CONF-890736--9

SAND89-1602C

The ASSESS Outsider Analysis Module

SAND--89-1602C

DE89 014800

Alfred Winblad, Mark Snell, Sabina Erteza Jordan
Sandia National Laboratories*, Albuquerque, New Mexico, U.S.A.
Brad Key, Bryan Bingham, Scott Walker
Science & Engineering Associates, Inc., Albuquerque, New Mexico, U.S.A.

ABSTRACT

The Outsider Analysis (Outsider) module is part of the Analytic System and Software for Evaluating Safeguards and Security (ASSESS). Outsider and the ASSESS Facility Descriptor (Facility) module together supersede the Systematic Analysis of Vulnerability to Intrusion (SAVI) software package. Outsider calculates P(I), the probability that outsiders are interrupted during an attack by security forces at the facility, and P(W), the probability of security system win, and has other features not found in SAVI. Analysts can select intruders from a set of ten reference threats, ranging from well-equipped terrorists to intruders with no equipment at all. New analysis algorithms run 60 to more than 100 times faster. New reports detail how safeguards are defeated at each element in a path and give other data critical to effective upgrade decisions. Outsider takes as input a facility security system defined in Facility and produces intermediate results for the ASSESS Collusion module.

INTRODUCTION

The Outsider Analysis (Outsider) module is part of the Analytic System and Software for Evaluating Safeguards and Security (ASSESS) developed under contract to the U.S. Department of Energy [1].

Outsider calculates the vulnerability of facilities defined in the ASSESS Facility Descriptor (Facility) module to intrusion by outsiders [2]. Other ASSESS modules analyze facility security against other kinds of threats [3,4]. All ASSESS modules run on IBM-PC compatible computers within Microsoft Windows™, a graphical user interface.

Outsider and Facility together supersede the Systematic Analysis of Vulnerability to Intrusion (SAVI) software, developed in 1987 by Sandia National Laboratories and Science & Engineering Associates, Inc. [5,6]. Along with an improved user interface based on Microsoft Windows, Outsider has new modeling and reporting capabilities that make it faster and easier to set up and run intrusion analyses, to determine specific areas of vulnerability, and to identify and test potential upgrades.

THE OUTSIDER ANALYSIS MODULE

Outsider analyses are based on the SAVI model of timely detection, with major improvements in threat definition, algorithm performance, and deceitful intrusion modeling [7]. SAVI and Outsider both calculate the probability of interruption, P(I). P(I) is the probability that the security force at a facility can respond to an alarm and interrupt intruders before they complete their mission. Outsider also calculates P(W), the probability of system win. P(W) is defined as the product of P(I) and P(N), where P(N) is the probability the response force can neutralize the intruders once interruption occurs. Outsider can get P(N) from the ASSESS Neutralization Analysis module [8] or directly from the analyst. For more about how Outsider calculates P(I) see Reference 7.

The value of P(I) for a given path is determined by locating the last point in the path, called the Critical Detection Point (CDP), where an alarm can cause the response force to deploy with enough time left to stop the intruders. Protection elements before the CDP provide detection; those after the CDP provide delay. Thus, in calculating P(I) for each path, delay safeguards in protection elements before the CDP and detection safeguards after the CDP are not effective. Outsider can find the ten most vulnerable (lowest P(I)) paths for a range of ten response force times (RFTs).

Outsider is a Microsoft Windows application. As such, it looks and works like other Windows applications, such as Facility and Microsoft Excel. Figure 1 shows the Outsider application as it might look after an analysis has been completed. A Control Panel displays and sets threat and analysis settings, and three support windows, Diagram, Results, and Graphs, display analysis information. Each support window can be moved and sized independently inside the main window. Outsider provides both mouse and keyboard control.

