NUREG/CR-0849, Vol. 3
UCRL-52715-79-3

Safeguards Material Control and Accounting Program: Quarterly Report, April–June 1979

Donald R. Dunn

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-0849, Vol. 3
UCRL-52715-79-3
RS

NUREG/CR--0849-Vol.3

TI86 000173

Safeguards Material Control and Accounting Program: Quarterly Report, April–June 1979

Manuscript Completed: December 1979
Date Published:

Prepared by
Donald R. Dunn

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

FOREWORD

This work was supported by the U.S. Nuclear Regulatory Commission (Office of Nuclear Regulatory Research) under Interagency Agreement DOE 40-550-75 with the U.S. Department of Energy. The NRC FIN number is A-0115.

The scientific editor, Donald R. Dunn, wishes to acknowledge the work of those individuals responsible for each section listed below. In addition I wish to thank Frank Brunotts for his valued editorial assistance.

2.0	Assessment Methodology Development	
	2.1 Structured Assessment Approach	A. Parziale
	2.2 Safeguard System Vulnerability Analysis Methodology	M. Dittmore
3.0	MC&A Upgrade Rule Support	J. Lim
4.0	Aggregated Systems Model Development	R. Al-Ayat
5.0	Adversary Modeling	R. Schechter
6.0	Components Performance	J. Candy

CONTENTS

Foreword. iii

Abstract. ix

1.0 Introduction 1

2.0 Assessment Methodology Development 3

2.1 Structured Assessment Approach (SAA). 3

2.1.1 Condensation and Processing of Large Monitored Graphs 3

2.1.2 Development of a Limited Collusion Analysis. 5

2.1.3 Development of a Method to Perform an Extended Collusion Analysis. 6

2.1.4 Incorporation of a False Alarm Rate (FAR) Calculation into the Level 2 Analysis. 6

2.2 Safeguard System Vulnerability Analysis Methodology (SSVAM) . 7

3.0 MC&A Upgrade Rule Support. 8

4.0 Aggregated Systems Model (ASM) Development 11

4.1 Introduction. 11

4.2 Modeling of Event Sequences 12

4.3 Modeling the Resolution Process 14

4.4 Remarks and Future Directions 14

5.0 Adversary Modeling 16

5.1 Introduction. 16

5.2 Trip to the Securities and Exchange Commission (SEC). 16

5.3 Visit with Bob Curtis, Security Consultant. 18

6.0 Components Performance 21

References. 23

LIST OF ILLUSTRATIONS

1. Schematic of a value-impact analysis. 12
2. Sequence of events leading to alarm 13
3. Test for resolution 15

ABSTRACT

Activity for the quarter April-June 1979 in the Material Control Safeguards Evaluation Program, conducted for the U.S. Nuclear Regulatory Commission (NRC) at Lawrence Livermore Laboratory, is summarized. Progress was made in developing a computer-based methodology for identifying vulnerabilities in Material Control and Accounting (MC&A) systems in nuclear fuel-cycle facilities. Work was advanced in assisting the NRC in developing the forthcoming MC&A upgrade rule, a redirection of our program since January 1979. Other areas of activity reported on here are aggregated systems model development, adversary modeling, and components performance.

1.0 INTRODUCTION

The LLL NRC Material Control Safeguards Evaluation Program is currently active in two areas. The first concerns the continued development of a computer-based methodology for assessing the vulnerabilities of Material Control and Accounting (MC&A) systems of fuel-cycle facilities. The second area involves assisting the NRC in the development of guidance for the forthcoming MC&A upgrade rule and reflects a redirection of our program circa January 1979.

The assessment methodology work has involved the development and testing of new and more efficient algorithms, including user-oriented input/output interfaces, for the Structured Assessment Approach (SAA) computer code. An additional intent was to do a Phase II assessment of Facility X, a nuclear fuel-cycle facility, with our Safeguard System Vulnerability Analysis Methodology (SSVAM) which has been a companion effort to SAA. The Phase II assessment was to be based upon visits and detailed discussions with Facility X personnel. However, we have not been successful in arranging a visit to Facility X. To compensate for this we have been incorporating changes into SSVAM which would expedite the anticipated Facility X assessment. Section 2 describes recent progress for both SAA and SSVAM.

Sections 3-6 summarize activities which are in support of the NRC MC&A upgrade rule development. Section 3 focuses on attributes of Material Accounting (MA) systems and has involved in-depth modeling of the G.E. Vallecitos Nuclear Center (VNC) system. Other issues addressed have to do with MA functional decomposition and protection of MC&A data from falsification.

Section 4 represents extensions to our Aggregated Systems Model (ASM) development for doing value-impact analyses for major MC&A loss detection systems and for safeguard measures designed to protect against falsification.

Section 5 discusses our initial efforts to characterize the insider threat

to nuclear safeguards through a study of security problems in analogous industries.

In Section 6 we describe our very preliminary activities for investigating SNM loss indicators for the concentrator and precipitator unit processes at Facility X.

