NUREG/CR-[redacted]
UCRL-52724

Safeguard Vulnerability Analysis Program (SVAP) Executive Summary

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

Lawrence Livermore Laboratory

Prepared for
U.S. Nuclear Regulatory
Commission

NOTICE

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

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-1169, ES
UCRL-52724
RS

NUREG/CR--1169-ES

TI86 000156

Safeguard Vulnerability Analysis Program (SVAP) Executive Summary

Manuscript Completed: December 1979
Date Published:

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

Lawrence Livermore Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
SAFER
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A-0115

EB/gsw

FOREWORD

This report gives an overview of the Safeguard Vulnerability Analysis Program (SVAP) developed at Lawrence Livermore Laboratory (LLL). SVAP was designed as a method of analyzing the safeguard systems at nuclear facilities for vulnerabilities--vulnerabilities which if uncorrected might allow opportunities for 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 makes no attempt to analyze for threats by violent insiders or by outsiders of any type, nor does it address issues of sabotage.

For a thorough understanding of SVAP the reader should consult two companion documents, the SVAP Data-Gathering Handbook[1] and the SVAP User's Manual.[2]

CONTENTS

LIST OF ILLUSTRATIONS

ABSTRACT

The steps involved in making a Safeguard Vulnerability Analysis Program (SVAP) application to a nuclear facility are summarized. NRC analysts are expected to execute SVAP on nuclear facilities to check facility safeguard systems for soundness and to reveal vulnerabilities, if any. The ultimate objective is to create safeguard systems that will effectively deter theft or diversion of special nuclear materials. The Input Phase of a SVAP application consists of data-gathering, data-recording in a handbook, and data-entering into a Tektronix computer. At that point, the facility data are transferred to a main frame computer for processing, and in the Output Phase the main frame computer delivers a complete descriptive analysis of the facility's safeguard system, disclosing its vulnerabilities.

INTRODUCTION

Of the several potential hazards inherent in the nuclear power industry, perhaps none poses a greater challenge to control and solution than the hazard of nuclear materials theft. Reactors and other nuclear installations can readily enough be designed to allow for predictable characteristics of nuclear fuels, and the attendant structures and systems that convert energy from fission reactions into usable electricity are similarly amenable to reliable control through engineering design. But safeguard problems in the nuclear industry--the protection of nuclear materials from theft and sabotage--present challenges of an entirely different order because one must not only consider the design of structures but also try to predict the behavior of human beings.

To be sure, under federal regulations nuclear fuel-processing facilities can be and have been designed in such a way as to constrain the movement of special nuclear materials (SNM) and thereby to limit the probability of malevolent acts. However, any facility, no matter how carefully designed for physical security and material control, and no matter how rigorous its material accounting system, may yet contain serious vulnerabilities not immediately apparent to the examiner's eye. The challenge for the safeguard analyst has always been, how--in the complex array of portals, areas, equipment, accounting records, and monitoring devices--to detect those vulnerabilities. Because of the complexities in any facility its safeguard defects cannot be catalogued simply, even after careful examination by a trained analyst. The data are too many and too intricately interrelated.

In response to this situation, a variety of approaches have been put forward to unravel the complexities. Until recently, the most promising technique was a digraph/fault tree methodology that when applied thoroughly to a facility would disclose all the possible modes or pathways of successful diversion of SNM. The principal flaw in the fault tree approach was that, although it effectively disclosed vulnerabilities, it mimicked the complexity of the system it analyzed and, therefore, the analyst using it had to be highly trained in fault tree theory.

Faced with these circumstances, LLL scientists searched for a means of transferring from a human analyst to a computer the inefficient labor of gathering and analyzing burdensome arrays of data. The result of that search is a computerized input package which is interfaced with a powerful analysis code[3] to form the Safeguard Vulnerability Analysis Program (SVAP).

The basis of SVAP is its ability to reveal all of the acts or sets of acts by authorized nonviolent insiders that could possibly defeat a safeguard system. Such vulnerabilities are disclosed by an analyst gathering data from a nuclear facility, arranging the data in the SVAP Data-Gathering Handbook, and entering the data into a Tektronix 4051* graphics terminal, either in Washington, D.C., or on-site at the facility being evaluated. The data entered into the Tektronix terminal by the analyst are transmitted to a main frame computer for processing, and the output is then returned to the Tektronix computer.

Besides the obvious advantages of speed and efficiency, SVAP offers a means of uniform assessment from facility to facility and from analyst to analyst. The data requirements are laid out systematically in a handbook and, by using that handbook, the analyst can easily gather the data from any facility and enter them into the Tektronix terminal. He or she needs no special training in diagraph/fault tree methodology or in computers. Finally, the SVAP codes can easily be updated to accommodate new information the NRC might want to gather and process.

*Tektronix 4051, 4052, and 4054 are interchangeable.

INPUT PHASE

Gathering data for SVAP is the responsibility of the NRC analyst. As we have said, this analyst would need no special training in computers or software. The analyst should have experience, however, in safeguards, so that upon visiting a facility and examining its documents the pertinent data can be identified and collected.

In SVAP the data-gathering process is made simple and easy through a handbook[2] that asks the analyst for detailed information in an organized, step-by-step fashion. The handbook guides the analyst in labeling every area, portal, monitoring device, guard station, and so on, and the labeling information plus all other pertinent information is recorded in the handbook. (See Fig. 1 for an example handbook page.) The data consists of the following types:

1. A plant layout diagram showing all areas, portals, fences, and indicating those portals that are locked and/or allow access from only one direction.
2. A description of each monitor, its type, location, operational procedures, tamper-indicating functions, etc.
3. A description of the areas and portals to which the guards respond when a particular monitor alarm is set off.
4. A schematic diagram of the monitor transmission network showing how each monitor is connected to the central alarm station.
5. A schematic diagram and description of the monitor utility network showing how the utility system supplies power to each monitor.
6. A description of the material control documents and how they are used to move material into, around, and out of a facility.
7. A list of the areas containing SNM and the quantities in the areas.
8. A description of the accounting system loss detection mechanisms, including the areas in which the mechanisms function and the time at which they function.

