NUREG/CR-0849, Vol. 1
UCRL-52715-79-1

Safeguards Material Control and Accounting Program Quarterly Report, October–December 1978

D. R. Dunn, A. Maimoni

Lawrence Livermore Laboratory

Prepared for
U.S. Nuclear Regulatory
Commission

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Printed copy price: $3.75

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-0849, Vol. 1
UCRL-52715-79-1
RS

Safeguards Material Control and Accounting Program Quarterly Report, October–December 1978

NUREG/CR--0849-Vol.1

TI86 000141

Manuscript Completed: December 1978
Date Published: June 1980

Prepared by
D. R. Dunn, A. Maimoni

Lawrence Livermore Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
Office of Nuclear Regulatory Research
Division of Safeguards, Fuel Cycle and Environmental Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A-0115

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

FOREWORD

This work was supported by the U.S. Nuclear Regulatory Commission under Interagency Agreement DOE 40-550-75 with the U.S. Department of Energy.

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

ABSTRACT

Work is summarized for the quarter October to December, 1978, in the Material Control Safeguards Evaluation Program, conducted for the U. S. Nuclear Regulatory Commission (NRC) at Lawrence Livermore Laboratory. The main activities related to the continuing development of the assessment methodologies and their application to the assessment of a fuel cycle facility.

Much progress was made in the Digraph--Fault-Tree Methodology, leading to the Safeguards System Vulnerability Assessment Methodology (SSVAM). In addition, the development of the Structured Assessment Approach (SAA) continued on schedule. Both techniques were used to assess the vulnerabilities of the safeguards system at an existing fuel recovery facility (Facility X).

Other activities during the quarter included (1) the continuing development of the Agggregated Systems Model (ASM), an evaluation tool designed to aid the NRC in the setting safeguards criteria; (2) the continuing structuring and data gathering for the adversary model portion of the ASM; and (3) the continuing development of computer codes for chemical process modeling/material estimation/material loss detection.

1.0 INTRODUCTION

The general objective of this project, sponsored by the Nuclear Regulatory Commission (NRC) at Lawrence Livermore Laboratory (LLL), is to develop the methodology and software that the NRC will need for assessing Material Control and Accounting (MC&A) systems at fixed site nuclear fuel facilities. The purpose of the methodology is to determine the capability of an MC&A system in detecting an adversary sequence. Specific objectives are as follows:

1. To devise an assessment methodology and a set of tools that will allow the NRC to evaluate the MC&A portion of a fuel facility safeguards system.
2. To devise a methodology that will assist in creating performance-based regulations for licensing a facility.
3. To design tools and techniques for upgraded MC&A systems.

The LLL assessment methodology was described in the first quarterly report.[1*]

The main activities in the period October to December, 1978, related to the continuing development of the assessment methodologies and their application to the assessment of a fuel cycle facility.

Substantial progress was made in the Digraph--Fault-Tree Methodology, leading to the Safeguards System Vulnerability Assessment Methodology (SSVAM), which is inherently easier to automate. The development of the Structured Assessment Approach (SAA) continued on schedule. Both techniques were used to assess the vulnerabilities of the safeguards system at an existing fuel recovery facility. This report briefly describes the SSVAM and SAA methodologies and illustrates their usefulness by indicating the type of results obtained in the assessment of Facility X.

Other activities during this quarter included the following:

1. The continuing development of the Aggregated Systems Model (ASM), an evaluation tool designed to aid the NRC in setting safeguards criteria;

[*] References for each chapter are listed at the end of the chapter.

2. The continuing structuring and data gathering for the adversary model portion of the ASM; and
3. The continuing development of computer codes for chemical process modeling/material estimation/material loss detection.

We also conducted a joint study with Sandia personnel to assess the computer needs and options available to the NRC for implementing the automated assessment methodologies being developed at this Laboratory, Sandia, and other facilities.

REFERENCES: CHAPTER 1

**1. L. L. Cleland, W. A. Johnson, A. Maimoni, I. J. Sacks, and L. R. Spogen, Safeguards Material Control at Licensed Processing Facilities, Lawrence Livermore Laboratory, Livermore, CA, UCID-17515-77-1 (March 1, 1977).

**Available for purchase from the National Technical Information Service, Springfield, VA 22161

2.0 ASSESSMENT METHODOLOGIES

2.1. INTRODUCTION

The main objection of the Material Control and Accounting (MC&A) program at Lawrence Livermore Laboratory (LLL) has been the development of a computer-assisted methodology for performing a detailed assessment of the vulnerability of a MC&A system at a given facility to insider actions.

Our initial concepts[1] evolved and were first demonstrated through the assessment of the Test Bed.[2] At that time our methodology was based on the generation by a safeguards analyst of a directed graph (digraph) representing the safeguards system, followed by the systematic generation of the corresponding fault tree.

Because of the possible difficulties in automating the Digraph--Fault-Tree Methodology, we also studied, in a parallel effort, other modeling approaches for developing an assessment methodology.[3]

Both approaches were successful. The Digraph--Fault-Tree Methodology led to the Safeguards System Vulnerability Analysis Methodology (SSVAM) and the parallel effort led to the Structured Assessment Approach (SAA). Progress in both these techniques is described in this quarterly report. Both techniques have been demonstrated by the assessment of Facility X. The SAA is the first version of a fully automated assessment procedure, a milestone for which a due date of January, 1979 had been established.

2.2 SYSTEM VULNERABILITY ASSESSMENT METHODOLOGY

2.2.1 General Description (M. Dittmore)

LLL has been developing analytical tools to help the Nuclear Regulatory Commission (NRC) assess the vulnerabilities of plants that process or handle SNM. The vulnerabilities of interest to us are that they increase the ease of theft by one or more nonviolent insiders. One approach has been to define groups of events that, if they all happen or can be made to happen, will ensure a probability of success of unity given an attempt to steal. Each event describes a specific system vulnerability and each group so described is called an "event set."

The event set approach was inspired by an early attempt to apply fault-tree techniques to the vulnerability problem. That early attempt led us to the development of the Digraph--Fault-Tree Methodology.[4] However, in its original form, this methodology was difficult to automate; we have been able to modify the method to overcome the problem. The modified digraph we now call a logic diagram, and it has been incorporated into our total SSVAM.[5]

Figure 2-1 is a schematic diagram of the component parts of the SSVAM procedure. Note that event sets form a natural division of the method into two parts:

1. The generation of the event sets, and
2. the analysis of the event sets.

Since each event set describes a specific vulnerability of the plant, it is quite natural that they should lie at the heart of the procedure.

The front half of SSVAM provides a step-by-step procedure for generating the event sets (Fig. 2-1). Historically, event sets have been derived from fault-trees, which, in turn, were constructed directly from the system description. However, between the system description and the fault-tree, the analyst was faced with two difficult problems:

1. Understanding how the safeguards components were interconnected, and
2. understanding how the total system interacted.

SSVAM helps to solve these problems by providing a structured step-by-step procedure to go from "System Description" to the event sets. As shown in Fig. 2-1 the first step (after a particular target has been identified and selected) is to construct a block diagram. The block diagram for a simple safeguards system is shown in Fig. 2-2. The blocks represent the physical components of the system. M1 is a monitor watching A1, a room. P1 is the front gate of a facility and G the guards. On the other hand, the lines represent the events (sometimes called the system variables).

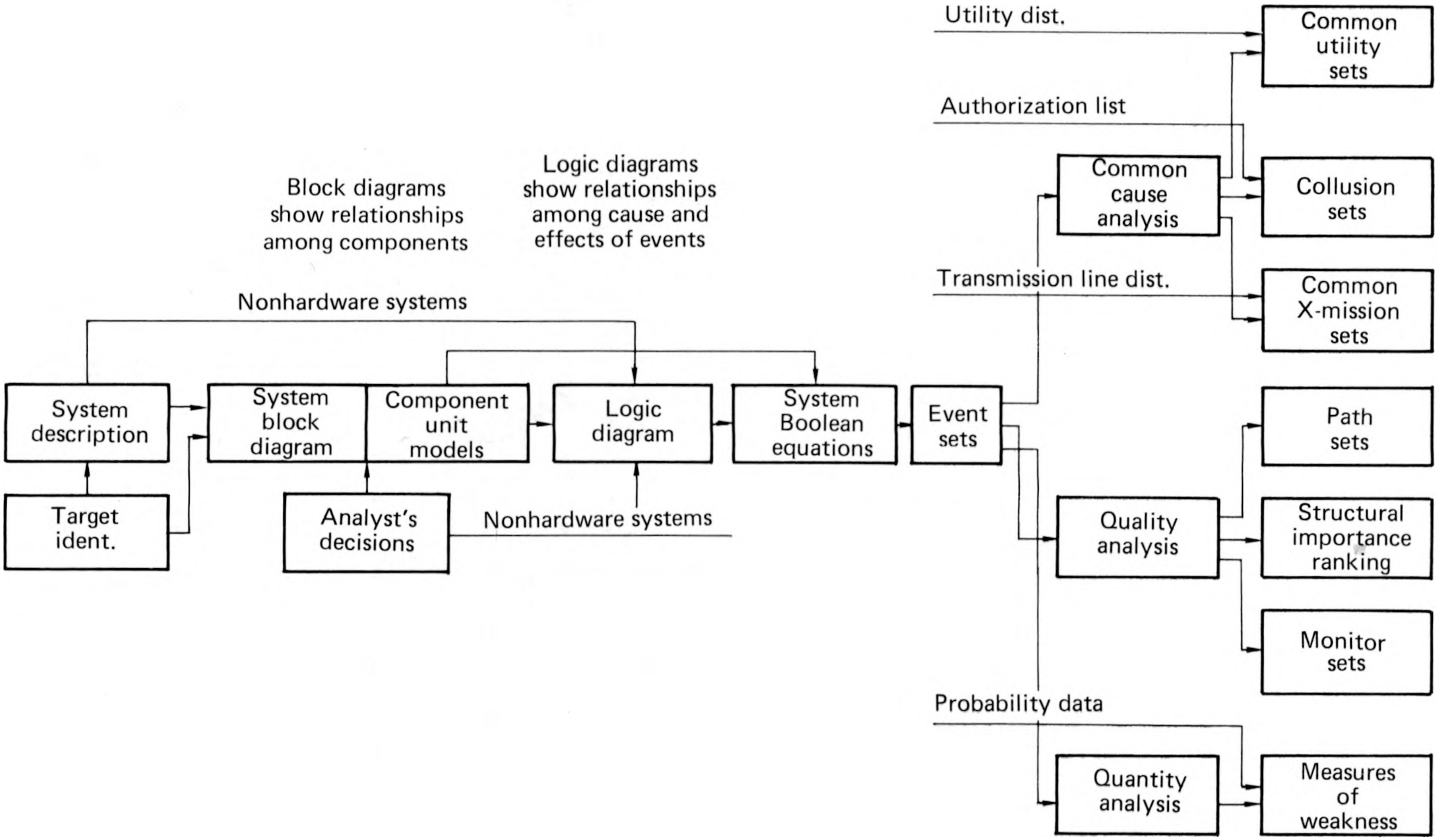


FIG. 2-1. Procedure for Safeguards System Vulnerability Analysis methodology.

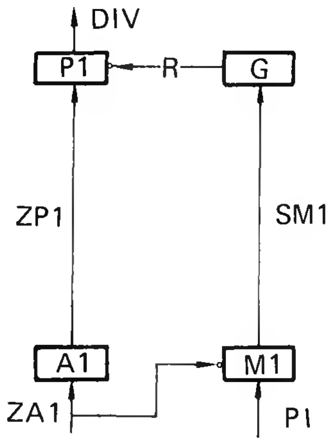


FIG. 2-2. Block diagram for a simple safeguards system.

Examples of system variables are PI, the power input to M1; SM1, the signal out of M1; ZA1, the presence of the thief in A1; and ZP1, the presence of the thief in P1. All the variables are Boolean (i.e., they are either true or false), and they must be quantities that can be measured at a point.

The system components (i.e., the blocks in Fig. 2-2) have transfer functions associated with them. These functions relate each input variable to each output variable. The gains of the transfer functions are either zero or one. Potential component failures are introduced as conditional gains of the transfer functions. For example, consider monitor M1, which has P1 as its input variable and SM1 as its output. (ZA1 is neither an input nor output variable; it is rather a control variable.)

We can identify any number of conditions on the transfer function associated with M1, but for this example we shall define only two:

1. The gain is one if ZA1, "thief is in the area," is true, and
2. zero if M1F, "monitor M1 fails" is true.

When the block diagram has been completed and the conditions on the gains of the transfer functions established, the next step in the procedure is to draw the logic diagram. The logic diagram is a transform graph of the block diagram. The variables (represented by the lines in Fig. 2-2) transform into nodes on the logic diagram. The conditional gains of the transfer function are represented on the logic diagram by two logical constructs: the inhibit gate and the enable gate.

The inhibit gate is used to represent the condition when B is the input . variable of a given transfer function, A is the output variable, and C is an event (i.e., another variable) that "conditions" the gain to zero. Therefore, the logical equation for the inhibit gate A = B * C.

The enable gate is used to represent the opposite condition: that is when E is the input variable, F the output variable, and D is an event that "conditions" the gain to unity. The logical equation for the enable gate is F = D * E. The equations for the inhibit and enable gates constitute the fundamental building blocks for the system equations. When the system equations are combined, reduced, and simplified by SSVAM, the event sets are obtained.

The block diagram in Fig. 2-2 shows the relationships among the system components. On the other hand, the logic diagram shows the cause and effect relationships among events. Nonhardware systems (such as material accounting systems) have no identifiable physical components. Therefore, block diagrams are difficult to visualize and construct. However, for such systems, the cause and effect relationships among the events can be identified. Thus, we have successfully modeled a material accounting system directly onto the logic diagram without the need to construct a block diagram first. The material accounting model is described in Section 2.2.2.

From either the block diagram or the logic diagram, a set of simple Boolean relationships can be written. There is one equation for each transfer function. Taken together this set of relationships describes the total system vulnerabilities; the set is also called the system equations.

Of all the variables occurring in the system equations, one represents the event that is of primary interest to the particular analysis being done. We call this event of primary interest the top event. For a safeguards system, the top event would be "diversion of SNM." When the top event has been identified, the system equations can be combined through substitution, expanded, and reduced by standard Boolean algebra techniques to yield the ensemble of event sets for the top event.

As described above, each event set is a list of possible failures that if all happen, will result in the top event happening. Therefore, each event set is a scenario for the top event; and, as such, they can naturally serve as inputs to an array of common cause, probabilistic, and other types of analyses.

For a safeguards vulnerability analysis, each event set contains several types of events:

1. Events describing the path through the plant taken by the adversary;
2. Events describing the monitor failures needed to leave the given path unguarded;
3. Procedural events such as falsifying documents or defeating the two-man rule; and
4. Tampering acts needed to mask the theft in the accounting system.

With the event sets broken down this way, we are prepared to answer almost any question about the vulnerability of the safeguards system. Some examples are as follows:

1. How many paths are available to a thief between a given theft point and the outside?
2. Are any of these paths completely unguarded by monitors?
3. Given that we know the random failure rates of each monitor, what is the probability that a given path is unguarded? Or, what is the highest probability that a path is unguarded?
4. Given that we know the utility distribution, what utility supplies must fail to leave a given path unguarded?
5. Given that we know the authorization available to each worker, can one man have access to enough hardware to disable all the monitors on any given path?
6. What is the smallest combination of workers (and who are they) that can defeat the safeguards system? And what scenario do they use?

The event sets contain all the system vulnerabilities; therefore, the capability of the analysis is limited only by the imagination of the analyst.

The event set generation techniques in SSVAM were originally developed to assess vulnerabilities of safeguards systems. However, the techniques can be applied equally well to a wide variety of reliability and safety problems. In particular the block diagram-logic diagram-system equation sequence makes it possible to calculate event sets for noncoherent systems. All systems that contain control loops are noncoherent. SSVAM makes it possible to extend the traditional fault-tree type of analysis to this entire large group of complicated systems.

2.2.2 Modeling Adversary Tampering of Accounts and Records in a Material Accounting System (J. J. Lim)

2.2.2.1 Introduction. During the quarter of October-December, 1978, one major area of emphasis was the modeling of adversary tampering of accounts and records in a material accounting system. Prerequisite to the modeling was the delineation of the material accounting system structure and the procedures which it employs to perform its function. A logic diagram model was developed to integrate the responses of the accounting system to the actions of the adversary when he attempts to disguise an SNM theft by altering accounts and records. Analysis of this logic diagram provided the following outputs for the Facility X assessment (Section 3): (1) the minimal sets of accounts and records that must be tampered with to disguise an SNM theft, and (2) the minimal sets of plant personnel who have access to these accounts and records.

2.2.2.2 Description of a Material Accounting System. A typical nuclear material accounting system is a highly complex, redundant structure that uses double-entry bookkeeping. Its primary purpose is to provide long-term assurance that material is present in assigned locations and in correct amounts.[6] This is accomplished through a set of procedures and records that classifies, records, and summarizes all physical movements, chemical changes, and losses of materials. These procedures and records are an intrinsic part of the nuclear safeguards system.

To verify that all the proper material actually resides at the facility, a plant physical inventory is taken on a bimonthly basis. The material at the facility is measured against a reference number computed from the material entries recorded in the central accounting books, usually a general ledger. If the difference between the physical measure and the reference number is less than the LEID (limit of error for inventory difference) the facility is assumed to contain all the material for which it is responsible. If the difference is greater than the LEID, an inventory difference is noted, and plant investigative actions ensue.

The bookkeeping structure of a material accounting system consists of an asset side and a liability side. Accounts on the asset side are those for which the presence or absence material may be verified by measurement; accounts on the liability side are those for material that cannot be measured and whose transactions can be verified only by account entries. Figure 2-3 shows the various asset and liability accounts. Whenever a transaction occurs, an entry is credited against the account from which the material leaves and debited to the account to where it goes. To ensure accuracy of the records, the books are balanced on a bimonthly basis at the time of physical inventory so that the fundamental accounting equations of assets = liabilities and credit = debits are satisfied. Any imbalance causes a book balance discrepancy.

The accounts reside in a central book, the general ledger. In addition, separate ledgers are usually kept by the area custodians for the various asset accounts. The general ledger and each subsidiary ledger are compared on a bimonthly basis when the books are balanced. Any difference causes a ledger discrepancy.

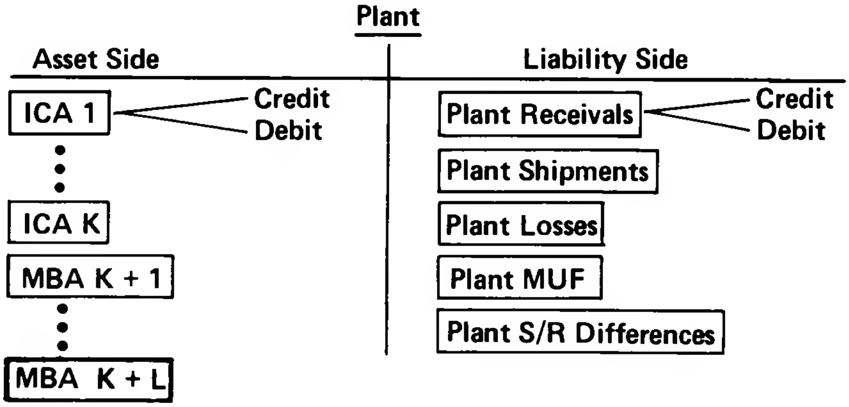


FIG. 2-3. Asset/liability account structure.

All book entries in the accounting system must be supported by proper source documentation. Thus, the entries in the general ledger are audited against source documents annually. The audit may be either a complete or a random partial check. Any unsupported book entry generates an audit discrepancy.

Consequently, the material accounting system provides assurance that material is indeed present in the correct amounts and locations with the following mechanisms to indicate anomalies:

- Inventory Difference
- Book Balance Discrepancy
- Ledger Discrepancy
- Audit Discrepancy.

The facility accounting system also interfaces with the NRC accounting system in which each facility is an account. The mechanisms which cause federal investigative action are the NRC Shipper/Receiver discrepancy resulting from Shipper/Receiver measurement differences between facilities and the NRC ledger discrepancy resulting from differences between the facility material balances and the NRC fault account balances.

Figure 2-4 summarizes the detection mechanisms contained in both the facility material accounting system and the NRC accounting system.

2.2.2.3 <u>Construction of the Logic Diagram Model</u>. Although the NRC and facility material accounting systems contain the above checks, an adversary can still disguise an SNM theft by altering the accounts and records. A directed graph, or logic diagram, is used to model the interactions of the accounting systems and the adversary when he attempts to thwart them. The fundamental structures of the logic diagram that facilitate this modeling are the inhibit gate, the enable gate, and the OR gate. The inhibit gate prevents the flow of information or occurrence of events while the enable gate allows the flow or occurrence. Each gate has a unique graphical and Boolean representation as shown in Fig. 2-5.

