UCRL-82224
PREPRINT

SAFEGUARDS RESEARCH AT LAWRENCE LIVERMORE LABORATORY

D. R. Dunn
J. G. Huebel
A. J. Poggio

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

March 20, 1980

Lawrence Livermore Laboratory

SAFEGUARDS RESEARCH AT LAWRENCE LIVERMORE LABORATORY *

D. R. Dunn, J. G. Huebel, and A. J. Poggio
Lawrence Livermore Laboratory
Livermore, California, USA 94550

Abstract

The safeguards research program at Lawrence Livermore Laboratory is reviewed. Each of the major projects is described as are their goals and progress. The breadth and scope of the program is clearly delineated.

1. Introduction

The Lawrence Livermore Laboratory (LLL) has a broad based safeguards research program which primarily has supported the U.S. Nuclear Regulatory Commission (USNRC). The program has supported the USNRC in its development of regulatory licensing criteria and inspection procedures for fixed-site, commercial nuclear fuel-cycle facilities as well as its development of methodologies for assessing compliance of licensee safeguards plans. We also are conducting safeguards research for the U.S. Department of State, Arms Control and Disarmament Agency (ACDA) which involves analyzing the international nuclear material accounting system.

The LLL research activities have been specifically directed towards the development of 1) Inspection Methods for Physical Protection, 2) Detailed Assessment Methodologies, 3) Aggregated Systems Models, 4) Statistical Methods for Material Accounting, and 5) Design Guidance for Compliance with Licensing Rules. We have also performed research in the determination of vulnerabilities of material accounting systems (including the IAEA system), in the feasibility of a USNRC integrated safeguards rule and in safeguards process monitoring. This paper provides a synopsis of the above LLL safeguards research activities.

2. Inspection Methods for Physical Protection

The Office of Inspection and Enforcement of the U.S. Nuclear Regulatory Commission is charged with inspection of commercially licensed nuclear facilities to determine their compliance with federal regulations. As a part of this process, physical protection equipment, personnel, and procedures must be inspected.

The time demands on an inspector while conducting an inspection as well as the demands of maintaining a technical baseline to keep up with the degree of sophistication appearing in physical protection systems are significant. Because of diverse backgrounds and professional knowledge, each inspector interprets the Regulations and Physical Security Plans differently. Each naturally inspects most heavily within the area of individual expertise, leading to nonuniformity of inspection methods and criteria from inspector to inspector. The problem is compounded further because the existing large body of information about physical protection is not presently in a form or format that is readily usable by an inspector during an inspection of a facility's physical protection system.

LLL in conjunction with the USNRC Office of Nuclear Regulatory Research, presently is identifying the informational needs of the field inspectors, is structuring that information in the form of inspection procedures (also denoted "modules") and is developing training methods in the use of these procedures or modules. The objectives primarily are twofold: (1) to standarize the basis of field inspections and evaluations so as to achieve uniformity and completeness, and (2) to upgrade the technical orientations of the inspection methods.

Procedures are being developed for the following major areas: nuclear power reactors, nonpower reactors, fuel-cycle facilities and transportation. The format of the procedures consists of objectives, requirements, guidance, applicable regulations and references, and technical considerations. For example, twenty-three inspection procedures have been developed for power reactors ranging from procedural-oriented types such as security organization to equipment-oriented procedures such as detection aids, communications, and lighting. A field evaluation of the LLL-produced inspection procedures is currently underway.

3. Detailed Facility Assessment Methodologies

LLL has been involved in the development of two computer-based methodologies for assessing the Material Control and Accounting (MC&A) safeguards systems at fixed-site fuel cycle facilities (e.g., fabrication, processing, and reprocessing plants) for vulnerabilities relating to the theft or diversion of nuclear materials. The two methodologies are denoted SVAP - Safeguards Vulnerability Analysis Program[1] and SAA - Structured Assessment Approach[2,3].