MONITOR DATA-COLLECTION FORM (1 of 2)

MONITOR ID CODE MON-A04

DESCRIPTION ULTRA SONIC MOTION DETECTOR

1) LIST BELOW THE ID CODES FOR THE PERSONNEL WHO HAVE AUTHORIZED ACCESS TO THIS MONITOR; THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 7 (MONITOR-LOCK/AUTHORIZATION MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

GUARD-01 AND MAINT-01

2) LIST BELOW THE PROBABILITY OF FAILURE FOR THIS MONITOR THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 8 (MONITOR-LOCK/ FAILURE MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

0.1

3) LIST BELOW THE ID CODES FOR ALL THE TRANSMISSION LINE COMPONENTS THAT CONNECT THIS MONITOR TO THE GUARD CENTER; THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 10 (MONITOR-LOCK/TRANSMISSION LINE MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

CA-03 AND JB-02 AND CA-02 AND JB-01 AND CA-01

4) LIST BELOW THE ID CODES FOR ALL THE UTILITY COMPONENTS THAT FEED THIS MONITOR; THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 12 (MONITOR-LOCK/UTILITY MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

CA-23 AND JB-22 AND (CA-22 AND JB-21 AND CA-21 AND PUBPWR OR CA-32 AND BATTERY2)

FIG. 1. Example page from the SVAP data handbook.

5) LIST BELOW THE ID CODES FOR ALL THE AREAS AND DOORS TO WHICH SECURITY RESPONDS WHEN AN ALARM IS RECEIVED FROM THIS MONITOR; THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 16 (MONITOR-LOCK/RESPONSE MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

AREA-03

6) LIST BELOW THE ID CODES FOR ALL THE PERSONNEL WHO RESPOND TO AN ALARM FROM THIS MONITOR; THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 17 (RESPONSE/AUTHORIZATION MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

GUARD-01

7) LIST BELOW THE ID CODES FOR ALL DOCUMENTS REQUIRED TO PASS THIS MONITOR WITHOUT SETTING AN ALARM; THEN, ENTER THE LIST WITH THIS MONITOR ID CODE IN FILE 19 (MONITOR-LOCK/DOCUMENT MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

F-706

FIG. 1. (Continued.)

9. A description of the records and forms which provide input into the loss detection mechanisms.

10. A list of plant personnel, including their job descriptions and access authorizations.

The data handbook provides a convenient bridge between the aforementioned plant descriptions, plant blueprints, operating procedures, and the SVAP input into the 4051. It is designed to remind the analyst what questions should be asked for each area, portal, and monitor. It then directs the analyst how and where to put the answers such that the input into the 4051 is simplified. For example, the handbook requires the analyst to assign each area and door an alphanumeric ID code that will be used throughout the analysis. The analyst also identifies which doors are uni-directional and which are locked. For each area and portal, the analyst identifies which facility personnel have authorized access, and each area containing SNM is identified along with the quantity present.

Once the plant layout has been completed, the data handbook guides the analyst's examination of the monitor system. The examination raises questions about the transmission lines and utility lines servicing each monitor. Also, the guard responses to each monitor alarm and the tamper monitors watching each monitor are requested by the handbook. At this point the analyst is asked to supply monitor failure rate data. The last question in the monitor section asks the analyst to list the documents and/or combination of documents that will allow material to pass by each monitor. (See Fig. 1.)

The last section of data deals with the accounting system. The analyst is asked to identify the accounting system loss detection mechanisms functioning in each area containing SNM. (See Fig. 2.) He then is asked to describe the forms and records that provide input to the loss detection mechanisms. Finally, the analyst identifies the time at which the loss detection mechanism functions; e.g., one week, six months, one year.

Our hope is that the data-gathering handbook will be sufficiently self-descriptive so that it can be sent to a facility ahead of the analyst and

LOSS DETECTION METHODS
DATA-COLLECTION FORM

LOSS DETECTION METHOD ID CODE MIS-ITM

DESCRIPTION MISSING ITEM

1) LIST BELOW THE ID CODES FOR ALL THE RECORDS REQUIRED TO DETECT A LOSS WITH THIS DETECTION METHOD; THEN, ENTER THE LIST WITH THIS LOSS DETECTION METHOD ID CODE IN FILE 26 (LOSS DETECTION METHODS/ RECORDS MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

ITEMREC

2) LIST BELOW THE IC CODES FOR ALL PERSONNEL AUTHORIZED TO MAKE ENTRIES OR CHANGES TO THIS LOSS DETECTION METHOD; THEN, ENTER THE LIST WITH THIS LOSS DETECTION METHOD ID CODE IN FILE 30 (LOSS DETECTION METHODS/AUTHORIZATION MATRIX) LOCATED IN THE DATA RECORDING SECTION OF THIS HANDBOOK.

PLA-MGR OR ENG-21 AND ENG-22 AND ACCT-01 AND ACCT-02

FIG. 2. A loss detection methods data-collection page from the SVAP data handbook.

the facility personnel can fill in all the data. The analyst would then simply verify the inputs during his tour of the facility.

After the data handbook has been completely filled out, the analyst is ready to enter the data into the Tektronix 4051.[2] As mentioned previously, the data handbook is designed to simplify the 4051 data input procedure. Because of this simplicity, we expect that all data from a typical facility can be entered into the 4051 in approximately 1 day. After the data have been entered, the analyst will transmit them to a main frame computer like a CDC7600, which was used by LLL scientists in developing SVAP. The SVAP codes in the main frame computer are then executed with a single command and the

results are written onto tape. A single run of SVAP will assess up to 10 targets in a facility. After the data have been processed by the main frame computer, the results that have been loaded onto the output tape are fed to the Tektronix 4051 for display. A hard-copy printed output can also be made at this time.