2.0 ASSESSMENT METHODOLOGY DEVELOPMENT

2.1 STRUCTURED ASSESSMENT APPROACH (SAA)

I. Sacks, A. Parziale, P. Renard, C. Patenaude, R. Harvey

Much of the development for the SAA has been directed to improving and integrating the SAA package for its eventual use in future assessments pertaining to Part 73 Fixed Site Physical Protection upgrade regulations. Specific areas of development are discussed in the following order:

- Condensation and processing of large monitored graphs.
- Development of a limited collusion analysis.
- Development of a method to perform an extended collusion analysis.
- Incorporation of a false alarm rate calculation into the Level 2 adequacy computer programs.

2.1.1 Condensation and Processing of Large Monitored Graphs

The objective of the SAA Level 1 analyses is to determine collections of elements, such as locations, which are traversed or encountered by an adversary in meeting his objective. The collection of elements along a diversion path is called a target set (TS). The collection of monitors safeguarding the elements associated with a target set is called a monitor target set (MTS). The Level 1 analysis output provides a list of all MTS which an adversary can encounter in meeting his objective. Unmonitored target sets or diversion paths may be found and are identified for the analyst.

The Level 1 analysis and subsequent levels of analysis are centered on the identification of the MTS. Thus, the efficient identification of MTS is important, especially with large and complex facility systems which can be modeled as monitored bidirectional graphs. Such a graph contains nodes representing elements or locations, where the connected nodes represent the topology of the facility system. Nodes in a graph may or may not be safeguarded by a monitor. This discussion focuses on advances which have been made in processing large monitored graphs for the purpose of determining the MTS.

Three graph reduction concepts were incorporated into the Level 1 analysis computer programs to improve the efficiency of these algorithms in determining the MTS. These were

- Removal of unreachable nodes.
- Condensation of unmonitored nodes.
- Removal of "finger" nodes.

Some nodes of the graph may be isolated from all others, either due to the structural configuration of the facility or due to assumptions made about the adversary's ability to penetrate through physical barriers, such as walls. Such nodes can neither be reached nor occupied by personnel and therefore can be eliminated from the facility graph whether monitored or not. The current algorithm finds isolated nodes and performs this elimination.

Condensation or grouping together of unmonitored nodes is possible in many cases, where these nodes or locations are immediately adjacent. Such condensation is possible without loss of information about the MTS embedded in the graph. The condensation concept is built into the Level 1 algorithms and has the potential of greatly reducing the size of the graph.

The final graph reduction concept is the removal of "finger" nodes, unmonitored nodes which are connected to a single monitored node. Such nodes may appear after the application of the condensation concept. These nodes may be removed from the graph whenever they are not used as the beginning or ending location of the material diversion path.

Further detailed discussion of these graph reduction concepts and their incorporation into the Level 1 analysis programs is presented in Refs. 1, 2, 3 and 4.

2.1.2 Development of a Limited Collusion Analysis

A simple or limited collusion analysis has been incorporated into the SAA. This analysis is called a Level 1.5 and follows the determination of the MTS in Level 1. The Level 1.5 programs perform an analysis similar to that performed by the Science Applications, Inc. developed Matrix Analysis of the Insider Threat (MAIT) discussed in Ref. 5.

The motivation for developing the Level 1.5 collusion analysis was that all necessary information for doing so was available and that identification of collusion vulnerabilities early in the SAA analyses would be a valuable output to the analyst.

The basic concept of the Level 1.5 collusion analysis centers on MTS, which are lists of monitors encountered by the adversary, and which are determined from the Level 1 programs. Through a straightforward substitution process, collections of insiders in collusion who can defeat an MTS are identified given the collusion group's authorized access to facility locations and safeguard system monitors. The collusion vulnerabilities are identified for each MTS under each facility mode circumstance, where facility modes complicate the Level 1.5 analysis by inhibiting the operation of particular monitors.

The Level 1.5 collusion analysis has limitations in that it considers only the authorized direct access and/or control of monitors or procedures and does not consider indirect effects. There may be situations, however, in which a single individual could cause an essential support component for several monitors to fail, thus disabling those monitors. Subsequent levels of analysis expand the MTS to include essential supporting components, such as signal transmission lines and utility components, and a second collusion analysis, called a Level 3.5, will be performed for the purpose of identifying collusion vulnerabilities in which the collusion groups use indirect access and control. The Level 3.5 collusion analysis is the subject of the following section.

The Level 1.5 collusion analysis is discussed in greater detail in Refs. 5, 6 and 7.

2.1.3 Development of a Method to Perform an Extended Collusion Analysis

The Level 1.5 collusion analysis is limited to a restricted point of view, in that only authorized direct access and/or control of safeguard monitors is considered. Thus, at Level 1.5, collusion groups who can defeat a MTS or diversion path coverage by disabling supporting utility and signal transmission components are not identified. This situation is remedied by the introduction of a Level 3.5 collusion analysis which expands an MTS to include supporting components.

