of modeling measures the time required to collect and input data for the model, and the computing resources required to run the model and document the results. Realism of the model can be thought of as the amount of detail present in the model results. Global models should not be regarded as intrinsically less realistic than simulations. They might be simulations, but at present are not.

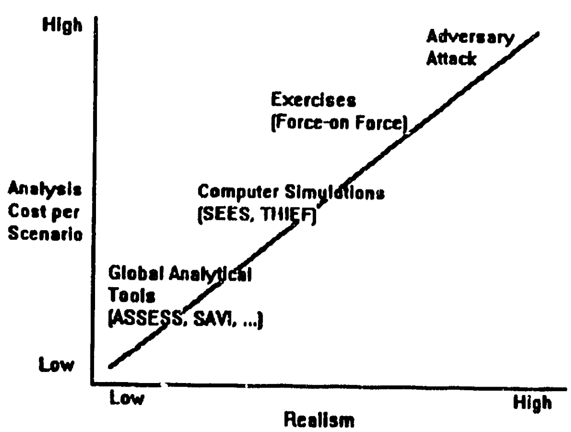

Figure 7. Cost vs Realism

Global analyses are a relatively abstract, approximate representation of reality. Lowest costs are the result of a design for efficient calculation. This is a deliberate tradeoff against model detail. Breadth of analysis is achieved at low cost. Security weaknesses are found and ranked, narrowing the focus of more penetrating, but more expensive analyses to relevant issues.

Computer simulations model many but do not model all aspects of a real attack. For example, morale factors are beyond the scope of computer simulations. Costs involve running time on more powerful, more expensive computers. Savings come from the lack of need for real exercises with a full complement of combatant personnel, etc.

Next more realistic is a force-on-force exercise. It involves the real site and personnel. Stress levels are less than realistic, however; and MILES weapons, if used, are approximations to the performance of real weapons. Cost is high because of the time required for the exercise, and the number of personnel required to run the exercise as direct participants and in support roles.

The ultimate in realism is an actual adversary attack. The cost is highest because barriers are actually penetrated and probably destroyed. Lives may be lost.

SUMMARY

Figure 8 summarizes the major complementary characteristics of ASSESS and SEES.

ASSESS	SEES
Finds scenarios that exploit security weaknesses	Test tactics to nullify attack
Statistical analysis	Shot by shot simulation
Quick calculation	Time required to disclose detail

Figure 8. Summary

This work was supported by the U. S. Department of Energy under Contract DE-AC0476DP00789.

END

DATE
FILMED
10/01/93