Both SAA and SVAP provide a capability for determining all the acts or sets of

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

acts by authorized, nonviolent insiders working individually or in collusion that could possibly defeat a safeguards system. SVAP only considers normal entry/exit portals when analyzing potential diversion paths. SAA on the other hand can analyze threats where the adversary is given the capability to create new entry/exit portals (e.g., penetrating a wall). SAA also considers the safeguards issue associated with acquisition of SNM material through manipulation of the controls for the facility piping network.

SVAP is a user-oriented tool which uses an interactive input media including a data handbook and mini-computer for preprocessing the large amounts of detailed safeguards data. Its output includes concise summary data as well as the detailed vulnerability information. A very detailed and complex analysis is performed by SVAP to generate collusion event sets from Boolean representations of the safeguards information. This step is accomplished using the computer code Set Equation Transformation System (SETS)[4]. The analysis provides all combinations of adversary acts such as monitor tampering, transmission line tampering, utility system tampering, document falsification, and guard failures that lead to diversion. The analysis then combines the aforementioned adversary acts with the personnel that can perform each act. Finally the analysis folds in the effect of random monitor failures on the adversary acts required for diversion. When the analysis is complete the collusion sets are given in terms of personnel required for successful diversion and any random monitor failures that are also required. Example personnel categories include: analytical laboratory operator, SNM custodian, guards, technicians, etc.

SAA performs an analysis conceptually similar to SVAP. Instead of using SETS, SAA employs an LLL developed code called CLAMOR[5]. It also considers scenarios where the adversary may abuse normal authority to greatly expand his sphere of influence over the safeguards system. SAA can perform a more detailed analysis than SVAP because it allows for a greater threat spectrum--and correspondingly requires more detailed information about a facility safeguards system. Current activities in the SAA development include efforts to make it more user-oriented.

Both SAA and SVAP have been and are being applied to the assessment of USNRC regulated fuel-cycle facilities.

4. Aggregated Systems Model

In its role of regulating the nuclear industry, the U.S. Nuclear Regulatory Commission is required to provide a Value-Impact (V-I) analysis for all recommended regulations. The Aggregated Systems Model (ASM)[6] has been developed at LLL to aid the USNRC in establishing MC&A regulations for safeguarding Special Nuclear Material (SNM).

The ASM has been applied to several safeguards decision problems. These include setting acceptable performance levels for safeguards systems and performing value-impact analyses for USNRC regulations. Our value-impact analysis has specifically involved quantifying the benefits (values) and costs (impacts) of safeguards systems designed to comply with USNRC regulations.

The ASM permits decision makers to integrate various forms of safeguards information so as to provide an evaluation and ranking of complex safeguards alternatives. The various factors considered are characteristics of the adversaries who attempt to divert SNM, facility safeguards responses to these attempts, costs of safeguards systems, and the consequences of diverted SNM.

The adversaries description includes information on their resources, their strategies for diverting SNM, the quantity of material they desire and the way they value the possible outcome of an attempt. Examples of generic types of adversaries are process technicians/engineers, project supervisors, guards, material custodians and analytical lab operators.

The performance of alternate safeguards designs is evaluated against a spectrum of adversary threats. The interaction is modeled in detail with a decision-tree format which is based upon the sequence of events describing a particular adversary type. For each adversary type, we consider the following major events:

Timely Detection: The ability of a safeguards system to detect an attempt while it is taking place is modeled. Detection here consists of two events, first an alarm indicating abnormality and then resolving whether the alarm is real or false. If the adversary knows that an attempt has raised a timely alarm he/she may decide to abort the attempt. Adversaries are assumed to make this decision depending on their preference for the outcome for success or capture quantified by their utility function.

Late Detection: If no timely alarms were indicated or if the timely alarm were not resolved, a late detection may occur. Again, detection consists of two events, alarm and resolution.

Identification: To capture an adversary or prevent him/her from repeating an attempt an identification of the adversary (adversaries) must be made. The last step in the evaluation is to judge the system's ability to identify the diverter.