The Level 3.5 collusion analysis is performed in a similar manner as the Level 1.5 collusion analysis, but has a more complicated substitution process. This is primarily due to the backup or redundancy characteristic which supporting components can take on. Also, there normally will be multiple signal transmission paths associated with monitors and MTS.

An algorithm for performing the Level 3.5 collusion analysis has been developed. Computer programs which perform the analysis are scheduled to be available in 1980. The Level 3.5 collusion analysis algorithm is discussed in more detail in Ref. 7.

2.1.4 Incorporation of a False Alarm Rate (FAR) Calculation into the Level 2 Analysis

A calculation which determines the overall false alarm rate (FAR) of the fast-response safeguard detection system has been incorporated into the Level 2 MTS adequacy analysis programs. This overall FAR output is a valuable statistic to the analyst because if the FAR is too high it may distract the physical security response force, and if it is too low it may cause vigilance degradation in the response force.

The input statistics required to perform the calculation and the assumptions underlying the calculation are discussed in more detail in Ref. 8.

2.2 SAFEGUARD SYSTEM VULNERABILITY ANALYSIS METHODOLOGY (SSVAM)

M. Dittmore, F. Gilman, W. Orvis, P. Wahler

During this quarter significant improvements have been made in SSVAM. These improvements have been in the areas of modeling techniques, for the physical security and material control systems, and output formating for the SSVAM results. Two main criticisms have been that the modeling done in SSVAM is very complicated and the solution of the models requires a person skilled in Boolean algebra. With the new modeling techniques both of these problems have been resolved. The new modeling techniques use the same data as was previously used; however, the data is input in a different format so that the computer code SETS can easily solve for the adversary event sets without any user interaction.

Work on the output format has led to a condensed user-oriented output package. This package contains the adversary paths, monitor target sets, uncovered adversary paths, uncovered response sets, and a quantitative analysis which generates a plot of probability of success vs number of colluders. The quantitative analysis plot takes into account the adversary paths, monitors, tampering, random failures, and collusion.

All these improvements in SSVAM have enabled us to take a significant step toward complete automation. Work in the next quarter will be directed toward an interactive input program that will allow the NRC to create data at facility sites and then execute SSVAM in Washington.

Work was also done this quarter on gathering data for a SSVAM analysis of G.E. Vallecitos, which will serve as a practical application. We expect this work to continue into the next quarter. We also expect, as a second practical application of SSVAM, to do a Phase II Facility X assessment.

3.0 MC&A UPGRADE RULE SUPPORT

P. Alesso, J. Huebel, J. Lim, R. Sanborn, R. Thatcher

The primary purpose of this task is to systematically evaluate and critique the current MA regulations. To evaluate the MA regulations a generic, minimal material accounting system model is being developed which reflects the requirements, both explicit and implicit, specified by the regulations and by accounting systems in general. To critique the MA regulations this minimal system will be analyzed by an adaptation of the fixed-site safeguards assessment methodology.[9] The analysis will identify the vulnerabilities inherent in the current MA regulations.

The approach used to develop the generic, minimal MA systems is to first construct models of specific MA systems. In particular, the MA systems at Facility X and at VNC are being modeled. The next step is to incorporate in a new model only those features that are required by the current MA regulations, eliminating all others.

The two specific MA systems used to initiate the development of the generic, minimal MA system were quite different from one another. The Facility X system was a manual-based MA system which seemed to adhere to the accounting structures defined by traditional financial accounting. For example, the Facility X system contained such accounting structures as ledgers, accounts, etc., that were clearly delineated and recognizable. The model for the Facility X system was developed from our interpretation of the licensee documentation provided to the NRC and our interpretation of the MA regulations. No direct contact with the licensee occurred.

However, the VNC system was a computer-based MA system significantly different from the Facility X system. For instance, the VNC system contained a central facility data base from which various accounting reports were generated. The model for the VNC system was developed from our direct interaction with facility personnel, our interpretation of facility documentation and personnel discussions, and, in addition, a new perspective on our interpretation of the MA regulations.

The major components of a model for the MA system at VNC are bookkeeping practices, measurement systems, and limit-of-error inventory differences (LEID). Within the overall structure we are including the collection of subsidiary accounting systems which operate in material balance areas (MBA), item control areas (ICA), and criticality limit areas (CLA). These subsidiary accounting structures, together with a system of checks and balances tying them together, make up the facility MA system.

The NRC regulations dealing with the accounting system per se were compiled. We then dissected the VNC MA system to determine how it complied with the regulations. In the course of this work, ambiguities in the NRC material accounting regulations as interpreted by licensees were identified. The primary problem was the lack of precise definition of the terminology used to describe the accounting requirements. For example, the following prescriptive terms are subject to sundry interpretations:

- centralized accounting system,
- double-entry bookkeeping,
- subsidiary accounts,
- control accounts,
- reconciliation of subsidiary accounts to control accounts.

The different features contained in the two specific MA systems compelled us to interpret some of the terminology used in the current MA regulations broadly. The definitions of basic terminology such as "account," "double-entry," "subsidiary," etc., must be established before a generic, minimal MA system can be developed.

