SANDIA REPORT

SAND2004-4712
Unlimited Release
Printed September 2004

Dynamic Vulnerability Assessment

Cynthia L. Nelson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2004-4712
Unlimited Release
Printed September 2004

Dynamic Vulnerability Assessment

Cynthia L. Nelson
Security Technology
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0780

Abstract

With increased terrorist threats in the past few years, it is no longer feasible to feel confident that a facility is well protected with a static security system. Potential adversaries often research their targets, examining procedural and system changes, in order to attack at a vulnerable time. Such system changes may include scheduled sensor maintenance, scheduled or unscheduled changes in the guard force, facility alert level changes, sensor failures or degradation, etc. All of these changes impact the system effectiveness and can make a facility more vulnerable. Currently, a standard analysis of system effectiveness is performed approximately every six months using a vulnerability assessment tool called ASSESS (Analytical Systems and Software for Evaluating Safeguards and Systems). New standards for determining a facility's system effectiveness will be defined by tools that are currently under development, such as ATLAS (Adversary Time-line Analysis System) and NextGen (Next Generation Security Simulation). Although these tools are useful to model analyses at different spatial resolutions and can support some sensor dynamics using statistical models, they are limited in that they require a static system state as input. They cannot account for the dynamics of the system through day-to-day operations. The emphasis of this project was to determine the feasibility of dynamically monitoring the facility security system and performing an analysis as changes occur. Hence, the system effectiveness is known at all times, greatly assisting time-critical decisions in response to a threat or a potential threat.

Dynamic Vulnerability Assessment

1 Introduction

With increased terrorist threats in the past few years, it is no longer feasible to feel confident that a facility is well protected with a static security system. Potential adversaries often research their targets, examining procedural and system changes, in order to attack at a vulnerable time. Such system changes may include scheduled sensor maintenance, scheduled or unscheduled changes in the guard force, facility alert level changes, sensor failures or degradation, etc. All of these changes impact the system effectiveness and can make a facility more vulnerable. Currently, a standard analysis of system effectiveness is performed approximately every six months using a vulnerability assessment tool called ASSESS (Analytical Systems and Software for Evaluating Safeguards and Systems). New standards for determining a facility's system effectiveness will be defined by tools that are currently under development, such as ATLAS (Adversary Time-line Analysis System) and NextGen (Next Generation Security Simulation). Although these tools are useful to model analyses at different spatial resolutions and can support some sensor dynamics using statistical models, they are limited in that they require a static system state as input. They cannot account for the dynamics of the system through day-to-day operations. Analysis tools that can understand the dynamic changes that occur in a facility within the constructs of the current vulnerability analysis tool set are needed. The emphasis of this project was to determine the feasibility of dynamically monitoring the facility security system and performing an analysis as changes occur. In this sense, the system effectiveness is known at all times. This will greatly enhance the response decisions that are critical during an attack or to prevent an attack.

This work highly leveraged the capabilities in ASSESS to define elements, their safeguards, and their associated performance values. It also leveraged capabilities in ATLAS to obtain critical system performance values. A software simulation was developed as a proof-of-concept to demonstrate the capability of providing a continual analysis of system effectiveness on a dynamically changing security system. A description of facility information used from ASSESS and ATLAS is provided in Section 2. Section 3 describes the overall software architecture of the Dynamic Vulnerability Analysis (DVA) simulation. A description of the operation of the simulation is presented in Section 4. The project is summarized in Section 5.

2 Background

A key component of performing a vulnerability analysis on a facility is a description of its physical security system. The facility information is defined using an Adversary Sequence Diagram (ASD), which is a schematic representation of a facility and its safeguards components (See Figure 1). Each area of the facility that separates the offsite area with the target area is represented by a horizontal bar. Path elements are the portals that connect the areas. A path element exists for each possible access method into and out of the area. Types of path elements include door (DOR), personnel portal (PER), vehicle portal (VEH), gate (GAT), fence (FEN), surface (SUR), duct (DUC), shipping door (SHP), emergency exit (EMX), etc.