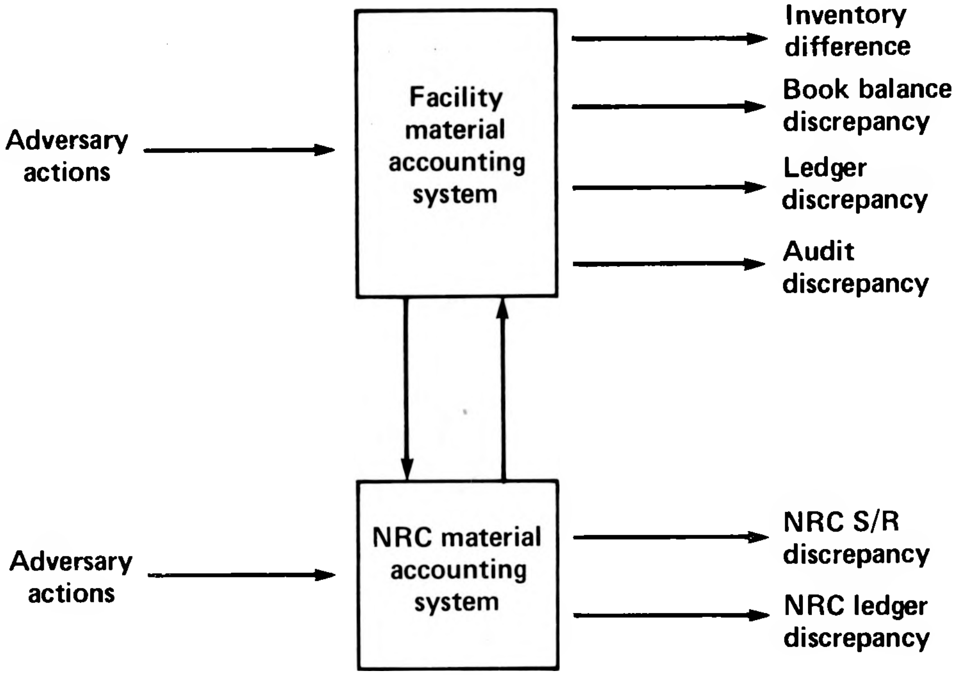


FIG. 2-4. Detection mechanisms in facility and NRC material accounting systems.

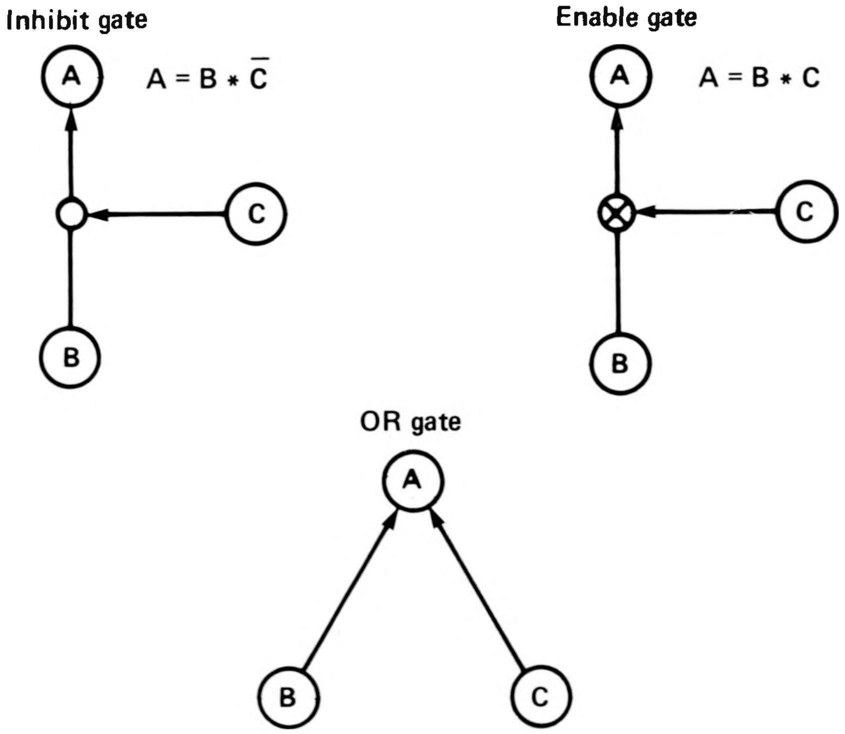


FIG. 2-5. Logic diagram structures and Boolean representations.

The basic strategy used to construct the logic diagram[7] is the following:

1. Model the normal safeguards accounting information flow triggered by a SNM theft.
2. Model the actions of the adversary and other natural events which inhibit the normal safeguards accounting information flow.
3. Model the consequences of the adversary actions, that is, the normal safeguards information flow resulting from the detection mechanisms in the accounting system.
4. Repeat from Step 2 until the adversary has thwarted the accounting system.

Figure 2-6 shows a partial logic diagram that illustrates the application of this strategy.

The dotted portion of Fig. 2-6 is the normal information flow triggered by a SNM theft. The events in the dotted nodes are as follows:

SNMA16	SNM theft from area 16
DSNM16	Decrease in SNM amount residing in area 16
DGM16	Decrease in gross amount of material residing in area 16

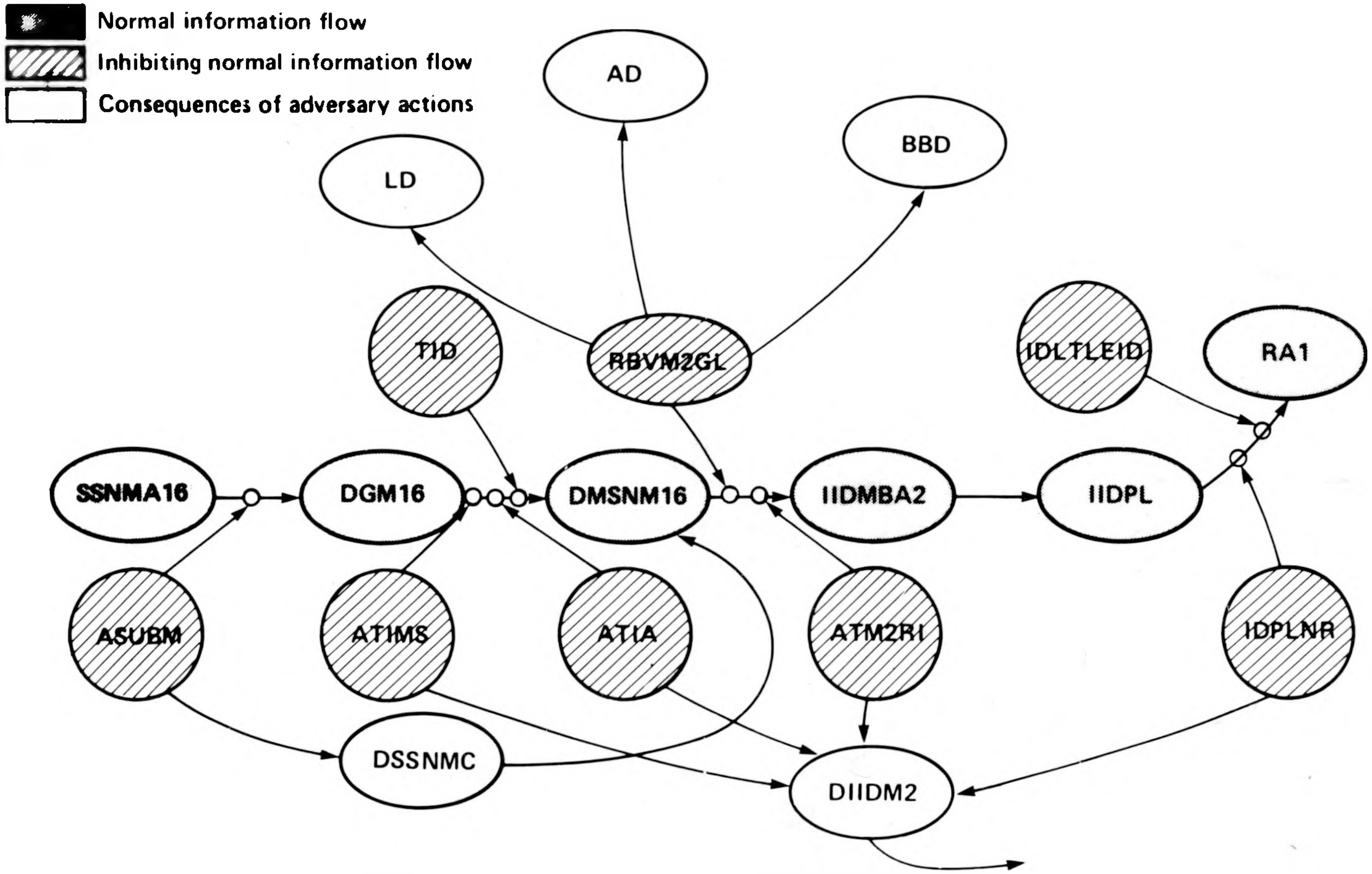


FIG. 2-6. Logic diagram for a material accounting system.

DMSNM16	Decrease in measured SNM amount residing in area 16
IIDMBA2	Increase in MBA2 inventory difference (area 16 is in MBA2)
IIDPL	Increase in plant inventory difference
RAI	Response #1 from material accounting system.

The dashed portions of Fig. 2-6 are the adversary actions and natural events that inhibit the normal information flow. The events in the dashed nodes are defined by the following:

ASUBM	Adversary substitutes material
ATIMS	Adversary tampers with inventory bulk measurement system
AIAA	Adversary tampers with inventory chemical assay
TID	Time until inventory occurs
ATM2RI	Adversary tampers with MBA2 reported inventory
RBVM2GL	Reduced book value for MBA2 account in general ledger
IDPLNR	Plant inventory difference not reported
IDLTLEID	Plant inventory difference less than the limit of error.

The white portions of Fig. 2-6 are the consequences resulting from the adversary actions to inhibit the normal occurrence of events or information flow. The events in the white nodes are defined by the following:

DSNMC	Decrease in SNM concentration
DIIDM2	Delayed increase in MBA2 inventory difference
LD	Ledger discrepancy
AD	Audit discrepancy
BBD	Book balance discrepancy.

In short, the iterative application of the strategy outlined above will yield the complete logic diagram model. In Fig. 2-6, the circular nodes will not be developed further (no inputs) and represents the limits of resolution for the model. Note that the event IDLTLEID includes any statistical measurement errors and is not developed further. Emphasis in this model is on the bookkeeping system rather than the measurement system of the accounting system. The oval nodes in Fig. 2-5 will be further developed (inputs). For instance, the event RBVM2GL is the point at which adversary tampering of accounts and records enter the model and must be "traced-back" to source documentation.

As shown in Section 2.2.1, a set of Boolean equations can be derived from the logic diagram, where the dependent variable is successful SNM theft with no detection by the material accounting system within a specified time frame. Solving the set of equations for the prime implicants[8] gives the various accounts and records an adversary must tamper with to disguise a SNM theft.

A common-mode failure analysis[9] of the prime implicants provides the collusion requirements (who and how many) needed to successfully tamper with the accounts and records.

2.2.2.4 Technical Highlights and Problems in Model Construction and Analysis. In constructing the model for the material accounting system, the following points were noted regarding the logic diagram:

1. It aids in modeling noncoherent systems, such as a total system consisting of an adversary and an accounting subsystem, to determine the possible causes of the event being analyzed. When properly used, the logic diagram often leads to the discovery of event combinations that might not have been recognized as causes. In the material accounting problem, the logic diagram provides the accounts and records that must be tampered with to disguise an SNM theft.
2. It provides a convenient and efficient format in which to partition and analyze a system when a national decomposition of the system is not clear. The material accounting system is such a system (unlike the physical protection system whose components are clearly delineated).
3. It serves as a display of results. If the system design is not adequate, the logic diagram can be used to show what the weak points are and how they lead to undesirable events. If the design is adequate, the logic diagram can be used to show that all conceivable causes have been considered.

Although the logic diagram is a powerful modeling tool, computational (not mathematical) difficulties arise in solving the equations derived from it. The equations are biformal Boolean equations that require the use of efficient prime implicant algorithms[8] for their solution. Current computer codes (SETS and FTAP) cannot easily handle these equations. Further research is continuing to develop efficient solution of the logic diagram equations to obtain the desired outputs.

2.2.3 Boolean Reduction Algorithm Development

(P. Alesso and J. Huebel)

The logic diagram of the SSVAM is analyzed by first representing it as a Boolean equation. When this equation is "reduced" it yields the complete set of prime implicants. These prime implicants are the minimum set of events that must occur in order to have diversion.

Originally, the Set Equation Transformation System (SETS)[10] code was used to manipulate the Boolean equation to find the complete set of prime implicants. Unfortunately due to the biform* character of the Boolean equation, SETS was unable to handle problems for more than about 50 nodes. This, however, represents a relatively small logic diagram.

To find the complete set of prime implicants for a more practical size problem of several hundred nodes, improved efficiency in reducing the biform Boolean equation was necessary.

The following theorems were developed and proved in an effort to increase the efficiency in reducing the Boolean equation.

Theorem 1: If Φ is any disjunctive normal form, such that, $\Phi = \Phi + \psi$ (where ψ is the biform $f_1 \cdot f_2 + f_1 \cdot f_3$) then setting $f_1 = 1$, $f_1 = f_1$ before applying double complementation to Φ, is equivalent to setting $f_1 = 1$, $f_1 = f_1$ after double complementation.

Theorem 2: Let Φ be any disjunctive normal form such that it can be expressed, $\Phi = \phi U \psi$

where

(1) $\ell(\phi)\ \ell(\psi) = \{\phi\}$ (no literal in common) and

(2) ψ is monoform

*Biform means that both a literal and its complement appear in the equation.

then

$\Phi = \phi U \psi$ gives the complete set of prime implicants.

Theorem 3: Let Φ be any disjunctive normal form such that it can be expressed $\Phi = \phi U \psi$

where

(1) ψ is monoform

(2) $\psi = \{\chi | x$ is any literal such that its negation is not present in $\Phi\}$,

then

$\Phi = \phi U \psi$ gives a Boolean equation which will yield the complete set of prime implicants, after applying only Boolean absorption laws.

Theorem 1 was beneficial in utilizing SETS for the analysis of Facility X. It eliminated nonuseful terms in the Boolean equation before the difficult step of Boolean reduction took place, thereby allowing SETS to handle a larger than normal problem.

Theorems 2 and 3 offer large savings for reduction efficiency because they decompose a long biform Boolean equation into two disjoint parts that may then be reduced separately. In addition, these theorems offer a basis for an algorithm which could, iteratively decompose a biform Boolean equation into all its disjoint parts. Such an algorithm would efficiently reduce a biform Boolean equation of a relatively large logic diagram (about 500 nodes).

In addition to theorem development, an exhaustive literature search was conducted for general Boolean reduction techniques. An efficient algorithm[11] for monoform Boolean reduction was made available to ADA, who found its ideas about exclusive operators useful in their work for SAA.

In developing these theorems, useful knowledge was obtained that was used in assessing Facility X. That is, the ideas contained within the theorems were used to modify the Facility X Boolean equation so that it could be processed by SETS.

2.2.4 Requirement for a Graphic Input-Output Station for Safeguards System Vulnerability Assessment Methodology

The SSVAM computer code under development at LLL now has a multistep manual process for the input of the facility data. An interactive graphics subsystem was proposed to simplify this input process with a corresponding increase in data reliability. The current input process consists of the following steps:

1. The user manually converts the MC&A system information from the form received in the license submitted data to a logic diagram in the form of a diverted graph (digraph).
2. The user writes Boolean equations representing the information contained in the digraph.
3. The user manually enters these Boolean equations into the computer, which then processes the data and generates a safeguards effectiveness report that the user then evaluates.
4. If an error in the model is detected, the error in the input data must be located, and some or all of Steps 1, 2, and 3 repeated. If the model is corrected and a safeguards vulnerability has been detected, then the licensee must upgrade the safeguards system and modify the license submittal data accordingly. All four steps of the analysis would then need to be repeated.

The proposed interactive graphics subsystem could be used to automate part of Step 1 and all of Steps 2 and 3. The subsystem could be used to interactively enter the digraph in a graphical form with the user entering the data utilizing a graphical CRT and either a light pen or graphic digitizer. The subsystem would then automatically generate the Boolean equations and pass them to the large computer for processing and generation of the safeguards effectiveness report.

The hardware required to implement such a system was determined. It would consist of an interactive graphic CRT with light pen, a data tablet, minicomputer with on-line disk storage, a printer-plotter, and miscellaneous communication and peripheral equipment. Use of the system would provide both faster entry of data and more accurate data than the present manual method, and would thus allow the user to operate in a much more cost-effective manner.

2.3 STRUCTURED ASSESSMENT APPROACH
(I. Sacks and A. Parziale)

This section provides a brief overview of the SAA. Extensive documentation has been produced for most aspects of the SAA, and it is listed in Refs. 12 through 23. The results of the analysis of a typical fuel cycle facility are given in Section 3. The following subsections briefly describe the major aspects of the SAA approach.

2.3.1 Methodology Overview

The SAA methodology is staged. It subjects the facility to a series of increasingly stringent performance tests that range from a determination of whether a nontampering adversary can break the facility with no risk at all to subtle questions dealing with the availability of the detection system and the dynamics of the diversion sequence. The advantage of the staged approach is that it allows much analysis to be done without judgmental input from the analyst. To the extent possible, the procedures are based directly on data from License Submittal Documents and from NRC data bases. Because each stage subjects the facility to more exacting criteria, passing a given stage does not mean that the facility is acceptable, but failing at any point means that the facility should be rejected. One of the main advantages of a staged approach is that a sensitivity analysis can be performed at each stage to identify the weakest points in the system. This insight allows the analyst to focus the detail in the next stage of the analysis on those areas in which it is more likely to uncover system problems.

Both the methodology and the conclusions from the staged assessment approach provided by SAA are subdivided into four levels that are characterized by four basic adversary models. These levels, shown schematically in Fig. 2-7 are as follows:

- Level 1. Can a nontampering adversary divert strategic nuclear material (SNM) with no risk of detection?
- Level 2. Can a nontampering adversary divert SNM with some level of risk, and does the probability of detecting that adversary meet the NRC criteria?
- Level 3. What system states, such as failed components or collusion among employees and adversaries, would allow the adversary to divert SNM? Does the system meet single-failure criteria?
- Level 4. Can the adversary tamper with the system--both through altering physical systems and through colluding with others--in order to divert SNM without detection?

Table 2-1 gives a general description of the four levels of the structured approach. Each level is summarized by a general description; the characteristics that are assumed for all adversary types; and the major inputs and outputs for the level of analysis. Each level corresponds to a different stage in the SAA.

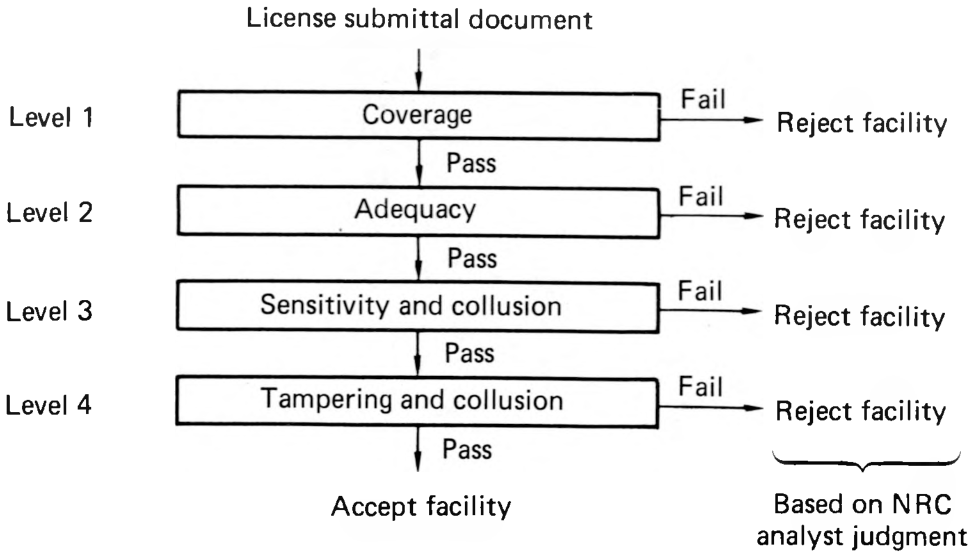


FIG. 2-7. Steps in the Structured Assessment Approach.

TABLE 2-1. General description of Structured Assessment Approach.

Level	General description	Characteristics common to all adversary types	Major inputs	Major outputs
1	MC&A system coverage:	Nontampering, risk-averse enemy:	Plant physical description:	Outputs for each adversary type:
	Assuming that all MC&A components are available, does the system cover all target sets for all adversary types?	Adversary does not tamper and has no knowledge of system availability. He will attack any uncovered target set.	-Area adjacency matrix -Process element adjacent matrix -MC&A System adjacency matrix -Monitor field-of-view matrix	-Uncovered target sets -Monitor target sets
			Adversary information:	
			-List of adversary types -List of material access points for each adversary type.	
2	Adequate system availability:	Nontampering, risk-taking enemy:	Plant physical description:	Output for each adversary type and for each monitor target set:
	Is the system reliable enough against each adversary type and for each monitor target set?	Adversary does not tamper. He knows the system operating mode but is ignorant of component availabilities. He attacks once at a random time, hoping that MC&A system is down.	-Utility adjacency matrix -Utility/MC&A connection matrix (or unit models) -Mode list	-Probability of detection -Sensitivity to failed components
			Availability data:	
			-Component availability by mode.	
3	System vulnerability to adversary with special knowledge:	Smart, nontampering enemy:	Observation sets:	Output for each adversary type:
	How vulnerable is the system to an adversary who knows the availability of some or all MC&A system elements?	Adversary does not tamper. He knows modes and some or all component availabilities. Types of adversary knowledge states are:	-For each adversary type list of components whose status is known.	A. Frequency with which each target set becomes uncovered. Frequency with which system becomes uncovered.
		A. Complete knowledge of all component availabilities, attacks only uncovered target sets.	Availability data: -Mean time to failure	B. Ranking of system components by impact of single component failure and by impact of adversary observing single component.

TABLE 2-1. Continued.