In addition to the above, a functional decomposition of an adequate MA system is under development which involves three material balance equations at the levels of the NRC, the facility, and the MBA/ICA. These equations reflect the intent of assuring the NRC that SNM theft has not occurred from some facility, the facility management that SNM theft has not occurred within its boundaries, and the MBA/ICA custodians that SNM theft has not occurred within the confines of the MBA/ICA. This effort will provide input into the NRC NMSS task: Development of Guidance for Material Control and Accounting System Design.

A functional decomposition of MC&A regulations and upgrade rules also has been prepared as a starting point for the task effort on protection of MC&A data from falsification. The purpose was to structure them in some way so that we could clearly and concisely express their meaning and what they are trying to accomplish. The final result expresses regulations as capability statements in boxes and displays them in a functionally disaggregated diagram form. We next examined the Task Force goals[10] for both Material Control and Material Accounting; information pertinent to current regulations was also included in the functional diagram.

4.0 AGGREGATED SYSTEMS MODEL (ASM) DEVELOPMENT

R. Al-Ayat, J. Huntsman (ADA) and B. Judd (ADA)*

4.1 INTRODUCTION

Work on the ASM this quarter was devoted to building a structure for evaluating the potential values and impacts of safeguards (S/G) measures. This structure is required to provide the NRC with a value-impact (V-I) analysis to support the development of the upcoming MC&A upgrade rule. This structure represents an application to (and to some extent an extension of) the aggregated systems model.[11]

In a V-I analysis we need to integrate in a systematic fashion information on the S/G design and the threat characteristic to evaluate the effect of a proposed regulation on both the industry and the public. Fig. 1 shows a schematic for a V-I analysis; the performance of a S/G design in response to a proposed regulation is evaluated (Adversary/Facility Interaction) against a spectrum of threats (Adversary Model). The outcome of an evaluation is the value of the S/G system for a set of well-defined measures of performance such as the ability of the MC&A system to detect abnormalities and correctly determine their cause. In the box labeled S/G design the impacts are evaluated. Impact measures include S/G costs and the S/G effects on a facility's operational efficiency and safety. In this summary we only describe the process of evaluating the performance (value) of a S/G system; i.e., the Adversary/Facility Interaction.

Judging the value of an S/G system requires an explicit model of the system's detection sequence. A detection sequence consists of two stages; first, an anomaly is indicated and, second, one must determine whether the anomaly is real or a false alarm (i.e., resolve an alarm). In the next two sections we briefly describe our modeling procedure for both the event sequence leading to an alarm and that of the resolution process. In Ref. 12 we show how this modeling process is used to generate performance indicators for judging the effectiveness of an MC&A system.

---

*Applied Decisions Analysis, Inc.

4.2 MODELING OF EVENT SEQUENCES

Figure 2 contains a tree showing the sequences of events leading to alarms. The first node in the tree represents the occurrence of an initiating event. The next branching splits the initiating event into the two possibilities, that of an error condition or of an adversary making an attempt. In the adversary branch is a probability node which indicates that there are a variety of adversaries who might make attempts, each with different resources, access to different areas of the facility, and different intent. After the adversary has chosen a strategy and begun the attempt, a variety of safeguards may detect the action.

There are two types of security systems that will sense an attempt and give an alarm. The adversary first encounters those systems that may give timely alarms--for example, a procedures check. The second kind of security system encountered is that which gives an alarm after a loss has occurred, such as an inventory check. The column on the right side of Fig. 2 indicates which, if any, of the alarms occurs for each sequence of events. Thus, for each alarm type there is a set of possible scenarios that produce the alarm. This modeling process aids in determining which initiating event is most likely to give a particular alarm; e.g., inventory difference alarm (AID) or procedure violation alarm.

