SAND76-0428
Unlimited Release

SAFEGUARDS SYSTEM EFFECTIVENESS MODELING*

Drayton D. Boozer
Systems Studies and Engineering Division 1754

Bernie L. Hulme
Numerical Mathematics Division 5122

Sharon L. Daniel
Reactor Safety Studies Division 5411

G. Bruce Varnado
Nuclear Fuel Cycle Systems Safety Division 5412

Harold A. Bennett, Leon D. Chapman, and Dennis Engi
Systems Analysis Division I 5741
Sandia Laboratories
Albuquerque, NM 87115

ABSTRACT

A general methodology for the comparative evaluation of physical protection system effectiveness at nuclear facilities is presently under development. The approach is applicable to problems of sabotage or theft at fuel cycle facilities. In this paper, the overall methodology and the primary analytic techniques used to assess system effectiveness are briefly outlined.

Printed in the United States of America

Available from
National Technical Information Service
U. S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161
Price: Printed Copy $4.50; Microfiche $2.25

*Presented at the 17th Annual Meeting of the Institute of Nuclear Materials Management, Seattle, WA, June 22-24, 1976.

ACKNOWLEDGMENTS

The authors are indebted to Diane Holdrige for her development of subroutines which implement the shortest path algorithms in versions tailored to our special needs and to R. B. Worrell for his suggestions on the application of set equation manipulation routines to the vital location analysis.

SAFEGUARDS SYSTEM EFFECTIVENESS MODELING

Introduction

Sandia Laboratories is currently engaged in several ERDA and NRC sponsored programs dealing with the physical protection of nuclear materials and nuclear facilities. To provide a systematic approach to the problem of physical security, a methodology has been developed which considers the interrelations of elements within the overall system and provides a framework for the system integration of each element.

To implement the methodology, several analytic tools have been developed to identify key plant protected areas and to evaluate various alternatives to the security system.

Methodology

The safeguards effectiveness evaluation methodology discussed here combines several analytic techniques to provide a means of assessing the relative vulnerability of fixed facilities to sabotage or theft. The elements of the analytic procedure are shown in Figure 1.

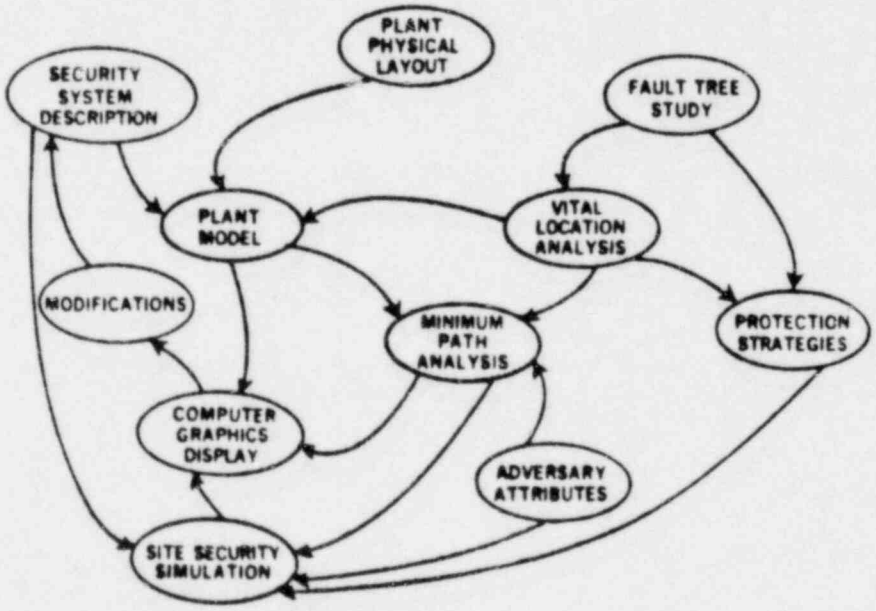

Figure 1. Safeguards Effectiveness Evaluation

The basic input information required includes: 1) definition of what can be done to cause the undesired event (Fault Tree Study), 2) physical description of the facility (Plant Physical Layout), 3) details of the security system (Security System Description), and 4) characteristics of the adversary (Adversary Attributes). From this initial information a model of the facility is developed which reflects the physical characteristics of the site and the likely targets for sabotage or theft. Specific adversary action sequences which place the greatest stress (in some sense) on the security system are analytically selected for detailed analysis. These sequences are defined in terms of paths from the boundary of the facility to one or more target areas. The barrier penetration times, alarm probabilities, and guard response information for the paths are used along with the adversary attributes in a simulation model to obtain a relative measure of the effectiveness of the security system. Alternative security systems are evaluated by modifying the appropriate parameters in the plant model and cycling through the path analysis and simulation model. The variation of system effectiveness with changes in the model parameters can be rapidly evaluated by repeated application of the process. An interactive computer graphics display system provides an efficient means of changing input data and reviewing the results at different stages of the cycle.

