LA-UR -83-1156

CONF-830423--8

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

LA-UR--83-1156

DE83 011142

TITLE: OPTIMIZING THE DESIGN OF INTERNATIONAL SAFEGUARDS INSPECTION SYSTEMS

AUTHOR(S): J. T. Markin, C. A. Coulter, R. G. Gutmacher, and W. J. Whitty

SUBMITTED TO 5th Annual ESARDA Symposium, Versailles, France, April 19-21, 1983

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO. 836 R4
ST. NO. 2629 5/81

OPTIMIZING THE DESIGN OF INTERNATIONAL SAFEGUARDS INSPECTION SYSTEMS*

J. T. Markin, C. A. Coulter, R. G. Gutmacher, and W. J. Whitty
Los Alamos National Laboratory, Los Alamos, New Mexico, USA

Abstract

Efficient implementation of international inspections for verifying the operation of a nuclear facility requires that available resources be allocated among inspection activities to maximize detection of misoperation. This report describes a design and evaluation method for selecting an inspection system that is optimal for accomplishing inspection objectives. The discussion includes methods for identifying system objectives, defining performance measures, and choosing between candidate systems. Optimization theory is applied in selecting the most preferred inspection design for a single nuclear facility, and an extension to optimal allocation of inspection resources among States containing multiple facilities is outlined.

1. Introduction

Inspections of nuclear facilities by the International Atomic Energy Agency (IAEA) and the Euratom Inspectorate employ both materials accounting and containment/surveillance to assure that no nuclear material is diverted for unintended uses. Because international safeguards resources for verifying State compliance with safeguards agreements are limited, an efficient method for allocating inspector verification activities and their associated technology is desirable. In effect, design of an inspector's safeguards system must address the tradeoff of resources between activities such as materials accounting and containment/surveillance to attain the greatest return on the Inspectorate resource investment. For example, inspector verification of facility activities may include sampling and measurement of material items, surveillance of storage areas, tamper protection of materials and equipment, and statistical analyses of accounting data. The safeguards design problem may be viewed as selecting the appropriate level of activity or technology for each of these possible inspector activities. However, where there are many potential inspector activities and each activity has several options, the choice of the best system configuration is not obvious. This report describes a method for selecting a combination of inspector activities that maximizes the likelihood of detecting materials loss or unauthorized facility operations while observing a constraint on safeguards resources.

Selecting an inspector's safeguards system for a facility consists of the following steps: (1) identify system objectives, (2) define candidate system designs by specifying fundamental activities that accomplish the objectives, (3) define the adversary's characteristics and sequences of adversary actions, (4) develop performance measures that evaluate the degree of accomplishing system objectives, and (5) select a most preferred option from the candidate designs.[1-3] For each of these steps, this report suggests lists, diagrams, and other tools for organizing the design and evaluation process. These methods are intended to supplement the judgment of the system designer by making explicit the assumptions and value judgments inherent in the design process.

2. Safeguards Objectives

Specifying objectives for an inspection system is essential to design development because (1) the personnel, technologies, and procedures comprising the design will depend on the objectives, and (2) the degree of accomplishing the objectives is a measure of the worth of the system design. A convenient method for deriving objectives is a hierarchy[4] that begins with general objectives and successively refines them into lower-level, more specific ones. A representative hierarchy for Inspectorate objectives in a light-water reactor (LWR) is given in Fig. 1. Objectives at each level in the diagram are the means of accomplishing objectives at the next higher level. Each level guides the design process: low-level objectives suggest specific inspector activities; middle-level objectives suggest the function of combined activities such as materials accounting, tamper protection, and surveillance; and general objectives form the basis for design performance measures. Clearly, a hierarchy could be expanded to many levels depending on the amount of detail to be included.