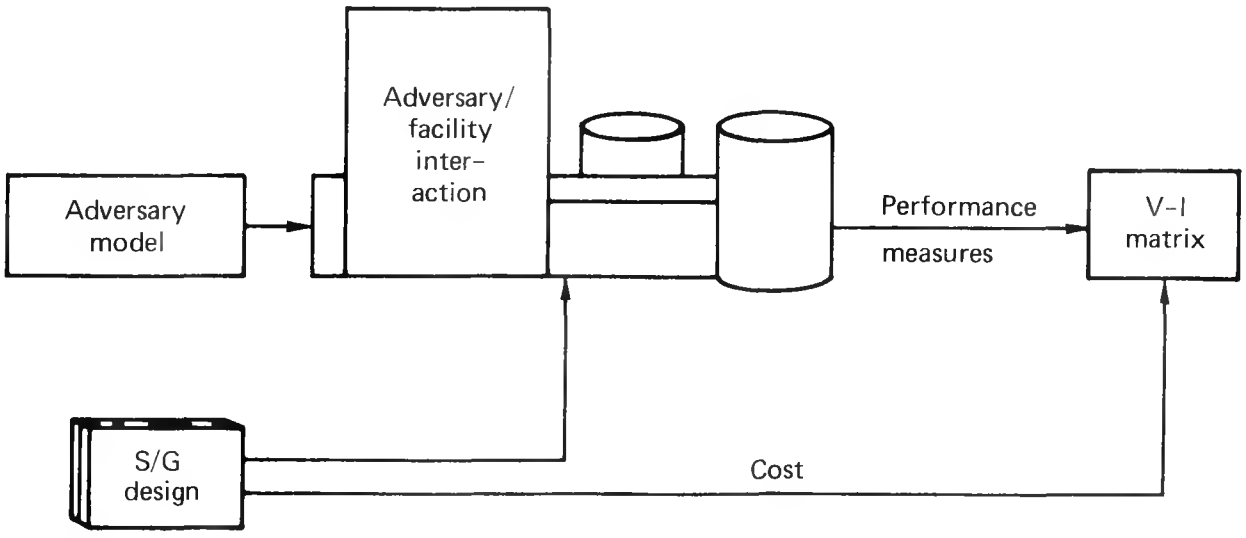

FIG. 1. Schematic of a value-impact analysis.

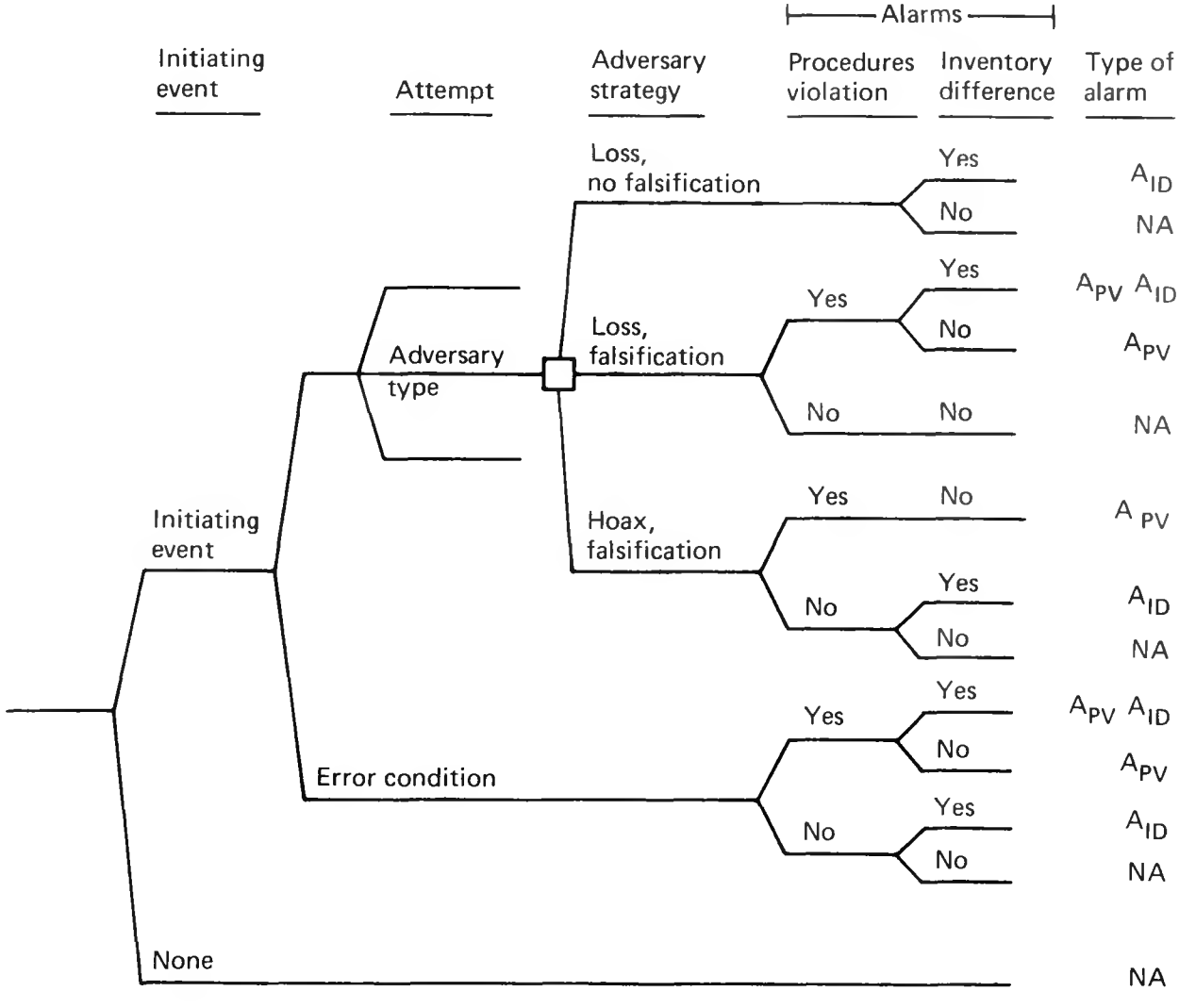

FIG. 2. Sequence of events leading to alarm.