Figure 3 shows a block diagram for a possible interconnect between an analyst operating in the field--either at a facility site or at NRC Regional Headquarters--and NRC Headquarters in Washington. Another, slower way to handle data flow would be for the tape generated in the field by the analyst's 4051 to be shipped or carried to Washington. A third arrangement, as suggested earlier, would be for the analyst not to use a field Tektronix 4051 at all, but to return to Washington with the data handbook filled out and enter the data there.

OUTPUT PHASE

The outputs from a SVAP run may be produced in two forms. The first is a hard copy output; the second form is a magnetic tape. The content of both output forms is the same.

In the scenario of Fig. 3 the magnetic tape output produced in Washington will be transferred to the field analyst's 4051 by telephone line. When the output arrives at the analyst's 4051, it will immediately be stored on disc and also printed on the 4051's printer. This hard copy output will consist of a title page, table of contents, introduction, several output sections, and the raw input data. The hard copy output will in fact be a complete printed report describing the assessment of one target at the facility. If several targets were assessed, there will be one report for each target.

We shall now describe the sections that make up the body of the output report, following the order shown on the SVAP output table of contents in Fig. 4.

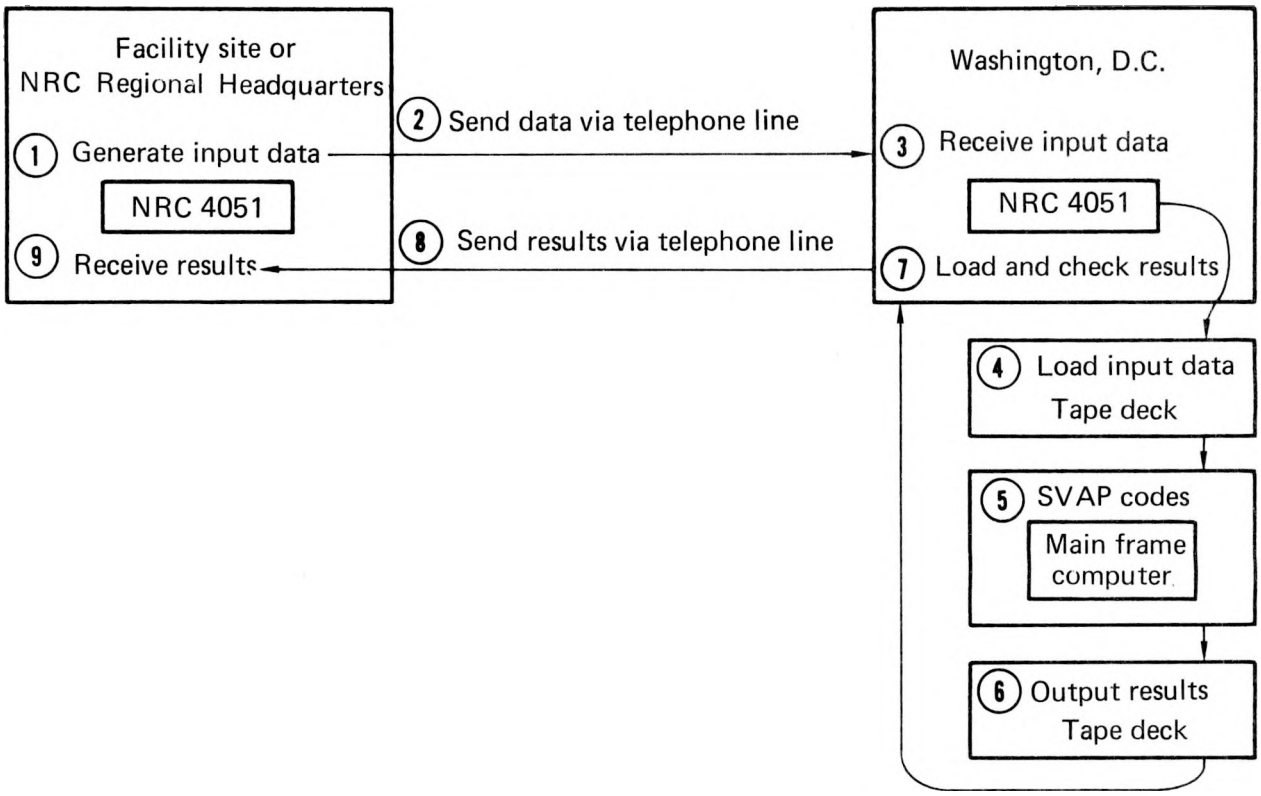

FIG. 3. Block diagram showing one possible scenario for handling data flow in a SVAP application to a nuclear facility. Facility data, which have been gathered by an analyst and recorded in the SVAP Data-Gathering Handbook, are entered into the NRC's field Tektronix 4051, either at the facility's site or at NRC Regional Headquarters (1). When loaded, these data are sent by telephone line (2) to NRC Headquarters in Washington, where another Tektronix 4051 receives the input data (3), which is then loaded onto tape (4) and fed to the NRC's main frame computer (such as CDC 7600) (5). After the SVAP codes have processed the input data, the output results are fed to a tape deck (6), which in turn feeds the results to the NRC Headquarters' 4051. The results then can be sent by telephone line to the Regional Headquarters or the facility site (9). One advantage to this arrangement is that NRC Headquarters and the field analyst can communicate through the 4051s, for the screens on each end show the same displays. This enables the two ends to assess or correct input and output data. Hard copies of the output may be printed at either end on a Tektronix printer.

TABLE OF CONTENTS

FIG. 4. Table of contents page from a sample SVAP output. The printed SVAP output is in fact a complete report of one target in a facility; a separate output report is made for each target.