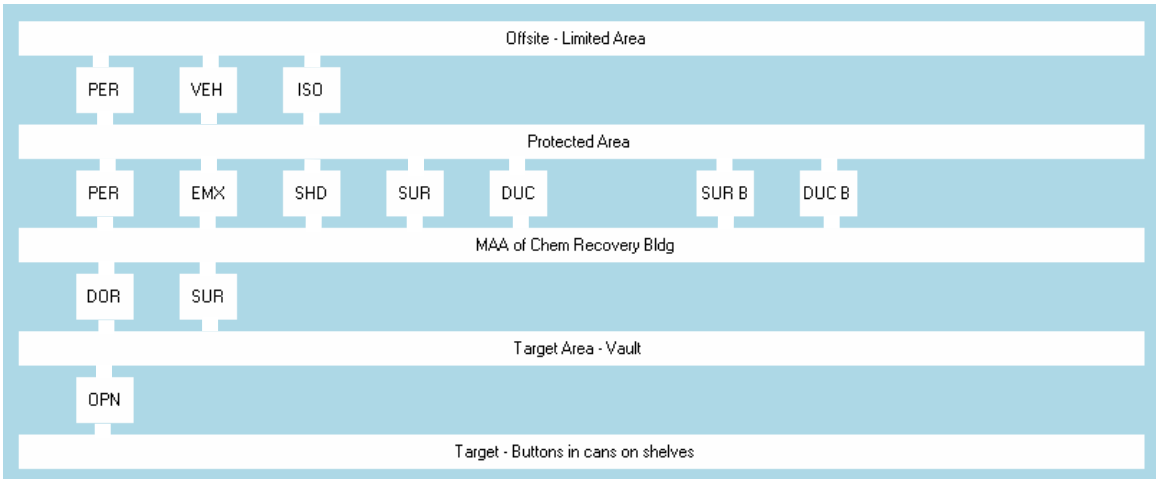

Figure 1. Adversary Sequence Diagram with areas and path elements defined.

Each path element has certain characteristics (Alarm Assessment, SNM Sweep, Traffic Flow, Background Radiation, and Material Container) that are addressed by a set of safeguards. The safeguards define the security at the associated path element. There are seven categories of safeguards: Access Control, Contraband Detection, SNM Detection, Material Transfer Control, Intrusion Detection, Access Delay, and Security Inspectors. Each element may have a different set of possible safeguards for each category. The data that describes the security system of the facility is saved in a file. This is the baseline description of the safeguards that are used for dynamic vulnerability assessment.

Performance characteristics are defined for each safeguard. These may change depending on the threat that is being addressed. The performance values are used to statistically determine critical paths to the target and the probability of interruption of the intruder (PI) under different threat conditions.

3 DVA Software Architecture

A proof-of-concept software simulation was developed to perform vulnerability analysis dynamically on a facility security system. The main goals of the project were to (1) automatically detect changes in safeguards, which may affect the system effectiveness, (2) analyze a changing system over a period of time so that at any time during that period, the system effectiveness is known, and (3) provide a visualization tool for an operator showing critical paths to the target that are updated as the system effectiveness changes. A high level design of the simulation system is shown in Figure 2. DVA Monitor is a process that receives status information about the system. This includes the status of safeguards, the current guard force schedule, scheduled maintenance, on or off hour operation, etc. DVA Response is a process that reads the DVA results and displays the information to an operator.