4.3 MODELING THE RESOLUTION PROCESS

Once an initiating event happens and an alarm occurs, certain tests (or procedures) are used to determine what the initiating event was. The accuracy and the timeliness of the test determines the effectiveness of the resolution procedure.

Figure 3 shows the series of tests performed for an initiating event representing an error condition. Similar trees can be drawn for other initial conditions, such as loss, loss with falsification, and a hoax attempt. The first test performed is an audit. If the error was an inaccurate measurement, the audit will not find the source of the error. However, if the error was a numerical miscalculation, the audit could identify it. Thus, the audit may resolve the situation as an error condition or it may leave the case unresolved, in which situation another test is performed.

The next test is a reinventory followed by a shutdown inventory (Ref. 10). Finally, if all procedures were followed and the initiating condition wasn't found to be an error, the resolution would then be either that a loss had occurred or the case would be unresolved--that is, "no conclusive resolution." One of the aims of the explicit modeling of the resolution process is to reduce the number of cases without conclusive resolution.

Depending on the tests that are performed and the likelihood of a resolution that no loss occurred, there is a probability distribution on the time until resolution. Combining a structure such as Fig. 3 and knowledge of specific plant procedures and response plans, the expected time to resolution can be calculated.

4.4 REMARKS AND FUTURE DIRECTIONS

Explicit modeling of the event and resolution processes form an important step in evaluating the performance of a S/G system. Next, probabilities

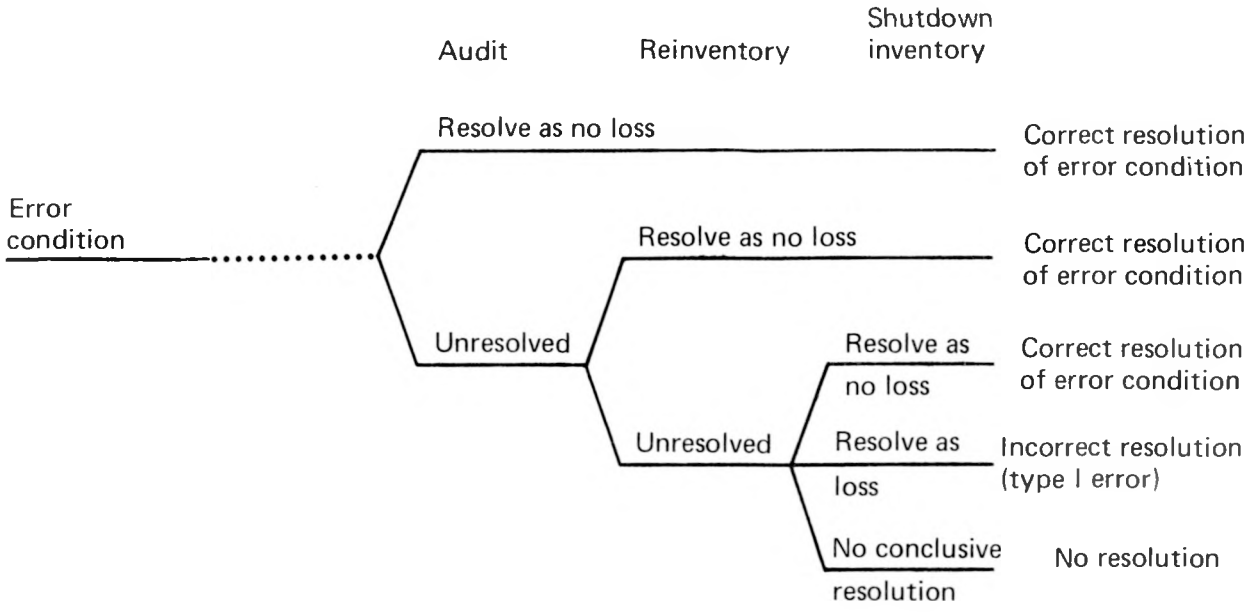

FIG. 3. Test for resolution.

will be assigned to each branch in the trees generated. Information needed will be a mix of objective technical data and subjective data elicited from experts. The S/G system performance can then be assessed by rolling back these probability trees. Expected times to resolve both timely and late alarms are also among the system's performance measures to be evaluated.

Steps have been taken toward the end of this quarter to demonstrate our V-I analysis methodology at an operating facility handling SNM. Results of this application will be reported on in the next quarterly.

5.0 ADVERSARY MODELING

R. S. Schechter and J. M. Heineke*

5.1 INTRODUCTION

As part of our contract with the NRC to characterize the potential insider threat to nuclear activities, we continued to meet with experts in the field of industrial security. By interviewing persons having extensive experience with internal security problems analogous to our own, we hope to gain valuable insights concerning the protection of nuclear activities. Highlights of two trips will be discussed below.

5.2 TRIP TO THE SECURITIES AND EXCHANGE COMMISSION (SEC)

The first trip was taken to the Securities and Exchange Commission in Washington, D.C. Here we met with Assistant Director Marvin G. Pickholz and several of his associates who are familiar with investigations of cases involving misappropriation of corporate funds, corporate fraud, and inventory manipulation.