3. Fundamental Inspection Activities

Fundamental safeguards activities, which are the means for accomplishing the lower-level objectives, are the building blocks of the inspection system. Each fundamental activity is specified by parameters that uniquely define the personnel, equipment, and procedures for the

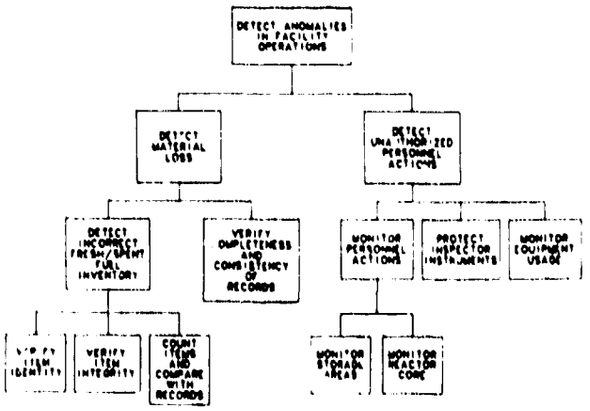

Fig. 1. Objectives hierarchy for LWR safeguards.

*Work performed under the auspices of the US Department of Energy, Office of Safeguards and Security.

activity. Table I gives some representative fundamental activities for an LWR. A table of this type is useful for identifying possible system configurations; varying the activity parameters generates candidate systems for consideration.

Frequently, individual fundamental activities must be coordinated to attain an inspection objective. For example, verifying the inventory of spent-fuel assemblies in a storage pond requires integration of the following activities: (1) obtain operator's inventory records, (2) select a sample of items, (3) verify the item identity, and (4) verify the item integrity. Generally, the integrating relationship among inspector activities takes the form of an information exchange in which information from one activity is a prerequisite for completion of a related activity. A convenient method for expressing these relationships is an interaction matrix such as the simplified one in Fig. 2 that describes information exchange between inspector activities in an LWR. A blank indicates little or no direct interaction between the activities, and a one indicates significant interaction. The system designer should use interaction matrices to identify where channels for information exchange are needed and provide the means for the exchange within the system design.

4. Adversary Scenarios

The Inspectorate perception of potential State actions for diverting nuclear material will be a strong determinant of the mix of inspector activities for verifying facility operations. Diversion or adversary scenarios are specified by (1) adversary attributes such as technical knowledge, special equipment, and number of personnel; (2) the location and amount of material targeted for diversion; and (3) the sequence of adversary actions for obtaining and removing the material from the facility. A representative sequence of actions for diverting spent fuel from a LWR is summarized in Table II, which is a threat/countermeasure summary that is explained more fully below. This scenario is chosen because it exercises many aspects of the inspection system and is not suggested as a credible adversary option.

TABLE I

REPRESENTATIVE FUNDAMENTAL ACTIVITIES IN AN LWR

Activity	Parameters
Audit facility records for self consistency	Frequency of audit, portion of records verified
Verify fresh fuel inventory	Sampling plan, method of verifying item identity and integrity
Monitor core reload	Surveillance method, sensor location, observation frequency, method of reviewing record
Verify spent fuel inventory	Sampling plan, method of verifying item identity and integrity

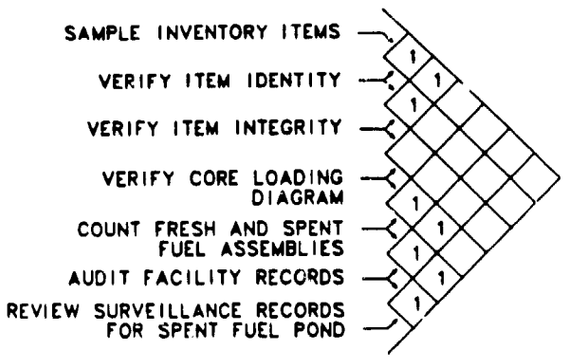

Fig. 2. Interaction matrix for selected activities in an LWR.

Adversary actions for avoiding detection by the inspector's system are of three types.

(1) Stealth. The adversary makes no attempt to avoid detection, relying instead on uncertainties or omissions in the inspector's plan for success.

(2) Facility Misoperation. The adversary manipulates the facility operations to avoid detection. This includes disrupting electrical power, falsifying reported measurements, modifying the facility design, or replacing nuclear material with a replica.