The ASM methodology summarized above has been demonstrated at an operating facility. The Table below shows a sample result for an application. Data utilized was a mix of objective technical data and subjective data elicited from experts; this approach is an advantage of our methodology because subjectivity is explicitly identified and may be subjected to further sensitivity analysis. An aggregate measure of the system performance called the diversion index was also computed. This measure represents the expected amount of SNM diverted in a given year. The information displayed in the Table aids the decision maker in identifying the alternative that meets the rule in cost-effective manner. Obviously in making a decision, the regulator/designer must make a trade off between value--represented by the Alarm, Resolution, and Diversion performance measures and impact or cost.

The results of applying our value-impact analysis methodology at an operating facility demonstrated the viability of the methodology as an aid to the safeguards regulators/designers. The consistent evaluation of safeguards rules and the value-impact tradeoffs provided by the analysis identify those regulations that achieve adequate protection within a reasonable cost, hence a rational means of developing and evaluating safeguards regulations.

Table
Value-Impact Analysis of Safeguard Rules (designs)

	Alternative Rules (designs) 1**	2	3	4	5
VALUES*					
Alarm					
P(Late alarm No timely alarm)	.78	.69	.91	.91	.78
E(Time to alarm Late alarm)	16wk	12wk	5wk	15wk	16wk
Resolution					
P(Correct resolution)	.69	.56	.82	.82	.69
E(Time to alarm and resolution Late resolution	16wk	14wk	6wk	15wk	16wk
Diversion index (expected grams year)	15	10	15	15	15
IMPACTS					
Incremental operator cost (person-days/week)	0	1	3	1	1

* Performance measures include probability (P) and mathematical expectation (E).
** Design 1 is a base case.

5. Materia Accounting System Vulnerability Analysis

LLL has been conducting an insider falsification threat study supporting the development of a USNRC MC&A upgrade rule for material control and accounting systems. The purpose of this work is to evaluate the potential vulnerabilities of the assurance role of a materials accounting system which follows only Parts 70.51-70.59 of the U.S. Code of Federal Regulations. The results of our research will determine which critical elements of a material accounting system must be protected, and will aid in the development of improved capabilities of material control and accounting systems.

To evaluate the material accounting regulations a generic, minimal material accounting (GMMA) system was formulated[7]. The GMMA system was developed by studying two specific systems regulated by the USNRC guidelines, and constructing a new system which includes only those elements which are common to both and are specifically required by the regulations. The resulting GMMA system could be representative of a material accounting system used by USNRC licensees complying with federal regulations.

The model of the generic minimal material accounting system was developed using a modified logic diagram. The generic material accounting system model delineated the various data sources, data types, data checks, and data access controls which characterize any material accounting system in compliance with the current regulations. The generic model contained no site-specific licensing elements and consisted of three SNM loss detection and identification procedures:

1) Inventory Procedure
2) Item Verification Procedure
3) Item Quantity Procedure.

Thus, the capabilities of material accounting systems in compliance with the current USNRC material accounting regulations were derived from the accounting elements in the above three procedures.

To critique the material accounting regulations the generic minimal system was assessed by an adaptation of the LLL fixed-site safeguards assessment methodologies. The assessment not only indicated the vulnerabilities inherent in the current material accounting regulations, but also elements of protective path sets. In general, a protection path set is the minimal set of system elements which must function in order to insure that the system functions. In our context, a path set is the minimal set of system elements which must be protected so that the generic, minimal system will become as "tamper-proof" as required.

From a graphical presentation of the vulnerability event sets for the GMMA system it was readily determined that many material accounting elements are common to each protective path, and as a result they must be protected. For protection against both item and bulk thefts each protective path contained twenty-four common elements plus several others. Since many protective paths exist, a wide choice is available for several others and selection will depend on effectiveness and other factors. A minimal protective path will contain a minimum number of elements which, in the cases studied, was thirty-two.

