UCRL- 94265
PREPRINT

THE STRUCTURED ASSESSMENT APPROACH: A MICROCOMPUTER-BASED INSIDER-VULNERABILITY ANALYSIS TOOL

Cheri Jo Patenaude and Alan Sicherman
Lawrence Livermore National Laboratory
Livermore, California

Ivan J. Sacks
R & D Associates
Arlington, Virginia

This paper was prepared for submittal to
INMM 27th Annual Meeting
New Orleans, Louisiana
June 22-25, 1986

Lawrence Livermore National Laboratory

THE STRUCTURED ASSESSMENT APPROACH: A MICROCOMPUTER-BASED INSIDER-VULNERABILITY ANALYSIS TOOL

Cherie Jo Patenaude and Alan Sicherman
Lawrence Livermore National Laboratory*
Livermore, California

Ivan J. Sacks
R & D Associates
Arlington, Virginia

UCRL--94265
DE86 012818

Abstract

The Structured Assessment Approach (SAA) was developed to help assess the vulnerability of safeguards systems to insiders in a staged manner. For physical security systems, the SAA identifies possible diversion paths which are not safeguarded under various facility operating conditions and insiders who could defeat the system via direct access, collusion or indirect tampering. For material control and accounting systems, the SAA identifies those who could block the detection of a material loss or diversion via data falsification or equipment tampering. The SAA, originally designed to run on a mainframe computer, has been converted to run on a personal computer. Many features have been added to simplify and facilitate its use for conducting vulnerability analysis. For example, the SAA input, which is a text-like data file, is easily readable and can provide documentation of facility safeguards and assumptions used for the analysis.

Overview of the Structured Assessment Approach

The Structured Assessment Approach (SAA) was developed by a team at Lawrence Livermore National Laboratory to help assess the vulnerability of physical security and material control and accounting (MC&A) systems to insiders at facilities handling special nuclear materials. The underlying structure of the approach allows an assessor to encode in a unified model the layout and operations of a facility together with its safeguards system. By analyzing this facility model, the SAA can reveal vulnerabilities that may not have been apparent using informal analysis, thereby leading to recommendations for improved safeguards.

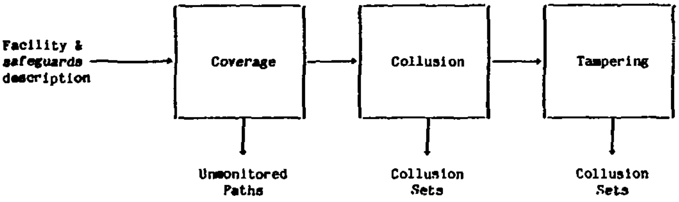
Development of the SAA was funded by the U.S. Nuclear Regulatory Commission Office of Regulatory Research and was first applied to the assessment of a nuclear fuel facility in late 1978.[1] A complete description of the SAA was published in 1980.[2] The SAA was originally designed to run on a mainframe computer. Recently, the SAA was converted to a user-friendly program that runs on a personal computer (PC). Using the SAA program, an assessor can analyze the vulnerability of safeguards systems in a staged, systematic manner.

In a physical security analysis, the SAA determines which insiders, working alone or in colluding pairs, can create diversion paths which are not safeguarded (i.e., not monitored) by the physical protection system. The analysis is performed in three stages using a text-like data file created by the assessor. Typically, the physical security system should pass the scrutiny of each stage before proceeding to the next. At the first stage of analysis, the SAA determines if there are any unmonitored paths for any set of plant operational conditions. The SAA displays the paths and safeguards system components (monitors) an adversary must defeat to pass successfully from a designated starting point to a designated stopping point. The first stage is called "coverage" because key paths should be covered by some safeguards component. If not, an obvious vulnerability exists and should be remedied before proceeding further.

Having completed the stage 1 analysis, the assessor then expands the SAA data file to include more detail on the personnel access to and control of the physical security system components. The program then processes this expanded data file to determine insiders who can create unmonitored diversion paths for any set of plant operating conditions specified by the assessor. The results are presented as individual adversaries and pairs of adversaries ("collusion" sets) who can defeat the system via their direct authorized access.