Level	General description	Characteristics common to all adversary types	Major inputs	Major outputs
		B. Knowledge of status of some components, ignorance of others.	-Mean time to repair	
4	System vulnerability to tampering:	Smart, tampering enemy:	Location data:	For each adversary type, assuming tampering:
	What is system performance against adversaries who have special knowledge and who tamper? What is the unconditional probability of successful diversion for each adversary type?	Adversary will tamper if he can reach the area where he has access to a component. Levels of analysis are classified by dynamics and knowledge:	-Areas from which components can be compromised.	-Uncovered target sets -Probability of detection for covered target sets
		Dynamics	Timing data	For SNM facility:
		4.1 No sequencing constraints No timing constraints	Sequencing data	-Acceptable or unacceptable
		4.2 Sequencing constraints No timing constraints	Availability data	
		4.3 Sequencing constraints Timing constraints		
		Knowledge		
		A Level 1 plus tampering B Level 2 plus tampering C Level 3 plus tampering		

2.3.2 Levels of the Structured Assessment Approach

2.3.2.1 Level 1. The intent of Level 1 is to determine if a nontampering adversary can divert SNM with no risk of detection. In other words, assuming that no component has failed, are all potential diversion paths "covered" by the MC&A system?

The key concept in Level 1 is the generation of target sets (TS), which are lists of elements that will be encountered by an adversary seeking SNM. A TS is defined by exhaustive enumeration of the areas and portals used by the adversary in entering and leaving a facility, and the process volumes such as tanks whose state will be altered as the SNM leaves the system. The list of monitors protecting a target set is called a monitor target set (MTS). The data required to define the MTS include a physical description of the plant, monitor field-of-view data, and adversary information.

The output from the Level 1 analysis identifies all uncovered TS, the ones for which the MTS contains no elements. In addition, the MTS is listed for each covered TS.

2.3.2.2 Level 2. The Level 2 analysis extends the Level 1 analysis to consider system reliability. The system reliability is calculated for each adversary type and for each MTS.

We assume that the adversary does not tamper with the system, that he has no knowledge of the system status except the operating mode, and that he makes only one attempt to divert SNM. Consequently, the appropriate system availability measure is the probability that a given MTS will be uncovered if attacked once by a given adversary type at a random entry time during any given operating mode of the facility.

The calculation of the probability of detection conditioned on adversary type, mode, and MTS is complicated by the common mode failure problem. Utilities such as electricity or compressed air can fail, thus causing several MC&A components to fail simultaneously. The utility structure is part of the input to the Level 2 analysis, allowing dependence among components to be modeled explicitly.

2:3.2.3 Level 3. Level 3 introduces more sophisticated adversary types with special knowledge of the status of the MC&A system. These adversaries do not tamper with the system, but they do have knowledge of the status of some or all of the MC&A system components.

Complete knowledge is equivalent to observing a status board with a light that goes on for every operational component and that goes out for every failed component. Under complete knowledge without tampering (Level 3A), we assume that an adversary will attack only uncovered TSs. The output for this type of adversary is the frequency with which various TSs become uncovered and the frequency with which the facility becomes uncovered.

Adversaries with partial knowledge of the system (Level 3B) know the status of some components and are uncertain about the status of the remaining components. Level 3B analysis is currently used for sensitivity analyses of single component failures. The output of this analysis ranks the individual components according to the net change in probability of detection caused by their random failures.

2.3.2.4 Level 4. Level 4 asks the question: What is the unconditional probability of successful diversion for each adversary type? This is the most sophisticated level of analysis, and if completed successfully and modeled in the same level of detail as the previous levels, it will include all the results of Levels 1, 2, and 3 as special cases. Special cases for Level 4 are based on adversary dynamics and adversary knowledge. Dynamics are characterized by the constraints of sequencing and timing on the adversary. Knowledge states are introduced in Level 4 that are analogous to those of Levels 1, 2, and 3.

Currently, the principal output from Level 4 is whether a tampering adversary can cause a target set to be uncovered. Future work will be required to compute the probability of detection given tampering.

Some parts of the SAA are more fully developed than others. At each stage of the analysis, at least a "prototype" computer code exists. This means that although more efficient computer codes may be developed in the future, the key system performance measures at each stage have been defined, and algorithms have been developed to measure them.

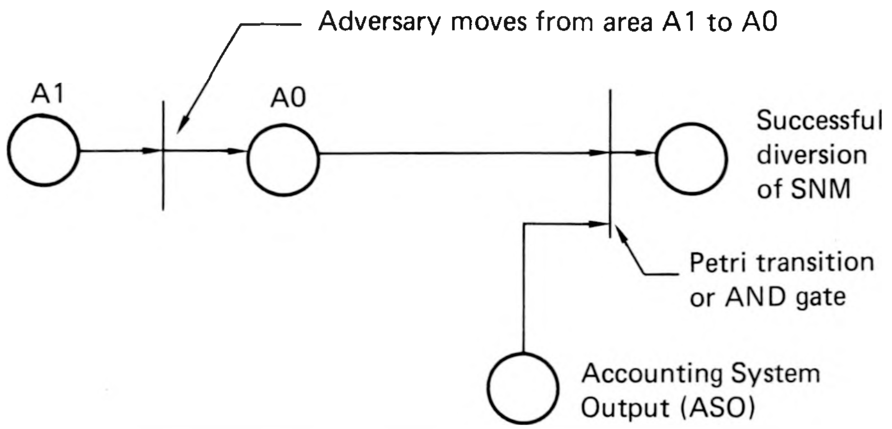
2.3.3 Example of a Level 4 Analysis of an Accounting System

Level 4 analysis is focused on whether an adversary can defeat the MC&A detection mechanisms for the material containment and material accounting systems by tampering. We will use an accounting system as an example for this discussion of tampering vulnerability analysis.

In modeling an accounting system, the basic concepts of the Petri Net modeling described in Refs. 15 and 19 are followed. The Petri Net will be used to determine if an adversary (or a team of adversaries) can tamper with the accounting system to block an anomaly detection. In a complete analysis, analyses of SAA Levels 1, 2, and 3 would be used to determine the performance of the accounting system in the absence of tampering. If the accounting system was found to perform adequately in the nontampering case, then the Level 4 tampering analysis would be applied. The system was assumed to have passed the nontampering analyses and required a Level 4 analysis. The basic idea in this tampering vulnerability analysis is to determine if adversary actions can cause the monitor side of the Petri Transition (an AND gate) to be up. Figure 2-8 shows this concept. In this figure the adversary could not pass through the Petri Transition unless the ASO side is also up. Thus, if the monitor being modeled is the accounting system, we must determine if the adversary can propagate his effects so as to cause the system to produce a nondetection.

In the terminology of Petri Nets, the effect of the adversary would be to "mark" a place (node) with a token. The transitions would be the events that define information flow steps. In the analytic procedure presented, transitions will not be explicitly called out except for controlled transitions.

The monitor (e.g., accounting system) is modeled after all the anomaly detection mechanisms from the point of view of adversary tampering access. This model is shown schematically in Fig. 2-9. In Fig. 2-9, the following three anomaly mechanisms have been modeled:



Adversary moves from area A1 to A0
A1
A0
Successful diversion of SNM
Petri transition or AND gate
Accounting System Output (ASO)

FIG. 2-8. Response model of Petri Technique.

1. The Sum of the Assets (ΣA) equal Sum of the Liabilities (ΣL).
2. The Sum of the Credits (ΣC) equals the Sum of the Debits (ΣD).
3. The book assets less the physical inventory is less than the limit of error for the inventory difference (LEID).

This model is designed to show how the effects of adversary access to the detection system would propagate. For example, if the adversary had access to the node labeled "Physical Inventory" of Fig. 2-3, he could cause the Inventory OK node to be marked (or up).

A fourth procedure for accounting system detection is often used. This procedure is an audit in which book entries are verified against their source documentation and against duplicate (or subsidiary books). This procedure is shown schematically in Fig. 2-10 for a system with one Material Balance Area (MBA). In this system, the adversary would have to gain access to the source files S1C and G1C and to the two accounts SMBA-1C and GMBA-1C to propagate his effect to the ΣC node.

To determine if the adversary can cause the detection nodes to be marked, it is necessary to determine access to each node in the system. To accomplish this end, each node is expanded by means of a unit model. These unit models follow the format of the general Petri Net modeling technique described in Ref. 8. A typical unit model for an account is shown in Fig. 2-11.

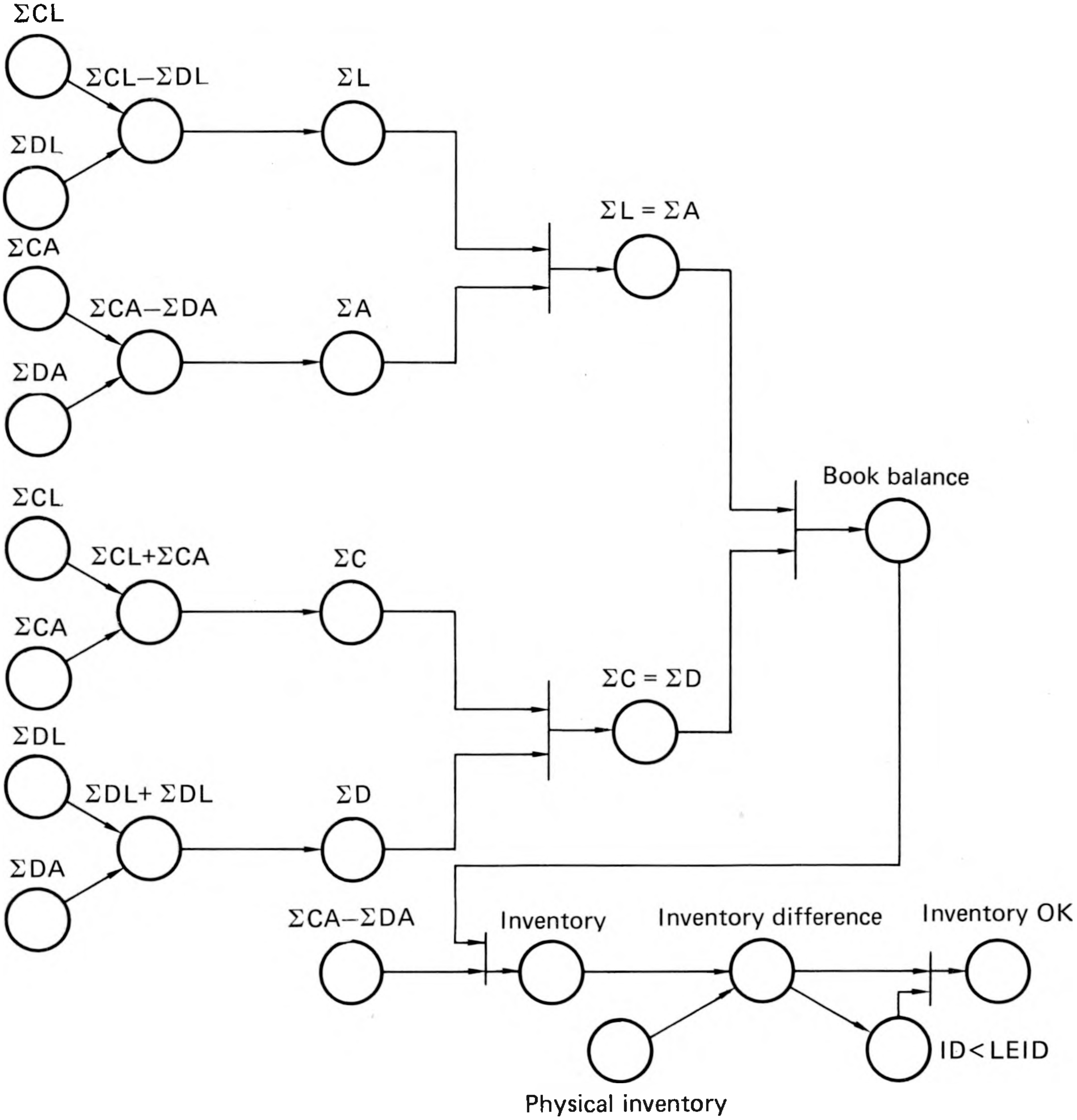


FIG. 2-9. Accounting system detection mechanisms.

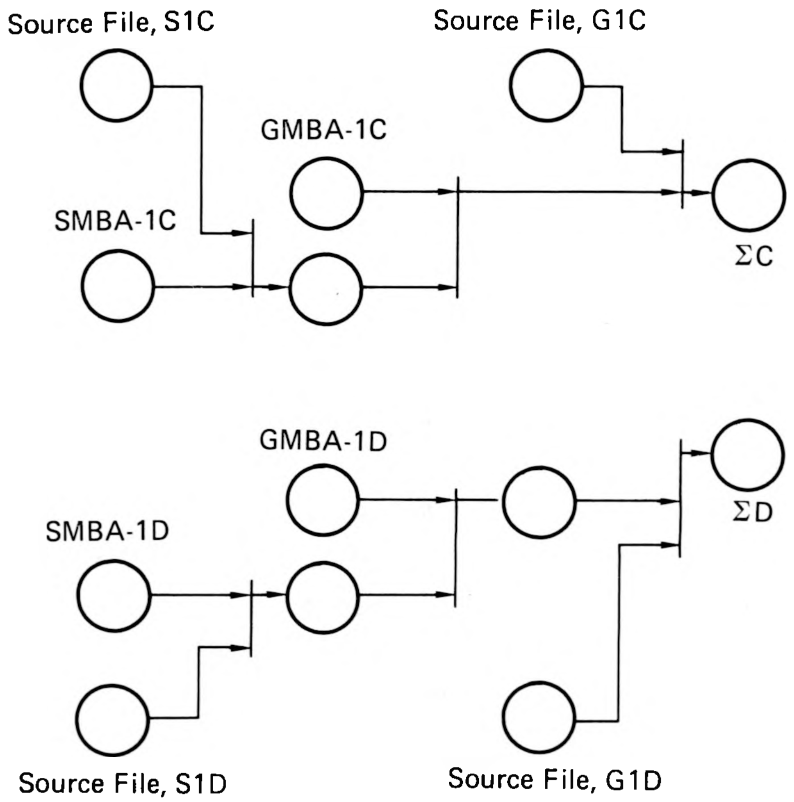


FIG. 2-10. Audit detection mechanism.

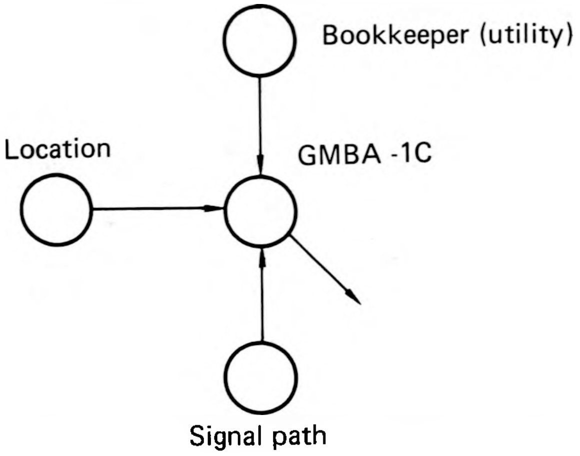


FIG. 2-11. Basic unit model for book account.

The essentials of this model are as follows:

1. The utility or individual or individuals who normally modify or enter data into the account, i.e., the bookkeeper;
2. the physical location of the account; and
3. the signal path or normal information flow paths into the account.

The general model shown is oriented toward unauthorized data modification, i.e., tampering. It will then be used to determine what actions the adversary must take to cause the accounting system output to be marked. This marking is the flag that indicates successful tampering. For example, in Fig. 2-9, the adversary would have to gain access to the ΣCL, ΣDL, ΣCA, and ΣDA nodes to mark the Book Balance node. (This means that the adversary could cover an actual book imbalance.) The use of detailed information, such as that provided by the accounts structure, the information flow mechanism, and the unit models will show that in real systems many of the nodes have common elements, i.e., can be reached from a common node.

The analysis procedure can be broken into three distinct steps:

1. Preparation of the data input;
2. entry of the data into Level 4 computer code CLAMOR; and
3. analysis of the results.

The data preparation step should be performed by the license applicant, but it could be done by the NRC licensing analyst. In second step, the NRC analyst must input the data into the CLAMOR computer code. The CLAMOR code generates all paths through the network described by the input data from every node to every node. This output is a listing that represents a Reachability Matrix, that is, it describes whether any given node can be reached from any other node. The nodes that must be reached for adversary success are the system detection outputs. The nodes that define the starting point are the adversary identities (and/or physical locations).

2.4 ALGORITHM DEVELOPMENT FOR THE STRUCTURED ASSESSMENT APPROACH (T. Rice and S. Derby, Applied Decision Analysis)

This section summarizes the work performed at Applied Decision Analysis (ADA) in support of the SAA. The ADA contributions have been primarily in the development of algorithms for calculating the probability of complex events for the analyses of Levels 2 and 3 of the SAA. These efforts have been thoroughly documented.[12]

2.4.1 Description of the Factoring Algorithm

The factoring algorithm developed for Level 2 of the SAA rearranges a minimal path representation of the Boolean expression for the detection event associated with a diversion path into mutually exclusive terms. In this form, the probability of detection is reduced to the sum of the probabilities for each term. Each term is composed of a set of factors and the individual safeguards system component probabilities in a reduced path representation. The path representation in each term is then reduced by factoring until there are no common components in the paths. The probability of the mutually exclusive term can then be calculated. Since the path representation contains no common components, this probability is also a simple calculation.

A simple example illustrates the Boolean manipulation used to factor paths. Two Boolean operations are used:

$A + AB = A$ (Logical reduction)

$B = BA \oplus B\bar{A}$ (Logical expansion)

where $\oplus$ represents a mutually exclusive OR and A represents NOT A.

By using these operations, a path representation of the detection event that contains common components can be factored into a set of mutually exclusive terms containing paths without common components. Let the detection event be described by the following expression:

$$D = AC + AB + BC.$$

Detection occurs if safeguards system components A and C, or A and B, or B and C are operational.

By factoring out the event A and using the first Boolean operation, a set of mutually exclusive terms is defined:

$$
\begin{aligned}
D &= A(C + B) + BC \\
&= A(C + B) + (A \oplus \bar{A})BC \\
&= A(C + B + BC) \oplus ABC.
\end{aligned}
$$

Next, using the second Boolean operation of logical reduction, the reduced path representation is simplified:

$$D = A(C + B) \oplus \bar{A}BC \quad .$$

The probability of detection is then simply the probability of the two mutually exclusive terms being summed together:

$$P_D = p(D) = p(A)\ p(C + B) + p(\bar{A})\ p(B)\ p(C) \quad .$$

Table 2-2 lists the steps in the factoring algorithm. It describes in simple steps the procedure used to generate the mutually exclusive terms. These steps first select the component event that is to be the factor. It then creates two new mutually exclusive terms, each term containing the factor and a new reduced path. If the paths remaining in each new term have a common component, the algorithm repeats the factoring procedure until the paths in all terms have no common components. The end result is an expression of mutually exclusive terms. The sum of the probabilities of these terms is the probability of detection.

2.4.2 Major Result

ADA's contributions have had direct impact on the Facility X assessment. Algorithms for calculating the probablility of detection were computationally successful in the sensitivity analyses for SAA Levels 2 and 3. These results are discussed in greater detail in Ref. 12.

·TABLE 2-2. Description of the factoring algorithm.

First term

1. Select the most common component.
2. Compute the probability of the component working.
3. Eliminate the factored component from each path in which it occurs.
4. Reduce the factored paths (if possible).
5. Store both the probability of the factor and the reduced set of paths for further factoring if paths remain dependent (have common elements). If independent, calculate probability.

Second term

6. Compute the probability of the component not working.
7. Eliminate all paths from the original set that contain the factored component.
8. If the reduced set of paths contain common components, continue factoring (return to Step 2). If independent paths then calculate probability.

PROBABILITY OF DETECTION: Sum of term probabilities

2.4.3 Concluding Remarks

ADA's assistance in both the methodological development of the SAA and in dealing with the computational issues that arise with application has been satisfactory and enlightening.

REFERENCES: CHAPTER 2

**1. A. Mainomi, "Safeguards Research: Assessing Material Control and Accounting Systems," Energy and Technology Review, UCRL-52000-77-11/12, pp. 11-19.

2. F. Gilman, H. E. Lambert, and J. J. Lim, "The Results of a Directed Graph-Fault Tree Assessment of an MC&A system," J. Inst. Nucl. Mat. Mgmt Proc., 19th annual meeting, VII, 117-125 (1978).

**3. A. Maimoni, "Safeguards Material Control Program," Quarterly Report, October-December, 1977, UCID-1725-77-4.

**4. J. J. Lim, H. E. Lambert, and F. M. Gilman, Digraph-Fault Tree Methodology for the Assessment of Material Control Systems, UCRL-52710, NUREG/CR-0777, Lawrence Livermore Laboratory (April, 1979).

**5. J. J. Lim, F. M. Gilman, and M. H. Dittmore, Vulnerability Analysis, Phase I Report, UCRL-52714, Lawrence Livermore Laboratory (September, 1979).

*6. United Stated Nuclear Regulatory Commission, "Report of the Material Control and Material Accounting Task Force," Summary, NUREG-0450, Vol. 1, (April, 1978).

7. H. E. Lambert and J. J. Lim, "The Modeling of Adversary Action for Safeguards Effectiveness Assessment," Inst. Nucl. Mat. Mgmt. Proc., (1977).

8. B. L. Hulme and R. B. Worrel, "A Prime Implicant Algorithm With Factoring," IEEE Trans. Computers (November, 1979).

*9. United States Atomic Energy Commission, "Appendix IV, Common Mode Failures," Reactor Safety Study, WASH 1400 (1974).

10. R. B. Worrell, Set Equation Transformation System (SETS), SLA-73--0028A, Sandia Laboratories, Albuquerque, New Mexico (May, 1974).

11. S. Rai and K. K. Aggarwal, "An Efficient Method for Reliability Evaluation of a General Network," IEEE Trans. Reliability, R-27, No. 3 (August, 1978).

*12. A. Parziale, I. Sacks, T. Rice, and S. Derby, "Structured Assessment of Facility X, Volumes I and II, UCRL-52765, NUREG/CR-0791, Lawrence Livermore Laboratory (January 8, 1979).