The fundamental analytical tools used in the analyses are fault tree analysis, graph-theoretic modeling, and system simulation modeling. The application of each of these mathematical techniques to the effectiveness evaluation process is discussed below.

Fault Tree Analysis

A fault tree is a logic diagram which graphically represents all of the combinations of component and subsystem events which can result in a specified undesired system state. The undesired state for our purposes is either the theft of nuclear material or the sabotage of a nuclear facility. The fault tree analysis provides a means to inventory the combinations of initiating events which can produce the undesired event.

The fault tree study provides the information on what must be done to cause the undesired event. In regard to sabotage, the fault tree specifies the combinations of destructive or damaging manipulations an adversary must complete to cause the release of radioactivity from the facility. Each combination of initiating events is specified as a term in a logic equation[1,2]. The fault tree study can be performed on a generic basis (to some level of detail) to define the subsystems and components which require protection in a given type of facility.

The next step in the modeling process is to determine where in the facility the various initiating events can be accomplished (Vital Location Analysis). Each initiating action in the system fault tree is replaced by the location or combination of locations at which the action can be accomplished. This amounts to a transformation of variables[3] in the event equation to obtain a location equation for the undesired event, that is, to determine the combinations of

locations to which the adversary must gain access. The location information is directly related to physical protection of the site because the locations are identified as buildings, rooms, and compartments for which barrier, alarm, and assessment systems can be designed.

Strategies for protection of the facility can be formulated by further processing of the location equation. By forming the complement of the equation, one can determine the minimum sets of locations which must be protected in order to assure that none of the action sequences can be completed. Measures such as cost or impact on operability may also be applied to the locations to obtain an ordering of the complement terms with respect to the desired measure. The effect of response measures other than guard force action can also be assessed. Damage control measures, which provide a defense against certain sabotage acts [4], can reduce the requirements for physical protection in some areas of the plant. Analyses such as these can help set priorities for protection of vital locations.

The usefulness of these techniques is illustrated in their application to the LWR sabotage problem. The fault tree for a typical LWR contains approximately 250 initiating actions. There are literally thousands of combinations of these initiating actions which will cause the undesired event, far too many for a detailed analysis of each. The initiating actions can be accomplished at 35 locations with 125 possible combinations leading to completed sabotage action sequences. The minimum complement set contains 11 locations. Therefore, it would be possible to preclude all of the thousands of possible sabotage sequences at an LWR by assuring that the adversary could not gain access to 11 specific locations.

The next step is to select for detailed analysis one or more paths from the boundary of the facility to each of the locations of interest. The paths chosen should be ones which optimize the adversary's probability of success and therefore place the greatest burden on the safeguards system. The process for selecting these "most stressing" paths is discussed in the following section.

Minimum Path Analysis

In a facility as large and complex as a nuclear power reactor plant, there is an enormous number of possible paths an adversary can take to complete a particular action sequence. In order to systematically study these possibilities, a discrete model of the plant layout called a graph [5] has been developed. A graph is simply a network of nodes and arcs. In our model the nodes represent locations (i.e., points on the plant boundary, on internal barriers, and at vital hardware locations), and the arcs are ways to travel between locations. Both the nodes and arcs are assigned weights which are measures of some quantity to be minimized. By looking for certain paths in the graph that are shortest in the sense of the given weights, one can find physical routes through the plant that are optimal for the adversary. When shortest-time paths are sought, the boundary and barrier node weights are minimum penetration times, the hardware node weights represent minimum removal or destruction times, and the arc weights are minimum transit times.