Section I (not illustrated here) contains a short description of SVAP. Included in this description are the assumptions used in the version of SVAP that was run. The content of this section remains the same with each run of SVAP.

Section II is an assessment description (see Fig. 5). This description contains pertinent information about the assessment being performed. The main

```
SVAP REPORT EXAMPLE
ANALYST F. M. GILMAN
DATE:  DEC 12, 1979

ALL DATA TYPES HAVE BEEN CONSIDERED.
THE EXAMPLE FACILITY IS A WEAK FACILITY SO THAT ALL
THE OUTPUTS OF SVAP CAN BE DEMONSTRATED.

CA = CABLE RUN.  RUNS 1 TO 11 ARE SIGNAL CABLES.  RUNS 21 TO 32
     ARE POWER CABLES.
JB = JUNCTION BOX.  BOXES 1 TO 3 CARRY SIGNALS.  BOXES 21 TO 23
     CARRY POWER.
PUB-PWR = PUBLIC UTILITY POWER.
FIA = FENCE INTRUSION AREA.
PWR-EMP = AN EMPLOYEE OF THE PUBLIC UTILITY.


THE FOLLOWING TARGETS WILL BE ANALYZED IN THIS RUN OF SVAP

          TARGET        EXIT
          ------        ----

          AREA-04       AREA-01
```

FIG. 5. Section II of the Output Report: the assessment description consists of analyst comments pertinent to the assessment. It usually includes the analyst's name, date, facility being analyzed, assumptions, time periods used in the accounting system. The targets that were run are printed here automatically by the program. This section can contain any text the analyst wants to save with the output results.

body of this section is from input file 1,* which the analyst generated with the input data. This section also identifies the targets under analysis in the SVAP run.

Section III (not illustrated) informs the analyst that the input data for SVAP is found in the data handbook and at the end of the report.

Section IV is a summary of the results from the SVAP analysis of the material control, material accounting, and physical security systems (see Fig. 6). This summary is intended to allow the analyst to determine quickly if there are any overall system weaknesses. The summary consists of five pages of printouts: one list and four plots. The list (Fig. 6) indicates whether or not a certain vulnerability exists without describing the details of the vulnerability. To determine the details, the analyst would look at the specific section of interest. For example, if the analyst wants to see the three document sets, he would look in Section V, Subsection 5 (see Fig. 12). The four plots of

---

*See the Data-Gathering Handbook (Ref. 1). The SVAP inputs are divided into a series of files, each containing different classes of data. File 1 is a free format text file.

SUMMARY RESULTS

TARGET	EXIT
AREA-04	AREA-01

PATHS WITH 3 OR FEWER MONITORS	0
UNCOVERED RESPONSE SETS	2
TRANSMISSION SETS WITH 2 OR FEWER TRANSMISSION ELEMENTS	10
UTILITY SETS WITH 2 OR FEWER UTILITY ELEMENTS	4
DOCUMENT SETS	3
PHYSICAL SECURITY - MATERIAL CONTROL COLLUSION SETS	8
ACCOUNTING SYSTEM LOSS DETECTORS TIME 1	0
ACCOUNTING SYSTEM LOSS DETECTORS TIME 2	1
ACCOUNTING SYSTEM LOSS DETECTORS TIME 3	1
ACCOUNTING SYSTEM LOSS DETECTORS TIME 4	1

FIG. 6. Section IV of a SVAP Output Report, a summary section that allows the analyst quickly to determine gross weaknesses in the safeguard system. Section IV consists of a list or table as shown here, which gives the number of event sets for successful diversion of SNM with respect to the material control, physical security, and material accounting systems, and also of four plots (see Fig. 7), which show the probability of success vs the number of colluders in each of the four accounting time periods. Thus, from the example given here, we see that the facility under review has no monitor paths with 3 or fewer monitors--all have more--and therefore an adversary would have to defeat at least four monitors along any diversion route in the facility to divert SNM. On the other hand we see the facility has 10 transmission event sets, each with fewer than 2 transmission elements that must be defeated for successful diversion--and these are weaknesses that perhaps should be corrected.

Section IV, of which only one is illustrated here (in Fig. 7), show the probability of adversary success vs number of colluders for the four given time periods. The four time periods represent the fact that the accounting system performs different functions at different times and so the colluders necessary to defeat the safeguard system (physical security, material control, material accounting) can change depending on how long the diversion is supposed to go undetected. Each data point on the plots indicates that at least one combination of colluders have a given probability of success. To