**13. I. Sacks, A. Parziale, and P. Renard, "Modeling of Procedures," Lawrence Livermore Laboratory, Internal Document MC 78-1374-D, December 18, 1978. (Draft)

**14. T. Rice, and S. Derby, "Overview of the Structured Assessment Approach and Documentation of Algorithms to Compute the Probability of Detection," Applied Decision Analysis (ADA), Lawrence Livermore Laboratory, UCRL-13937 (December 15, 1978).

**15. I. Sacks, "Techniques for the Determination of Potential Adversary Success With Tampering (Level 4.1)," Lawrence Livermore Laboratory, Internal Document MC 78-928-D (October 17, 1978).

**16. D. Siljak, "On Structural Properties of MC&A Systems," Lawrence Livermore Laboratory, MC 78-998 (September 29, 1978) and MC 78-758-D (August, 1978).

**17. T. Rice and S. Derby, "Characterization of Analytical Procedures to Calculate the Probability of Successful Diversion of SNM," Lawrence Livermore Laboratory, MC 78-1037 (September 25, 1978).

**18. I. Sacks and A. Parziale, "Unit Models," Lawrence Livermore Laboratory, Internal Report MC 78-884 (September 20, 1978).

19. J. Peterson, "Petri Nets," Computing Surveys 9 No. 3 (September, 1977).

**20. A. Parziale, "Modeling Adversary Tampering of a Safeguards System with a Petri Net," Lawrence Livermore Laboratory, MC 78-514 (June 30, 1978).

**21. A. Parziale, "Analysis of Utility Networks and their Significance in Identifying Vulnerability in a Safeguards Communication System," Lawrence Livermore Laboratory, MC 78-403 (May 31, 1978).

**22. A. Parziale, "Determining Dominant Paths in a Network and Their Significance in Analyzing the Safeguarding of Adversary Area Traversal," Lawrence Livermore Laboratory, Internal Report MC 78-301 (May 2, 1978).

**23. I. Sacks, A. Parziale, M. Shrot, and J. Long, "A Structured Approach to the Assessment of Material Control and Accounting systems," Lawrence Livermore Laboratory, MC 78-203 (March, 1978).

*Available for purchase from the NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, and the National Technical Information Service, Springfield, VA 22161

**Available for purchase from the National Technical Information Service.

3.0 FACILITY X ASSESSMENT

3.1 INTRODUCTION

The initial demonstration to the Nuclear Regulatory Commission (NRC) of the validity and practicality of the approach of Lawrence Livermore Laboratory (LLL) to the Material Control and Accounting (MC&A) system assessment was undertaken in February, 1978. On that date we briefed NRC staff on the results of assessing the vulnerability of the Test Bed,[1] a plutonium nitrate solution storage area. At that time, NRC and LLL agreed that an assessment of a fuel cycle facility other than a reprocessing plant would be most useful in developing, testing, and demonstrating the LLL-assessment methodology. The facility chosen is denoted in this report as Facility X.

The following should be kept in mind in reading the material in this section:

1. The initial assessment was based only on information currently available at the NRC and did not include specifics that could be obtained only during a site visit.
2. Specific information about Facility X and the vulnerabilities of their safeguards system are classified and are not discussed.
3. The results in Section 3.3 reflect a number of assumptions made by the LLL personnel developing and testing the Structured Assessment Approach (SAA) and have no direct relation with operating practice at Facility X.
4. Following the presentation of the results of these assessments to NRC staff and Facility X personnel, we plan to visit Facility X and modify and extend our information to assess this currently operating safeguards system.

3.2 ASSESSMENT PROCEDURE
(F. Gilman)

In late 1977, a predecessor to Safeguards System Vulnerability Assessment Methodology (SSVAM), Digraph--Fault-Tree Methodology, was tested on a facility contrived by LLL. The results of the assessment were presented to the NRC and it was then decided to further test and develop the methodology on a real facility. This would serve three purposes: (1) teach LLL personnel about the real world; (2) further develop the LLL methodology; (3) demonstrate the LLL methodology on a facility (Facility X) the NRC was familiar with. It was also decided to break the Facility X assessment into two phases. Phase I would be an assessment using data currently available at the NRC, with no site visit. Phase II would involve site visits and direct interaction with Facility X personnel.

Phase I was started in April, 1978 and completed in December, 1978, exclusive of the report writing. During this period, numerous meetings were held with personnel from NRC Headquarters and Region I. Three major briefings were given during Phase I. These briefings covered data gathering, logic diagrams, and preliminary results. This section describes a few of the accomplishments of SSVAM during the WRJ assessment.

In the application of SSVAM to Facility X, four assumptions were made to define the problem. These assumptions described the adversary we were modeling and are required for any safeguards analysis. The assumptions were the following:

1. The adversary is nonviolent.
2. The adversary has access to the target.
3. The adversary has a container available at the target.
4. The adversary uses only existing doors and windows for his exit.

Assumptions 2, 3, and 4 could easily be removed since only Assumption 1 is basic to SSVAM.

The procedure whereby adversary event sets (AESs) are generated was also formalized and strengthened. The system equations for Facility X were large and complex; however, the AESs were generated and analyzed with SETS. SETS is a large and very powerful computer code that not only solves the system equations, but also performs the qualitative and collusion analysis.[2]

3.2.1 Assessment Results

The specific results of the Facility X assessment are classified; however, a description of the types of results generated is given here. The AESs were generated for three systems: (1) Physical Security, (2) Material Accounting, and (3) the complete Facility X Safeguards Systems. Several event-set subsets were then obtained for each system. These included (1) paths used by the adversary, (2) monitors that must fail for successful diversion, (3) event sets for which monitor failure is forbidden, and (4) single events that fail the Material Accounting System.

A detailed collusion analysis was also done for all three systems. The Facility X personnel who, in collusion, could defeat each of the three systems was determined first. Then, for several sets of colluders, the event sets that they perform to defeat each system were determined. These results were particularly interesting since they combined collusion, random failures, and human error in one set of event-sets. This type of result holds strong promise as a good measure of system effectiveness and will be tested and demonstrated further in the Phase II work.

3.2.2 Concluding Remarks

The assessment of Facility X demonstrated the versatility and usefulness of SSVAM. Much work was accomplished toward a completely formalized and packaged assessment tool. Many interesting and useful results were generated and much insight was gained into what could become measures of system effectiveness. Through the application of SSVAM to Facility X on Phase II, the quantitative measures of system effectivenss will be formalized and demonstrated.

A report on the preliminary results of the Phase I assessment will be issued in early spring of 1979 and the main report will follow shortly thereafter.

3.3 FACILITY X ASSESSMENT USING THE STRUCTURED ASSESSMENT APPROACH (I. Sacks)

3.3.1 Introduction

This section summarizes the results of an assessment of the MC&A system at Facility X, conducted through the use of the SAA methodology (Section 2.3). The analysis emphasized the determination of the vulnerability of the MC&A system to random failures and to deliberately induced system failures (via tampering); vulnerability of collusion was explicitly studied. A complete description of the results and the detailed analysis can be found in Refs. 3 and 4.

The structure of the SAA is such that it requires a number of specific inputs and details about the facility at each stage of the assessment. Such information was either not available to us or not available within the very short time allotted to the assessment of Facility X using the SAA. For this reason, arbitrary assumptions were made about the configuration and operational procedures at the facility. The results of the assessment reflect these assumptions. The results shown in what follows illustrate the capabilities and output that can be obtained from an assessment and should not be construed to describe the vulnerabilities of Facility X.

3.3.2 Background

Two distinct types of monitoring systems were analyzed: short-time systems that are designed to detect an adversary as he is diverting SNM, and long-time systems that are designed to detect material imbalances. We refer to the short-time systems as the Material Containment Monitoring or Material Control Systems and the long-time systems as the Accounting Systems.

There are several key assumptions and limitations to this particular application of the SAA methodology:

1. The assessment is partially based on an existing facility, however, the vulnerabilities which were found reflect the assumptions made and are not representative of the facility.

2. The signal flow structure that ties the monitors to the Physical Security System was not available to the project team. Consequently, the data supplied was enhanced by assumptions concerning transmission lines, maintenance policies, and the like.
3. The response of the Material Containment Monitoring System has been modeled for a nontampering adversary, and the response of the Accounting System has been modeled for a tampering adversary. No analyses were made of (1) the response of the Material Containment Monitoring System to a tempering adversary and (2) the response of the Accounting System to a nontempering adversary.

The allocation of analytical resources to the tampering case for the Accounting System and to the nontampering case for the Material Containment Monitoring System was not arbitrary. The response time from incidence to detection for the Accounting System is on the order of months, while the response time for the Material Containment Monitoring System is on the order of seconds or perhaps minutes. Consequently, plausible scenarios can be generated for a nontampering adversary to evade the Material Containment Monitoring Systems, but is almost impossible to imagine a nontampering adversary winning against the Accounting System. Defeating the Accounting System by its very nature is a tampering act. Consequently, we focused our tampering analysis in the area where it was most needed, and demonstrated the other parts of the analysis where we felt they could provide some insight into the problem.

3.3.3 Assessment Results

The results of the analysis of the Facility X MC&A system have been separated into two distinct portions, that of the Material Containment System and that of the Material Accounting System. The Containment System has been subjected to Levels 1, 2, and 3 of the formal analysis procedure whereas the Accounting System was analyzed by Level 4 only. The results of the assessment are summarized in Table 3-1.

The Levels 1 and 2 conclusions about the Material Containment System were expected because the assessment is being performed on an NRC-licensed facility

TABLE 3-1. Summary of assessment results.

Level	Material Containment Monitoring System	Accounting System
1	There are no uncovered target sets.	NA
2	All sets are protected to the 0.94 assurance level. The system reliability is most dependent on the external electrical power supply.	NA
3	The system reliability is sensitive to ● external power ● internal power tranmission lines ● guard station availability.	NA
4	Partial Analysis: The system is vulnerable to two maintenance men in collusion.	The Accounting System is internally vulnerable to the Nuclear Materials Assistant and any Material Balance Area (MBA) Operator working in collusion. Under certain conditions it is vulnerable to the MBA-2 Operator or the Analytical Laboratory Operator acting alone.

that has been subjected to in-depth design reviews and I & E inspections. The Level 4 conclusion indicates a vulnerability to the two maintenance men in collusion with the diverter. It therefore provides some insight into the details of vulnerability of the facility, but the reader is cautioned that these conclusions depend on assumptions made in the analysis.

The Level 4 conclusion about the vulnerability of the Accounting System to the MBA-2 Operator rests on the nondetection of abnormally large account corrections by the NMA or by active collusion with the NMA. The vulnerability to the Analytical Laboratory Operator depends on the same nondetections by both the MBA-2 Operator and the NMA. We have not credited the NRC Inventory Monitoring System with any detection performance due to our lack of understanding of this system. Nonetheless, the internal plant detection mechanisms appear to be very vulnerable to NMA and any MBA Operator collusion.

The Material Containment System and the Material Accounting system should not be considered as separate systems. That is, vulnerability in one system may be covered by the other system. For the facility being assessed, the analysis found that the discovered accounting system vulnerability would be covered by the Material Containment System.

We have not analyzed any interactions between the facility physical protection force and the MBA Operators. Such interactions possibly could negate the dual protection systems.

3.3.4 Assessment of Material Containment Monitoring System

The Material Containment Monitoring System at Facility X was analyzed by preproduction versions of the SAA computer codes for Levels 1, 2, and 3. The results are conditioned on many assumptions about the detailed utility and signal flow structures and as such may be at variance with the actual Facility X system.

The analysis of the Material Containment Monitoring System was conducted in three steps, corresponding to Levels 1, 2, and 3 described above. The system analysis is summarized in Fig. 3-1. The major inputs are area adjacency, component descriptions, information flow, and utility distribution information. Area adjacency information describes the physical connectivity of rooms, portals, fences, and the like. Component descriptions include reliability data for all components including utilities, monitors, and transmission lines as well as field-of-view data for the monitors. Information flow describes the connections from all monitors through transmission components to the security centers. Finally, utility distribution input describes utility components and connectivity of all utility systems that support the monitors and information flow components.

The major outputs of the system analysis are distinguished by four levels of results, each higher level pertaining to more detailed and complex questions about the Material Control Monitoring System. Results associated with each of the levels are discussed below:

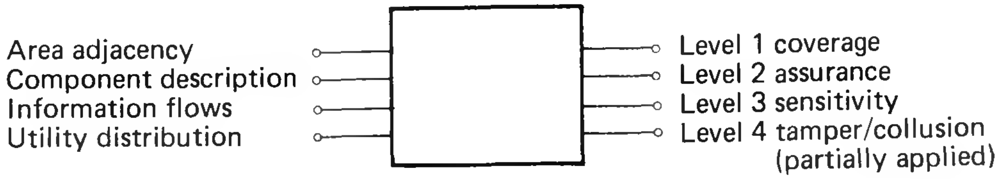


FIG. 3-1. Material Containment System model.

Level 1: All potential diversion paths were found to be covered by at least one material containment monitor (in fact, all were covered by at least four monitors). A "dominance" argument was applied to identify 49 essential monitor target sets (MTSs) which covered all physical diversion paths. An MTS is simply a diversion path defined in terms of the monitors encountered along the path. The dominance concept allowed the reduction from approximately 950 physical paths to 49 essential MTSs. Coverage of these 49 MTSs ensures the complete coverage of all 950 diversion paths.

Level 2: The Level 2 result is that the system is protected to the 0.94 assurance level. Because the system reliability is dominated by the electrical system, all MTSs have close to the same reliability. In effect, the unreliability of the electrical system has reduced the 49 MTSs of Level 1 to a single MTS in Level 2.

Level 3 Sensitivity Analysis: The key Level 3 result is that the system reliability is sensitive to the availability of the external ac power line, the internal power supply lines, and the guard stations. The sensitivity to the external and internal power supply lines is logical since the electrical system dominates the system reliability calculations. The availabilities of the guard stations are sensitive to the electrical supply due to an assumption that each has a single input power line.

Level 4 Collusion Analysis: An informal collusion analysis shows that two maintenance men in collusion can defeat the system. To limit the amount of analysis performed with the prototype computer codes to a reasonable level, the Level 4 computer code was not used for collusion analysis. Instead, collusion among the maintenance men was modeled by assuming that several maintenance functions were represented as a single node; e.g., that a single colluding group had access to all the components serviced by several people. Grouping two maintenance functions was sufficient to allow access to all the monitors in a number of MTSs. Thus, two maintenance men in collusion can defeat the Material Containment Monitoring System. Scenarios that will defeat the Material Control System can be constructed from the results of this collusion analysis. One such scenario involves a diverter (insider or possibly outsider) waiting for the loss of the external power source. When this occurs, all the monitors in several target sets fail because two maintenance men, in collusion with the diverter, have tampered with the interal battery packs. Interior emergency lighting also fails for the same reason. The diverter can then remove material without the possibility of detection by the Material Control System.

Level 4 Assessment of the Accounting System: The Accounting System at Facility X has been analyzed by a preproduction version of the Level 4 SAA computer code. The results presented within this report are conditioned on many assumptions about the detailed structure and internal detection mechanisms of the system and as such may be at variance with the actual Facility X system.

The analysis of the Accounting System has been conducted in two steps. The first of these addresses the following question:

> Is it possible for any individual or combination of individuals to negate the basic Accounting System detection mechanisms? These include Book Balance (Assets = Liabilities and Credits = Debits), subsidiary/general ledger checks, and account audits against source data.

The second stage in the analysis addresses the issue of whether the employees at the facility can use false or falsified information forms to cause fictitious account entries so as to mask a diversion.

The Accounting System is viewed as a black box as shown in Fig. 3-2. The inputs to this system are the workers at the plant; the Nuclear Materials Assistant (NMA), the Item Control Area-1 Operator, I10, the Material Balance Area-2 Operator, M20, and the ICA-3 Operator, I30. The outputs of this system are the detection mechanism outputs, the book balance, physical inventory difference, and the NRC inventory difference.

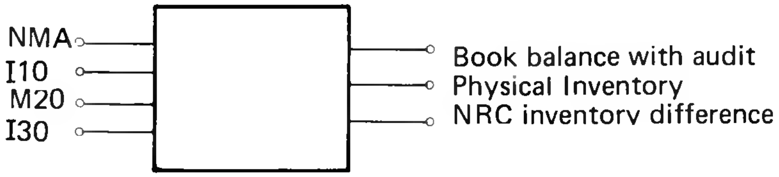


FIG. 3-2. Accounting System model.

The Accounting System has been analyzed by Level 4 of the SAA with respect to both the basic account/detection stage and the information flow stage. We found the following:

> The Nuclear Materials Assistant in collusion with any MBA (or ICA) Operator can defeat the Accounting System audit and book balance detection systems.

This conclusion is shown as a truth table in Fig. 3-3. This truth table presents the Accounting System vulnerability for all workers at the facility. It shows that the NMA and any other MBA Operator can cause the "books to balance" without any chance of a discrepancy check by an audit independent of the actual material situation.

NMA	I10	M20	I30	Book balance & audit
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

System vulnerability

FIG. 3-3. Truth table for Level 1 Accounting System vulnerability.

The second stage of the assessment of Accounting System vulnerability considers the deliberate misuse of the internal information flows. The problem analyzed here is a more difficult test for the Accounting System to pass. The goal of this analysis is to determine if the MBA (or ICA) Operators can send erroneous or deliberately falsified Material Transfer Tickets to the NMA to "maintain" a book balance.

The result of the stage two analysis of the Accounting System shows that it is vulnerable to the following:

1. the MBA-2 Operator alone;
2. the Analytical Laboratory Operator alone; and
3. the NMA in collusion with any other MBA (or ICA) Operator.

The results of the second stage of the Level 4 analysis on the Accounting System are given in the truth table of Fig. 3-4.

NMA	I10	M20	I30	ALO	Book balance	
—[a]	—[a]	—[a]	—[a]	1	1	
0	0	0	0	—[a]	0	
0	0	0	1		0	
0	0	1	0		1	System vulnerability
0	0	1	1		1	System vulnerability
0	1	0	0		0	
0	1	0	1		0	
0	1	1	0		1	System vulnerability
0	1	1	1		1	System vulnerability
1	0	0	0		0	
1	0	0	1		1	
1	0	1	0		1	
1	0	1	1		1	
1	1	0	0		1	System vulnerability
1	1	0	1		1	
1	1	1	0		1	
1	1	1	1		1	

[a] Irrelevant

FIG. 3-4. Complete truth table for Accounting System vulnerability.

The second stage of the Accounting System analysis is a more difficult test for a system to pass. In the Facility X system, the only possibilities for the input of false data into the system are from the following:

1. a S/R difference correction,
2. a Lagoon Loss* correction, or
3. a correction for material unaccounted for (MUF).

All these data are initiated by the MBA-2 Operator. The Shipper/Receiver Difference correction is the only data input not checked against process limits. That is, the MUF correction would have to be less than LEMUF in order not to alert the Nuclear Materials Assistant and the Lagoon Loss would have to be less than the expected process losses. The NMA could, however, be simply using false Analytical Laboratory results given to him by the Analytical Laboratory Operator. If the NMA was in collusion with the MBA-2 Operator, no in-plant detection of excessive MUF or Lagoon Losses would be made.

Thus, the complete solution for the Accounting System vulnerability is as follows:

```
NMA with ICA-1 Operator
         MBA-2 Operator
         ICA-3 Operator
               OR
MBA-2 Operator with MUF < LEMUF OR
                    Lagoon Loss < Expected Loss OR
                    S/R Difference < Expected S/R Difference
               OR
Analytical Laboratory Operator with MUF < LEMUF OR
                                    Lagoon Loss < Expected Loss OR
                                    S/R Difference < Expected S/R Difference
```

3.3.5 Concluding Remarks

The resources necessary to perform this assessment were approximately 360 man-hours and approximately $2000 computer time.

*This does not mean that these individuals can successfully divert material but only prevent detection of a diversion by the Accounting System. They must still defeat the Material Containment Monitoring System.

These numbers do not include the documenting assessment results or the gathering of the data in the License Submittal Document. This assessment was performed using preproduction versions of subroutines of the Structured Assessment Analysis code.

3.4 MONITOR CHARACTERIZATION FOR FACILITY X
(D. Dunn, LLL, and D. Richardson et al., SRI)

The monitor* characterization work for the Facility X assessment is near completion. The objectives of the study were twofold: (1) to characterize the personnel intrusion and SNM detector monitors listed in Table 3-2, and (2) to develop a methodology for comparing these monitors on the basis of their susceptibility to adversary action. This study was done under contractual support by SRI, International, and final documentation is in preparation.[5]

Each monitor in Table 3-2 was examined to determine its principle of operation, performance, reliability, and vulnerability using available analytical and experimental data. The gathering and screening of information by SRI required considerable effort because much of the equipment was old and original sources of information were missing or difficult to locate. This information as it became available was incorporated by LLL into the logic model (event tree) for Facility X as part of the assessment procedure. In addition, SRI identified other parameters (e.g., installation variables and operational considerations) that could affect the performance of the monitors.

Detection monitors are designed to operate effectively under normal environmental and adversary-related conditions, when recommended installation and operational procedures are followed. Within a broad range of conditions probability of detection, P_d, approaches unity. Conversely, under certain other environmental conditions or against a few adversary techniques, P_d is essentially zero. For the typical physical security detection monitor, P_d is significantly different from either zero or one only for a small number of conditions and adversary actions. A list of the environmental parameters and adversary actions or characteristics that degrade monitor performance comprised the essential characterization by SRI for the vulnerability analysis. The

*Physical security monitors.

TABLE 3-2. Monitor list.