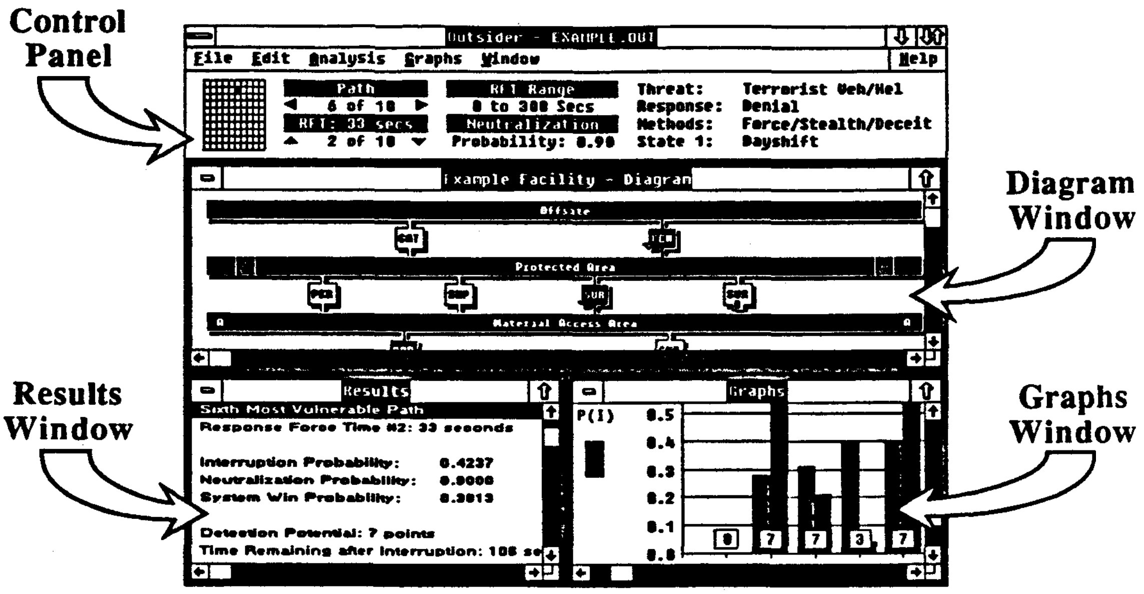
*This work was supported by the United States Department of Energy under Contract DE-AC04-76DP00789.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.



Path
◀ 6 of 10 ▶
RFT: 33 secs
▲ 2 of 10 ▼
RFT Range
0 to 300 Secs
Neutralization
Probability: 0.90
Threat: Terrorist Veh/Hel
Response: Denial
Methods: Force/Stealth/Deceit
State 1: Dayshift

Sixth Most Vulnerable Path
Response Force Time #2: 33 seconds

Interruption Probability: 0.4237
Neutralization Probability: 0.9000
System Win Probability: 0.3813

Detection Potential: 7 points
Time Remaining after Interruption: 108 se

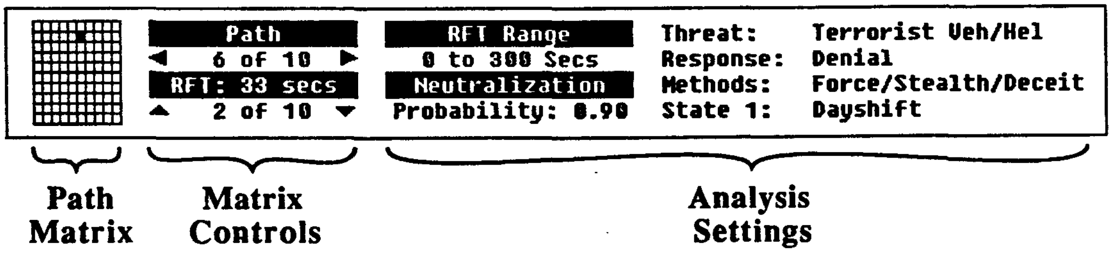
Figure 1. The Main Outsider Analysis Screen

After starting Outsider, an analyst can load a physical protection system description created in Facility or a previously saved analysis. The protection system, in the form of an Adversary Sequence Diagram (ASD), appears in the Diagram window. The analyst can then choose threat and response force settings using the Control Panel, and run the chosen analysis. After the analysis is finished, the Control Panel is used to select any path and see it highlighted on the Diagram. A detailed textual description of the path including intrusion methods and individual safeguard performance values is shown in the Results window. The Graphs window displays user-selectable information about sets of paths, including a graph of the protection system's sensitivity to response force deployment time. After reviewing the analysis results, the analyst can save them to a file, print reports, create a collusion analysis support file, or modify settings and reanalyze.

Control Panel

The Control Panel shown in Figure 2 displays all of the settings that control an Outsider vulnerability analysis.