In a companion LLL directed study, each protective path is considered from an internal auditor's standpoint to determine realistic element vulnerabilities and to develop alternative procedures which, if applied, would yield different Boolean expressions with solutions showing greatly reduced system vulnerabilities. The results produced and the procedures suggested will support the formulation of changes to the USNRC regulations concerned with material control and accounting systems.

6. Design Guidance For Compliance With Licensing Rule

The Regulatory Improvements Branch of the Division of Safeguards, USNRC, is in the midst of developing an upgrade regulation (rule) for material control and accounting systems. This rule will be applicable to fixed-site, U.S. commercial nuclear fuel-cycle facilities. One objective of the upgrade process is to strive for performance-based regulations which give facilities as much flexibility as possible in meeting the regulatory requirements. LLL has had significant involvement with the USNRC in the structuring and motivation of the performance-based safeguards capabilities, specifically with regard to detection of SNM losses and to alarm resolution due to true alarms (loss of SNM) and false alarms.

In conjunction with issuing the MC&A upgrade rule, the USNRC is required to provide guidance with respect to the various ways of meeting the safeguards capabilities spelled out in the regulation. LLL is assisting the USNRC in this effort by developing specific guidance products suitable for an MC&A Guidance Compendium. Our contributions to this task fall into three broad categories. The first is motivation to assist the facility safeguards designer in understanding the objectives of the MC&A upgrade regulation. This will be achieved with a logic tree which decomposes the high-level capabilities into lower-level capabilities. The lower-level capabilities can then be identified as specific jobs to be performed. The second category involves the identification of alternative safeguards components (hardware, procedures, etc.) which can be used to accomplish the lower-level capabilities or specific jobs. The last category involves arriving at a methodology for assessing the viability of a licensee's safeguards plan in meeting the MC&A upgrade regulation.

The Guidance Compendium task at LLL is ongoing and is drawing heavily upon the experience gained from other LLL safeguards projects such as those described above.

7. Other Research Activities

In addition to the above primary areas of research activity, LLL is also involved in several other areas. These include Statistical Methods Research for Material Accounting, an Analysis of the IAEA Material Accounting System, a study of the Feasibility of an Integrated Rule for Physical Protection and Material Accounting, and research into "real time" safeguards process monitoring. These items are summarized below.

Statistical Methods for Material Accounting.

The properties of measured data for nuclear materials are important for the determination of the ultimate resolution of the material accounting system. Ongoing projects at LLL include Statistical Analysis of the Bias Correction Problem. In the former study the question of under what mathematical conditions is it advantageous to unbias safeguards measurement data is answered. Also considered are questions relating to decision rules for use in deciding when the conditions apply to a particular set of data, what is an optimal procedure for use in bias correction and what is the cost/impact of the procedure. After rigorously defining the safeguards alternatives for correcting bias, the project will focus on the development of estimation and hypothesis testing techniques.

In a companion study called Evaluation of the Application of Loss Estimators and Decision Rules, the statistical properties of several loss estimators under various distributional assumptions as well as with respect to several loss scenarios are being investigated. Thus, a statistical measure of goodness for loss detection of an estimator and corresponding decision rule will be developed.

Analysis of IAEA Safeguards Material Accounting System.

The purpose of this project for U.S. Department of State is to provide guidance for the application of international safeguards in support of the implementation of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). The ultimate goal of this effort will be the designation of specific safeguards approaches, and the establishment of the relationships between the implementation of these approaches by the IAEA and the consequent effectiveness of international safeguards. These safeguards approaches must insure timely detection of diversion and also must be designed within the constraints imposed by the Subsidiary Arrangements of each member state and by the limited resources available to the IAEA. The first phase of this project involves the delineation of model IAEA safeguards approaches and the assessment of their performance in providing timely detection of diversion of significant quantities of nuclear material. Then the design and analysis of possible future safeguards measures or systems employed by the IAEA will be conducted.

Feasibility of an Integrated Rule for Safeguards.