The theft problem is to find all the shortest paths from any boundary node to any one hardware node and then back to any boundary node. In the sabotage problem different combinations of the hardware nodes in the graph form minimal sets of hardware whose destruction can cause a nuclear release, and the adversary's escape is not essential. The sabotage problem then is to find all the shortest paths from any boundary node through all of the hardware nodes or locations in one of the sets that could lead to completion of a sabotage sequence without returning to the boundary. Unfortunately, the sabotage problem is difficult to solve efficiently. Therefore, a lower bound on the sabotage times is obtained by studying the worst-case situation of simultaneous sabotage by several teams each having only one hardware node as a target.

Even with a computer it is impossible, in a reasonable amount of time, to identify and evaluate the length of every path of the type to be minimized because the number of such paths can be factorial in the number of nodes. However, a technique has been developed for applying to both the theft [9] and the simultaneous sabotage [15] problems an algorithm due to Dijkstra [6, 5] as modified by Yen [7, 8]. This algorithm is the best known search procedure for finding the lengths of the shortest paths in a graph from one node to all others because it is guaranteed to work and the computer run time is proportional to only the square of the number of nodes. A process which retraces and saves all of the shortest paths as well as their lengths has been added to the Dijkstra algorithm.

Computer Graphics Package

An interactive computer graphics program has been developed to compute and display the shortest paths in a graph model of a nuclear power reactor plant. The physical layout of the plant (locations of buildings, obstacles, equipment, and vital materials) can be displayed in plan view on the graphics screen together with the shortest paths to the vital locations. The interactive capability allows the analyst to change plant characteristics from the graphics terminal and thereby to rapidly assess the effect of upgrades in plant defenses.

The internal barriers subdivide a plant into regions, and each level of a building contains one or more regions. To display the details of either a level or a region, it is necessary to digitize 1) the lines defining the level or region, 2) the coordinates of the graph nodes (boundary, barrier, and hardware) of the level or region, and 3) the coordinates of pseudo-nodes which outline obstacles within a region. These coordinates are also used to automatically compute the arc weights for the graph model as follows.

The arc weights are the transit times between each pair of nodes of a region. In each region an auxiliary graph is constructed by connecting every node and pseudo-node by a straight line to every other node and pseudo-node, except that such lines intersecting obstacles in the region are deleted. Floyd's algorithm [10, 5] is applied to each auxiliary graph to find the lengths of the shortest paths between every pair of nodes in the corresponding region. Because of the way the auxiliary graph is constructed, these distances are the lengths of routes which go around, not

through, obstacles within a region. Therefore, distances for shortest physical routes between nodes are obtained, and these are divided by travel velocities to obtain the desired arc weights. The path analysis program provides barrier sequences and delay time information for use in the simulation modeling.

Simulation Models

Dynamic simulation models have been developed to obtain a better understanding of the complex interactions between adversaries and security system components. Many of the relationships used in these models are difficult to define and so are based on either experience or intuition. As such, many would be quick to discount the potential of such a model on the basis of inadequate data; however, the purpose of a model should be to explore the interrelationships of the variables, their relative importance, and required accuracy. In addition, constructing the model forces the analyst to openly describe relationships between components, acknowledge inconsistencies, and critique results. It also offers a straightforward solution to otherwise hard-to-envision multidimensional interactions.

Within the framework of the above statements, the dynamic models can provide a relative evaluation of proposed changes in safeguards systems.

Forcible Entry Safeguard Effectiveness Model (FESEM) -- The Forcible Entry Safeguard Effectiveness Model [11] is used to evaluate alternative fixed-site protection systems. The model requires as input the characteristics of the fixed-site to be evaluated. Response forces must be characterized by number, size, response time, and probability of their receiving valid communication of both external and internal attacks. (External implies no inside assistance while internal means the adversary has inside assistance.) Barriers must be specified by number, type, and thickness. If the barrier is alarmed, the probability of the alarm working for external and internal attacks must be specified. The distance between barriers and the probability of a high explosive (HE) detonation being detected if the adversary uses HE to penetrate a barrier must be inputs to FESEM.

The model is capable of selecting the adversary attributes at random for attacks against the fixed-site design. These attributes include the number of adversaries, types of weapons (side arms or automatic weapons), and their resources for barrier penetration (such as tools but no HE, or tools plus HE). In addition, four types of adversary attacks are considered - sabotage/internal, sabotage/external, theft/internal, and theft/external. Internal attacks imply that the adversaries have an insider working at the fixed-site who may, by intent or under duress, degrade the alarm and communication systems. The mode of transportation (vehicles, no vehicles, or air vehicles) and the dedication of the adversaries can be treated as random variables in the generation of adversary attributes.