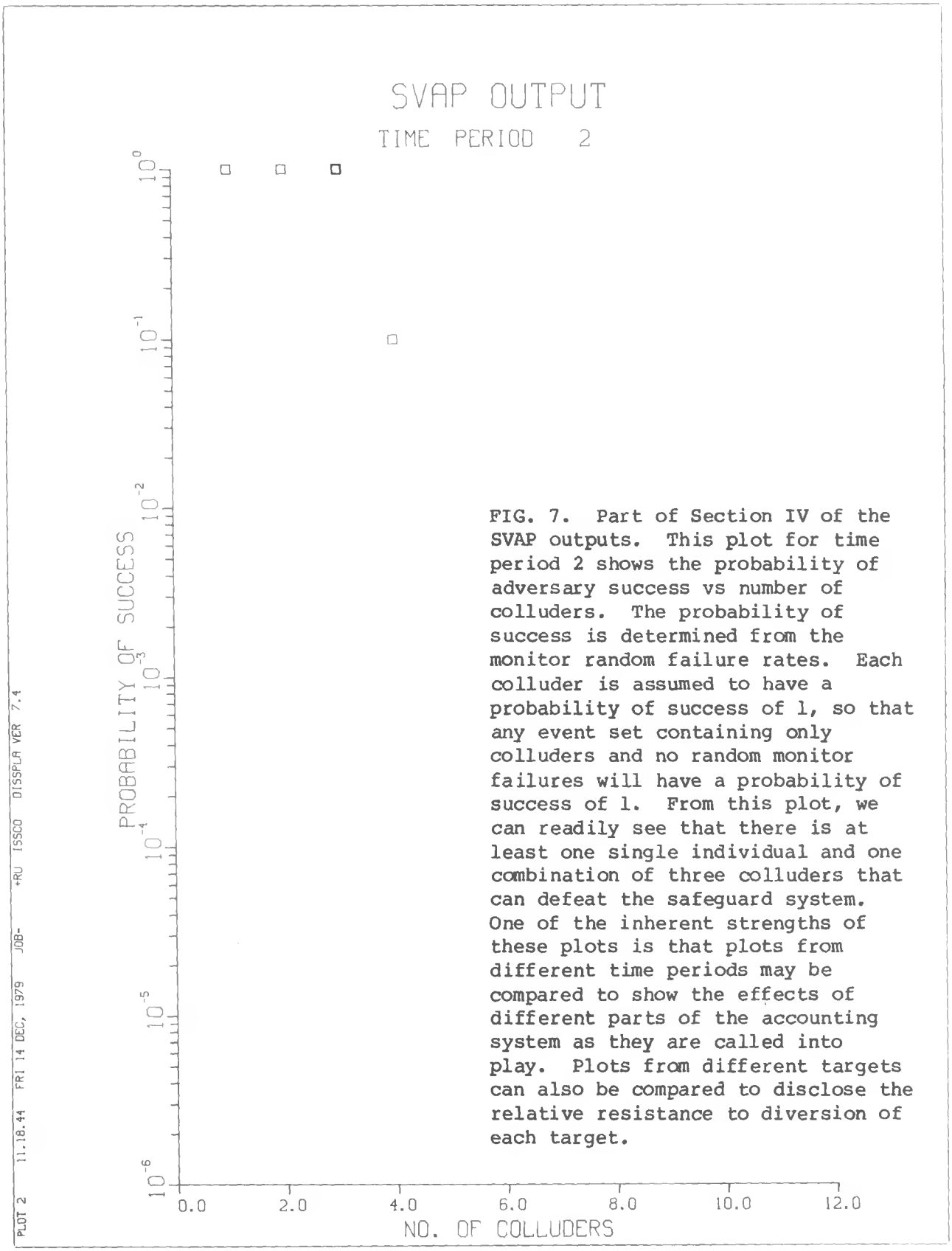

FIG. 7. Part of Section IV of the SVAP outputs. This plot for time period 2 shows the probability of adversary success vs number of colluders. The probability of success is determined from the monitor random failure rates. Each colluder is assumed to have a probability of success of 1, so that any event set containing only colluders and no random monitor failures will have a probability of success of 1. From this plot, we can readily see that there is at least one single individual and one combination of three colluders that can defeat the safeguard system. One of the inherent strengths of these plots is that plots from different time periods may be compared to show the effects of different parts of the accounting system as they are called into play. Plots from different targets can also be compared to disclose the relative resistance to diversion of each target.

see how many actual combinations there are, and who is in each combination, the analyst would look at the appropriate safeguard system colluder output section for the time period of interest, Section VII, which contains the data that are used to generate the plots.

Section V contains the detailed physical security/material control analysis results. The section is divided into six subsections, each of which will now be described.

Subsection 1 (Fig. 8) is a monitor analysis; it consists of two parts: a list of all monitor sets in the facility and a list of adversary exit paths with three or fewer monitors--in other words, the exit paths that are the most vulnerable to diversion. We define a monitor set as the minimum set of monitors an adversary must pass in a diversion route to exit the facility. We

MONITOR SETS

1	4	MON-A04 * MON-FIA * MON-P02 * LOC-P02B +
2	5	MON-A04 * MON-P01 * LOC-P01 * MON-P02 * LOC-P02B

PATHS WITH 3 OR FEWER MONITORS

THERE ARE NO MONITOR PATHS WITH 3 OR FEWER MONITORS

The numbers in the leftmost column are monitor set reference numbers; the numbers to the right (4, 5) are the number of monitors in the set.

Legend

MON-A04	-	Monitor Area-04
MON-FIA	-	Monitor Fence Intrusion Area
MON-P02	-	Monitor Portal-02
LOC-P02B	-	Lock Portal-02B
MON-P01	-	Monitor Portal-01
LOC-P01	-	Lock Portal-01

FIG. 8. Physical security/material control output (Section V, Subsection 1): monitor analysis. In this hypothetical example, there are two monitor sets in the facility, one with 4 monitors, the other with 5. This means that an adversary must defeat a minimum of 4 monitors or locks to move from the target to an exit point. This example was run for a small, oversimplified plant and so there were not many monitor sets; however, for a large plant there might be 50 to 100 monitor sets. For this reason a second list of monitor paths with 3 or fewer monitors is made. Monitor paths differ from monitor sets in that they include both the path, in terms of areas and doors, and the monitors. In this example since the smallest monitor set is 4 there are no monitor paths with 3 or fewer monitors.

take all components of a route--rooms, hallways, doors, etc.--not only monitors, into account in defining an exit path. If there are no monitor sets then there is at least one path by which the adversary can exit the facility without passing any monitors. The reason our output sorts out and lists exit paths with 3 or fewer monitors is of course to highlight the most vulnerable exit pathways.

Subsection 2 lists all the uncovered response paths. Response paths are sets of areas and portals the adversary uses to exit a facility and those areas and portals to which the guards respond when they get an alarm from a monitor on the path in question. (See Fig. 9.) An uncovered response path is a case where the adversary sets off alarms as he exits the facility but when the guards receive the alarm signals they go to areas and portals which the adversary is not using in his exit.

