UCRL-82222
PREPRINT
CONF-800315--3

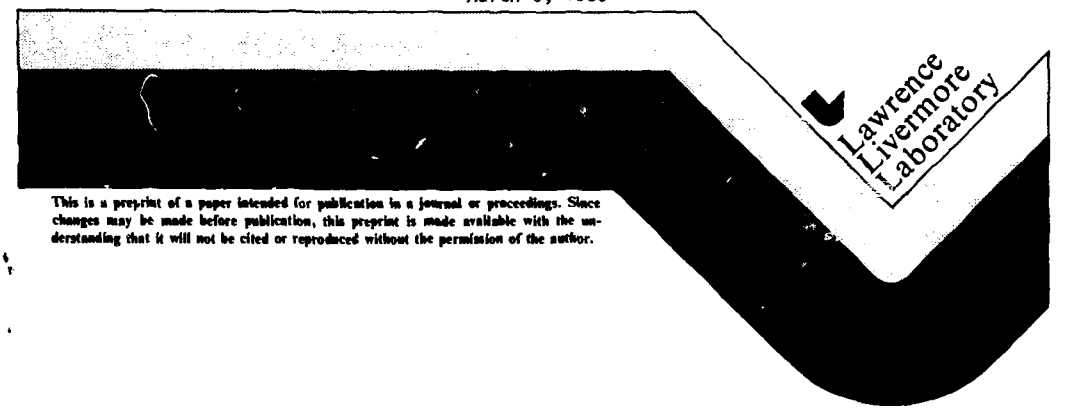
MASTER

THE STRUCTURED ASSESSMENT APPROACH A PROCEDURE FOR THE ASSESSMENT OF FUEL CYCLE SAFEGUARD SYSTEMS

A. A. Parziale
C. J. Patenaude
P. A. Renard
I. J. Sacks

This paper was prepared for submittal to
2nd Esarda Symposium on Safeguards and
Nuclear Materials Management
Edinburgh, Scotland on March 26 - 28, 1980

March 6, 1980



THIS PAPER WAS PREPARED FOR SUBMISSION TO THE
2ND ESARDA SYMPOSIUM ON SAFEGUARDS
AND
NUCLEAR MATERIALS MANAGEMENT

The Structured Assessment Approach - A Procedure For The Assessment Of Fuel Cycle Safeguard Systems*

A. A. Parziale, C. J. Patenaude and P. A. Renard
Lawrence Livermore National Laboratory

I. J. Sacks
Analytic Information Processing, Inc.

Abstract

Lawrence Livermore National Laboratory has developed and tested for the United States Nuclear Regulatory Commission a procedure for the evaluation of Material Control and Accounting (MC&A) Systems at Nuclear Fuel Facilities. This procedure, called the Structured Assessment Approach, SAA, subjects the MC&A system at a facility to a series of increasingly sophisticated adversaries and strategies. A fully integrated version of the computer codes which assist the analyst in this assessment was made available in October, 1979. The concepts of the SAA and the results of the assessment of a hypothetical but typical facility are presented.

1. Introduction

A computer assisted procedure has been developed at Lawrence Livermore National Laboratory to assist the NRC Material Control and Accounting license reviewer in determining the acceptability of an application for a license for a nuclear fuel cycle facility.

The procedure is called the Structured Assessment Approach (SAA)[1,2,3,4,5] and subjects the MC&A System at the facility to a series of increasingly stringent performance tests, ranging from a determination of whether a non-tampering adversary can break the facility with no risk at all, to subtle questions dealing with the reliability of the detection system and the dynamics of the diversion sequence. The advantage of the staged approach is that it allows a great deal of analysis to be done with a minimum of judgmental input from the analyst. To the extent possible, the procedures are based directly upon data from applicant supplied 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 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 where it is more likely to uncover system problems.

A current version of computer code for performing the stages of the analysis was made available to the NRC and was used in an assessment of a hypothetical nuclear fuel facility in October, 1979. Prototype codes of all levels of the analysis were previously exercised on a hypothetical, but representative facility in late 1978[1]. This paper has two objectives:

To demonstrate the methodology of the SAA by applying it to a representative "facility".

To illustrate the output of the analysis, based on each stage of the SAA assessment.

2. Methodological Overview and Major Conclusions

Both the methodology and the conclusions from the staged assessment approach are subdivided into four levels that are intended to answer four basic questions. (Figure 1) The questions these levels pose are:

Level 1 - Can a non-tampering adversary divert SNM with no risk of detection? Who is this adversary?

Level 2 - Can a non-tampering adversary divert SNM with some level of risk, and does the probability of detecting that adversary meet NRC performance criteria?

Level 3 - What system states, such as failed components or collusion amongst 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?