Given these inputs, along with an attack path, the computer model can simulate a large number of adversary attacks against the site design to evaluate the effectiveness of the design concept. Barrier breaks, delays provided by barriers, crossing times between barriers, and advancements along the paths are simulated by a random sample from probability distributions. Alarms at a given barrier may trigger communications to the on-site guard force which corresponds to the scene and assesses the situation. Off-site guards are called if a serious alarm condition exists. Upon the arrival of any guard force, an engagement is initiated with the adversary. During the engagement simulation [12, 13, 14], the adversary advancement is assumed to be interrupted. If the adversary wins the engagement, then his advancement continues until interrupted by the arrival of the off-site guard force or completion of the theft or sabotage. This ends one simulation. After a large number of attacks has been simulated, statistics can be accumulated to determine the relative effectiveness of the site design against the given level of threat.

FESEM provides a framework for performing inexpensive experiments on fixed-site security systems and for determining the relative cost-benefit of different safeguards options. What has evolved with the development of FESEM is a structured approach that is analytically based and which can provide an evaluation of proposed fixed-site security changes. The validity of the model should improve as improved data become available and different site configurations are studied.

Insider Safeguard Effectiveness Model (ISEM) -- The purpose of ISEM is to simulate the interaction of insiders with the security system of nuclear facilities. In ISEM insiders are assumed to be the threat, whereas in FESEM insiders serve to degrade the effectiveness of the safeguards system against an external threat. The initial model development has concentrated on the personnel control system, that is, the set of sensors, portals, barriers, and security forces used to control personnel within a nuclear facility. ISEM can model various attack modes (force, stealth, deceit) for theft or sabotage.

The plant consists of three basic entities: areas, portals, and barriers. Portals may be either personnel, material, or vehicle types. Gates and doors are also considered to be special cases of portals. Area, point, or line sensors may be located at any plant entity. Examples of area sensors are CCTV's, microwave, and ultrasonic sensors. Point sensors include SNM sensors in portals and pressure sensors in glove boxes. Line sensors are typically located at fences and may respond to one of several parameters such as pressure, seismic shock, etc.

Plant personnel are either guards or employees. Personnel have authorized access to specified plant areas. Guards are further subdivided into on-station and patrol guards. Typically, patrol guards are used for response to more serious alarms whereas on-station guards are used to operate portal sensors and to assess alarms from these sensors. Skill and authorized access attributes are used for employees identified as insiders to determine the sensor alarm

probabilities. This probability is also affected by the personnel density and the number of CCTV's in the area. Following an assessment delay, an action is taken based on a preplanned response to each alarm.

It is evident that a large number of possible insider exit paths exists if one allows the possibility of forcible "breakout" scenarios. Generally only a subset of plant entities and sensors are involved in a particular insider path; however, ISEM is structured so that initially all required plant data can be input and then used only on the paths for which it is applicable.

For a particular path, the model is best illustrated by the sequence shown in Figure 2. This particular path involves insider exit from a material access area, through two portals, to the plant exterior. For this case, two sensor systems are shown. The response typically involves guards; however, action such as locking portals can be taken.