Subsection 3, concerning transmission lines and transmission line components, is a listing correlating monitors and the transmission network emanating from the monitors. (The transmission network is that aspect of the monitor system which transmits signals from the monitored areas to the alarm or receiving locations, as for example the line connecting an area detector and a guard's alarm panel. Transmission lines are to be distinguished from utility lines--see Subsection 4 below.) The monitors are arranged into sets which can be silenced if one or two transmission line components are tampered with. (See Fig. 10.) Arraying the monitor system into such sets helps to determine the degree of monitor vulnerability on any given pathway; for example, these correlated sets of monitors and transmission lines will disclose to an analyst whether the ten monitors covering a certain path can all be failed by tampering with one junction box.

Subsection 4, concerning utility lines, is similar to Subsection 3 but here we determine if an adversary can silence all the monitors along a path by gaining access to 2 or fewer utility components. (See Fig. 11.) Utility components are off-site AC power, internal DC power, backup batteries, and emergency diesel generators. Like Subsection 3 this output identifies weaknesses in the monitor system, but in this case the weaknesses are in power supply systems to monitors rather than in the signal transmission network, though the looked-for effect is the same--the failing of a monitor.

```
2)     RESPONSE ANALYSIS

THE RESPONSE ANALYSIS DETERMINES WHETHER THE PHYSICAL
SECURITY RESPONSE RULES ADEQUATELY COVER ALL THE ADVERSARY
EXIT PATHS.  THE OUTPUT LISTING CONTAINS UNCOVERED MONITOR
RESPONSE SETS.  AN UNCOVERED MONITOR RESPONSE SET IS MADE
UP OF THE PATH THE ADVERSARY USES TO EXIT THE FACILITY ALONG
WITH THE AREAS (PRECEDED BY A SLASH) THAT THE GUARDS
RESPOND TO ASSUMING THAT ALL THE MONITORS ALONG
THE EXIT PATH ALARM.  (THE PATH IS NOT ORDERED IN
THE OUTPUT LISTING.)
-------------------------------------------------------------------------

1       8   AREA-01 * AREA-02 * AREA-03 * AREA-04 * FIA * PORT-02B * FENCE * \PORT-01 +
2       8   AREA-01 * AREA-02 * AREA-03 * AREA-04 * FIA * PORT-02B * PORT-04 * \PORT-01
```


Legend

Area-XX	-	Area location XX
Port-XX	-	Portal location XX
\Port-01	-	Guard response location 01

FIG. 9. Physical security/material control output (Section V, Subsection 2): uncovered response analysis. In this example there are 2 uncovered response sets. The first response set indicates that the adversary exits along a path of: Area-01, Area-02, Area-03, Area-04, FIA, Port-02B, FENCE, while the guards are responding to: \Port-01. By giving both the adversary exit path and the guards' response location the response rule changes can easily be determined.

```
 1        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \CA-01 * \CA-09 +
 2        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \CA-01 * \JB-03 +
 3        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \CA-01 * \CA-10 +
 4        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \JB-01 * \CA-09 +
 5        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \JB-01 * \JB-03 +
 6        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \JB-01 * \CA-10 +
 7        7   MON-A04 * MON-P01 * MON-P02 * LOC-P01 * LOC-P02B * \CA-01 * \CA-08 +
 8        7   MON-A04 * MON-P01 * MON-P02 * LOC-P01 * LOC-P02B * \JB-01 * \CA-08 +
 9        7   MON-A04 * MON-P01 * MON-P02 * LOC-P01 * LOC-P02B * \CA-02 * \CA-08 +
10        7   MON-A04 * MON-P01 * MON-P02 * LOC-P01 * LOC-P02B * \JB-02 * \CA-08
```

Legend

MON-AXX	-	Monitor in area XX
MON-PXX	-	Monitor in portal XX
LOC-PXX	-	Lock on portal XX
\CA-XX	-	Cable run number XX
\JB-XX	-	Junction box number XX

FIG. 10. Physical security/material control output (Secton V, Subsection 1): transmission system analysis. The transmission system analysis is done to determine to what extent a plant's transmission network is vulnerable to tampering. The output contains those monitor sets which can be completely nullified by tampering with 2 or fewer transmission elements (the transmission elements are preceded by slashes). Transmission elements are usually junction boxes or cable runs. This example gives the monitor sets for which 2 or fewer transmission element failures will leave an adversary exit path unmonitored. The first transmission set can be interpreted in the following way. If \CA-01 and \CA-09 fail or are tampered with, then MON-A04, MON-FIA, MON-P02, and LOC-P02B will not function, and so the adversary path they were protecting will be open.

```
 1        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \JB-22 * \JB-23 +
 2        6   MON-A04 * MON-FIA * MON-P02 * LOC-P02B * \JB-22 * \CA-29 +
 3        7   MON-A04 * MON-P01 * MON-P02 * LOC-P01 * LOC-P02B * \JB-22 * \JB-23 +
 4        7   MON-A04 * MON-P01 * MON-P02 * LOC-P01 * LOC-P02B * \JB-22 * \CA-30
```

Legend

MON-AXX	-	Monitor in area XX
MON-PXX	-	Monitor on portal XX
LOC-PXX	-	Lock on portal XX
\CA-XX	-	Cable run number XX
\JB-XX	-	Junction box number XX

FIG. 11. Physical security/material control output (Section V, Subsection 4): utility system analysis. The utility system analysis is done to determine to what extent a plant's utility system is vulnerable to tampering. The output contains those monitor sets which can be completely nullified by tampering with 2 or fewer utility components (the utility components are preceded by slashes). Utility components are such things as air ducts, batteries, off-site power lines. This example gives the monitor sets for which 2 or fewer utility element failures will leave an adversary exit path unmonitored. The first utility set can be interpreted in the following way. If \JB-22 and \JB-23 fail or are tampered with, then MON-A04, MON-FIA, MON-P02, and LOC-P02B will not function, and so the adversary path they were protecting will be open.

