UCRL- 82244
PREPRINT
CONF-800655--23

MASTER

The Safeguard Vulnerability Analysis Program (SVAP)

F. M. Gilman
M. H. Dittmore
W. J. Orvis
P. S. Wahler

This Paper was Prepared for Submittal to
INMM Conference
Palm Beach, Florida
June 30, July 1 & 2, 1980

June 23, 1980

Lawrence Livermore Laboratory

THE SAFEGUARD VULNERABILITY ANALYSIS PROGRAM (SVAP)*

F. M. Gilman
M. H. Dittmore
W. J. Orvis
P. S. Wahler

Lawrence Livermore National Laboratory
Livermore, California 94550

ABSTRACT

This report gives an overview of the Safeguard Vulnerability Analysis Program (SVAP) developed at Lawrence Livermore National Laboratory. SVAP was designed as an automated method of analyzing the safeguard systems at nuclear facilities for vulnerabilities relating to the theft or diversion of nuclear materials. SVAP addresses one class of safeguard threat: theft or diversion of nuclear materials by nonviolent insiders, acting individually or in collusion.

SVAP is a user-oriented tool which uses an interactive input medium for preprocessing the large amounts of safeguards data. Its output includes concise summary data as well as detailed vulnerability information.

I. Introduction

SVAP, the Safeguard Vulnerability Analysis Program, is a computer based system for analyzing the vulnerability of nuclear facilities to theft or diversion of material by the nonviolent insider. It was developed for the Nuclear Regulatory Commission (NRC) as part of an ongoing program at Lawrence Livermore National Laboratory.

Special nuclear material (SNM) must be protected, and the adequacy of this protection must be assured against, theft, diversion, sabotage or hoax. To address this problem, we have developed the computerized assessment package known as SVAP. SVAP is applicable to any fixed site material containment, control and accounting systems. SVAP has been tested on two licensed nuclear facilities and is adaptable to other material-protection analysis problems.

SVAP considers the problem of diversion of nuclear material by a nonviolent insider. Such an insider(s) may be: acting alone, acting in collusion, or acting within authority and abusing that authority. SVAP evaluates a facility's theft prevention and theft detection mechanisms. It locates paths in a facility between a target and a specified success goal (usually) outside of the facility. It then determines by whom and under what circumstances they can be traveled. The code considers: personnel, monitors, transmission components, utility components and documents in determining the circumstances. The results are sets of individual and their acts that could break the physical security system.

---

*This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

The code also investigates the accounting system to determine by whom and under what circumstances the diversion could be covered up. This investigation results in sets of individuals and their acts that could breakthe accounting system. A combination of these individuals and those from the physical security system gives the collusion analysis, showing who could divert material and conceal that diversion from detection.

The code has been made user-oriented through the use of a data gathering handbook (Wahler, 1980) and a mini-computer based data gathering system. The data gathering handbook in conjunction with the user's manual (Orvis, 1979), is designed to guide a user's data gathering as he (or she) moves through a facility. Once the data has been gathered, it is entered into the system through the use of a mini-computer (Tektronix 4050 series). The mini-computer checks validity and maintains internal consistency while providing a user-oriented interactive format for data input.

SVAP has been applied to two licensed nuclear facilities, the results of which confirm compliance with the relevant safeguards regulations. Selected portions of these are presented to highlight the effectiveness of the user-oriented tool. The full disclosure of our results is precluded by questions of sensitivity and classification.

II. The SVAP Input Phase

The SVAP input phase begins with a diagram of the facility in question, which has been subdivided into areas and portals. Located on this diagram are the various monitors, transmission components, utility components, and documents that make up the physical security system (Figure 1). Using the data gathering handbook, all pertinent data is then entered onto a set of forms. The data gathering handbook is designed to request information in an organized, sequential fashion. The analyst is thus guided in the collection of all pertinent safeguards information which is then recorded in the handbook. The same handbook can be used for all facilities, and serves as a convenient archival record.