When an Outsider analysis is completed, the most vulnerable intrusion paths through the facility protection system are accessed through the Control Panel's Path Matrix. Outsider can display up to 100 of the most vulnerable paths based on the number of requested paths and response force times. The Path Matrix columns represent the most vulnerable intrusion paths. The analyst may request that up to 10 of the most vulnerable paths be identified. Each row of the matrix represents a single response force time from the specified range, which may also have as many as 10 RFTs. Therefore, the Path Matrix can be as large as 10 by 10. The Path Matrix controls indicate the number of requested paths and RFTs as well as the current highlighted path in the matrix. All data associated with the highlighted path is displayed automatically in the Diagram, Results, and Graphs windows. Using these controls, the analyst can efficiently review the vulnerability of all paths in the matrix.



Path
◀ 6 of 10 ▶
RFT: 33 secs
▲ 2 of 10 ▼
RFT Range
0 to 300 Secs
Neutralization
Probability: 0.90
Threat: Terrorist Veh/Hel
Response: Denial
Methods: Force/Stealth/Deceit
State 1: Dayshift

Figure 2. The Outsider Analysis Control Panel

The Control Panel also displays all analysis settings including RFT Range, Neutralization Probability, Intrusion Threat, Response Mode, Intrusion Methods, and Facility State. The vulnerabilities of the facility are calculated based on these settings.

Outsider analysts choose the Threat to defend against from a list of ten adversary types. Adversaries are defined by the kind of equipment they carry and use to penetrate the facility. Equipment includes hand tools, power tools, high explosives, small arms, light anti-tank weapons, vehicles, and helicopters. Unlike SAVI, which supports only well-equipped threats, Outsider can identify vulnerabilities to poorly equipped adversaries such as political extremists who might not be able to penetrate all protection elements.

The Response setting specifies the response mode of the security force. This can be either Denial or Containment. Denial means the response force must interrupt the intruders before they reach the Target. Containment means the response force must interrupt the intruders before they leave the facility but after they have entered the facility and reached the Target. In SAVI, the denial response is referred to as an entry threat objective and the containment response as an entry/exit threat objective.

The Methods setting indicates the methods the intruders can use to penetrate the facility. The two choices are Force/Stealth and Force/Stealth/Deceit. Force/Stealth means intruders use violence, tools, and explosives to penetrate the facility; Force/Stealth/Deceit means intruders can also attempt to penetrate the facility using falsified credentials and smuggling contraband equipment, whenever it is to their advantage to do so.

The State setting indicates to which facility state the vulnerability analysis applies. Facility states are defined in the Facility Descriptor and refer to distinct differences in the protection system operation, such as day shift and night shift or normal operations and emergency.

The Control Panel settings are always valid; users can perform an analysis at any time with the current settings. If Denial is selected, Outsider generates the most vulnerable entry paths. If Containment is selected, Outsider generates the most vulnerable entry and exit paths. Both analyses use new, fast algorithms that generate paths in order of vulnerability [7]. Cells in the Path Matrix turn white as paths are found. When the analysis is finished, the upper left corner cell representing the most vulnerable path for the smallest RFT is highlighted and information about that path is displayed in the Diagram and Results windows.

Diagram

The Diagram window shows the ASD exactly the way it was created in Facility. When analysis results are available, the path currently selected in the Path Matrix is highlighted, and arrows show the direction of travel across each protection element. A blinking arrow identifies the element containing the CDP if there is a CDP for that path. Figure 3 shows the Diagram window displaying an entry path crossing each facility area from offsite to the target. The CDP is shown on the surface leading from the protected area to the material access area, indicating that the selected intruders must be detected by the time they reach this surface for the response force to have enough time to deploy and interrupt the intrusion.