The analysis of the MC&A system at the "facility" was performed separately on the material control, or timely detection system and

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

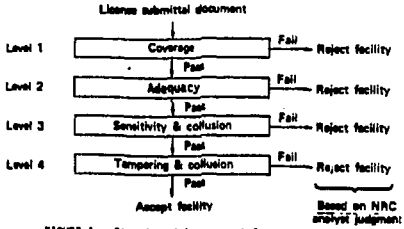


FIGURE 1: Structured Assessment Approach

the material accounting, or late detection (assurance) system. Levels 1 through 3 were performed on the MC system and Level 4 on the MA system.

Level 1 - Coverage.

The intent of Level 1 is to determine if a non-tampering 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 target set 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 that protect a target set is called a monitor target set (MTS). The data required to define the monitor target sets 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 target sets, the ones for which the monitor target set contains no elements. In addition, for each covered target set, the monitor target set is listed. Certain individuals at the facility have the authority and/or ability to control various monitors. These individuals using these abilities could cause the monitor coverage on a Target Set to be cancelled. Level 1 provides the NRC with all sets of individuals who can cause Target Sets to become uncovered.

All potential diversion paths at the "facility" were found to be covered by at least four material containment monitors and the material accounting system. A "dominance" argument was applied to identify 49 essential monitor target sets (MTS) which covered all physical diversion paths.[6] The MTS Matrix shown in Figure 2 summarizes which of the 32 monitors cover each of the 49 MTS. A "1" in the matrix means that the monitor is part of the monitor target set; a "0" means that it is not.

In addition, it was found that certain combinations of individuals could defeat the MC system. As an example, one of the MTS's could be defeated by a combination of the Guard in the primary alarm station and the Guard in Material Balance Area Two during dayshift operations.

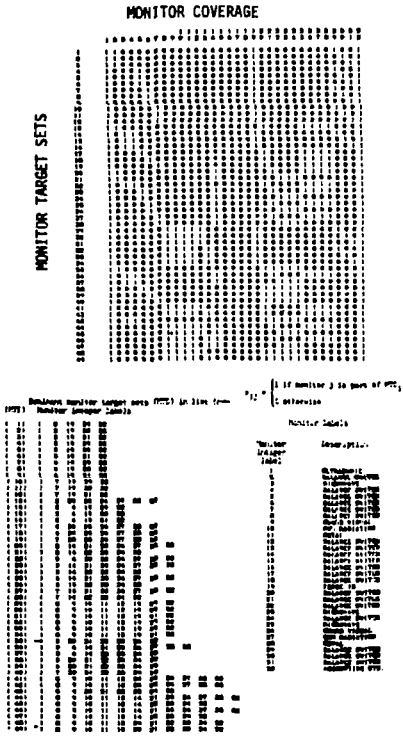


Figure 2 Monitor Target Sets

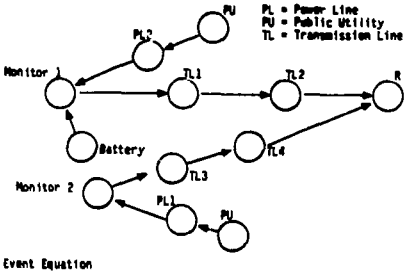
Level 2 - Adequacy.

The Level 2 analysis extends the Level 1 analysis to consider system reliability. For each adversary type and for each monitor target set, the system reliability is calculated.

It is assumed that the adversary does not tamper with the system, that he does not have knowledge of the system status except the operating mode, and that he makes only one attempt to divert SNM. Consequently, the appropriate system reliability measure is the probability that a given monitor target set 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 Level 2 analysis begins with each of the monitors identified as part of a MTS from Level 1. To each of these monitors is added the MC&A system components such as utility lines, back-up batteries, signal transmission lines,

etc. Reliability Boolean event equations for each MTS are then determined as shown in the simplified example of Figure 3. From this event equation, the probability of operation of the MTS is calculated.



Event Equation

$$MTS1 = M1 \cdot (PL2 \cdot PU + Batt) \cdot TL1 \cdot TL2 \cdot R + M2 \cdot PL1 \cdot PU \cdot TL3 \cdot TL4 \cdot R$$

Figure 3 Determination of Reliability Event Set

The calculation of the probability of detection conditioned on adversary type, mode, and monitor target set is complicated by the common mode failure problem. Utilities such as electricity or compressed air can fail causing several MC&A components to fail at once. The utility structure is part of the input to the Level 2 analysis, allowing dependence among components to be modeled explicitly.[7,8]

The result of Level 2 analysis of the "facility" was that the system is protected to the .94 adequacy level. Because the system reliability is dominated by the electrical system, all monitor target sets have close to the same reliability.

Level 3 - Sensitivity.

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 component that is operational, and that goes out for every component that has failed. Under complete knowledge without tampering, it is assumed that an adversary will attack only uncovered target sets. The output for this type of adversary is the frequency with which various target sets become uncovered and the frequency with which the facility becomes uncovered.

The output from this level of analysis is used to determine which system components are essential for monitor target set coverage. These components include all hardware MC&A system components such as monitors, transmission lines, utilities, etc., and personnel components such as physical security guards, process operators, maintenance men, etc. For the hypothesized facility, it was found that there was no single common mode failure which caused loss of coverage for any MTS. However, the system's reliability was sensitive to the availability of the AC power. The sensitivity analysis provided an informal collusion result. It was found that two maintenance men in collusion could cause several MTS's to become uncovered.