Type	Monitor	SRI comments
Perimeter Infrared (IR)	Arrowhead 55000/56000	Model number supplied (5500) refers to the series of numbers designating the transmitting and receiving components while 56000 refers to a post enclosure which holds several transmitting and receiving components.
Indoor Infrared (IR)	Mosler Infraguard 50	Monitor substituted for Solco microwave sensor.
SNM detector	Texas Nuclear 2651 or 2652	Texas Nuclear division of Ramsey Engineering acquired the survey meter portion of Nuclear Chicago. Original model specified (2650) refers to the meter without probe. Probe in the 2652 model contains a thinner window for better detection of alpha particles than probe in 2651 model.
Metal detector	Solco, Electro Search Model VII	Same as previously listed except model number is Roman numeral instead of Arabic.
Balanced Magnetic Switch	Johnson Controls Model DG 1002	Same as previously listed except Johnson Service Company became Johnson Controls, Inc.
Microwave	Johnson Controls Model GI or AG-1007	Johnson Service became Johnson Controls. Before the original list of monitors was completed, SRI persuaded LLL to change a "G7B" designation to a "G1B" designation because it was believed that no model 7 existed. However, since then we have learned that AG-1007 is colloquially referred to as G7, and that this series has two modifications (-A and -B). The number of modifications to the G1 is unknown. Particular model and modification will affect performance.
Ultrasonic	Advisor III	LLL-supplied model number 3AV103, was corrected to Model III; first digit refers to the monitor series but a Roman numeral is used. AV103 refers to the identification of the control unit used with this sensor system.

events degrading monitor performance (reducing P_d to significantly less than 1.0) were divided into two categories: (1) environmental parameters, and (2) adversary actions or characteristics. Each monitor was examined in this fashion and where available the conclusions were qualified with results from test data.

With respect to reliability considerations, SRI and LLL determined that equipment failure was a significantly less critical parameter for assessing monitor vulnerability than environmental parameters and adversary actions. The rationale for this conclusion was that all monitors except the metal and SNM detectors were designed to fail predominantly in the alarm mode. The immediate implication is that the adversary would derive no additional benefit from equipment failures since either equipment failure or a bona fide alarm would initiate the same response by security forces. The above conclusions coupled with very limited information on failure data and unavailability of detailed schematic diagrams led us to consider the reliability question as one primarily dependent on the response of a facility to an alarm. The final document on our monitor characterization work will contain, however, reliability estimates based on engineering judgments by individuals with experience in using the particular monitors.

The methodology for rating monitors on the basis of their susceptibility to adversary action will be reported in the next quarterly progress report.

REFERENCES: CHAPTER 3

1. I. J. Sacks et al., "Material Control System Design: Test Bed Nitrate Storage Area," January through April, 1977, UCID-17525-77-3 (May, 1978).

**2. R. B. Worrell, Set Equation Transformation System (SETS), SLA-73---0028A, Sandia Laboratories, Albuquerque, New Mexico (May, 1974).

*3. A. A. Parziale, I. J. Sacks, T. R. Rice, and S. L. Derby, The Structured Assessment Analysis of Facility X, NUREG/CR-0791, UCRL-52765, Volume I--Executive Summary, Lawrence Livermore Laboratory (November, 1979).

*4. A. A. Parziale, I. J. Sacks, T. R. Rice, and S. L. Derby, The Assessment of Facility X, NUREĞ/CR-0791, UCRL-52765, Volume II--Detailed Assessment Results and License Submittal Document, Lawrence Livermore Laboratory (November, 1979).

**5. David Y. Richardson et al., "Safeguards Monitor Characterization and Vulnerability Methodology Development," Final Report 7772-79-FR-10, prepared under contract for the Lawrence Livermore Laboratory by SRI International., January 1979.

*Available for purchase from the NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, and the National Technical Information Service, Springfield, VA 22161.

**Available for purchase from the National Technical Information Service.

4.0 AGGREGATED SYSTEMS MODEL

(R. Al-Ayat, LLL, S. Weissenberger, LLL, and B. Judd, ADA)

4.1 INTRODUCTION

This section briefly describes the Aggregated Systems Model (ASM) and summarizes the progress accomplished in this quarter. A report by Applied Decisions Analysis gives a detailed description of the model and its use.[1] The work was also reported in a paper by Judd and Weissenberger.[2]

The ASM is an evaluation tool designed to aid the Nuclear Regulatory Commission (NRC) in setting safeguards criteria. The analysis needed to set safeguards criteria is different from that of the detailed assessment (Section 2) of a given facility. In setting safeguards criteria, one must trade off the benefits of additional safeguards (i.e., reduced risk) with their cost. This trade-off is usually not relevant when assessing whether a particular facility meets a prescribed criterion.

Some of the techniques discussed here are also useful for evaluating security at a given facility. It can provide a "first cut" assessment of safeguards system performance, the result of which can guide the detailed assessment.

This summary describes the ASM; discusses a safeguards criteria setting; and points out additional areas for development.

4.2 DESCRIPTION OF THE AGGREGATED SYSTEMS MODEL

This section describes the major elements of the ASM illustrated in Fig. 4-1: (1) Diversion Model, (2) Consequence Model, and (3) Safeguards Technology Model. The Diversion Model contains data that characterize the adversary, the type of attempt, and the response of the system to the attempt. The name Diversion Model is used to mean the combination of the Adversary and the Facility Submodels. If a diversion attempt is successful, the Public

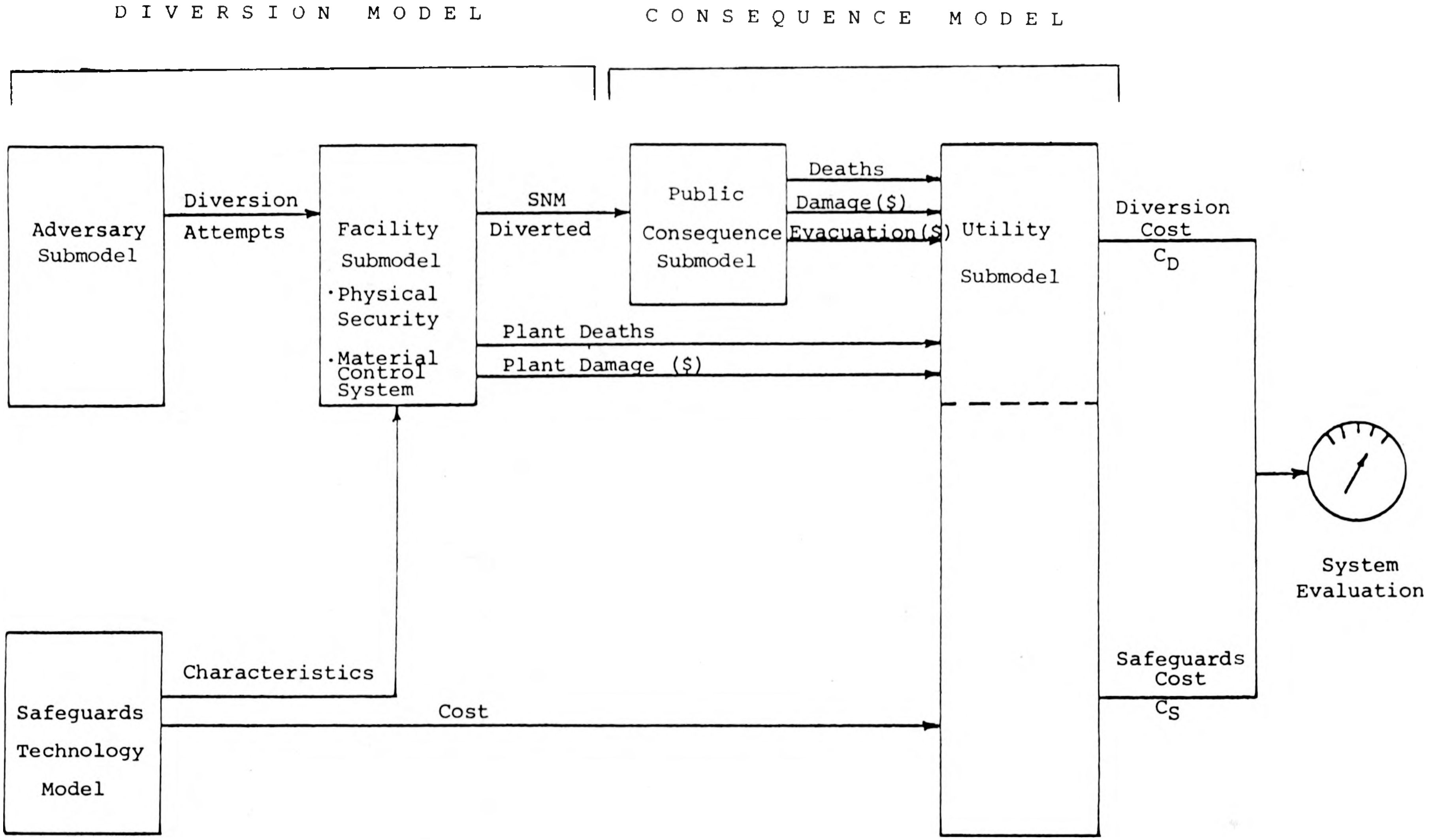
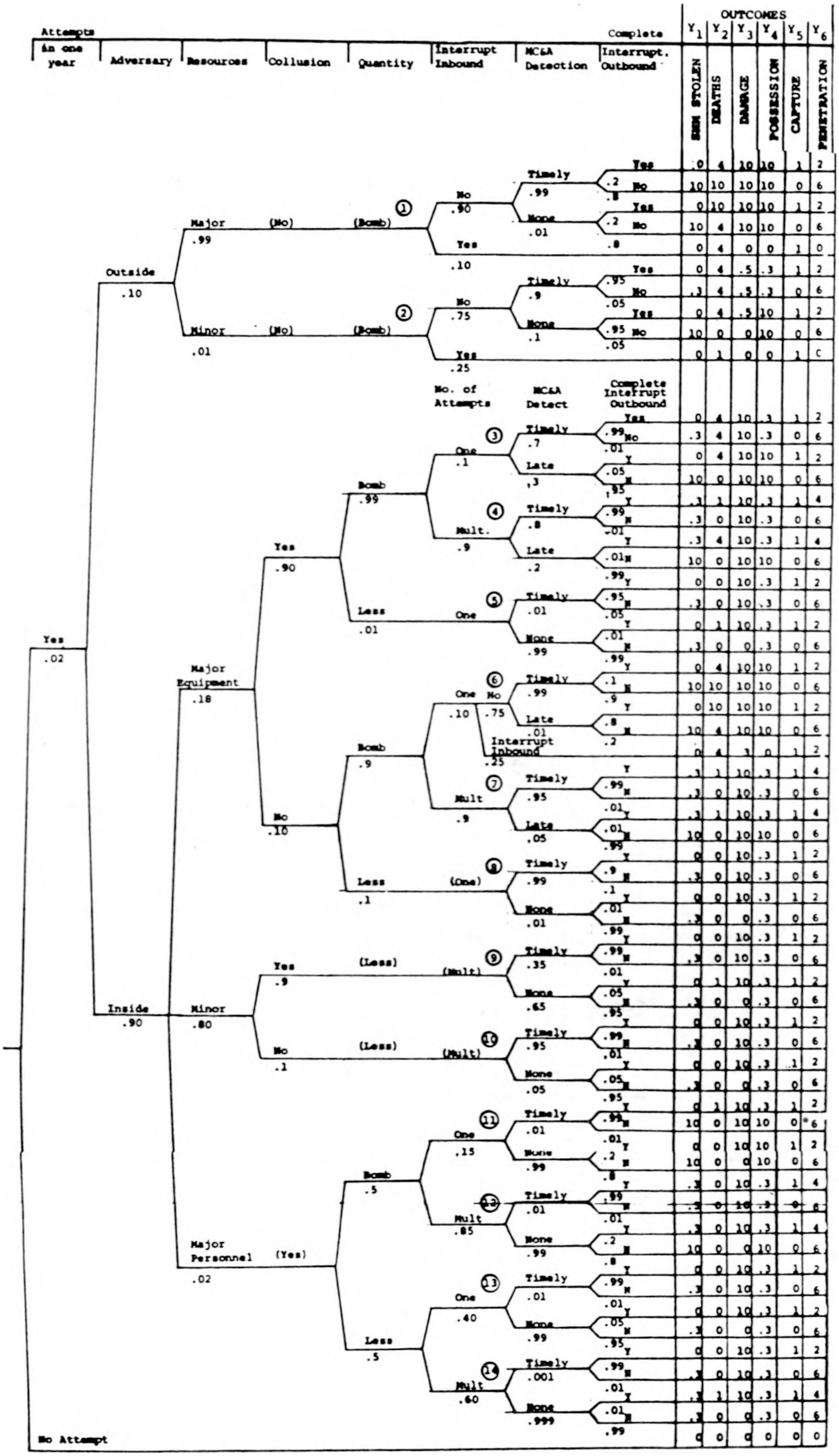


FIG. 4-1. Aggregated Systems Model overview.

Consequence Submodel describes possible malevolent uses of the stolen material and the consequences of diversion, and the Utility Submodel assigns values to all possible outcomes. The Consequence Model is the combination of both the Public Consequence and the Utility Submodels. While the Diversion and the Consequence Models quantify diversion risk, the Safeguards Technology Model quantifies "economic" costs of the safeguards system. The meter at the right of Fig. 4-1 implies a combined evaluation for all quantified factors.

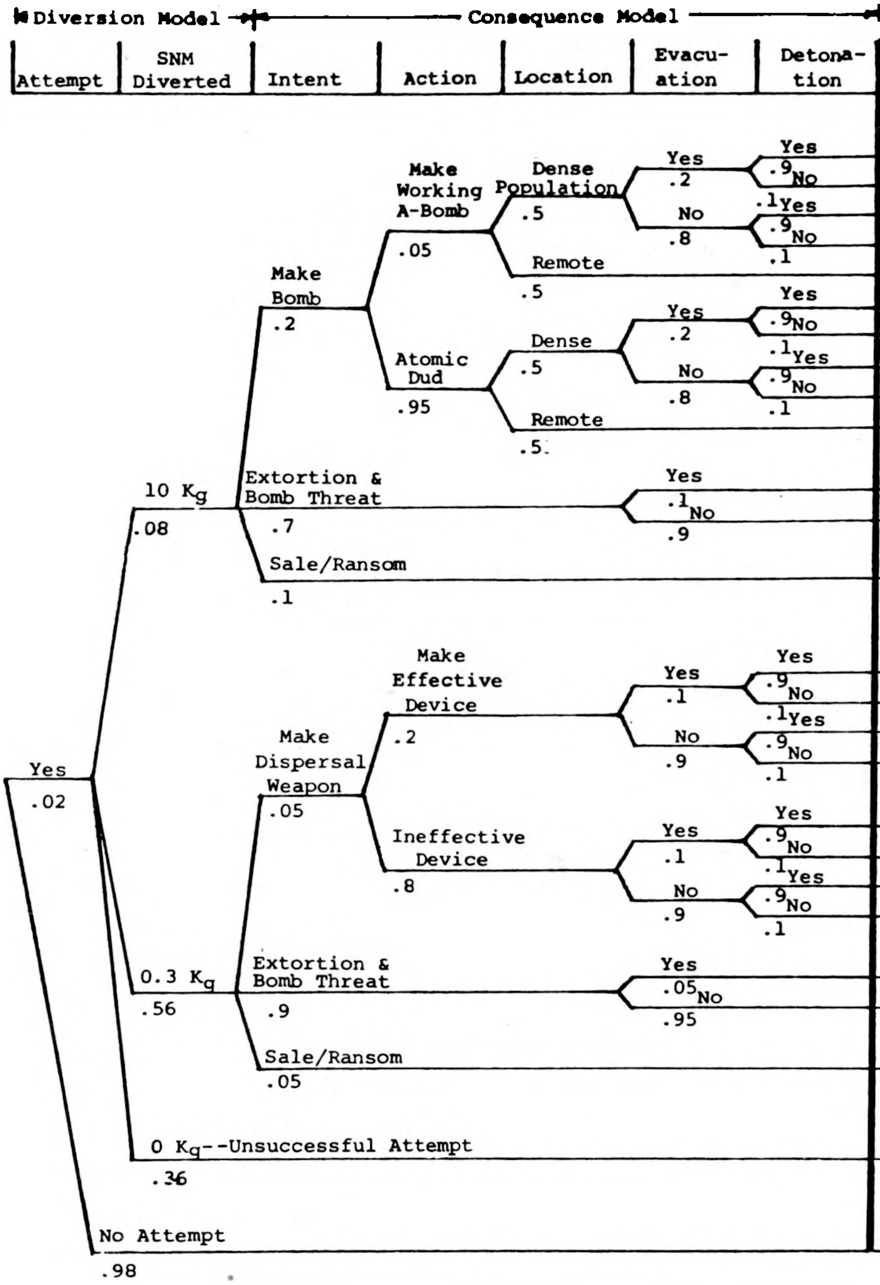
To use this evaluation framework, the policymaker chooses safeguards components--level of physical security and material control performance in a facility--so as to maximize the utility reading on the meter:

- Diversion Model: The Diversion Model consists of a probability tree that enumerates the set of events that could result from diversion events: whether there will be an attempt, adversary characteristics, adversary resources, the possibility of collusion, the target quantity of SNM, and whether the attempt is detected or interrupted. These six events define 14 types of attempts, each of which defines an adversary sequence. Figure 4-2 is an illustrative Diversion Model for a hypothetical commercial nuclear facility. Outcomes of a diversion attempt are evaluated according to the following six criteria: (1) quantity of SNM stolen, (2) fatalities among plant personnel, (3) damage to plant plus shutdown cost, (4) maximum amount of material ever in the possession of the adversary, (5) adversary capture, and (6) degree of penetration within the plant. One output of the Diversion Model is the expected value for each of these six criteria, which is easily computed by "rolling back" the probability tree.
- Consequence Model: Like the Diversion Model, the Consequence Model is a probability tree. The following uncertain events are considered here: the intended use of the diverted material; the success in making the appropriate nuclear device; the location of the resulting nuclear-related incidents; whether the local population is evacuated; and whether there is a detonation of the device. Figure 4-3 is an example of a Consequence Model. It also includes a summary of the Diversion Model shown in Fig. 4-2. The illustrative consequences of diversions are evaluated in terms of public fatalities and dollar damages, evacuation costs and deaths and damages at the plant.



OUTCOMES Y_1 SNM STOLEN	Y_2 DEATHS	Y_3 DAMAGE	Y_4 POSSESSION	Y_5 CAPTURE	Y_6 PENETRATION
0	4	10	10	1	2
10	10	10	10	0	6
0	10	10	10	1	2
10	4	10	10	0	6
0	4	0	0	1	0
0	4	.5	.3	1	2
.3	4	.5	.3	0	6
0	4	.5	10	1	2
10	0	0	10	0	6
0	1	0	0	1	C
0	4	10	.3	1	2
.3	4	10	.3	0	6
0	4	10	10	1	2
10	0	10	10	0	6
.3	1	10	.3	1	4
.3	0	10	.3	0	6
.3	4	10	.3	1	4
10	0	10	10	0	6
0	0	10	.3	1	2
.3	0	10	.3	0	6
0	1	10	.3	1	2
.3	0	0	.3	0	6
0	4	10	10	1	2
10	10	10	10	0	6
0	10	10	10	1	2
10	4	10	10	0	6
0	4	1	0	1	2
.3	1	10	.3	1	4
.3	0	10	.3	0	6
.3	1	10	.3	1	4
10	0	10	10	0	6
0	0	10	.3	1	2
.3	0	10	.3	0	6
0	0	10	.3	1	2
.3	0	0	.3	0	6
0	0	10	.3	1	2
.3	0	10	.3	0	6
0	1	10	.3	1	2
.3	0	0	.3	0	6
0	0	10	.3	1	2
.3	0	10	.3	0	6
0	0	10	.3	1	2
.3	0	0	.3	0	6
0	1	10	.3	1	2
10	0	10	10	0	*6
0	0	10	10	1	2
10	0	0	10	0	6
.3	0	10	.3	1	4
~~.3~~	~~0~~	~~10~~	~~.3~~	~~0~~	~~6~~
.3	0	10	.3	1	4
10	0	0	10	0	6
0	0	10	.3	1	2
.3	0	10	.3	0	6
0	0	10	.3	1	2
.3	0	0	.3	0	6
0	0	10	.3	1	2
.3	0	10	.3	0	6
.3	1	10	.3	1	4
.3	0	0	.3	0	6
0	0	0	0	0	0

FIG. 4-2. Illustrative diversion model.



Plant		Public		
Deaths	Dam.	Deaths	Dam.	Evac
	$\$10^6$		$\$10^6$	$\$10^6$
5	9	2000	4000	200
5	9	100	0	200
5	9	20000	4000	0
5	9	0	0	0
5	9	10	10	0
5	9	100	10	200
5	9	100	0	200
5	9	100	10	0
5	9	0	0	0
5	9	0	10	0
5	9	100	100	200
5	9	0	100	0
5	9	0	10	0
.2	2	100	100	50
.2	2	100	0	50
.2	2	100	100	0
.2	2	0	0	0
.2	2	100	1	50
.2	2	100	0	50
.2	2	10	1	0
.2	2	0	0	0
.2	2	100	50	50
.2	2	0	0	0
.2	2	0	10	0
.3	10	0	0	0
0	0	0	0	0

FIG. 4-3. Illustrative diversion/consequence model.

- To make an explicit trade-off between safeguards cost and diversion risk, one needs to measure the consequences in common units. The common units selected is dollars, as it provides a familiar scale. The trade-off value selected is $\$10^6$/death and $\$10^5$/ injury. This valuation is equivalent to saying that society is willing to pay $\$10^6$ to prevent the loss of one statistical life and $\$10^5$ to prevent one statistical injury. Obviously, changing the trade-off value can affect the optimal level of safeguards.
- Safeguards Technology Model: This element describes safeguards components that may be incorporated in a safeguards system design. Seventeen Material Control and Accounting (MC&A) and three Physical Security (PS) components were chosen for the analyses. A component performance is measured in terms of its ability to detect an interrupt in an attempt to divert SNM. The probabilities of detection or interruption for the various components were assigned subjectively. General Electric provided capital costs and operating cost for the chosen components. These costs were combined into a single annual cost using a fixed charge rate of 20 percent.