Next, the material accounting system is investigated. Using forms from the data gathering handbook, the relevant data concerning the loss detection mechanisms, and the records and forms that support them is gathered. SVAP investigates the accounting records, the information sources for the records, consistency checks and balances, access authority to records and forms, and up to four time frames for detection.

Once all of this data has been gathered, the Facility Description Program on the mini-computer is used to input the data. The facility description program was designed to allow the consistent and orderly conversion of facility data into a machine acceptable form. It is an interactive program that speeds data entry while maintaining internal consistency. It has various correction routines, plus an online version of the user manual to visually describe the data gathering process. The facility dscription program builds a data tape that contains all of the facility data. This data tape can then be transmitted to the mainframe computer (CDC 7600) for processing. The mini-computer can also serve as a data terminal for transmitting data over the telephone lines.

III. SVAP Analysis

The SVAP analysis codes evaluate a facility's theft prevention and theft detection systems for potential loss of nuclear material through collusion. The first part of the analysis investigates the theft prevention mechanisms. These include physical security, alarm response, and material control. The code determines all paths between a target in the facility and a specified success goal as a set of Boolean equations. Using a Boolean algebra code known as SETS (Set Equation Transformation System) (Worrell, 1974), the paths are reduced to their simplest forms. Next, using the monitor data, the locations in a path are replaced by the monitors that cover that path. This results in a set of monitor paths that indicate the coverage of the related physical paths.

In a similar manner, transmission components, utility components, and documents are substituted into the equations. When this is done, personnel with authorized access to the above components are substituted into the equations to get the personnel sets that, through collusion, could defeat the system.

The second part of the analysis investigates the loss detection mechanisms for up to four time frames. These mechanisms are part of the material accounting system with its associated records and forms. In a manner similar to that used above for the physical security system, sets of people who could defeat the material accounting system are determined. Combining these sets with those generated for the physical security system results in the complete collusion analysis. These final sets of people constitute the minimum sets of those who could divert material and cover up the diversion.

IV. SVAP Output

SVAP documents each analysis by producing a separate computer-generated report for each target in the facility. The report is completely self-contained, and provides a basis for a formal assessment report. The report is fully formatted with abstract, analyst's comments, table of contents, results summary, detailed results, and input data.

The SVAP output is available in two forms. One is the hardcopy generated at the maintrame computer. The other is a data tape that can be read and printed with the mini-computer.

The SVAP output is broken into four parts, the first of which is a summary of the whole analysis. The summary is listed in tabular form, with plots of the level of protection for each target for each time period considered. Next comes the detailed analyses of the theft prevention mechanisms, the theft detection mechanisms, and the collusion analysis. Each section gives detailed analyses of the theft scenarios, including: paths, monitor failures, tampering, document abuse and collusion requirements.

V. Conclusion and Uses

SVAP, as a facility assessment procedure, has been applied to two licensed nuclear facilities. The results of these analysis indicate compliance of the facilities to the relevant safeguards regulations, and did so in a repeatable and documentable manner. SVAP was applied to the plutonium handling facility at G. E. Vallecitos as a demonstration (Figure 2).

Several conclusions which can be drawn from the analysis are: 1) adequacy of the monitor system, 2) appropriateness of the physical security response procedures, 3) level of protection provided by material control procedures, and 4) effectiveness of the accounting system.

These conclusions are drawn from the summary list and the plots of the level of protection for each target (Table 1, Figures 3, 4). The graphical data is also listed in tabular form (Table 2) and indexed to the particular theft scenario. The theft scenarios themselves are located in the detailed analyses later in the report.

The primary value of SVAP is that it is an ordered, systematic and repeatable analysis. This eliminates much of the user bias and makes different facilities safeguards systems uniquely comparable.

Though SVAP was designed for nuclear facilities, its techniques are readily adaptable to other things that are protected by a safeguards system (money, documents, etc.).