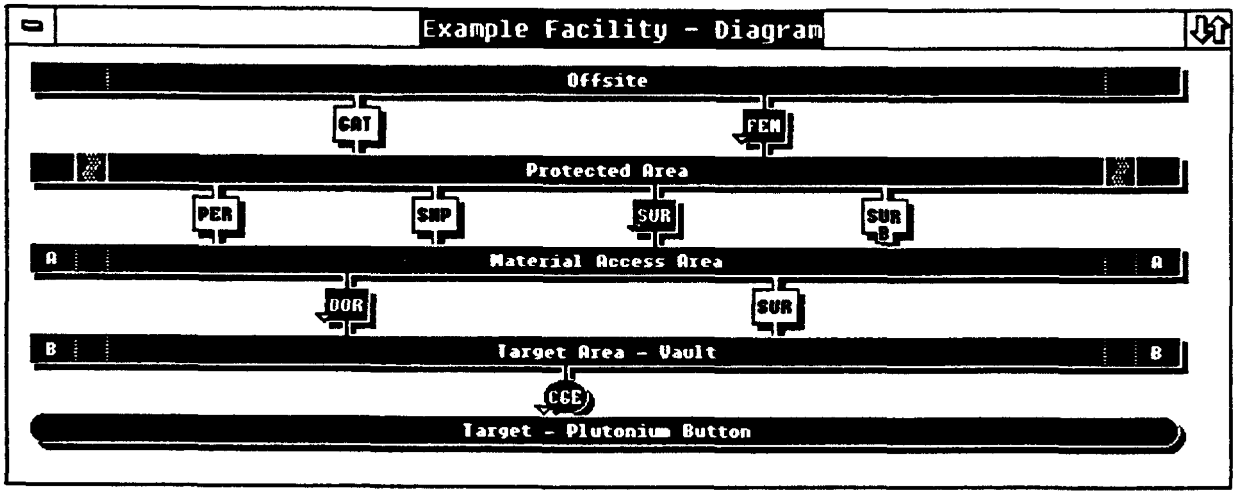
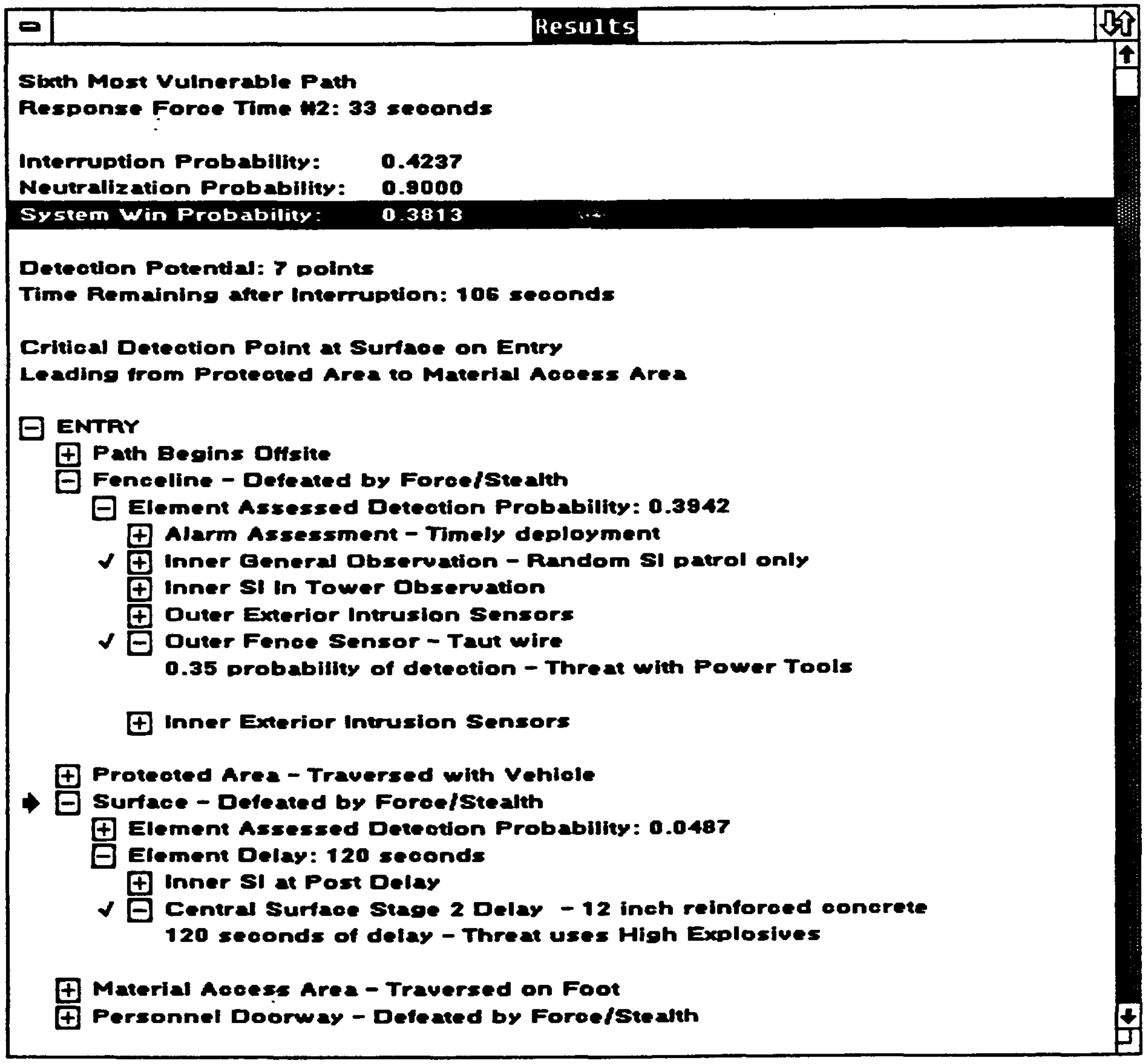