Once this analysis is completed, the assessor can conduct a stage 3 evaluation. First, the user is guided in how to expand the data file to include the details of the systems which support the physical security monitors. These "support systems" include maintenance, electrical power, and tamper monitors. The third stage of the SAA is used to determine individuals who can create unmonitored diversion paths through indirect access ("tampering") to support systems, as well as direct access. This data expansion process can

*Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.



The analysis can stop at any level.

Fig. 1. Stages of an SAA physical security vulnerability assessment.

be continued to yield an extremely detailed model of the facility and its physical security system. The text-like SAA data file also serves as a readable document which describes the physical protection system.

Figure 1 summarizes the three stages of an SAA physical security vulnerability assessment. The three stages allow incremental analysis of vulnerabilities by expanding the detail of the physical security system model. The coverage stage uses a description of the facility layout and the physical security monitors to reveal any obvious vulnerabilities. As the assessor increases the detail of the model, the SAA can reveal additional and less obvious vulnerabilities (e.g., disabling a power supply to make a monitor inoperable). Finally, with the gradual building up of model detail, vulnerabilities due to sophisticated tampering or collusion can be identified.

The SAA analysis of a material control and accounting system is designed to determine which sets of individuals could (1) prevent the detection of a material loss and (2) cause an erroneous loss indication (in support of a hoax). Instead of a facility and its physical protection system, this analysis is based on an information flow model of the accounting system. The information flow model includes facility records, inventory procedures, measurement and calibration techniques, and record verification.

The safeguards assessor generates a text-like data file following the incremental pattern of an SAA physical security assessment. In the expansion steps, the assessor adds detail for the support components of the MC&A system. These support components include equipment (e.g., for data recording, transmission and processing, and for material measurement) and the personnel who measure and process the accounting data. The SAA material control and accounting analysis then finds the sets of individuals who could defeat the loss detection systems. Again, the data file provides a readable description of the MC&A system. The SAA ultimately helps identify those who working alone or in collusion could defeat the MC&A system by indirect data falsification or equipment tampering. Currently, we are using the PC version of the SAA to evaluate insider-vulnerability of MC&A systems at several DOE facilities.

The remainder of this paper describes the nature of modeling safeguards systems using the SAA on a PC in more detail. Physical security and MC&A are discussed separately. While the modeling philosophy is basically the same for both physical security and accounting, the SAA has procedures and "canned" models tailored to each. For physical security, the focus is on facility layout, operating conditions, monitors, and utilities. For material accounting, the emphasis is primarily on information flow and equipment and personnel that generate, control, and utilize information.

Physical Security Modeling and Analysis

In a physical security analysis, a facility and its safeguards system are represented by indicating what movement is permitted between adjacent areas and what access is permitted to facility components. Figure 2 shows a simple example to illustrate the SAA modeling concepts. In the example, movement from the outside to the vestibule and from the vestibule to the outside is monitored by a balanced magnetic switch on the door. The vault is locked to prevent unauthorized personnel from entering it but the vault may be exited at any time because of a "panic bar" on the inside of the vault door. The vestibule is monitored by a microwave intrusion detector which is turned off during the day shift and any other processing, shipping, or operating times. When the intrusion detector is off, a two-person rule is in force.

A person either can get from one location to the next closest locations unconditionally or must defeat the monitors on his/her movement or activities. For example, the vault lock prevents an unauthorized person from getting to the vault from the vestibule. To defeat this safeguard, an unauthorized person must have access to (or control over) the lock. The SAA input file provides an easy way to represent adjacency and access as illustrated in Fig. 3. In Fig. 3, areas begin with the letter A and monitors (or controls) with the letter M in the data lines which are left justified. Unconditional access is denoted by using the number 1 after the second comma. Notice that the file is liberally commented, making it very easy to read the model descriptions. Without going into format detail, the SAA provides for