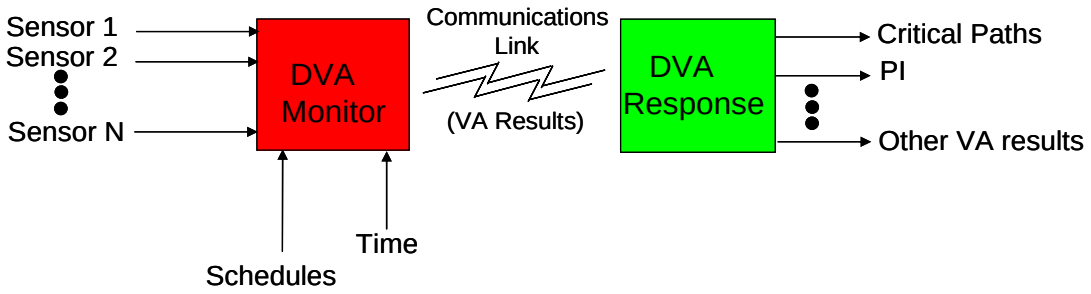

Figure 2. High level DVA System Architecture

The DVA Monitor process runs on a separate machine that is capable of receiving inputs from all sensors as well as mouse or keyboard input regarding schedule information. Schedule information may include times of day and night operations, guard schedule, guard absences, maintenance schedules, item movement schedules, and any other type of information that may affect the performance characteristics of the physical security system components. The sensors provide operational status information (i.e., on/off or working/not working). A degradation factor would also be applied to sensors. This may be based on the expected life of a sensor or by monitoring the strength of a sensor signal. If a sensor fails, its degradation factor is 100 percent. A clock input is provided in order to make automatic configuration changes of the physical security system at scheduled times and to perform a vulnerability analysis on the system at scheduled times. VA algorithms are called from this process. These algorithms are the same as those used with standard VA tools such as ASSESS or ATLAS. The databases used in these tools are also accessible on a dynamic basis. Whenever changes to the security system occur, the VA results are updated. They are saved in a file and are then sent to the DVA Response process for display.

The DVA Response process provides an interface between an alarm station operator and the dynamically changing vulnerability analysis results. The DVA information provided to the operator would help in quickly identifying weaknesses in the physical security system and would provide a key role in making decisions regarding guard placement or counter-attack strategies. Vulnerability analysis algorithms provide a substantial suite of information regarding the critical paths to a target and the probability of interruption (PI) of the adversary assuming various response force times. The critical paths and their associated PIs are displayed for the user. Other VA results are available for presentation to the operator if needed.

4 DVA Proof-of-Concept Operation

The Monitor process is initialized with a facility Physical Security System (.pps) file (Figure 3). This file contains all the information regarding the possible path elements and their associated safeguards for the selected facility. This file is created when an analysis is first done on a facility (See Section 2). The initial .pps file provides a baseline for future analysis and is used to establish the initial status of the DVA system when it is first initialized. The failure or degradation of safeguards is accounted for in the DVA Monitor process, but the baseline .pps file is not changed.

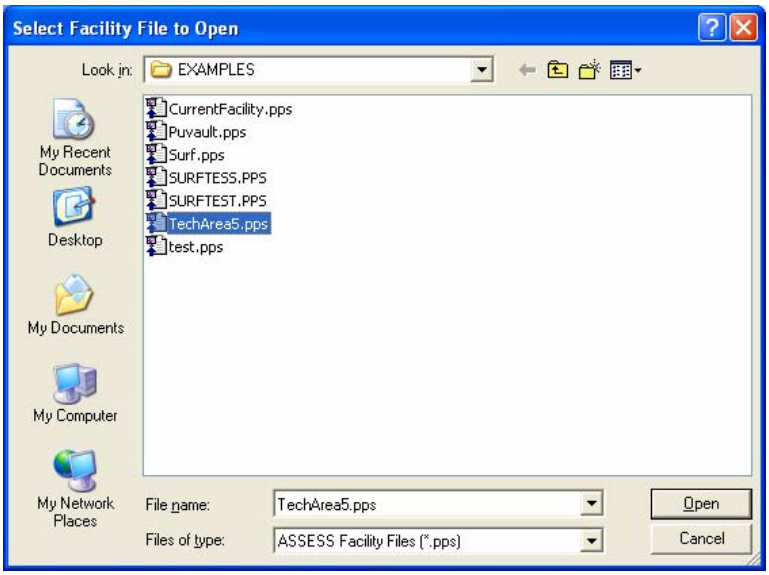

Figure 3. Selection of a Physical Protection System file for a facility.

Once the system is initialized with the appropriate .pps file, monitoring of the facility security status begins. A new vulnerability analysis can be run at any time on the facility by selecting the Run Analysis button on the user interface. For this simulation, the operational state of safeguards is manually changed using mouse input from menu selections. For example, in Figure 4, the MAA Portal element is selected from the Protected Area.