(3) Tampering with the Inspection System. The adversary avoids detection by manipulating the inspection system. This includes tampering with inspector standards, measurement instruments, or surveillance sensors.

Clearly, an adversary scenario for materials diversion may involve aspects of each of these three strategies.

5. Anomaly Detection

Associated with each adversary action are anomalies in the facility environment that may be detected by the inspector's system. Examples of anomalies created by adversary actions are an increased radiation environment when material enters a portal monitor, absence of a fuel assembly from an assigned location, and a discrepancy between an operator's and an inspector's measured value. A convenient method for summarizing adversary actions, associated anomalies, and relevant inspector countermeasures for anomaly detection is the threat/countermeasure summary in Table II that is representative of an LWR. This summary is useful for assuring that all anomalies are potentially detected by at least one inspection activity and that there is sufficient detection redundancy to avoid vulnerability to common-cause failures. Appropriate modifications to the inspection system are suggested by any inadequacies in anomaly detection that are

TABLE II

THREAT/COUNTERMEASURE SUMMARY

Adversary Action	Anomaly	Activity Sensitive to Anomaly
Tamper with seal on reactor containment	Seal identity and/or integrity not correct	Monitor seal condition
Clandestine movement of fresh-fuel assembly into core	Missing fresh-fuel assembly	Count assemblies, audit facility records, surveillance with optical or motion sensors
Tamper with storage pool surveillance monitor	Indication of tampering from tamper-protection device	Monitor status of tamper-protection device
Clandestine movement of spent-fuel assembly from core to pool	Incorrect pool inventory	Count assemblies, audit facility records
	Unauthorized activity in storage pool	Surveillance with optical or motion sensors
Clandestine removal of spent-fuel assembly from facility	Unauthorized shipment of spent fuel	Surveillance with optical or motion sensors
Falsify facility records	Inconsistency between facility records and inventory	Inspection of facility records

evident in this table. One of these tables should be constructed for each credible adversary scenario.

6. Performance Measures

Design principles presented in this report describe how to identify fundamental inspection activities and integrate them to accomplish Inspectorate objectives efficiently. Because these methods may lead to a number of admissible designs, the system designer requires some rationale for choosing a most preferred design. A useful decision tool for selecting a final design is a performance measure that assigns to each design a numerical value representing the degree of accomplishment of Inspectorate objectives. In this report, we consider the general objective "detect anomalies related to materials loss and/or unauthorized personnel actions" and employ as the performance measure the probability of detecting such anomalies.

For many inspection activities, assignment of a probability of detecting an anomaly is straightforward as in the sampling of a storage area to detect a missing item. However, for other activities, such as film camera surveillance, performance evaluation becomes more subjective. In those instances where such probabilities are not readily available, the analyst might assign a subjectively derived number representing his confidence that detection occurs.

A further issue in assigning a probability of detecting an anomaly is the effect of adversary actions on the performance of an inspector activity. For example, an attributes measurement on an item under normal circumstances should have a high probability of detecting a gross defect in the item. However, if an adversary action in the scenario includes tampering with the instrument, then the probability of detecting a defect could be degraded depending on the skill of the adversary. Alternatively, an inspection system that includes tamper protection would have some probability of detecting the adversary tamper act.

The probability that inspector use of an instrument for an attributes measurement leads to anomaly detection in a scenario that includes instrument tampering as an adversary action is calculated as follows: (1) if the inspection system does not include tamper protection of the instrument, a probability P_D of detecting an item defect with the tampered instrument is assigned; or (2) if the instrument is tamper-protected, the probability of detecting an anomaly either as an item defect or as a tampering attempt is given by $P_D(1 - P_T) + P_T$, where P_T is the probability of detecting tampering. Thus, by considering the inspection activity and the protection of that activity as a combined activity, it is possible to assign a combined probability of detecting an anomaly when an activity is tamper protected.