A simple model to determine overall system performance based on component performance data was developed. This model provided the relationship necessary for balancing safeguards system cost (C_S) with the benefits measured in terms of the overall system performance.

4.3 ILLUSTRATIVE SAFEGUARDS CRITERIA SETTING: AN EXAMPLE

The ASM described above is used here to demonstrate its ability in setting safeguards criteria. As a typical criterion we consider determining an optimal level of the probability (P_D) that the MC&A system will detect a particular adversary. Let us assume that the objective of the safeguards decision-maker is to minimize the sum of the annual cost of diversion C_D and the cost of plant safeguards C_S. Setting the criterion is demonstrated graphically in Fig. 4-4. MC&A system performance is measured by the probability of detecting an attempt to divert nuclear material by a plant

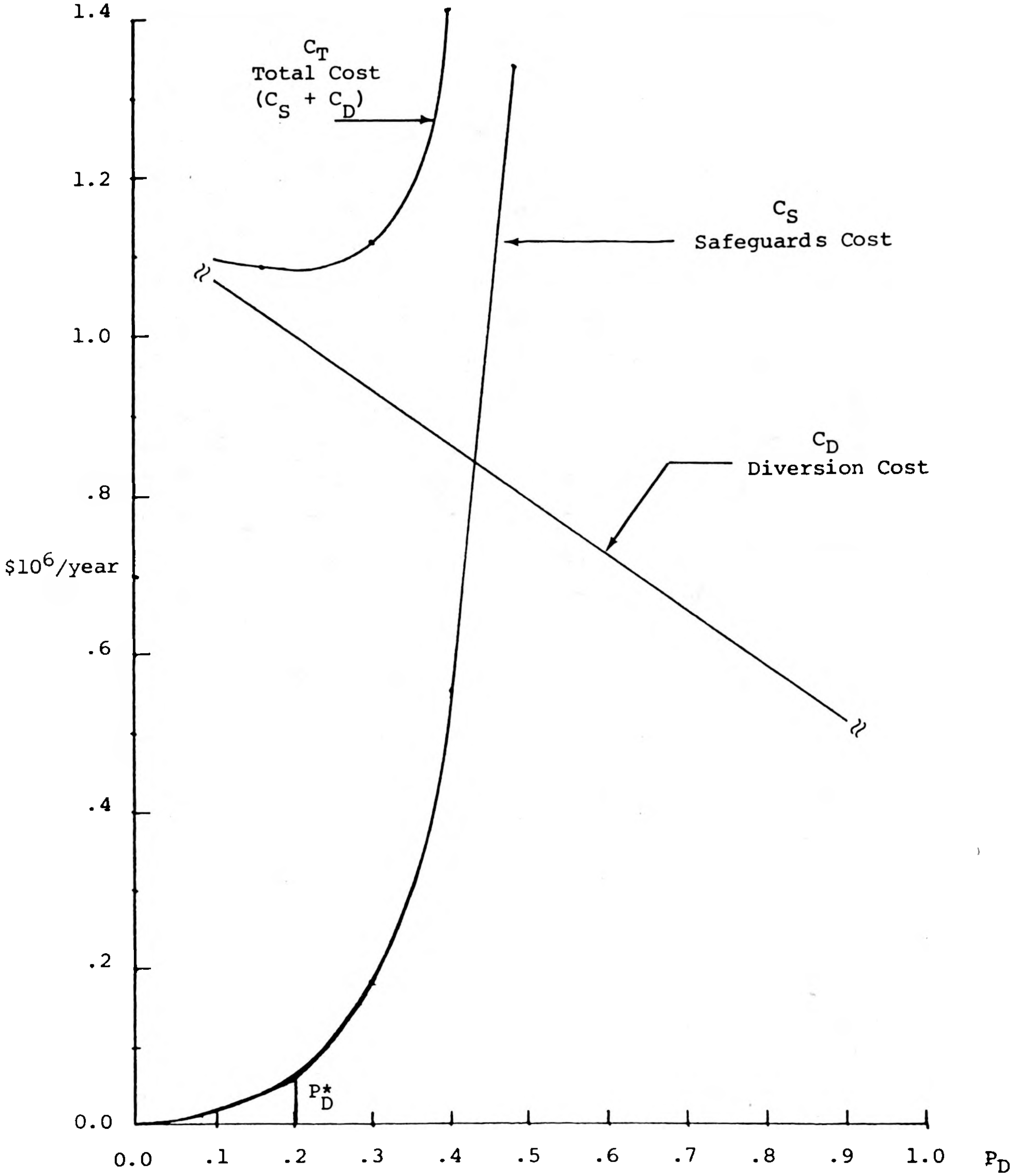


FIG. 4-4. Evaluation of MC&A system performance.

employee. Moving to the right in Fig. 4-4 means improving the MC&A system performance. The safeguards cost (C_S) and diversion cost (C_D) are measured on the vertical axis. The cost (C_S) of increasing MC&A system performance rises rapidly, while diversion cost (C_D) decreases as the MC&A system performance is improved. The sum of the safeguards and diversion costs C_T attains its minimum value at P_D^*. A decision-maker would then choose that level P_D^* of MC&A performance with the lowest total cost. Obviously, a higher performance level is excessively expensive and a lower level allows excess risk of diversion.

4.4 FUTURE EFFORTS

The Aggregate System Model presented above provides a quantitative tool for setting safeguards criteria. The analysis, however, highlighted several areas where refining these models could substantially improve the safeguards decision-making process. Refined models of safeguards system costs and associated performance are the most noticeable need. The linkage between the Diversion Model and the Consequence Models should also be refined. Another research need is establishing formal procedures for aggregating detailed probablistic information--such as those produced by the detailed assessment procedures (Section 2) in a form that can be used by the aggregated models presented here and hence by the decision-makers.

REFERENCES: CHAPTER 4.

**1. "Methodology and Preliminary Models for Analyzing Nuclear Safeguards Decisions," UCRL-13931, Applied Decision Analysis, Inc., Menlo Park, California (November, 1978).

**2. B. R. Judd and S. Weissenberger, "A Systematic Approach to Nuclear Safeguards Decision-Making," UCRL-81977, Lawrence Livermore Laboratory (February 6, 1978).

**Available for purchase from the National Technical Information Service, Springfield, VA 22161

5.0 ADVERSARY MODELING
(R. Schechter)

5.1 INTRODUCTION

A fundamental, but very difficult aspect of safeguards research is the characterization of the potential adversary threat to nuclear facilities. The basic goals of this endeavor are as follows:

1. To define a comprehensive set of adversary threats in terms which will allow for the evaluation of system vulnerabilities*;
2. To estimate the expected frequency of each type of threat; and
3. To assess the effectiveness of potential deterrence measures.

Although these goals are difficult to fulfill in an objective, clearly defensible manner, they are vital to many of the value-impact considerations that the Aggregated Systems Model (ASM) is intended to evaluate.

The following summaries illustrate two methodologies with which our subcontractors have approached the preceding goals. The first methodology involves the generation of different types of adversary threats on the basis of "attribute combinations," so as to allow for the systematic elicitation of frequency estimates from authorities deemed knowledgeable about potential adversaries to nuclear safeguards. The second methodology involves the collection of historical data from analogous criminal activities, which can be used to guide expert intuition on the issues of attempt frequencies and deterrence measures, in lieu of a substantive data base on actual safeguards incidents.

*This evaluation could be done using either the Facility Submodel of the ASM, or a detailed assessment plan such as the Structured Assessment Approach or the Safeguards System Vulnerability Assessment Methodology.

5.2 METHODOLOGY I[1]

The major purpose of this study was to develop a preliminary modeling structure to assist experts in describing, in quantitative form, their judgments about the characteristics of potential adversaries of Nuclear Material Safeguards (NMS) Systems. The effort began with the systematic characterization of the various possible adversaries using eight attributes: Motivation, NMS System Information, Technical Information, Consequence Information, Processing Capability, General Resources, Self-Risk Attitude, and Other's Risk Attitude. Four possible levels were defined for the first attribute, and two possible levels for each of the other attributes.

By using this structure, any particular adversary can be described by specifying levels for each of the eight attributes. For example, one possible adversary would have financial gain as his motive; high NMS System, technical and consequences information; high processing capability, and general resources, and a risk-seeking attitude toward both himself and others. There are 512 possible types of adversaries, each corresponding to a different combination of eight attribute levels. Of this total, 290 types were excluded from further consideration, on the grounds that they represented unlikely combinations of attribute levels.

The remaining 222 combinations were aggregated into 19 adversary "archetypes," each of which poses a distinctly different type of threat to the system. Each archetype was given a descriptive title, such as "Uninformed Outsider," "Disgruntled Employee," "High-Level Embezzling Group," and "Terrorist Group."

A linear programming algorithm was developed and programmed for computer use to take as input estimated probabilities of different levels for some of the attributes. This algorithm computes bounds imposed by the partial information on possible probabilities of attempts for each of the archetypes. A questionnaire and supporting written material were developed to elicit probability information from experts. Three members of this project were used as subjects in a trial run of the methodology. The wide divergence of judgment among these individuals raises doubts as to whether enough agreement can be reached among different respondents to obtain archetype probabilities that can defensibly be used in further analysis of NMS Systems.

5.3 METHODOLOGY II[2]

This study was intended to aid in the evaluation of potential threats to nuclear safeguards, through the statistical analysis of criminal records on analogous activities. To cover a broad range of both insider and outsider threats, three types of data were collected: (1) FBI statistics on banking crime, as well as 880 detailed histories of bank fraud and embezzlement (BF&E) cases involving over $10,000, obtained from the Federal Deposit Insurance Corporation (FDIC); (2) data on 190 aircraft hijackings from the files of the Federal Aviation Administration (FAA); and (3) case histories obtained from the files of the CIA and RAND Corporation on 249 terrorist incidents in which hostages were seized.

Analysis of the banking data indicates that theft by insiders accounts for annual losses roughly six times the magnitude of those sustained from outsiders. Surprisingly, high-ranking managers were found to pose the greatest insider threat, with presidents and directors accounting for full 32 percent of all BF&E cases of over $10,000. Roughly one-fourth of all BF&E cases studied involved conspiracy, with group size ranging between two and twenty. Fully 57 percent of these conspiracies included a bank president or director. The incidents which involved conspiracy were more successful than those that did not, in terms of both amount stolen and period concealed. The incidents of such cases have been growing rapidly over the past decade. Finally, a statistical regression analysis on BF&E cases revealed that routine bank examinations have a significant deterrence effect, as do higher banking salaries.

The FAA data were reviewed to assess the effectiveness of various deterrence measures for aircraft hijackings. As might be expected, the predicted attempt frequency is highly sensitive to the proportion of recent successful incidents. The predicted attempt frequency decreased with increasing mean length of prison sentence for perpetrators as well as with decreasing variability in sentence length. The number of hijackings has decreased dramatically during the period since mechanical screening devices were installed at U.S. airports. Approximately two-thirds of this decrease is attributable to the deterrence effects of the screening devices themselves, while one-third is due to the effect of increasing likelihoods of failure and lengthy prison sentence.

Finally, the analysis of terrorist events involving the seizure of hostages indicates that their frequency is positively related to the amount of media coverage that such incidents received recently. This finding lends credence to the belief that terrorist groups are reinforced by publicity, which enables them to disseminate their message. Similarly, a significant "contagion effect" was noted, whereby the predicted frequency of events is positively related to the frequency of such events.

5.4 CONCLUDING REMARKS

The two studies outlined above represent the initial results of our continuing effort to characterize potential adversaries of nuclear safeguards. While the elicitation of expert opinion may lead to widely divergent estimates among respondents, we are hopeful that future work in this area will at least provide a useful framework in which safeguards decisionmakers can systematically explore various assumptions inherent in their policy recommendations. Such a framework may serve to pinpoint the sources of disagreement between policymakers, and thus focus their debate accordingly.

The analysis of data from analogous criminal activities has produced some surprising results. We feel these results are of profound significance to the protection of nuclear materials. This effort is continuing with the collection of information on securities fraud, computer systems abuse, and thefts from drug manufacturers and distributors.

REFERENCES: CHAPTER 5

1. C. W. Kirkwood and S.M. Pollock, "Methodology for Characterizing Potential Adversaries of Nuclear Material Safeguards Systems," Woodward-Clyde Consultants, San Francisco, UCRL-13928 (November, 1978).
2. J. M. Heineke et al., "Adversary Modeling: An Analysis of Criminal Activities Analogous to Potential Threats to Nuclear Safeguard Systems," UCRL-13940 (December, 1978).

6.0 COMPONENTS PERFORMANCE

(D. Dunn, J. Candy, and R. Rozsa)

6.1 INTRODUCTION

During this reporting period, the Safeguards Signal Processing Task group contributed to the Material Control and Accounting program in the following areas:

1. Chemical process model development,
2. Material estimator/detector model development, and
3. Monitor (physical security) characterization for the Facility X assessment.

Section 6.2 provides a brief synopsis of the DYNSYL computer code, a general-purpose dynamic simulator for chemical processes primarily related to the nuclear fuel cycle. It incorporates, among other things, a library of mathematical models for selected chemical unit operations. Section 6.3 describes some modeling results for a plutonium evaporator/concentrator unit operation that will be incorporated into DYNSYL. Section 6.4 presents some results for a material estimator for the evaporator/concentrator based on a Kalman filter formulation. Emphasis is on the application of an estimator for material accounting and for studying material diversion scenarios. The above work represents a portion of the computational tools being developed by Lawrence Livermore Laboratory (LLL) for material control assessment and design of process monitors. An overview of these tools is provided in Ref. 1.

6.2 DYNSYL DEVELOPMENT

A preliminary version of DYNSYL, a computer code for simulating the dynamics of chemical processing operations such as the PUREX process, was completed and documented during this reporting period.[1,2]

The DYNSYL code uses modular program logic to simulate chemical plant dynamic behavior. The differential equations representing each process unit module are time-integrated by a stiff equation system integrator. Input data required include in and out process stream numbers, operating parameters (e.g., size, rate constants, and operation mode), and stream parameters (e.g., flow rate, temperature, pressure, and concentrations) for each unit as well as graphical and printed output specifications, and simulation time specifications. Operator-initiated process changes may be inputted by terminal.

Output results include an input data echo, all stream parameter values, unit parameter values at the end of each time interval, and printplot and plotter results for selected stream parameters as a function of time.

The program was developed to simulate chemical processes in the nuclear fuel cycle. The following unit subroutines (modules) are available.

1. A general-purpose transport unit for equilibrium stage computations with heat transfer (liquid-liquid or liquid-vapor) or for stirred-tank mixing and reaction;
2. a controller with various modes;
3. a pipe;
4. a pump;
5. a highly accurate extractor for uranium and plutonium co-extraction or separation in Purex plants;
6. a plutonium precipitator; and
7. a plutonium concentrator.

As an example, Fig. 6-1 represents an extraction column with 14 stages. The dynamics for each stage and its interconnections are modeled in DYNSYL by four nonlinear ordinary differential equations with auxiliary algebraic expressions. Typical simulation results for the extraction column model are given in Fig. 6-2, which shows the transient response and subsequent steady-state conditions after startup and after a process upset. The process upset in this case was diversion of part of the feed stream at time 5000 seconds. Such simulations provide data for material accounting studies, particularly for on-line schemes, and allow studies of dynamic plant operation either for assessment or design.

In the real world, some or all process variables might be measured by a set of bandlimited monitors that corrupt true measurement values with random noise.

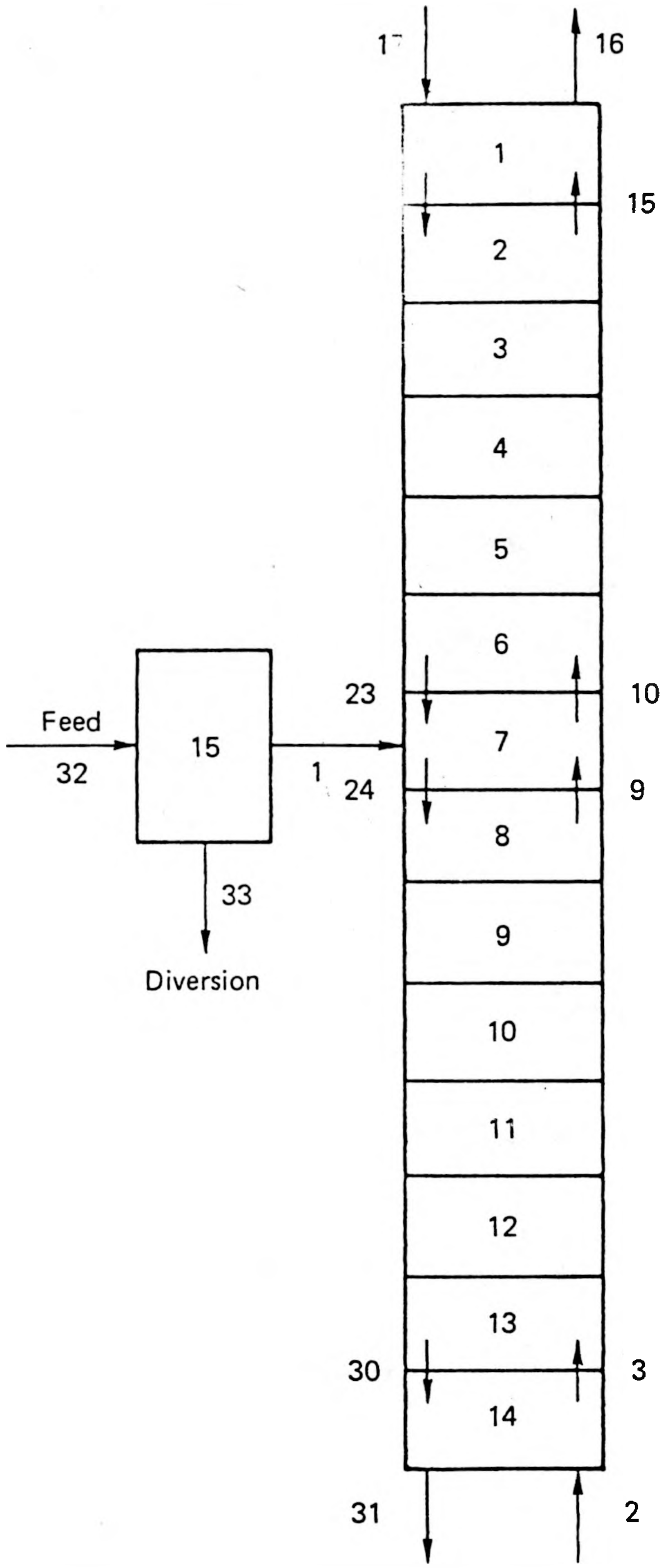


FIG. 6-1. Diagram of example extraction column. Unit 15 is of nearly zero volume for diversion simulation.

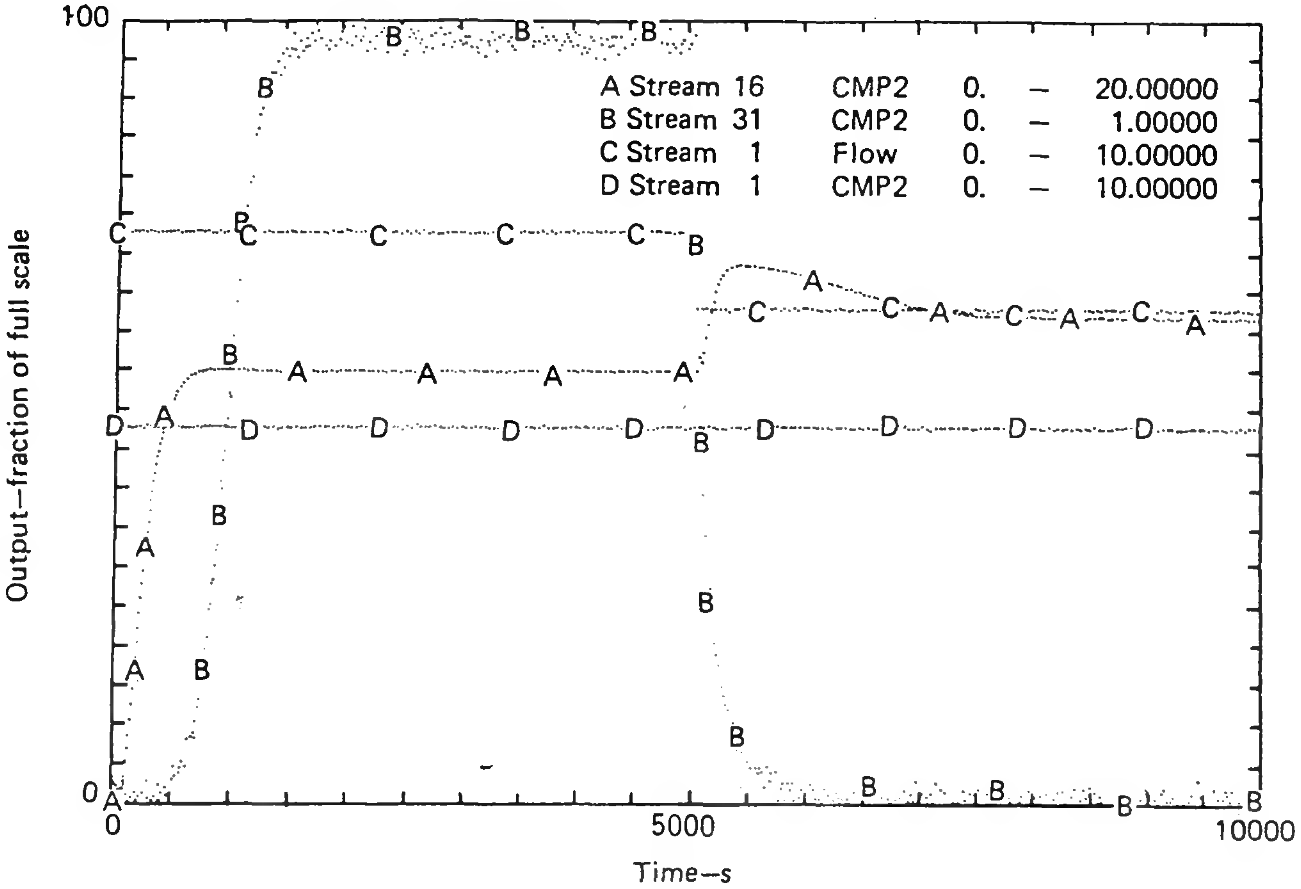


FIG. 6-2. Graphical output of four selected variables from the 14-stage extractor simulation (10,000 s). Diversion occurs at 5000 s.