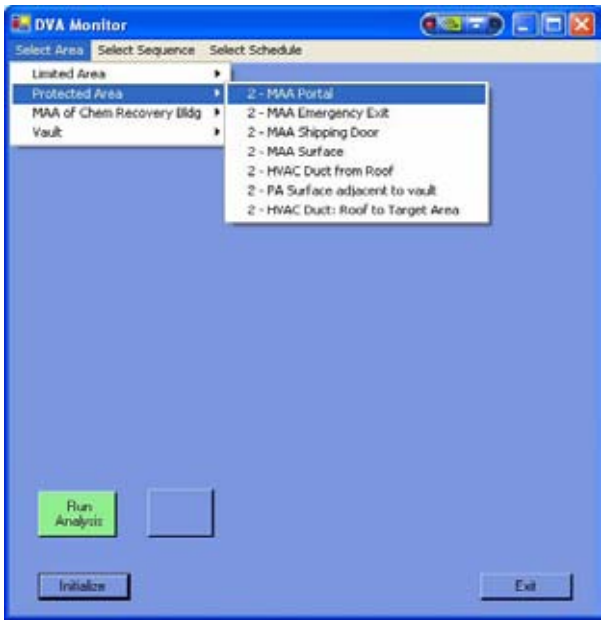

Figure 4. Selecting a path element that is defined for the facility.

Once the element is selected, the safeguards that are available for that element are listed, as shown in Figure 5. The individual safeguards can be turned on or off by checking or un-checking the box in front of each. Degradation can also be applied by highlighting an individual safeguard and using the slider to indicate the percentage of operational value for that safeguard. In the

example shown in the figure, the Portal Metal Detector is deactivated (failed). The ID Actuated Lock 1 is set to 70% operational (a degradation of 30%). When a change is applied that affects the system effectiveness, the VA algorithms are executed.

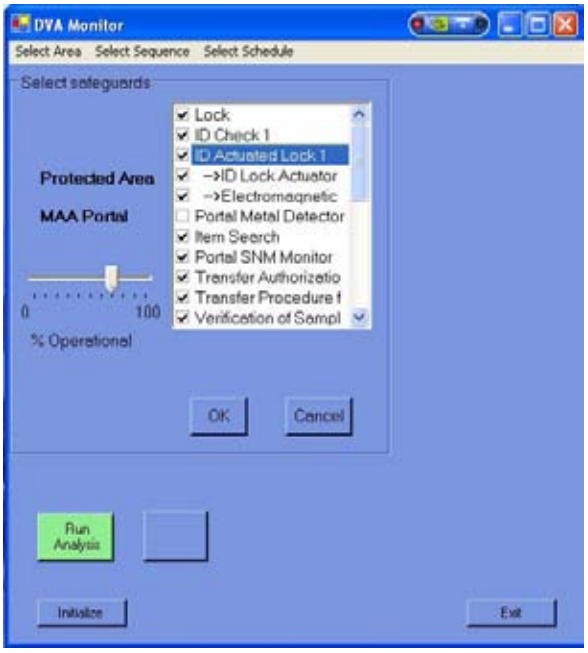

Figure 5. Manually changing operational status of element safeguards.

A continual timeline can also be set up for the DVA Monitor for simulation purposes (See Figure 6). Each bar along the timeline represents a selected period of time (e.g., 1 hour). During the progress of the timeline, the operational state of the physical security system is monitored. During this time, safeguards can be modified as described earlier, different monitoring scenarios can be applied (e.g., daytime vs. nighttime operation, movement of assets, etc), and different guard schedules can be applied. Whenever a change to the security system is made that may affect the system effectiveness, a new VA is automatically performed.

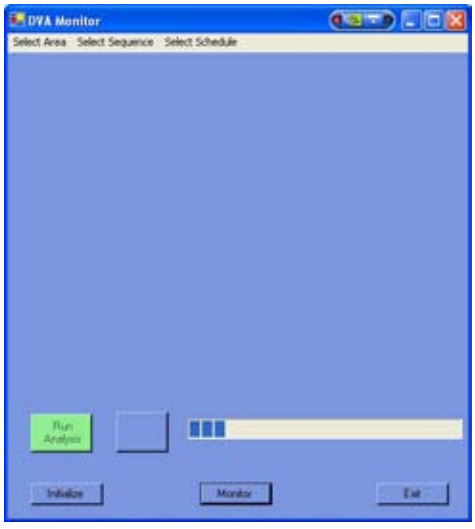

Figure 6. DVA of a facility over a continual time period.