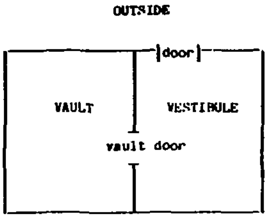


Fig. 2. Simple example to illustrate SAA concepts.

```
                                  **** STEP 1 ****

               AREA ADJACENCY
A_OUTSIDE,A_VESTIBULE,M_DOORSWITCH             THE FACILITY IS ISOLATED FROM THE OUTSIDE BY A DOOR
A_VESTIBULE,A_OUTSIDE,M_DOORSWITCH             WHICH IS MONITORED BY A BALANCED MAGNETIC SWITCH


A_VESTIBULE,A_VAULT,M_LOCKEDDOOR               THE VAULT IS PROTECTED BY A LOCKED VAULT DOOR

A_VAULT,A_VESTIBULE,1                          PERSONNEL IN THE VAULT CAN EXIT WITHOUT UNLOCKING
                                               THE DOOR BY MEANS OF THE "PANIC BAR"
```

Fig. 3. Portion of typical SAA data file.

analogous representations of personnel access to the monitors, utilities which support monitors (e.g., power supplies) and conditions under which monitors are not available. This simple construct is the heart of the SAA PC version. By systematically adding more detail to each feature identified by the modeling process, an extremely detailed and comprehensive model of the facility and its safeguards system can be created.

To understand the construct, simply interpret data line 1 of Fig. 3 as follows: "Access to the OUTSIDE and the DOORSWITCH implies access to the VESTIBULE from the OUTSIDE. Data line 3 is read "Access to the VESTIBULE and the LOCKEDDOOR implies access to the VAULT from the VESTIBULE. Line 4 is read "Access to the VAULT implies access to the VESTIBULE from the VAULT. These constructs can be combined to model the connectivity of the facility and its components by logical "chaining." For example, if having keys implies access to a lock and having access to a drawer implies access to the keys, the SAA code recognizes that access to the drawer implies access to the lock.

The SAA program on the PC allows for a computer-aided step-by-step analysis of vulnerabilit:es. Initially, the data input reflects the basic area adjacency, monitors and direct personnel access to monitors for the facility. Subsequently, utilities supporting the monitors and access to those utilities (which can imply access to monitors via "chaining") are added in an expansion of the initial description. In this incremental manner, vulnerabilities are analyzed at levels of detail controlled by the program user. Initially, there may be few potential vulnerabilities (e.g., no single insider can defeat the system under typical operating conditions) when only direct access to monitors is modeled. However, as more detail is added and different operational conditions are examined (e.g., power outages, emergencies, etc.), the SAA can give insight into potential diversion paths and scenarios which may not have been apparent. To illustrate using our simple example, if the power supply essential to the intrusion detector and door switch is accessible from the outside, and the vault lock can be forced, then during nonoperating hours, an unmonitored diversion path is available from the outside to the vault and back again to anyone with access to the power supply. The SAA program reveals which insiders can compromise the safeguards due to their access and/or collusion capabilities.

The SAA procedures include guidelines on how to develop systematically the input data file for physical security, how to examine operating conditions and their effect on monitor effectiveness, and how to expand each element of the safeguards system to look for less obvious vulnerabilities. The steps for physical security analysis are as follows:

1. Model area adjacencies and controls for transitions between areas.

2. Add monitor coverage within areas.

3. Add conditions when monitors are inactive and perform coverage analysis.

4. Add personnel access and control and perform collusion analysis.

5. Add support for monitors and perform tampering analysis.

Steps 3, 4, and 5 reflect how the SAA can be "run" on an initial description of the facility or a portion thereof to provide quick feedback and results to the user. This capability is one of the advantages of using SAA on the microcomputer. Another advantage is provided by the program's interactive menu allowing the user to indicate which condition combinations to analyze (e.g., night shift and power outage, for example) and which monitors to "disable." In this way, an assessor can gain insight into the critical elements of the safeguards system and how they can be protected from compromise.

In concluding this discussion of physical security analysis using the SAA on the PC, we note that aids are provided with the SAA to facilitate systematic modeling of safeguards. These aids include "unit models" or "canned" data formats. These remind the user to specify the following for each safeguards system component: personnel with authorized access, personnel with authorized control, location of monitor, support utilities, conditions for not being active, signal transmission lines and maintenance requirements. Other aids include interactive review of monitors to help insure that all relevant situations (e.g., operational shifts and conditions, nonroutine conditions, and adversary attributes such as contraband) are considered. It is especially easy using the SAA on the PC to add relevant conditions previously not considered in performing a physical security safeguards analysis.