To evaluate this problem, the effects of measurement systems can be incorporated into DYNSYL by including mathematical models of the measurement dynamics. From a designer's point-of-view, therefore, DYNSYL can be used as a tool to investigate various measurement equipment and schemes on unit operations or even aid in the design of chemical process operations. From an assessment point of view, DYNSYL allows one to obtain simulated measurement data for numerous diversion or material loss scenarios and to evaluate or model the performance of various safeguards process monitors.

DYNSYL has several shortcomings that must be corrected to ensure its most effective use. Some of these are summarized as follows:

- The code produces no flowsheet schematic in its output to key into the numerical graphic output. Such a schematic would aid greatly in providing permanent documentation of the results.
- The graphic and interactive parts of the code are specific to the LLL computer system and must be rewritten for other computer systems.

- Many more unit module subprograms must be written for general use in the chemical industry. The new modules should be written as general as possible with specific applications determined by attached subroutines.

DYNSYL has already proved useful in producing simulated dynamic data for evaluation of on-line material control methods. Further applications of the code will gradually expand its usefulness.

6.3 EVAPORATOR/CONCENTRATOR MODEL DEVELOPMENT

Significant effort was expended on coding, debugging, and testing a plutonium evaporator/concentrator subroutine module for use in the DYNSYL library. A complicated computer model for describing the behavior of a plutonium concentrator similar to one at the Allied General Nuclear Services plant at Barnwell previously had been developed by Systems Control, Inc. (SCI) for LLL under contractual support.[3] Subsequent testing by LLL led to some recent code modifications in order to better utilize the code with the LLL computer system.

A schematic of the evaporator/concentrator modeled by SCI is shown in Fig. 6-3. It consists of a main vapor-liquid separation tank (left) and a steam driven recirculation system (right). The SCI model simulates in great detail the combined heat and mass transfer in the complete system, requiring the solution of ten nonlinear, ordinary differential equations with six auxiliary nonlinear algebraic expressions. Unfortunately, the small time constants of the recirculation loop dominate the transient behavior and long computation times (many minutes) are typical.

As a result of the excessive running times experienced with the SCI computer model, a simplified evaporator/concentrator model was developed by LLL to simulate the basic features of the process for inclusion in DYNSYL.[4] Figure 6-4 shows the simplified unit, which consists of a single vapor-liquid separation tank with assumed rapid heat and mass transfer effects. Simulations from the LLL model agree quite well with those from the SCI model as shown in Fig. 6-5. Furthermore, the LLL version has relatively short computation times (seconds). In contrast to the detailed SCI model, the LLL model is described

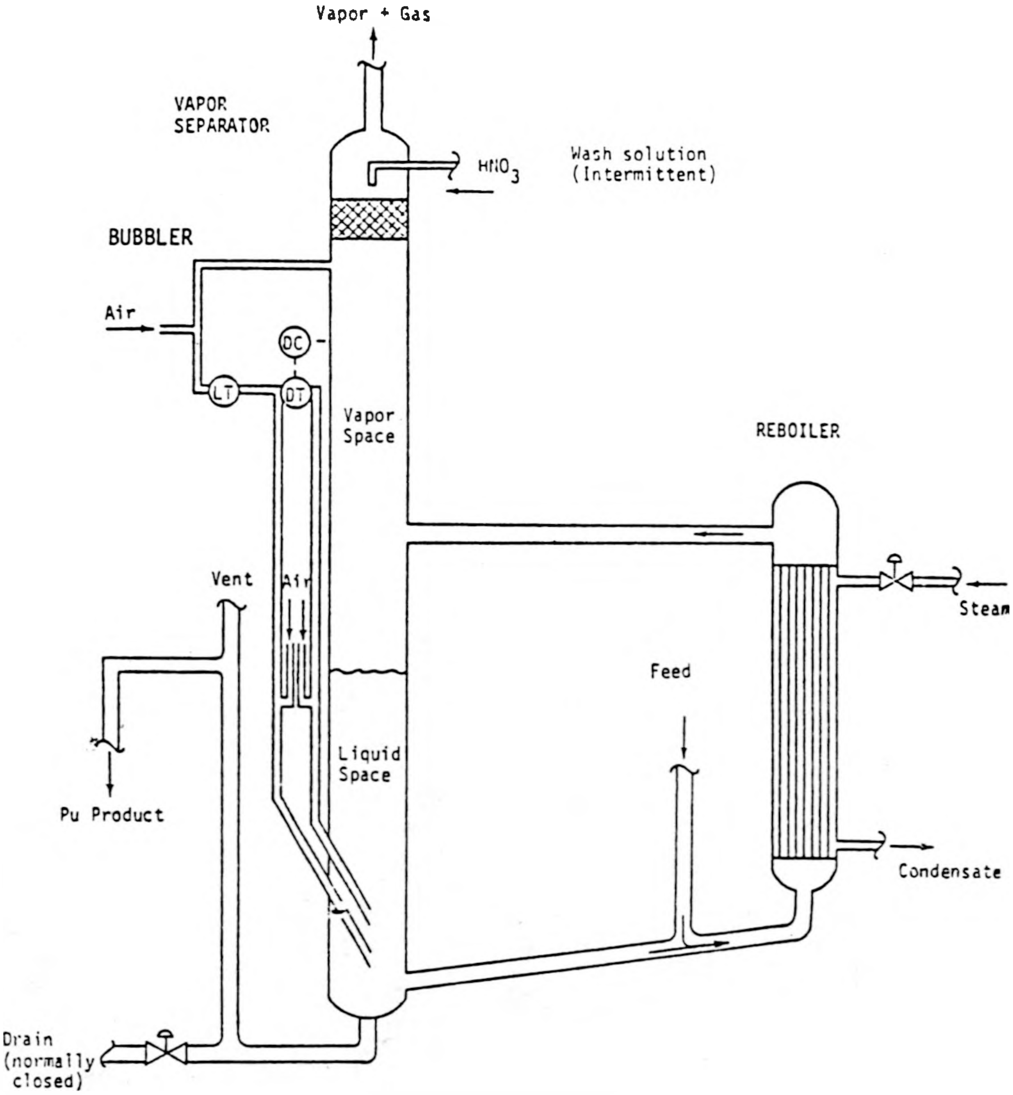


FIG. 6-3. Plutonium concentrator schematic showing main chamber and reboiler.

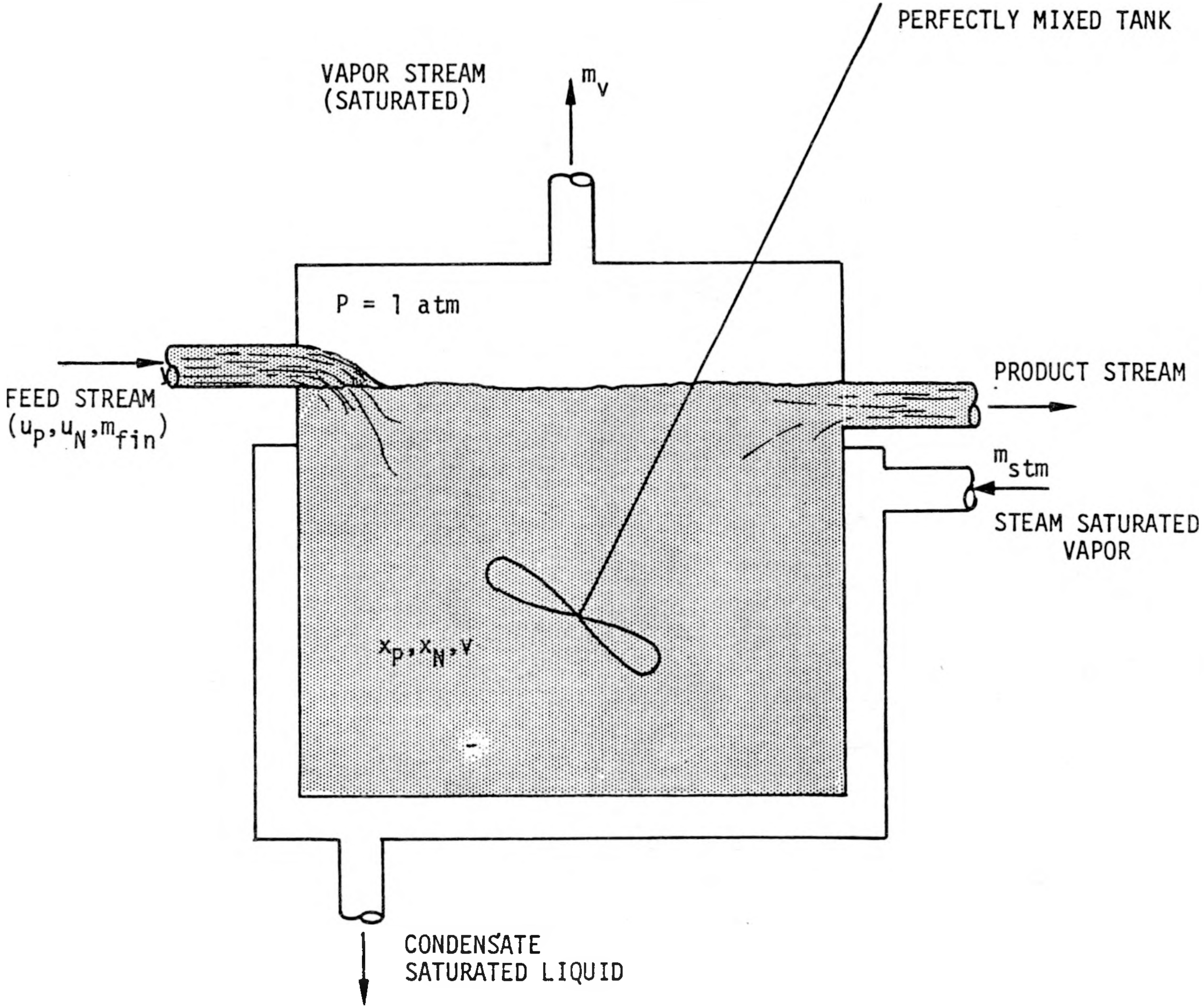


FIG. 6-4. Simplified plutonium evaporator/concentrator.

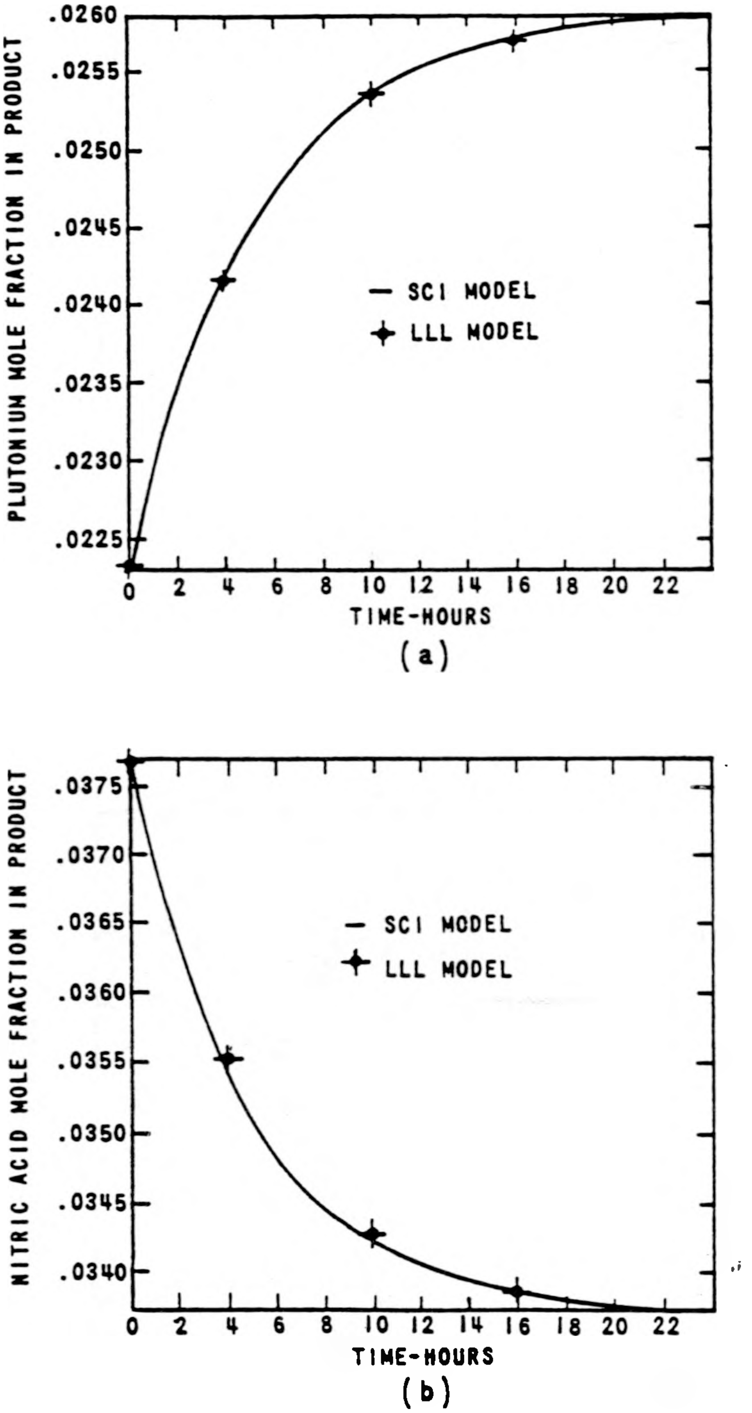
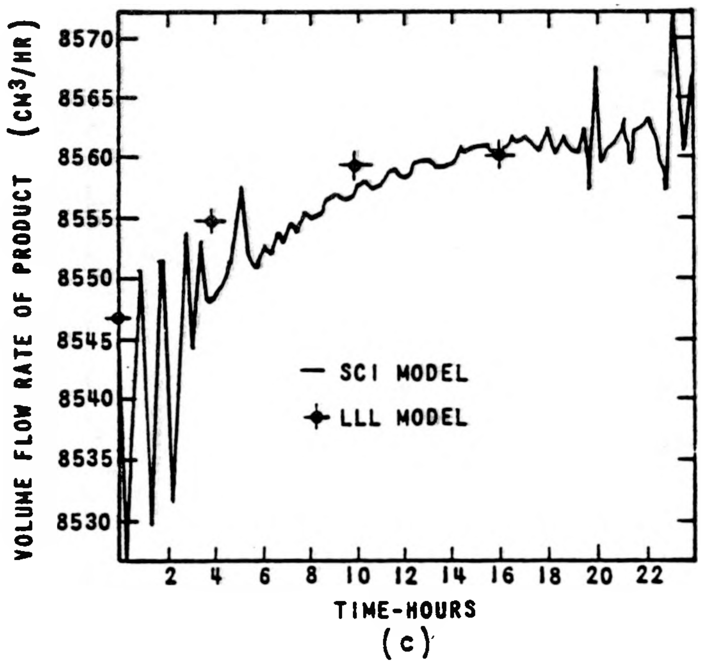
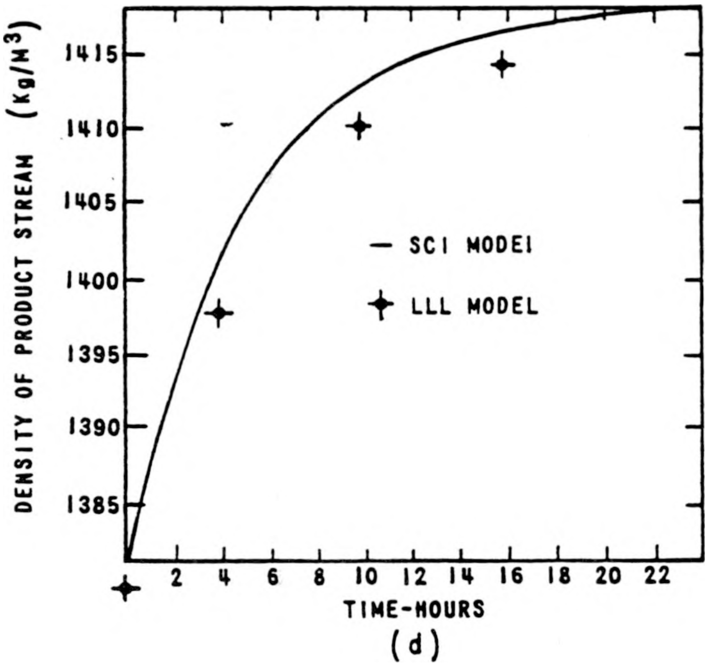


FIG. 6-5. Comparison of results from SCI and LLL models of plutonium concentrator (10 percent plutonium feed change from nominal steady-state operations).



(c)



(d)

FIG. 6-5. Continued.

by three nonlinear, ordinary differential equations with six coupled nonlinear algebraic equations which require iterative solution. A technical report describing these developments in detail and discussing several sample test runs should be completed during the next quarter.

6.4 MATERIAL ESTIMATION DEVELOPMENT FOR AN EVAPORATOR/CONCENTRATOR

The chemical processing models as discussed above have been motivated principally from a safeguards aspect to study various diversion scenarios and to aid in the characterization of material estimators and diversion detectors. This section reviews recent work in applying material estimation techniques to an evaporator/concentrator unit process.

The simplified concentrator model developed by LLL and discussed in the previous section was incorporated into the LLL-DYNEST code,[1,5] which is capable of simulating several estimation algorithms including the extended Kalman filter (EKF) formulation. The following describes some of our results in simulating the performance of a material estimator, using our EKF computer algorithm, for both normal operation of the concentrator and for two diversion scenarios. This work will be extended in subsequent analyses directed toward characterizing the performance of diversion detectors for an evaporator/concentrator unit process.

The design of an on-line material estimator for a concentrator using a Kalman filter requires a process model f(X) as well as a measurement model h(X). For the evaporator/concentrator the continuous process and discrete measurement dynamics were structured in state space format[*]:

$$\dot{X}_t = f(X_t) + g(X, u) + W_t$$

and

$$Z_k = h(X_{t_k}) + V_k \quad ,$$

[*] The process model actually consisted of three nonlinear ordinary differential equations and six coupled nonlinear algebraic equations, the latter requiring iterative solutions.

where the state vector is

$$X^T: = \left[X_p \; X_N\right]\nu,$$

the input vector is

$$U^T: = \left[U_p \; U_N\right] \quad ,$$

and W and V are white gaussian noise sources with corresponding covariance matrixes Q and R. Here (X_p, X_N) and (U_p, U_N) are, respectively, the mole fractions and corresponding feed stream fractions of $Pu(NO_3)_4$ and HNO_3. Concentrator volume is ν.

The measurement system h(X) was simulated with two bubbler differential-pressure measurements with Z_1 proportional to the density ρ and Z_2 proportional to the density and height, $\rho\ell$. The system is depicted in Fig. 6-6, and typical noisy output measurements are shown in Figs. 6-7 and 6-8.

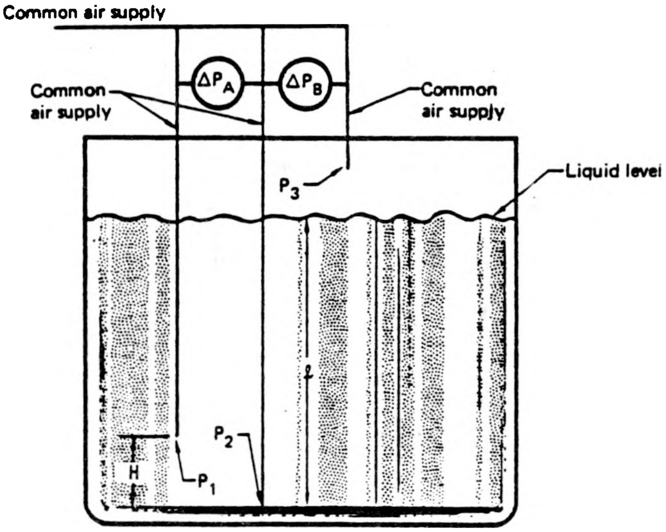


FIG. 6-6. Pneumatic density/height measurement system.

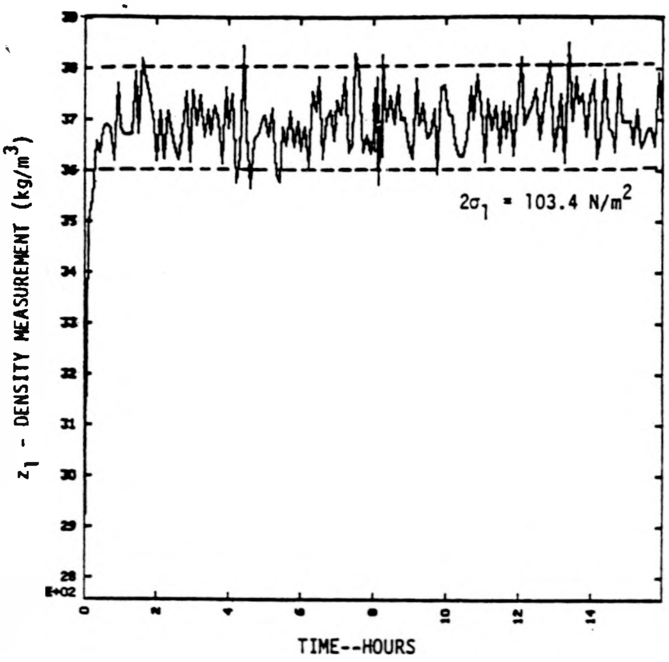


FIG. 6-7. Noisy density measurement, Z_1.