On the subject of adversary characteristics, Pickholz stated that they are most commonly very bright, imaginative people, for whom the challenge of perpetrating the scheme is more important than financial gain. More often than not, an attempt will involve collusion with an outsider, who will target an employee whom he feels is particularly vulnerable to corruption. This is most likely to be a talented but disgruntled employee with a positive self-image, who feels that he is not receiving the proper amount of recognition or compensation from his employer. Sometimes the outsider will find such a person by looking for an employee who has not been promoted for some length of time. The targeted employee will be approached in a subtle manner at first, perhaps by being asked if he is considering leaving his current position. This will induce him to air his gripes against his current employer. The outsider will sympathize with these problems, gradually

---

*Consultant.

gain the confidence of the insider, and eventually suggest the perpetration of a scheme.

Besides the disgruntled employee, other insider adversary types are the person who is under severe emotional strain, and the amoral employee who feels that he can operate by his own rules and is entitled to obtain anything he wants. In other cases, it is the employee who has pulled himself up by his bootstraps from poverty and feels that the fastest way to advance to the next stage of prosperity is through dishonest means. Another type is the person from a wealthy family background whose socioeconomic status has started to slip and who feels that he has to do anything to live up to his family's standards. And, finally, there are a number of alcoholics and drug addicts at even the highest executive levels, who sometimes fall into compromising situations which leave them vulnerable to blackmail.

We were told that corporate systems of checks and balances are often vitiated by the "buddy system," in which executives are too familiar with one another to allow for effective monitoring of their activities. Minor indiscretions such as the personal use of a company airplane are often overlooked under the rationale that "everyone does it"; it is likely that this attitude contributes to a moral atmosphere which is conducive to more serious incidents, as well as conspiracy formation. And in some situations, a brilliant executive is considered so indispensable to his firm that others are willing to tolerate his irregularities rather than risk losing his services. As in the banking industry, employee loyalty to one's immediate supervisor is considered a serious stumbling block to security, with employees often willing to lie to investigators to protect their bosses.

Security measures recommended by the SEC include a policy of separation and rotation of duties, as well as an effective procedure for reviewing employee grievances. In addition, they recommend that companies be monitored by an auditing firm which is independent of operational management and accountable only to the board of directors. For companies in which there is considerable overlap between managers and directors, this system can retain its effectiveness by having the auditors report to a committee consisting only of outside directors.

5.3 VISIT WITH BOB CURTIS, SECURITY CONSULTANT

R. Schechter conducted an interview with Bob Curtis of Dayton, Ohio, a leading authority on business security. Mr. Curtis has worked in the security field since 1939, and now runs his own consulting firm. He conducts vulnerability studies and loss-control seminars for businesses, and is the author of five books on business security. Those of particular interest to our problem include Security Control: Internal Theft (1977) and How to Keep Your Employees Honest (1978).

Curtis claims that the most important aspect of security is the type of management used by a company. The most detrimental is authoritative-exploitative management, the essence of which is, "Just do as I tell you and don't ask questions or you're fired." Under this system an informal organization tends to develop among subordinates in opposition to top management which will strive to undermine the company in every possible way. Some such firms have been known to suffer vandalism and theft from as much as 95% of the work force.

The most effective form of management is participative, in which management meets with employees on a compatible and equal basis. Employees share in developing solutions to problems and situations related to their own areas of work, and decision-making is spread throughout the company. Also, a team approach to operations is emphasized. This leads to greater overall efficiency, stronger morale, and less theft. Only through direct participation will employees feel involvement and responsibility.

The importance of management style to security stems from the vital role which employee frustration plays in most internal thefts. The person who is frustrated or frightened is likely to steal as a response to his feelings of depression or misplaced hostility; for this reason, many firms have trained professional counselors to help employees with private and on-the-job problems. But where this service is not available, it is essential that the manager or department head assume this role.

On the subject of security clearances based upon background investigations, Curtis feels that these are of some value. This is because persons who have stolen in the past are likely to repeat, since a person's basic character patterns are established by the age of 15. Thus, while the most important factor leading to insider theft is poor management, it appears that individuals vary in their susceptibility to its influence. However, Curtis claims that a personal interview is a more effective means of evaluating a person's character than a background investigation, and the former should be a vital aspect of any security program. The personal interview questionnaire designed by Curtis is intended to study a person's attitudes, motivation, stability, maturity and aptitudes. Interviewers should be sensitive to giveaway gestures during the job interview, and should try to uncover with further questions why a particular topic elicited such a reaction.

With respect to high-risk employees, Curtis has identified a number of different types which warrant special attention. First, there is the employee who is living beyond his means, who can sometimes be spotted by his bragging about costly new possessions. This person can be investigated thoroughly by a detailed credit check from a local credit bureau, as well as from contacts at local banks. Another likely suspect is the chronic gambler, who will often resort to stealing to obtain funds for his habit, or who may open the door to organized crime. According to a study of one thousand embezzlers made by the U.S. Fidelity and Guaranty Company, gambling was the most frequently cited motive for theft. Then there is the overly attentive employee, who ingratiates himself with his boss by doing him personal favors. This provides a smoke screen which leads the manager to believe that such a person would never steal.