REFERENCES

1. Gilman, F. M., M. H. Dittmore, W. J. Orvis, P. S. Wahler, (1979) "Safeguard Vulnerability Analysis Program (SVAP) Executive Summary," Lawrence Livermore National Laboratory, NUREG/CR-1087, UCRL-52724.
2. Orvis, W. J., (1979), "Safeguards Vulnerability Analysis Program (SVAP) User's Manual," Lawrence Livermore National Laboratory, NUREG/CR-1169, Vol. III, UCRL-52730.
3. Wahler, P. S., (1980), "Safeguards Vulnerability Analysis Program (SVAP) Data-Gathering Handbook," Volumes I and II, Lawrence Livermore National Laboratory, NUREG/CR-1169, Vol. I and II, UCRL-52731.
4. Worrell, R. B., (1974), "Using the Set Equation Transformation System in Fault Tree Analysis," Sandia Laboratories, N.M., SAND-74-0240.

FIGURE LIST

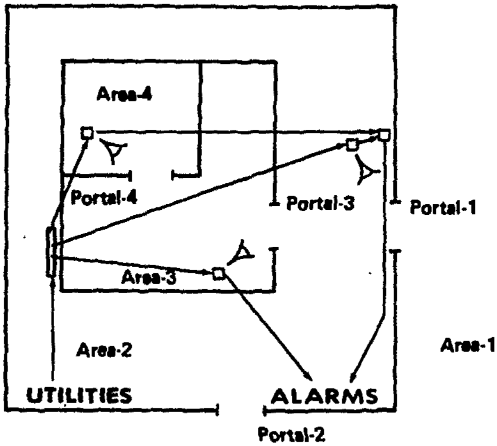

Figure 1 A simple safeguards system with areas, portals, monitors, transmission components and utilities.

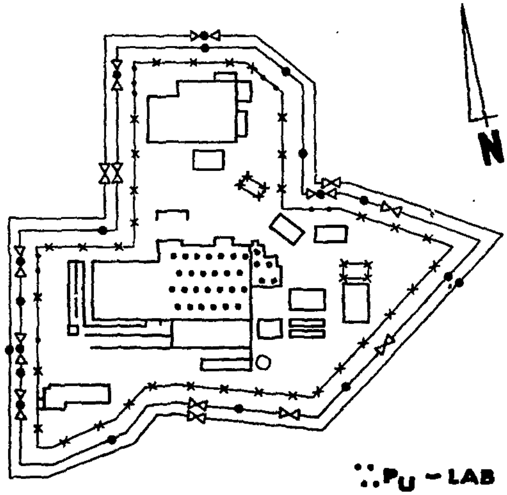

Figure 2 G. E. Vallecitos plutonium handling laboratory.