Figure 3. The Diagram Window

Results

The Results window in Figure 4 shows a detailed description of the sixth most vulnerable path for an RFT of 33 seconds as selected in the control panel. The probability of neutralization calculated by the Neutralization module is combined with the interruption probability to produce the probability of system win. A new measure of path vulnerability, detection potential, is also displayed in the results window. Detection potential is defined as the number of points on the path prior to the CDP where detectors could be installed. This is a rough measure of the depth of protection the path can provide. Given two paths with equal P(I), the path with the smaller detection potential is said to be more vulnerable. As in SAVI, the Time Remaining after Interruption (TRI) is also shown.

The description of the security system performance along the path is organized into dynamic headings that allow the analyst to examine the results to the desired detail. As in the Facility Descriptor, headings that can be expanded contain a button that the analyst can press to see more detail. The heading for the fenceline between offsite and the protected area is shown expanded in Figure 4. The probability of detecting the selected intruders at this fence is displayed along with a list of the detection safeguards that are encountered. The random security inspector patrol and the outer fence sensor provide a cumulative probability of .39 of detecting an intruder forcing the fence. This detection value includes the timely-deployment assessment probability. The analyst can expand any safeguard on the path to determine individual performance characteristics; for example, the taut-wire-fence sensor provides a .35 probability of detecting an intruder cutting the fence with power tools. This level of performance detail provides the specific information needed for an analyst to make intelligent upgrade decisions.



```
Sixth Most Vulnerable Path
Response Force Time #2: 33 seconds

Interruption Probability:     0.4237
Neutralization Probability:   0.9000
System Win Probability:       0.3813

Detection Potential: 7 points
Time Remaining after Interruption: 106 seconds

Critical Detection Point at Surface on Entry
Leading from Protected Area to Material Access Area

⊟ ENTRY
  ⊞ Path Begins Offsite
  ⊟ Fenceline - Defeated by Force/Stealth
    ⊟ Element Assessed Detection Probability: 0.3942
      ⊞ Alarm Assessment - Timely deployment
    ✓ ⊞ Inner General Observation - Random SI patrol only
      ⊞ Inner SI In Tower Observation
      ⊞ Outer Exterior Intrusion Sensors
    ✓ ⊟ Outer Fence Sensor - Taut wire
        0.35 probability of detection - Threat with Power Tools

      ⊞ Inner Exterior Intrusion Sensors

  ⊞ Protected Area - Traversed with Vehicle
➧ ⊟ Surface - Defeated by Force/Stealth
    ⊞ Element Assessed Detection Probability: 0.0487
    ⊟ Element Delay: 120 seconds
      ⊞ Inner SI at Post Delay
    ✓ ⊟ Central Surface Stage 2 Delay  - 12 inch reinforced concrete
        120 seconds of delay - Threat uses High Explosives

  ⊞ Material Access Area - Traversed on Foot
  ⊞ Personnel Doorway - Defeated by Force/Stealth
```

Figure 4. The Results Window

Graphs

The Graphs window allows the analyst to view graphic information about many paths or RFTs at once. The Vulnerability graph contains all the measures of vulnerability for each of the most vulnerable paths at a specific RFT. Figure 5 shows the Vulnerability graph for the ten worst paths with a response force time of 33 seconds. The paths are displayed in order of vulnerability with the most vulnerable path at the left. The P(I) and TRI for each path are represented as bar pairs. P(W) is represented by a black line on each P(I) bar and the detection potential is reported in the box at the base of each bar pair.

The Sensitivity graph details the sensitivity of a selected path to variations in RFT. Figure 6 shows the sensitivity of the sixth most vulnerable path to the RFT range specified by the analyst in the control panel. Notice that the probability of interruption decreases as the RFT increases. The Sensitivity graph is useful for determining the maximum RFT that a security system can afford before P(I) drops to an unacceptable level.