In ASSESS, there are only two conditions that are used (usually relating to daytime and nighttime operations). Each condition may have a different set of safeguards with different performance values. In this DVA project, multiple conditions can be added and different ones can be effective at different times. A "sequence" may be selected, which refers to a predefined order of events (scenario) over a given time sequence. For example, the time begins at 8:00am with a full guard force and daytime conditions. At 10:00, several guards leave, resulting in a reduced guard force. At 2:00, a scheduled maintenance takes place, removing several of the sensors from the security system. At 4:00 the maintenance should be complete and the sensors are expected to be back on-line. At 5:00, an off-hours security condition takes effect. Currently, there are two sequences of events that are possible, called Scenario 1 and Scenario 2. The application of different sequences during a given timeline can be selected as shown in Figure 7. More sequences can easily be added as needed for simulation purposes. Also, the selection of a full or reduced size guard force can be made during a given timeline (Figure 8). This capability could be extended to indicate the exact number of guards. This information affects the performance values of different safeguards and also assists the guard force in placing personnel as needed throughout the facility.

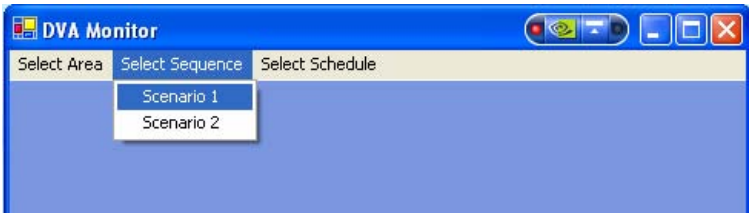

Figure 7. Sequence selection.

Figure 8. Schedule selection.

The DVA Response process executes on a separate machine, possibly the Alarm, Communications, and Display (AC&D) system. This provides the operator with a visual display of VA results. The communications line from the DVA Monitor Process is continually polled for updated analysis results. When new results are available, the DVA Response operator is notified and can refresh the display with the new information. The DVA Response process provides information that would allow the guard force to be aware of the most critical paths through the facility at all times. This would greatly assist in the placement of guards and in strategy decisions made during an actual attack.

The operator interface for the proof-of-concept simulation is shown in Figure 9. Here, an ASD is provided as well as a map of the facility. Each time new data is available, the Change Received button turns red. When pressed, the screen is updated with the most critical path through the facility with the shortest response force time. The operator can observe up to ten critical paths that are associated with up to 10 different response force times. The number of critical paths and the response force times available is determined apriori, when the facility file is first created and an analysis profile is determined.