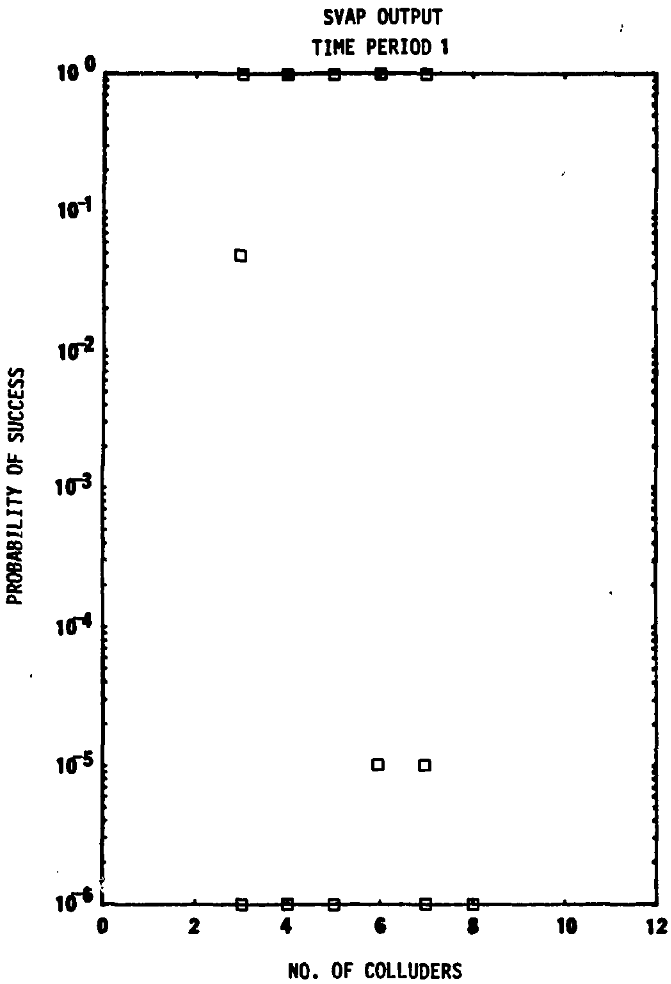

Figure 3 G. E. Vallecitos, level of protection at time period 1.

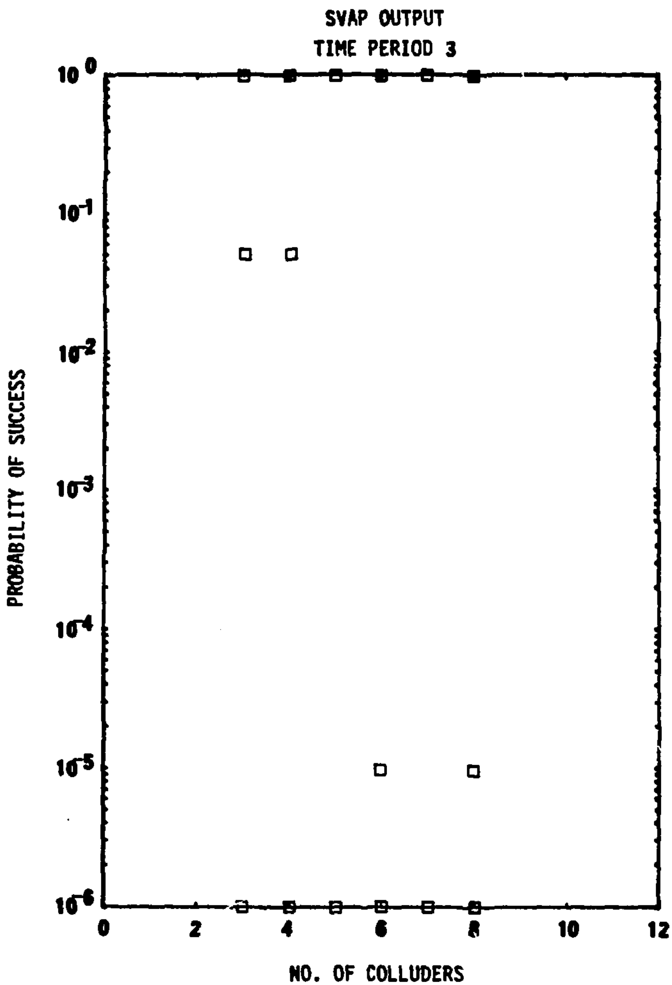

Figure 4   G. E. Vallecitos, level of protection at time period 3.

Table 1 Summary list from the SVAP analysis of G. E. Vallecitos for target 1.

Paths with 3 or less monitors	2
Uncovered response sets	0
Transmission sets with 2 or less transmission elements	27
Utility sets with 2 or less utility elements	1
Document sets	2
Physical security — material control collusion sets	145
Accounting system loss detectors time 1	0
Accounting system loss detectors time 2	0
Accounting system loss detectors time 3	1
Accounting system loss detectors time 4	1

Table 2 Tabular output of the graphical data presented in figure 3, indexed to the specific theft scenario.

TIME PERIOD 1

COLLUSION EVENT SETS RANKED BY PROBABILITY OF ADVERSARY SUCCESS

COLLUSION SET REFERENCE NUMBER	PROBABILITY OF ADVERSARY SUCCESS	NUMBER OF COLLUDERS	NUMBER OF RANDOM FAILURES
[illegible]	[illegible]	[illegible]	[illegible]
120	0.0000100	7	1
84	0.0000100	6	1
[illegible]	[illegible]	[illegible]	[illegible]