Level 4 - Tampering Vulnerability.

Level 4 introduces adversary types who tamper with the MC&A system using methods which are outside of their authorized access or direct control. These adversaries, with complete knowledge of the system, do not have to tamper directly with monitors in an MTS to produce an uncovered TS. They can tamper with auxiliary or support systems which may cause the failure of coverage. Most monitors and other components of the MC&A system are tamper monitored. Thus, this adversary may tamper with the tamper monitors.

As an example of a Level 4 analysis, the analysis of the hypothetical facility material accounting system will be summarized. This analysis was performed using a current version of the Level 4 code.

The Material Accounting System is viewed as a block box as shown in Figure 4. 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.

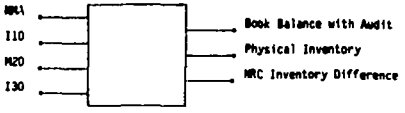


Figure 4 Accounting System Model

The Material Accounting System is modeled using the concepts of an extended Petri Net[9,3]. The net represents the information flow and personnel access which are the basis of the system. Figure 5 shows a simplified portion of the accounting system network.

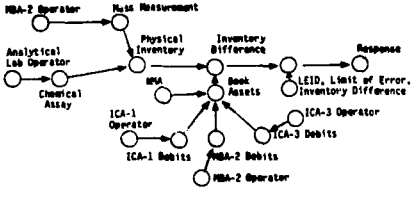


Figure 5 Simplified Information Flow Net for Material Accounting System

The tamper protection for this network is modeled by placing controlled transitions (AND gates) on all protected information flows. For example, the book assets in this system are validated by comparison to the book liabilities. This is shown in Figure 6. In this case, a tampering adversary would have to falsify both an asset and a liability account to successfully falsify the book assets used for Physical Inventory comparison.

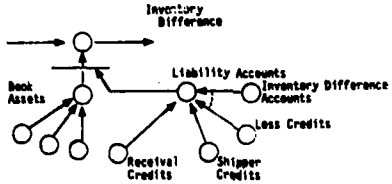


Figure 6 Asset Equal Liability Tamper Protection

By carefully specifying who has access to each account and how information arrives at each account, it is possible to determine the combination of individuals required to defeat the Accounting System.

The results of the analysis of the Accounting System at the "facility" are:

The Accounting System is vulnerable to:

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

3. Summary

A hypothetical but typical MC&A system has been analyzed using current versions of the computer codes of the Structured Assessment Approach. Significant vulnerabilities which were not apparent to the analyst were found. A current version of the code package was made available for NRC use in October, 1979.

Acknowledgement.

The assessment procedure described in this paper was the result of the efforts of many individuals. Foremost among these were Thomas Rice and Steven Derby of Applied Decision Analysis, Inc. and Mary Schrot and James Long of Lawrence Livermore National Laboratory.

4. References

[1] Parziale, A. A., Sacks, I. J., Rice, T. R., Derby, S. L., "The Structured Assessment Of Facility 'X'", Lawrence Livermore National Laboratory, NUREG CR/0791; UCRL-52765, Volume I and Volume II, November, 1979.

[2] Rice, T. R., and Derby, S. L., "Overview of the Structured Assessment Approach and Documentation of Algorithms to Compute the Probability of Adversary Detection", Applied Decision Analysis, December 1978.

[3] Parziale, A. A., Sacks, I. J., "Procedure For The Assessment of Material Control and Accounting Systems", Lawrence Livermore National Laboratory, UCRL-82213, July, 1979.

[4] Parziale, A. A., Ross, D. J., Sacks, I. J., "The Structured Assessment Approach Version I", Lawrence Livermore National Laboratory, NUREG CR/1233, UCRL-52735, Volume I, Volume II, and Volume III, January, 1980.

[5] Parziale, A. A., Freeman, D. W., Patenaude, C. J., Renard, P. A., Ross, D. J., Sacks, I. J., "Computational Analysis Package For The Structured Assessment Approach Version I", Lawrence Livermore National Laboratory, UCID-18146, January, 1980.

[6] Parziale, A. A., "Determining Dominant Paths in a Network and Their Significance in Analyzing the Safeguarding of Adversary Area Traversal", MC 78-301, Lawrence Livermore National Laboratory May, 1978.

[7] Derby, S. L., "Procedure for Combining Utility Networks with Signal Flow Networks", MC 78-10367, Lawrence Livermore National Laboratory (ADA), September, 1978.

[8] Parziale, A. A., "Analysis of Utility Networks and Their Significance in Identifying Vulnerability in a Safeguard Communication System", MC 78-403, Lawrence Livermore National Laboratory May, 1978.

[9] Peterson, J., "Petri Nets", Computing Surveys, Volume 9, Number 3, September, 1977.