Subsection 5 lists all of the document paths in the facility. A document path consists of the areas and portals the adversary uses to exit a plant and the authorizing documents necessary to move the material, past all the monitors, along that path. (See Fig. 12.) In any facility, we would expect to find at least one document path which represents how material normally and legally moves about the facility.

Subsection 6 contains the collusion event sets that can defeat the physical security and material control systems. A very detailed and complex analysis is performed to generate the collusion event sets. This analysis considers all combinations of adversary acts such as monitor tampering, transmission line tampering, utility system tampering, document falsification, and guard failures that lead to diversion. The analysis then combines the aforementioned adversary acts with the personnel that can perform each act (see Fig. 13). Finally the analysis folds in the effect of random monitor failures on the adversary acts required for diversion. When the analysis is complete the collusion sets are given in terms of the personnel required for successful diversion and any random monitor failures that are also required.

Section VI gives the results of the accounting system analysis for the time periods 1, 2, 3, and 4, respectively, in four subsections. Each subsection lists the accounting system loss detection mechanisms that are in effect for the given target at the given time period, and it also gives the records and forms that need to be tampered with to defeat the accounting system. In

```
1    6   F-706 * AREA-01 * AREA-02 * AREA-04 * PORT-01 * PORT-02B *
2    8   F-706 * AREA-01 * AREA-02 * AREA-03 * AREA-04 * FIA * PORT-02B * FENCE +
3    8   F-706 * AREA-01 * AREA-02 * AREA-03 * AREA-04 * FIA * PORT-02B * PORT-04
```

Legend

Area-XX	-	Area designated by XX
Port-XX	-	Portal designated by XX
FIA	-	Electronic fence intrusion area
Fence	-	Fence area
F-706	-	Form number 706

FIG. 12. Physical security/material control output (Section V, Subsection 5): document path analysis. A document path is an adversary exit path that can become open by the use of certain documents. Three such paths are shown here. The first indicates that material can move along the path Area-01, Area-02, Area-04, Port-01, Port-02B without tripping any alarms if Form-706 is present with the material.

```
1        1    PLA-MGR +
2        1    ENG-22 +
3        1    ENG-21 +
4        1    ENG-11 +
5        2    GUARD-01 * ACCT-01 +
6        2    GUARD-01 * MAINT-01 +
7        3    MAINT-01 * ACCT-01 * RFLOC-P02B +
8        6    ACCT-01 * RFMON-A04 * RFMON-P01 * RFMON-P02 * RFLOC-P01 * RFLOC-P02B
```

Legend

PLA-MGR - Plant manager
ENG-22 - Engineer type 22
ENG-21 - Engineer type 21
ENG-11 - Engineer type 11
GUARD-01 - Guard type 01
MAINT-01 - Maintenance man type 01
ACCT-01 - Accountant type 01
RFLOC-PXX - Random failure of the lock on portal XX
RFMON-AXX - Random failure of monitor in area XX

FIG. 13. Physical security/material control output: collusion analysis. This output lists 8 different combinations of plant personnel which can collude and successfully divert material from the target without generating any alarms in the physical security or material control system. For those combinations of personnel where a monitor random failure is also needed for successful diversion, the monitor is listed. The example above shows that 4 single insiders can divert material. Collusion set 8 gives an example of a collusion set which requires 5 monitor random failures for successful diversion.

addition, each subsection gives all of the colluder combinations (or accounting colluder event sets) that will defeat the accounting system for its time period, along with the forms and records that must be tampered with to carry out the collusion. Figure 14 shows an example of Subsection 2 under Section VI, the accounting system at time period 2.

Section VII (see Fig. 15) lists the collusion sets which were used to generate the plots described in Section IV (an example plot is shown in Fig. 7). The collusion sets for the entire plant are also ranked and printed as a part of Section VII with the probability of success, number of colluders, and number of random failures, as in Fig. 16.

Appendix I of the output run (not illustrated here) contains the raw input data and the probability data that the analyst had entered. This file was created so that the analyst could easily check what inputs he had used for each assessment run.

```
                                ACCOUNTING SYSTEM ANALYSIS FOR TIME PERIOD 2

          ACCOUNTING SYSTEM LOSS DETECTORS

1         2    INV-DIF * MIS-ITM


          RECORDS WHICH IF TAMPERED WITH WILL DEFEAT THE ACCOUNTING SYSTEM

1         3    ITEMREC * ASSAYREC * SEALREC


          FORMS WHICH IF TAMPERED WITH WILL DEFEAT THE ACCOUNTING SYSTEM

1         2    INVNTORY * ASAYFORM +
2         3    MOVEFORM * ASAYFORM * SEALFORM


          COLLUDERS AND THEIR ACTS WHICH WILL DEFEAT THE ACCOUNTING SYSTEM

1         3    PLA-MGR * ASAYFORM * INVNTORY +
2         4    PLA-MGR * ITEMREC * ASSAYREC * SEALREC +
3         4    PLA-MGR * MOVEFORM * ASAYFORM * SEALFORM +
4         5    ACCT-02 * GUARD-01 * ITEMREC * ASSAYREC * SEALREC +
5         5    ACCT-01 * GUARD-01 * ITEMREC * ASSAYREC * SEALREC +
6         6    ENG-21 * ENG-22 * GUARD-01 * MOVEFORM * ASAYFORM * SEALFORM +
7         7    ACCT-01 * ACCT-02 * ENG-21 * ENG-22 * ASAYFORM * INVNTORY * PROB1
```

Legend

INV-DIF	-	Inventory difference
MIS-ITM	-	Missing item
ITEMREC	-	Item record
ASSAYREC	-	Assay record
SEALREC	-	Seal Record
INVNTORY	-	Inventory procedure
ASAYFORM	-	Assay form
MOVEFORM	-	Movement authorization form
SEALFORM	-	Seal form
PLA-MGR	-	Plant manager
ACCT-02	-	Accountant type 02
GUARD-01	-	Guard type 01
ACCT-01	-	Accountant type 01
ENG-21	-	Engineer type 21
ENG-22	-	Engineer type 22
PROB1	-	Probability that engineer type 22 is chosen to perform inventory by a random selection process

FIG. 14. Accounting system output for time period 2 (Section VI, Subsection 2). The output contains 4 results: (1) Accounting system loss detectors active at the target during time period 2. (2) Records that will defeat the aforementioned loss detectors. (3) Forms which will defeat the loss detectors through their input to the records. (4) The colluders and the forms and records they tamper with to defeat the accounting system. In this example, the first set in the colluder analysis (the fourth and last part of the output) indicates that the "PLA-MGR) can defeat the accounting system through his access to the "ASAYFORM" and "INVNTORY."