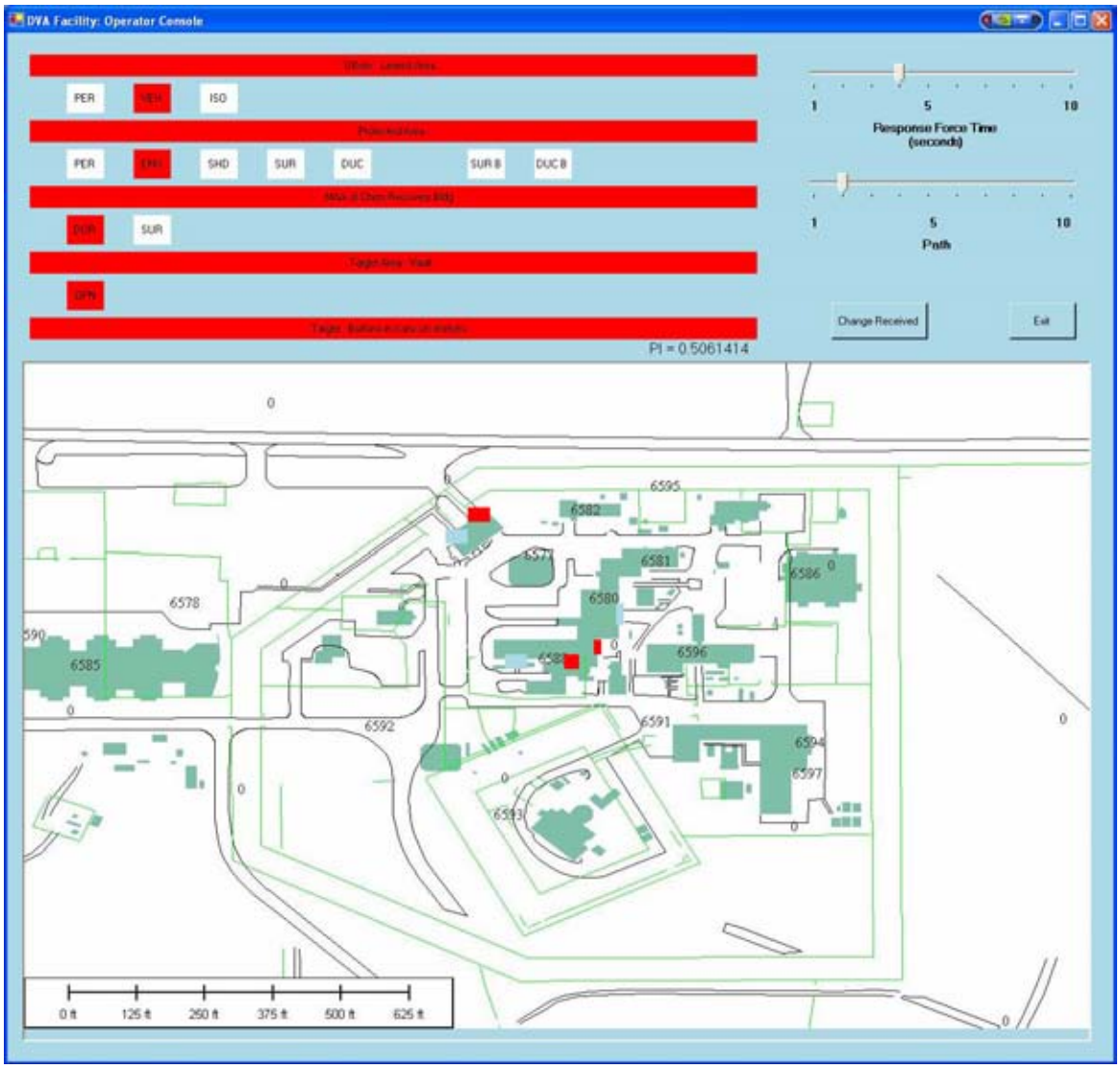

Figure 9. DVA Operator Interface.

In this display, a single high-level map is used to highlight elements in the critical path. Potentially, several layers of maps could be used in order to display path elements, and even safeguards, within buildings and rooms. The level of sophistication of the display would depend on map availability.

5 Summary

A need exists to determine the security system effectiveness of a facility on a dynamic basis. Although vulnerability analysis is generally performed bi-annually on a system, the system effectiveness changes continually. This may be due to sensor failures, degradation of sensors over time, removal or replacement of certain safeguards, guard shift changes, unexpected absences of members of the guard force, maintenance schedules, etc. When changes are made to the physical protection system, a new VA is executed, providing immediate results that could greatly influence the placement or movement of security forces and/or assets. A proof-of-concept

simulation of a system that could detect changes in the security system and automatically produce new VA results was developed for this project. This required accessing and manipulating data files and performance values that are created or maintained by existing VA tools in order to produce results on an as-needed basis. The analysis algorithms used in this simulation were from the "Outsider Analysis" tools in ASSESS. As long as the data is accessible, algorithms from ATLAS or NEXTGEN could also be used. The simulation shows that system effectiveness could be updated dynamically as system changes occur.

Follow-on work that would be beneficial to the concept of dynamic vulnerability analysis is to deploy the DVA Monitor and DVA Response processes in a real facility environment that uses the standard set of VA tools.

Distribution

1	MS	0232	H. R. Westrich, 1011
1		0780	Stephen Ortiz, 4138
5			Cynthia L. Nelson, 4138
1	MS	9018	Central Technical Files, 8945-1
2		0899	Technical Library, 9616