Presently, the USNRC has separate rules for Physical Protection and for Material Control and Accounting. This project addresses itself to the question of how cost effective would integrating safeguards be, utilizing existing process controls and procedures and existing safeguards technologies and methodologies. It will also make a preliminary assessment of potential improvements if appropriate technological developments can be achieved. Of particular interest in this study are interfaces between the safeguard subsystems and the areas where substantial payoffs can be achieved through integration.

Process Monitoring.

LLL has developed computer codes which are useful for studying the performance of process monitoring components. These include: (1) DYNSYL, a general-purpose dynamic simulator for modeling the physical phenomenology of various chemical unit operations and their associated measurement systems, (2) DYNEST, an estimation code for simulating the operation of some modern signal processing algorithms (Kalman filter formulation), and (3) a set of detection algorithms for simulating on-line material loss detection[8]. These codes can be used to address the issues of on-line material accounting and diversion detection for safeguarding SNM, and specifically with respect to arriving at meaningful performance measures for safeguards components[9,10]. The component performance measures can then be used in a detailed facility assessment or in a value-impact analysis.

B. References

1. F. M. Gilman, M. H. Dittmore, W. J. Orvis and P. S. Wahler, "Safeguards Vulnerability Analysis Program: Executive Summary," Lawrence Livermore Laboratory, Livermore, California, UCRL 52724, 1980.

2. A. A. Parziale and I. J. Sacks, "The Structured Assessment Approach Version 1 Analysis Package (Executive Summary)," Vol. 1, Lawrence Livermore Laboratory, Livermore, California, UCRL 52735, Vol. 1, and NUREG/CR-11233, 1980.

3. A. A. Parziale, C. J. Patenaude, P. A. Renard, and I. J. Sacks, "The Structured Assessment Approach, A Procedure for the Assessment of Fuel Cycle Safeguard Systems," 2nd ESARDA Symposium on Safeguards and Nuclear Materials Management, Edinburgh, Scotland, 1980. Also Lawrence Livermore Laboratory Report UCRL 82222.

4. R. B. Worrell, "Using the Set Equation Transformation System in Fault Tree Analysis," Sandia Laboratories, New Mexico, SAND 74-0240, 1974.

5. A. A. Parziale, D. W. Freeman, C. J. Patenaude, P. A. Renard, D. J. Ross, and I. J. Sacks, "Computational Analysis Package for Structured Assessment Approach Version 1," Lawrence Livermore Laboratory, Livermore, California, UCID 18146, 1980.

6. R. Al-Ayat, "An Aggregated Systems Model of Safeguards - Executive Summary," Lawrence Livermore Laboratory, Livermore, California, UCRL 52712 and NUREG/CR 1140, 1979.

7. J. J. Lim, J. G. Huebel, "Material Accounting as Required By The United States Nuclear Regulatory Commission: Capabilities and Vulnerabilities," Lawrence Livermore Laboratory, Livermore, California, UCRL 52734 and NUREG/CR 1192, 1980.

8. D. R. Dunn, J. V. Candy and J. G. Huebel, "Computational Tools for Material Control Assessment And Design of Processing Monitors: An Overview," Lawrence Livermore Laboratory, Livermore, California, UCRL 52702, October, 1978.

9. J. V. Candy, D. R. Dunn and R. B. Rozsa, "On-Line Safeguards Design: An Application of Estimation/Detection," Proc. of 1st ESARDA Symposium on Safeguards and Nuclear Material Management, 1979. Also Lawrence Livermore Laboratory Report UCRL 822110.

10. J. V. Candy, D. R. Dunn and D. T. Gavel, "Real Time Loss Detection For SNM In Process," Proc. of 2nd ESARDA Symposium on Safeguards and Nuclear Material Management, March 26-28, 1980. Also Lawrence Livermore Laboratory Report UCRL 82225.

LLL:1980/3

Technical Information Department · Lawrence Livermore Laboratory
University of California · Livermore, California 94550