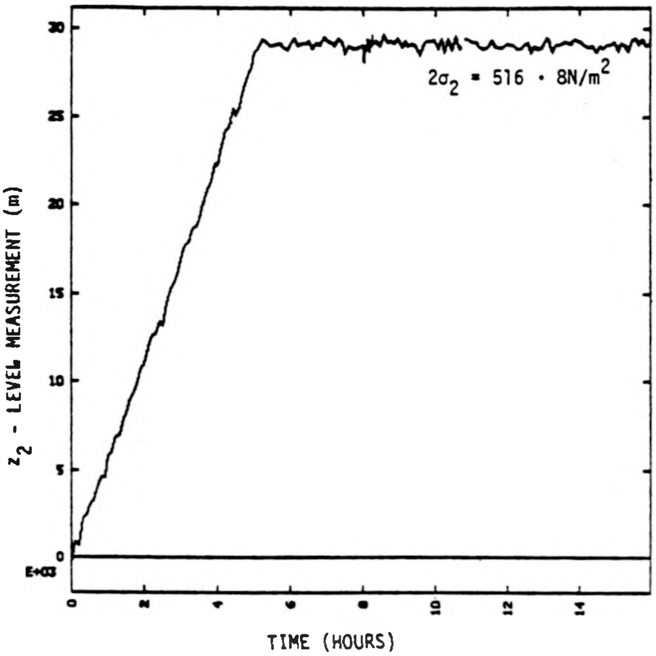


FIG. 6-8. Noisy level measurement, Z_2.

Initially the estimator was tuned for normal concentrator operations by adjusting the filter process and measurement noise covariances (Q and R). It was possible to track the states X_p and X_N quite well (e.g., steady-state rms error of ~1.0 × 10^{-4} corresponding to ~50 g Pu).* This response was not surprising since the reduced evaporator model is reasonably good in steady state. This precise level of tuning may not be entirely desirable, however, as will be seen from the issues discussed next.

The next question considered was whether the estimator could be tuned to track SNM diversions. We look at two scenarios:

1. solution is diverted from the drain during acid wash; and
2. up-stream solution is diverted from the process causing a feed (flow) change to the evaporator (steam flow is then altered to mask the diversion).

*In contrast, the total amount of Pu in the concentrator ranges from 10 to 15 kg.

Typical simulations of the concentrator EKF for two values of process noise covariance $(q_{11})^*$ are shown in Figs. 6-9 and 6-10 for the acid and feed flow diversion runs (diversion occurred at 8 hours). In both cases for decreasing values of q_{11}, the filter becomes less sensitive to noise variations; as a result of this narrow-bandwidth property, the effect of diversion is not readily tracked. Figure 6-10, however, illustrates that by tuning with relatively larger values of process noise ($q_{11} = 10^{-7}$) the filter is able to track the diversion but with correspondingly more uncertainty. These issues are discussed further in the following paragraphs but from a different perspective.

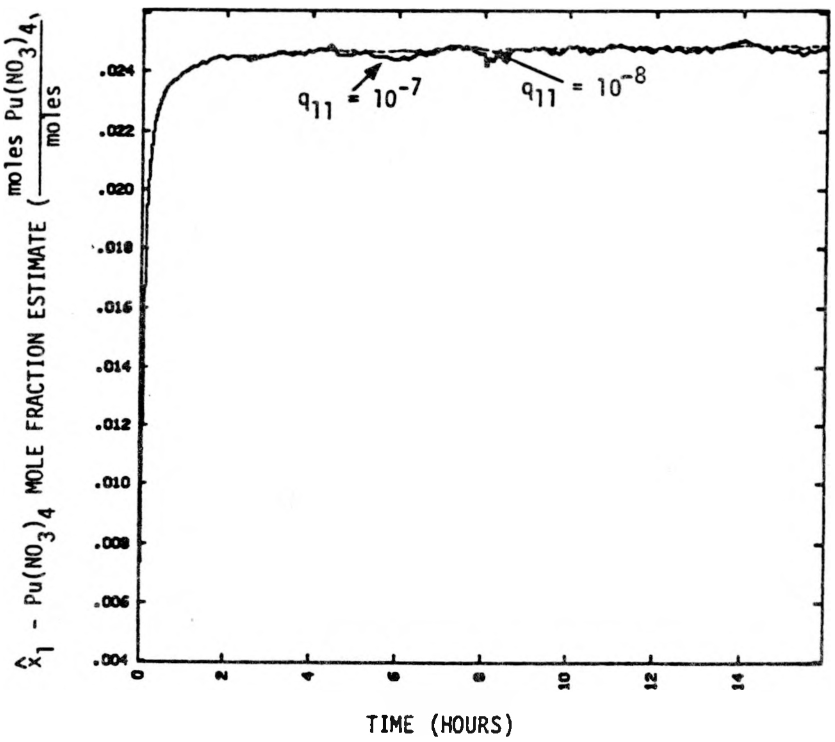


FIG. 6-9. Pu(NO$_3$)$_4$ estimator tuning for acid wash diversion.

*q_{11} units are [moles^2 Pu(NO$_3$)$_4$]/moles^2 where q_{11} is the i^{th} diagonal of Q.

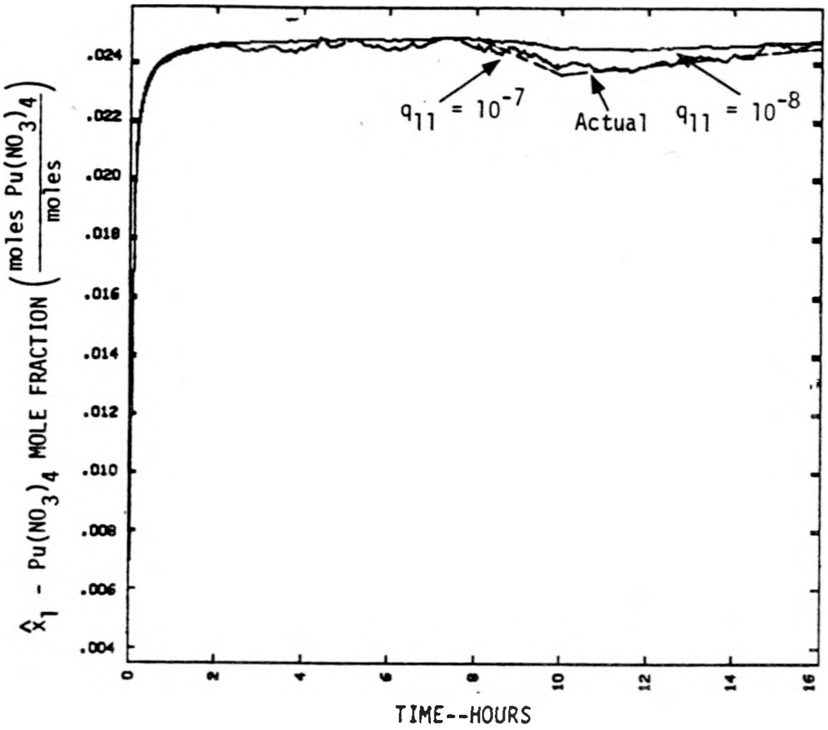


FIG. 6-10. $Pu(NO_3)_4$ estimator tuning for feed change/steam add diversion.

Plots of the tracking or estimator error ($\tilde{X}: = X_{TRUE} - \hat{X})^*$ for various values of q_{11} are shown in Figs. 6-11 through 6-14. Included on these plots are the corresponding 1σ rms error ($\sqrt{\pi_{ss}}$) curves predicted by the filter for each run. If the filter runs were simulated many times, then about 67 percent of the errors (X's) would fall within the 1σ bounds provided the filter was tracking. Under these conditions, the predicted steady-state error $\tilde{\pi}_{ss}$ is an accurate representation of the true tracking error variance and can be used in further analyses.[†] This procedure is also useful for checking the accuracy of the filter model with the "truth" model from DYNSYL; in an on-line application, a reduced-order model for the estimator may be necessary as well as desirable.

[*] In reality, we would not have X_{TRUE}; however, for simulation purposes it is available for use. X is estimator output.

[†] For example, to describe a probability density function for a performance model.

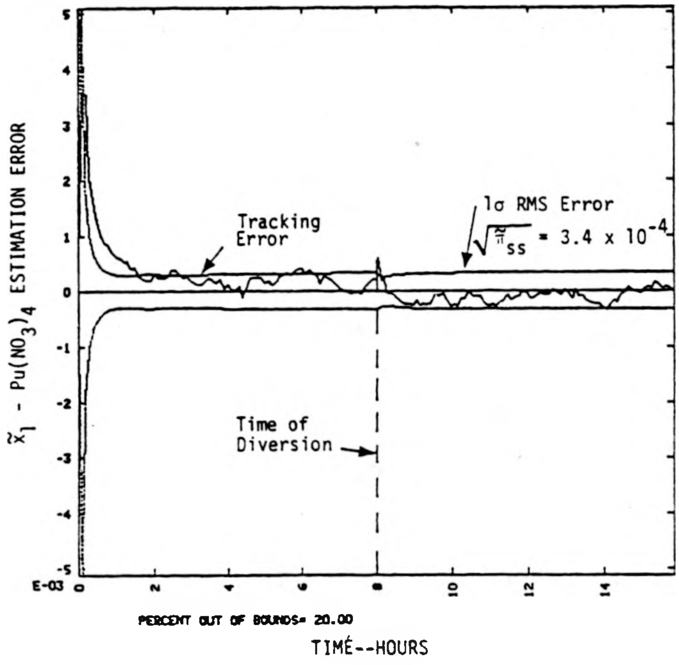


FIG. 6-11. $Pu(NO_3)_4$ estimation error for acid wash diversion ($q_{11} = 10^{-7}$).

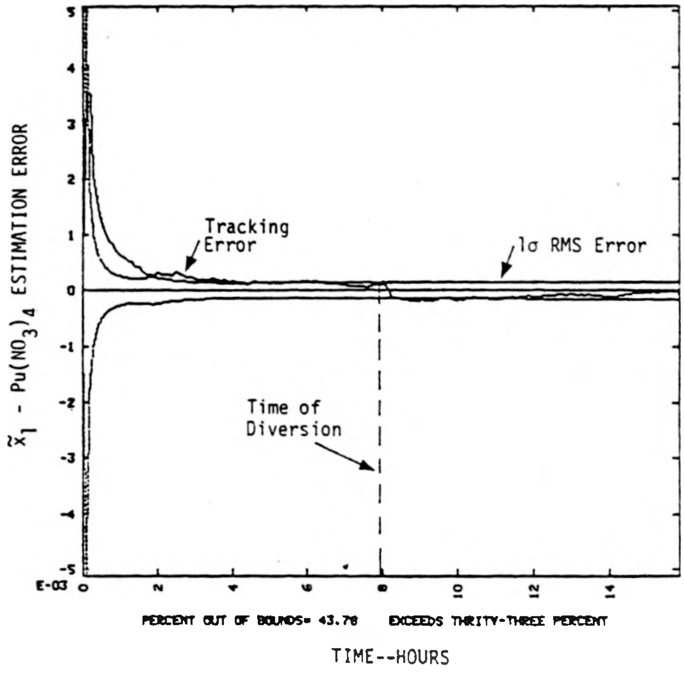


FIG. 6-12. $Pu(NO_3)_4$ estimation error for acid wash diversion ($q_{11} = 10^{-8}$).

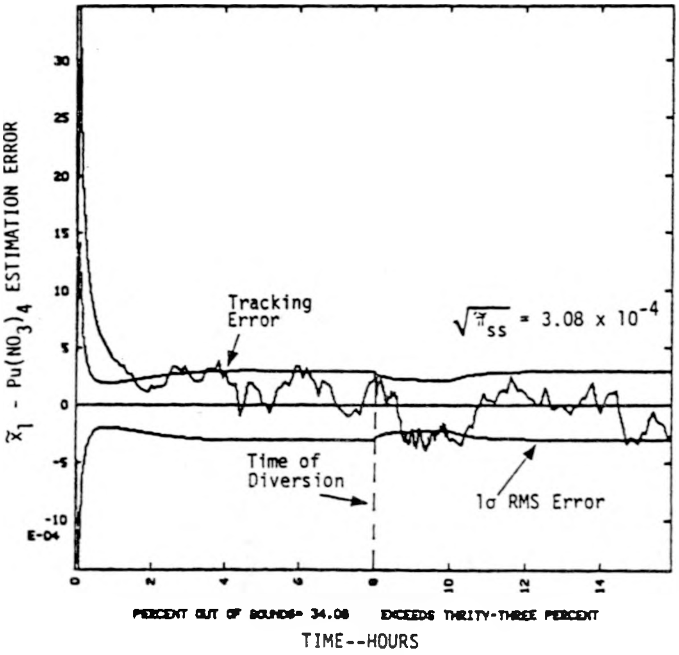


FIG. 6-13. $Pu(NO_3)_4$ estimation error for feed change/steam add diversion (q_{11} = 10^{-7}).

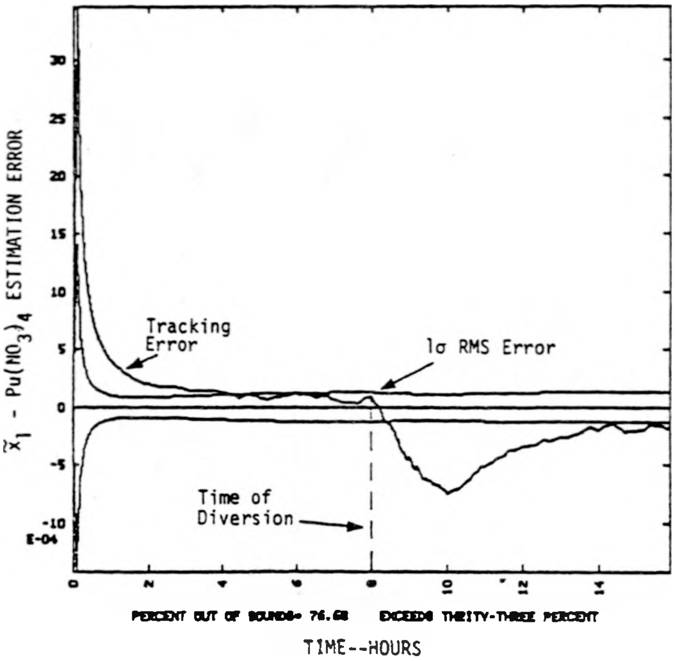


FIG. 6-14. $Pu(NO_3)_4$ estimation error for feed change/steam add diversion (q_{11} = 10^{-8}).

The tracking errors corresponding to the acid wash diversion are depicted in Figs. 6-11 and 6-12. For $q_{11} = 10^{-7}$, the estimator tracks with an rms error equivalent to 167 g Pu. For $q_{11} = 10^{-8}$ the estimator is not tracking since $\widetilde{X}$ is out of bounds excessively. Similar results are shown in Fig. 6-13 (Pu error ~153 g) and in Fig. 6-14 (estimator not tracking) for the feed (flow) change diversion.

These limited results appear promising from a material accounting viewpoint, since the actual $Pu(NO_3)_4$ can be reconstructed from the density/height measurements within reasonable precision (rms error $\pi_{ss} \simeq 3 \times 10^{-4}$ or 150 g Pu).

Future effort will be directed toward developing measures for quantifying the trade-offs in estimator responses.[*] These measures will not only aid in comparing material estimators of different designs, but they will also be useful for characterizing the overall performance of a process monitor which might include a material estimator and detector.[6]

[*] For example, estimator response time and resolution are two important parameters.

REFERENCES: CHAPTER 6

*1. D. R. Dunn, J. V. Candy, and J. C. Heubel, "Computational Tools for Material Control Assessment and Design of Process Monitors: An Overview," Lawrence Livermore Laboratory, UCRL-52702, NUREG/CR-0662, (October, 1978).

**2. G. K. Patterson and R. B. Rozsa, "DYNSYL: A General Purpose Dynamic Simulator for Chemical Processes," Lawrence Livermore Laboratory, Livermore, California, UCRL-52561 (September, 1978).

**3. Systems Control, Inc., Final Report: "Characterization and Modeling of a Plutonium Concentrator," Lawrence Livermore Laboratory, Livermore, California, UCRL-13864 (April 13, 1978).

**4. R. B. Rozsa and S. J. Underwood, "Simple Model of a Plutonium Nitrate Concentrator," Lawrence Livermore Laboratory, UCRL-52711 (February 2, 1979).

*5. R. N. Castleton and J. V. Candy, "DYNEST--A Dynamic Estimator Calculation Program," Lawrence Livermore Laboratory, Livermore, California. UCRL-52573, NUREG/CR-0531(December, 1978).

*6. J. V. Candy and R. B. Rozsa, " On-Line Estimator/Detector Design for a Plutonium Nitrate Concentrator Unit," Lawrence Livermore Laboratory, UCRL-52573, NUREG/CR-0531 (February, 1979).

*Available for purchase from the NRC/GPO Sa;es Program, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, and the National Technical Information Service, Springfield, VA 22161.

**Available for sale from the National Technical Information Service.

7.0 APPLICATIONS DEVELOPMENT FACILITY STUDY

In early November, 1978, the Nuclear Regulatory Commission (NRC) requested the Lawrence Livermore Laboratory (LLL) and Sandia Laboratories Albuquerque (SLA) to study the need of a facility at NRC Headquarters to give NRC analysts direct access to the automated methodologies being developed for NRC by several contractors, including LLL and SLA. The computer programs comprising the automated aspects of the methodologies now run on various computers and it is difficult for the analyst to use the programs in an efficient, integrated manner. In addition, some of the programs cannot be run directly from NRC Headquarters. As a result, the computer programs tend to fall into disuse because of the difficulty of running the programs. In an effort to rectify this situation, the NRC-RES has proposed establishing a computer system called the Applications and Development Facility (ADF) to provide user-oriented access to these computer programs.

The investigative team, composed of two people from LLL and one from SLA, set out to (1) determine the functional requirements of present and future safeguards effectiveness software; (2) determine what computing resources are directly or indirectly available to NRC, and, based on that information; (3) recommend a set of alternative configurations along with their potential costs and benefits. To determine the resource requirements of individual software systems, the team contacted software developers at LLL and SLA as well as Scientific Applications Inc. (SAI), La Jolla, California; TRW, Redondo Beach, California; and Informatics, Rockville, Maryland.

To investigate the computing resources potentially available to NRC, the team contacted the Automatic Data Processing group of NRC to determine immediately available resources; contacted LLL and SLA to investigate the possibility of obtaining computing services from them; and analyzed stand-alone computer systems to determine the possibility of basing the ADF on an in-house computer

The investigation was completed in December, and a presentation was made to NRC shortly thereafter. The presentation discussed the need that NRC has for such a facility, design goals for the ADF, general implementation considerations and trade-offs, computer systems available to NRC, and recommended actions. A phased implementation approach was suggested, which will give NRC the earliest possible access to SLA software, will later provide the graphic subsystem for the LLL software, and will give access to software to be developed in the future. An important unresolved issue is that of the classification level of the data and software. It is important that NRC determine the security classification of all input data, codes, and output data as soon as possible. A classified computer system would impose many requirements on the ADF that would not otherwise be imposed on it, and early acquisition of that information will minimize its impact on ADF system design.

RM/ew LLL:1980/5

NRC FORM 335
(7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-0849
UCRL 52715-79-1

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
SAFEGUARDS MATERIAL CONTROL AND ACCOUNTING PROGRAM
QUARTERLY REPORT, OCTOBER-DECEMBER 1978

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
D. R. Dunn, A. Maimoni

5. DATE REPORT COMPLETED
MONTH December | YEAR 1978

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Lawrence Livermore National Laboratory
NSS Safeguards Program, T-1202, Rm. 211, L-97
P. O. Box 808
Livermore, CA 94550

DATE REPORT ISSUED
MONTH May | YEAR 1980

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Technical Support Branch
Division of Safeguards, Fuel Cycle & Environmental Research
Office of Nuclear Regulatory Research
Washington, DC 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.

13. TYPE OF REPORT
NUREG

PERIOD COVERED *(Inclusive dates)*
October-December 1978

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

Work is summarized for the quarter October to December, 1978, in the Material Control Safeguards Evaluation Program, conducted for the U.S. Nuclear Regulatory Commission (NRC) at Lawrence Livermore Laboratory. The main activities related to the continuing development of the assessment methodologies and their application to the assessment of a fuel cycle facility.

Much progress was made in the Digraph--Fault-Tree Methodology, leading to the Safeguards System Vulnerability Assessment Methodology (SSVAM). In addition, the development of the Structured Assessment Approach (SAA) continued on schedule. Both techniques were used to assess the vulnerabilities of the safeguards system at an existing fuel recovery facility (Facility X).

Other activities during the quarter included (1) the continuing development of the Aggregated Systems Model (ASM), an evaluation tool designed to aid the NRC in the setting safeguards criteria; (2) the continuing structuring and data gathering for the adversary model portion of the ASM; and (3) the continuing development of computer codes for chemical process modeling/material estimation/material loss detection.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

8. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
unclassified

21. NO. OF PAGES
94

20. SECURITY CLASS *(This page)*
unclassified

22. PRICE
$