Material Accounting Modeling and Analysis

An accounting system vulnerability analysis using the SAA on the PC follows the general procedure used for a physical security analysis: model the system, solve for potential vulnerabilities, expand the model and solve again. In accounting, the information flow system is the focal point for analysis.

An accounting system can be represented by the set of detection systems which are designed to detect anomalies and the data flows which bring information to these systems. The basis of detection in a material accounting system is the material balance equation:

$$ID = BI - EI + TI - TO$$

where:

ID = Inventory Difference
BI = Beginning Inventory
EI = Ending Inventory
TI = Transfer In
TO = Transfer Out

The ending inventory corresponds to the result of a physical inventory and the other three right hand terms correspond to the data in the "books." Generally, the inventory difference is compared to a threshold value to determine whether a loss has occurred. In the case of a material accounting system for bulk material, this threshold is called LEID, limit of error inventory difference. For an item account system, LEID should always be zero.

Anyone who can change (or falsify) any of the terms of the material balance equation could compromise detection. In order to determine which individuals could falsify the data used in the detection test, the flow of data for each term of the material balance equation can be modeled using the SAA on the PC. Determining who can "get to" the data characterizes potential vulnerabilities of the accounting system.

Individuals who perform the physical inventory could compromise the loss detection system as well as those who maintain the books, perform the comparison to LEID, etc. A less vulnerable accounting system is one in which no individual has access to or control over critical data without another person's review.

The general steps in an accounting analysis are: a) identify detection systems designed to detect anomalies in material balance at various areas in the facility; b) model each detection system in terms of how data is generated, transmitted, processed, stored, etc.; c) add personnel access (including the people who measure, transmit, and process the MC&A data and also those involved in sampling, calibration, and other procedures which can affect the validity of accounting information) and perform a vulnerability analysis (including collusion); d) add support components and perform a tampering analysis.

As with physical security, user aids are provided with the SAA to facilitate modeling of accounting safeguards described in step b above. These aids include unit models for shipper/receiver tests, inventory measurements, and data validation. These unit models help the user to examine the series of steps in accounting system elements which can be overlooked in a less formal vulnerability analysis. Steps such as transmission and recording of data can be especially important in reviewing shipper/receiver and inventory procedures. Careful modeling of the two-man rule, for example, can reveal whether a truly effective two person check is present, or whether only a single person is actually recording data.

When running an accounting analysis using the SAA on the PC, the assessor selects an element of the facility as a "target" for falsification. The SAA program then displays personnel who can "get to" the element via access to related elements (i.e., using "chaining" logic as with physical security). The program can also display all other elements that, if accessed, can lead to falsification of the target. This display provides a trace-back of the paths or ways which can result in the compromise of existing safeguards.

Summary

The SAA program on the PC allows for a computer-aided step-by-step analysis of vulnerabilities for physical security and material accounting systems. At each step, the program aids the assessor in keeping the facility description logically consistent and in revealing vulnerabilities that may not have been apparent using informal analysis.

The text-like input file developed while using the SAA provides convenient and concise documentation of how the safeguards in a facility are modeled. The input serves not only as the means of running the analysis, but also for documenting the assumptions of the analysis. The program provides the framework for building up a detailed description of the facility in a way that can significantly increase the thoroughness of safeguards evaluation and documentation.

References

[1] A. A. Parziale, I. J. Sacks, T. R. Rice, and S. L. Derby, "The Structured Assessment of Facility "X"," Lawrence Livermore National Laboratory, Livermore, California, NUREG/CR-0791, UCRL-52765, Volumes I and II, January 8, 1979.

[2] A. A. Parziale and I. J. Sacks, "The Structured Assessment Approach Version I," Lawrence Livermore National Laboratory, Livermore, California, NUREG/CR-1233, UCRL-52735, Volumes I-IV, November, 1980.

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.