Other Features

Outsider can print path diagrams, graphs, and text reports to any Windows-supported printer. This is a major improvement over the limited printer set supported by SAVI. Intermediate vulnerability results for the ASSESS Collusion module can also be calculated and saved in a support file [4]. Outsider determines the most vulnerable path from offsite to each area in the facility and back to offsite for the current threat, state, and maximum RFT defined in the Control Panel. These paths represent an intruder stealing target material that was moved to each of the facility areas by an insider sometime earlier.

SUMMARY

Outsider is the ASSESS module responsible for determining the vulnerability of a facility to potential violent intrusion by outside threats, such as terrorists and extremists. Through the user-friendly Windows interface, analysts load facility descriptions created in Facility; choose threat and response force analysis settings; perform analyses using new, fast algorithms; and review the results in graphical and textual forms.

Outsider has faster algorithms, has better threat and deceit modeling, accepts larger ASDs, and generates more detailed results than SAVI. Together, Facility and Outsider supersede SAVI as state-of-the-art software tools for outsider intrusion vulnerability analysis.

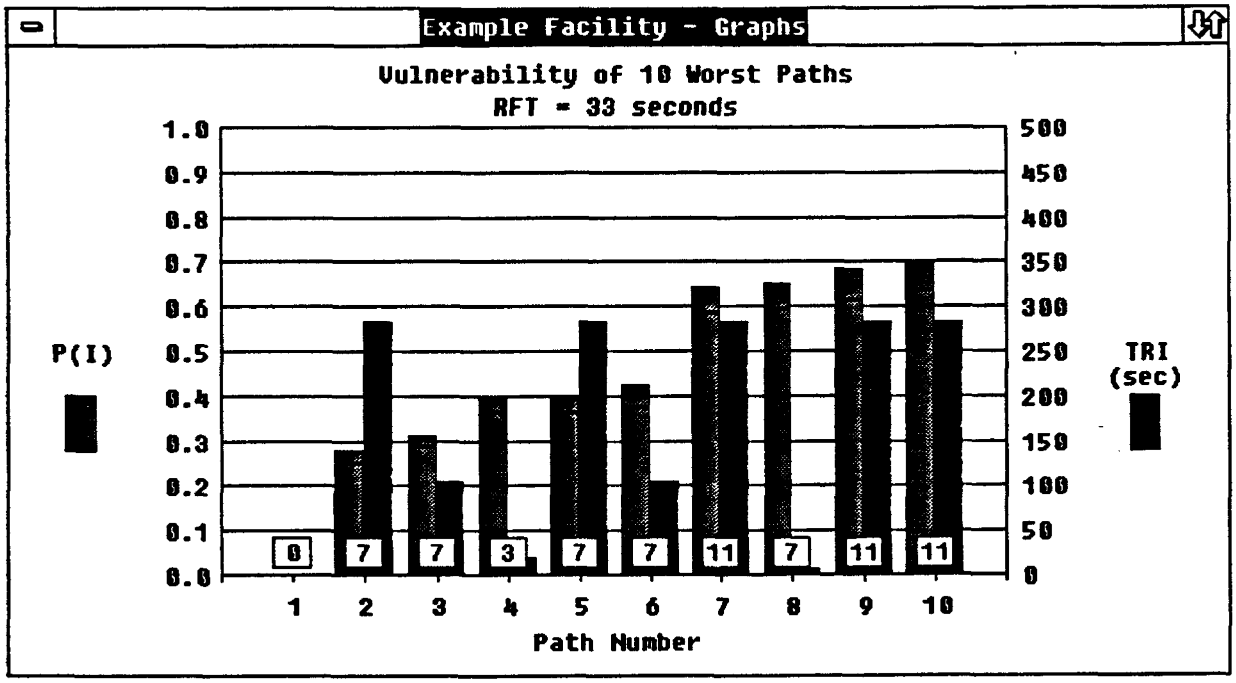


Figure 5. Vulnerability Graph

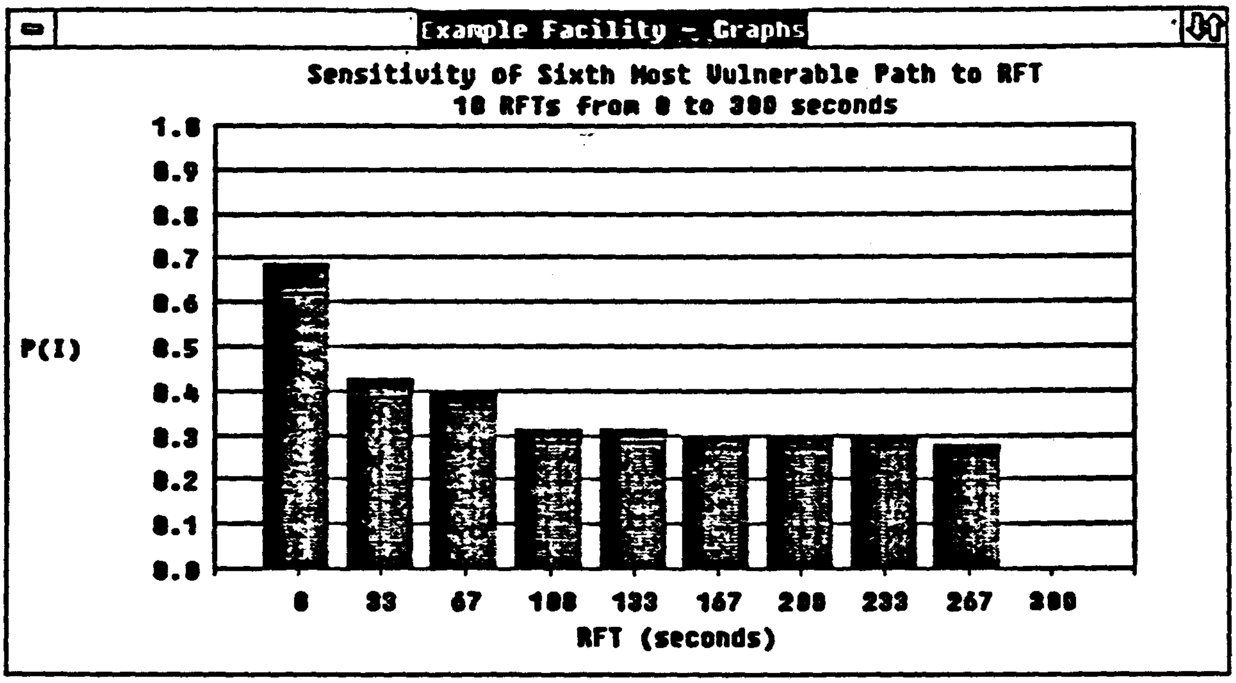