COLLUDERS AND RANDOM FAILURES WHICH WILL DEFEAT THE SAFEGUARD SYSTEM UP TO TIME2

1	1	PLA-MGR +
2	2	ACCT-01 * GUARD-01 +
3	3	ACCT-02 * GUARD-01 * ENG-11 +
4	3	ACCT-02 * GUARD-01 * MAINT-01 +
5	3	ACCT-02 * ENG-22 * GUARD-01 +
6	3	ACCT-02 * ENG-21 * GUARD-01 +
7	3	ENG-21 * ENG-22 * GUARD-01 +
8	5	ACCT-01 * ACCT-02 * ENG-21 * ENG-22 * PROB1

Legend

PLA-MGR - Plant manager
ACCT-XX - Account type XX
ENGR-XX - Engineer type XX
MAINT-XX - Maintenance man type XX
GUARD-XX - Guard type XX
PROB1 - Probability that engineer type 22 is chosen to perform inventory by a random selection process.

FIG. 15. Safeguard system collusion analysis (Section VII). The safeguard system collusion analysis combines the physical security, material control, and material accounting systems to generate a model of the complete safeguards system and then solves that model for the colluders and random monitor failures that can divert material from the target and not be detected up to a certain time. In this example there are 8 combinations of plant personnel that can divert material and not be detected up to time period 2. Included in the 8 combinations is one single insider, "PLA-MGR," who can defeat the safeguard system.

TIME PERIOD 2

16. COLLUSION EVENT SETS RANKED BY PROBABILITY OF ADVERSARY SUCCESS

COLLUSION SET REFERENCE NUMBER	PROBABILITY OF ADVERSARY SUCCESS	NUMBER OF COLLUDERS	NUMBER OF RANDOM FAILURES
1	1.0000000	1	0
2	1.0000000	2	0
3	1.0000000	3	0
4	1.0000000	3	0
5	1.0000000	3	0
6	1.0000000	3	0
7	1.0000000	3	0
8	0.1000000	4	1

FIG. 16. Collusion analysis numerical results (Section VII). This table of data provides the link between the plots in the summary section (Section IV, Fig. 7) and the collusion sets shown in Fig. 15. The following data are listed: (1) Collusion set reference numbers, which allow the analyst to link the quantitative results with the collusion sets shown in Fig. 15. (2) The probability of adversary success for the given collusion set. (3) The number of colluders involved in the collusion set. (4) The number of random failures involved in the collusion set.

The Safeguard Vulnerability Analysis Program (SVAP) is a user-oriented, automated assessment procedure, characterized by an interactive input format on a small computer (as, for example, a Tektronix 4051) which allows entering data at any location. The data entered into the small computer are transferred to a main frame computer (such as a CDC 7600) for processing. The data may be transmitted over telephone lines connecting a nuclear facility and NRC Headquarters in Washington or they may be put on tape and shipped to Washington. In the former option, the results could then be transmitted back to the field analyst via telephone lines and stored on magnetic tape or printed out instantaneously.

The telephone link would allow both the field analyst and NRC supervisors, who would also have a small computer terminal, to look at input data simultaneously on their respective Tektronix screens. One person can then make changes and corrections to input data while the other views these changes.

SVAP's outputs are based on descriptions of all the ways one or more insider adversaries can divert SNM. The specific outputs presented to the analyst include:

1. Adversary paths.
2. Monitor coverage.
3. Uncovered monitor paths.
4. Uncovered response paths.
5. Transmission line redundancy.
6. Utility line redundancy.
7. Document paths.
8. Collusion sets.
9. Accounting loss detection mechanisms for given time periods.
10. Records for falsification for a given time period.
11. Form falsification for a given time period.
12. Probability of adversary success vs number of adversary colluders.

These outputs are presented in a report that is generated by SVAP. This report, when combined with the data handbook, makes a complete, self-contained

assessment package and therefore when a SVAP analysis is completed the NRC will have a fully documented record of a facility's safeguard system. Moreover, as SVAP is designed to be readily modified and added to, when a facility makes changes in its safeguard system those changes can be accommodated by SVAP and the facility reassessed. Through such updating, an ongoing record of the facility's safeguard system can be maintained. By the same token, as field experience by the NRC accumulates and as new rules and regulations are proposed, SVAP will be able to grow to handle these new developments.

There is excellent potential for putting the entire SVAP procedure on the small Tektronix computer and hence removing the need for a large main frame computer altogether. This would allow the NRC to have a self-contained assessment capability which could be kept in Washington or taken to each facility as it is assessed.

REFERENCES

1. P. S. Wahler, Safeguard Vulnerability Analysis Program (SVAP) Data-Gathering Handbook, Volume I, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52731 (November 1979); NUREG/CR-1169, Vol. I.
2. W. J. Orvis, Safeguard Vulnerability Analysis Program (SVAP) User's Manual, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52730 (October 1979); NUREG/CR-~~1157~~ 1169, Vol. III
3. R. B. Worrell, Using the Set Equation Transformation System in Fault Tree Analysis, Sandia Laboratories, Albuquerque, N.M., SAND74-0240 (September 1974).

LLL:1980/3

FWB