7. System Optimization/Evaluation

Each inspection system design is evaluated against adversary scenarios by (1) listing the sequence of adversary actions and their associated anomalies, (2) determining the inspector activities that can detect each anomaly and the

probability of detection, and (3) calculating the total probability that at least one adversary action in the scenario is detected. This probability provides a rationale for preference ordering the designs.

Frequently, selecting the combination of fundamental activities that are to comprise the inspection system can become quite complex when the number of activities and options for each activity is large. In such instances, the system designer is faced with evaluating large numbers of potential system configurations in an attempt to find a design that maximizes system performance. This search is further complicated by a resource constraint such as an upper limit on cost, requiring that each candidate design be evaluated for resource usage. For even relatively small facilities, a straightforward evaluation of all designs becomes difficult to implement.

This report suggests that a more feasible alternative is to formulate the design problem as a mathematical optimization problem, which is solved by standard algorithms that are efficient in determining the optimal choice of inspector's activities. For the purpose of illustrating the proposed method, consider the list in Table III of potential inspector activities for an LWR. Each activity has several options, and the design problem consists of selecting an appropriate combination of activity options. Associated with each activity option in Table III is a probability of detecting an anomaly caused by the example adversary scenario, and the cost to the Inspectorate of implementing the option. The probabilities and costs in Table III were chosen arbitrarily and are not representative of actual inspection parameters. Note that even in this simple design problem there are more than 700 possible design configurations.

Representing the options for the i^{th} inspector activity A_i as a collection $A_i = \{a_{i1}, \ldots, a_{in}\}$, the probability that option a_{ij} detects an anomaly as $P(a_{ij})$, and the cost of option a_{ij} as $C(a_{ij})$, the design problem becomes

$$\underset{a_{ij} \in A_i}{\text{MAX}} \left\{ 1 - \prod_{i=1}^{N} \left[1 - P(a_{ij}) \right] \right\} ,$$

under the resource constraint,

$$\sum_{i=1}^{N} C(a_{ij}) \leq C ,$$

where just one a_{ij} is selected from each A_i, C is the total amount of available resources, and N is the number of inspector activities. The solution to this problem is a choice of activity options $\{a_{1j}, \ldots, a_{Nj}\}$ that maximize the probability of detecting the adversary actions while not exceeding the total cost C. A dynamic programming algorithm for solving this problem is found in standard texts such as Ref. 5.

A useful application of this method is studying the sensitivity of inspection system performance to the amount of resources invested in the system. Dependence of the probability of detecting the adversary scenario on available resources is illustrated in Table IV for the LWR inspection options given in Table III. Clearly, investing resources exceeding 20 units in this system is not efficient because the probability of detection does not increase appreciably above that amount. Table V gives the optimal choice of inspection options when 20 units of resource are available.

Although in this example problem only a single adversary scenario was used in optimizing the design, the method is applicable to system optimization against any number of potential adversary scenarios. For multiple scenarios, the design objective is to choose a system that maximizes the minimum detection probability against any of the postulated scenarios.

TABLE III

INSPECTOR ACTIVITY OPTIONS FOR AN EXAMPLE LWR

	Detection Probability	Cost
A. Examine Reports		
1. No report examination	0	0
2. Compare facility records with reports	0.2	1
3. #2 + determine consistency of facility records	0.4	2
B. Fresh-Fuel Verification		
1. No verification	0	0
2. Perform item count & compare to records	0.2	1
3. Sample items, verify identity & integrity	0.2	3
4. #2 & #3	0.8	6
C. Spent-Fuel Verification		
1. No verification	0	0
2. Perform item count & compare with records	0.2	1
3. Sample items & verify integrity & identity	0.2	5
4. #2 & #3	0.8	6
D. Surveillance of Core		
1. No surveillance	0	0
2. Seal core containment	0.3	3
3. Optical surveillance of core	0.5	5
4. Optical surveillance of core & tamper protect sensor	0.8	9
5. #2 & #4	0.85	10
E. Surveillance of Storage Pool		
1. No surveillance	0	0
2. Optical surveillance of pool	0.1	3
3. #2 & tamper protection of monitor	0.8	9