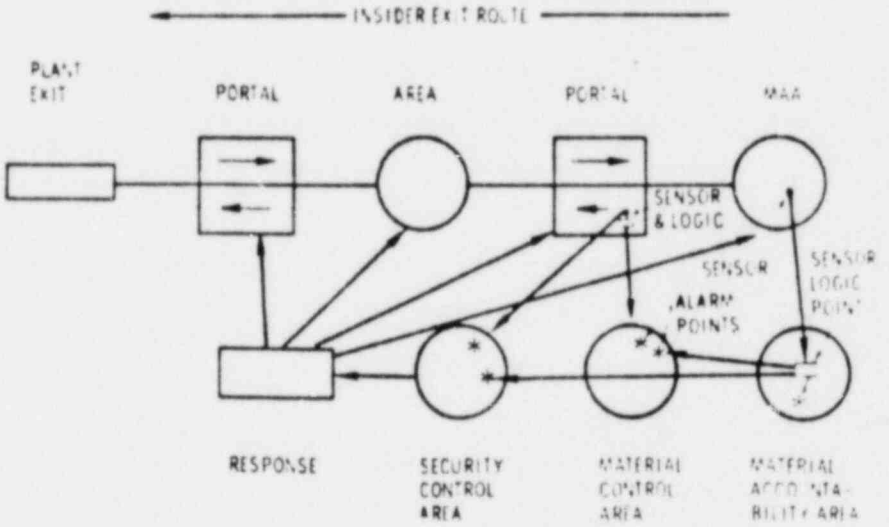

Figure 2. Insider Sequence/Safeguard System Interaction

The actual engagement between insiders and guards is modeled as a discrete-state/continuous-time stochastic process in which guard arrivals are counted and constrained to insure feasibility. Transition times between states are assumed to be continuous random variables which can be a function of force size, weapons, competence, and other parameters that are thought to be relevant and quantifiable. Distributions of the transition times, along with a count of the number of guard arrivals, completely specify the stochastic process which describes the engagement.

The Insider Safeguard Effectiveness Model (ISEM) is based on the following assumptions: 1) a critical insider path is identified at input, 2) one insider carries the material, 3) all insiders potentially degrade alarm systems, 4) guard responses are preplanned for each alarm,

5) employees and guards are treated as groups having composite attributes, and 6) insiders are identified on an individual basis. Further extensions to ISEM will involve development of an insider sequence generator, inclusion of individual personnel attributes, and continuing development of the engagement model. The primary contribution of ISEM is that it provides a consistent framework within which safeguard system effectiveness measures can be generated for the personnel control aspect of the insider problem.

Conclusion

The modeling techniques described above have been applied to a variety of nuclear facilities. Each of the models is being refined and extended as additional data and theoretical advancements become available.

The applicability of the overall methodology has been demonstrated in the analysis of a typical LWR plant. The results of that analysis are being used to guide the conceptual development of a balanced LWR safeguards system.

References

1. R. B. Worrell, Set Equation Transformation System (SETS), SLA-73-0028A, Sandia Laboratories, Albuquerque, New Mexico, July 1973.

2. M. D. Olman, Use of the Set Evaluation Program (SEP) in Fault Tree Analysis, SAND76-0168, Sandia Laboratories, Albuquerque, New Mexico, to be published, 1976.

3. R. B. Worrell, Common Event Analysis Using Variable Transformations, SAND76-0024, Sandia Laboratories, Albuquerque, New Mexico, to be published, 1976.

4. D. J. McCloskey, Safety and Security of Nuclear Power Reactors to Acts of Sabotage, SAND75-0504, Sandia Laboratories, March 1975.

5. N. Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice-Hall, Englewood Cliffs, 1974.

6. E. W. Dijkstra, "A Note on Two Problems in Connection with Graphs," Numer. Math., Vol. 1, pp. 269-271, 1959.

7. J. Y. Yen, "Finding the Lengths of All Shortest Paths in N-Node Nonnegative-Distance Complete Networks Using $1/2N^3$ Additions and N^3 Comparisons," J. Assoc. Comput. Mach., Vol. 19, pp. 423-424, 1972.

8. T. A. Williams and G. P. White, "A Note on Yen's Algorithm for Finding the Length of All Shortest Paths in N-Node Nonnegative-Distance Networks," J. Assoc. Comput. Mach., Vol. 20, pp. 389-390, 1973.

9. B. L. Hulme, Graph Theoretic Models of Theft Problems. I. The Basic Theft Model, SAND75-0595, Sandia Laboratories, Albuquerque, New Mexico, November 1975.

10. R. W. Floyd, "Algorithm 97, Shortest Path," Comm. ACM., Vol. 5, p. 345, 1962.

11. L. D. Chapman, Effectiveness Evaluation of Alternative Fixed-Site Safeguard Security Systems, SAND75-6159, presented at the 1976 Summer Computer Simulation Conference, July 12-14, 1976, Washington, D.C.

12. H. A. Bennett, Dynamic Model of a Terrorist Attack, SAND75-0658, Sandia Laboratories, Albuquerque, New Mexico, February 1976.

13. F. W. Lanchester, Aircraft in Warfare: The Dawn of the Fourth Arm, Constable, London, 1916.

14. P. M. Morse and G. E. Kimball, Methods of Operations Research, John Wiley and Sons, 1971.

15. B. L. Hulme, Pathfinding in Graph-Theoretic Sabotage Models. I. Simultaneous Attack by Several Teams, SAND76-0314, Sandia Laboratories, Albuquerque, New Mexico, June 1976.