Other high-risk employees include the heavy drinker, the drug-user, the rule violator, the spendthrift, the chronic liar, the person who comes in early and leaves late, and the person suffering from family problems. Also, it has been found that the congenital handicapped show a staggering theft rate; their attitude seems to be that they were cheated by life and are entitled to get even any way possible.

Curtis claims that the long-term employee will often begin to steal after he reaches the point in his career where he finally realizes that he will no longer make it to the top of his firm, which can be a severely frustrating experience. His willingness to steal is often enhanced by a feeling that the firm's assets belong to him, because of his length of service. And his basic knowledge of the firm's controls, combined with the fact that his activities no longer arouse suspicion make him an extreme theft threat in terms of dollar losses. Ironically, such an embezzler will often turn out to be the best employee.

6.0 COMPONENTS PERFORMANCE

J. Candy, D. Gavel, R. Rozsa

The primary objective of this task has been to investigate alternative SNM loss indicators for the concentrator and precipitator unit processes at Facility X. Since accessibility to Facility X has been delayed unexpectedly, we have devoted time to preparing for a site visit and to finishing previous modeling work for a plutonium nitrate concentrator.

We reviewed safety documents describing Facility X in preparation for our upcoming visit to gather information on their evaporator and precipitator operations. These documents contained some sketches of the units and radiation safety calculations but nothing of substance concerning the operation or makeup of the processing steps.

We also reviewed the Science Applications, Inc., (SAI) model of a plutonium oxalate precipitator[13] to see how much was usable in the Facility X task. The physical and chemical properties are obviously different and, upon detailed review, the mathematics also are not too useful. The SAI model has eight first-order differential equations, four of which relate to precipitated crystal properties (radius, area, etc.). The other four are species mass balances. The crystal properties are unique to plutonium oxalate and are not applicable to the Facility X operation and the form of the equations is a bit awkward. It will be easier to start with a fresh simple model consisting of species mass balances and a relationship between liquid and solid phase partitioning.

Some time was spent in reviewing the general scrap processing cycle in an attempt to find out more about the chemistry of the ammonium diuranate product; we have not found a good reference yet (perhaps Facility X can help).

A small amount of time was spent in further debugging and testing of the steam controller calculation in the simple plutonium nitrate concentrator model developed at LLL. The controller is a proportional-integral type

and sets a steam flow rate to achieve a desired density. Final detector diversion simulation runs also were completed for the concentrator using both the simple (reduced) and detailed (truth) concentrator models. A technical report entitled On-Line Estimator/Detector Design for a Plutonium Nitrate Concentrator Unit by J. V. Candy and R. B. Rozsa was published under LLL number UCID-18124.

REFERENCES

1. D. Siljak, C. J. Patenaude, A. A. Parziale, and I. J. Sacks, "Processing Large Monitored Graphs," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-242-D (April 23, 1979).

2. P. A. Renard, "Warshall on Symmetric Matrices," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-207 (February 15, 1979).

3. A. A. Parziale and I. J. Sacks, Lawrence Livermore Laboratory, T. R. Rice and S. L. Derby, Applied Decision Analysis, Inc., The Structured Assessment Analysis of Facility X, Volume II, (C) Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52765 (January 1979).

4. I. J. Sacks and C. J. Patenaude, "Level 1.5--Weak Collusion Test for the Structured Assessment Approach," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-338 (July 6, 1979).

5. T. L. McDaniel and L. Huszar, The MAIT Method for Analysis of Facility Safeguards Against Insider Collusion, User's Manual, SAI-78-960-LJ, Vol. 2; NUREG/CR-0532.

6. C. J. Patenaude, A. A. Parziale, I. J. Sacks, and D. J. Ross, "SAA User Interaction for October 1979," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-314 (June 15, 1979).

7. I. J. Sacks, "Level 3.5 Second Phase Collusion Test," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-313 (June 14, 1979).

8. A. A. Parziale, "Safeguard System False Alarm Rate," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-358-D (July 13, 1979).

9. H. E. Lambert, et al. A Digraph-Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52710, (May 1979); NUREG/CR-0777.

10. Report of the Material Control and Material Accounting Task Force, Volumes I-IV, U.S. Nuclear Regulatory Commission, Washington, D.C., NUREG-0450 (April 1978).

11. R. Al-Ayat and B. Judd, The Aggregated Systems Model of Nuclear Safeguards, Executive Summary, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-52712 (July 1979); NUREG/CR-0791.

12. R. Al-Ayat, J. Huntsman, and B. Judd, "Value-Impact Analysis for Safeguards Designs," Lawrence Livermore Laboratory, Livermore, Calif., internal memo MC 79-08-11 (August 1979).

13. Science Applications, Inc., Final Report: Dynamic Process Model of a Plutonium Oxalate Precipitator, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-13812 (November 1977).

FWB/ijm

LLL:1980/3