TABLE IV

DEPENDENCE OF EXAMPLE SYSTEM PERFORMANCE ON RESOURCE ALLOCATION

Resource Allocation Units	Detection Probability
1	0.20
5	0.61
10	0.90
15	0.96
20	0.99

TABLE V

OPTIMAL DESIGN FOR A 20-UNIT RESOURCE ALLOCATION

Activity	Number	Option[a] Cost	P_D
A. Examine reports	3	2	0.4
B. Fresh-fuel verification	4	6	0.8
C. Spent-fuel verification	4	6	0.8
D. Surveillance of core	3	5	0.5
E. Surveillance of storage pool	1	0	0.0

[a]Options are described in Table III.

8. Hierarchical Resource Allocation

This report has restricted consideration to optimizing the design of an inspection system for a single facility, but, in fact, the method also applies to optimal allocation of inspection resources among a number of states each having multiple facilities to be inspected. This hierarchical optimization problem is illustrated in Fig. 3, which describes the three levels where resources must be allocated to achieve the best global inspection system. Work on developing the mathematical algorithm for optimizing the design of a global inspection system is presently in progress in the Safeguards Systems Group at Los Alamos. When complete, this method would allow an international safeguards agency to allocate resources among States to achieve the best inspection system for the investment.

References

1. A. P. Sage, Methodology for Large-Scale Systems (McGraw-Hill Book Co., New York, 1977).

2. J. D. Hill and J. N. Warfield, "Unified Program Planning," IEEE Trans. Syst., Man, Cybern., Vol. SMC-2 (November 1972), pp. 610-621 .

3. J. T. Markin, C. A. Coulter, R. G. Gutmacher, C. C. Thomas, Jr., and W. J. Whitty, "Design and Evaluation Methods for an Integrated Safeguards System," Los Alamos National Laboratory, Safeguards System Group draft report.

4. R. L. Keeney and H. Raiffa, Decisions with Multiple Objectives: Preference and Value Tradeoffs (Wiley & Sons, New York, 1966)

5. G. L. Nemhauser, Introduction to Dynamic Programming (Wiley & Sons, New York, 1966).

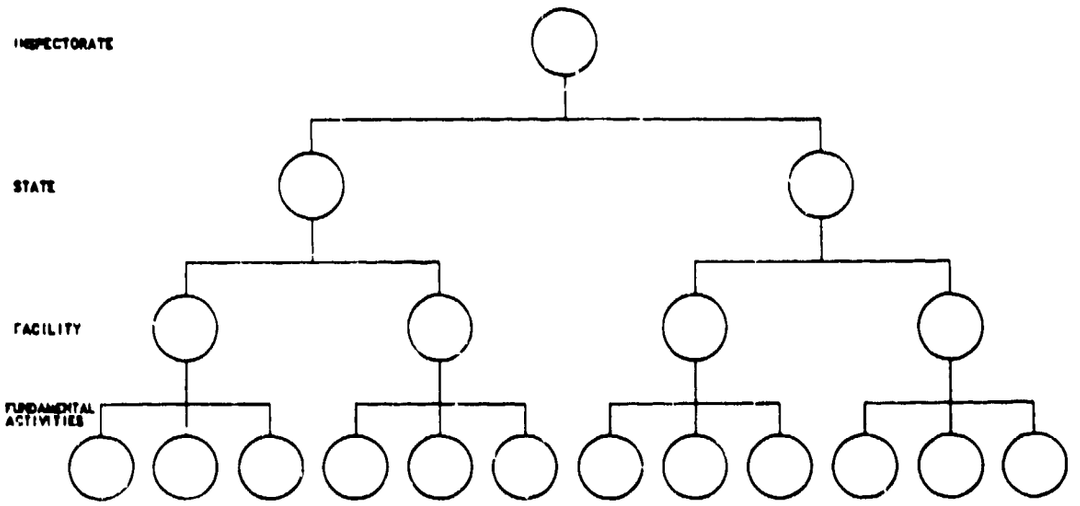

Fig. 3. Inspection-resource allocation hierarchy.