Figure 6. Sensitivity Graph

REFERENCES

[1] An Overview of ASSESS - Analytic System and Software for Evaluating Safeguards and Security, T.D. Cousins, R.A. Al-Ayat, and J.C. Matter, INMM 30th Annual Meeting Proceedings, 1989.

[2] The ASSESS Facility Descriptor Module, Sabina Erteza Jordan, Alfred Winblad, Brad Key, Scott Walker, Therese Renis, and Richard Saleh, INMM 30th Annual Meeting Proceedings, 1989.

[3] A Comprehensive Method for Evaluating Safeguards Against the Insider Threat, R.A. Al-Ayat, T.A. Renis, R. Saleh, and C.J. Patenaude, INMM 30th Annual Meeting Proceedings, 1989.

[4] Hand-off Collusion Module of the ASSESS Program, D.S. Fortney, W.A. Romine, and M.K. Snell, INMM 30th Annual Meeting Proceedings, 1989.

[5] The SAVI Vulnerability Assessment Model, Alfred E. Winblad, Sandia National Laboratories, INMM 28th Annual Meeting Proceedings, Volume XVI, July 1987, 24-28.

[6] The SAVI Vulnerability Analysis Software Package, R.J. McAniff, W.K. Paulus - Sandia National Laboratories, B. Key, B. Simpkins - Science & Engineering Associates, Inc., INMM 28th Annual Meeting Proceedings, Volume XVI, July 1987, 295-298.

[7] The ASSESS Outsider Interruption Algorithm, Mark K. Snell, Bryan Bingham, INMM 30th Annual Meeting Proceedings, 1989.

[8] The ASSESS Adversary Neutralization Module, Bill Paulus, Sabina Erteza Jordan, Martha Moore, and Junko Mondragon, INMM 30th Annual Meeting Proceedings, 1989.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.