LIGHT WATER REACTOR SAFEGUARDS SYSTEM EVALUATION

G. B. Varnado, D. M. Ericson, Jr., H. A. Bennett,
B. L. Hulme, S. L. Daniel

Sandia Laboratories
Albuquerque, New Mexico, U.S.A.

INTRODUCTION

This paper describes the development and application of a methodology for evaluating the effectiveness of nuclear power reactor safeguards systems. Analytic techniques are used to identify the sabotage acts which could lead to release of radioactive material from a nuclear power plant, to determine the areas of a plant which must be protected to assure that significant release does not occur, to model the physical plant layout, and to evaluate the effectiveness of various safeguards systems. The methodology was used to identify those aspects of reactor safeguards systems which have the greatest effect on overall system performance. Refinements of the methodology currently in progress will provide licensing reviewers and system designers a systematic procedure for assessing proposed or existing safeguards systems.

Prior studies of the vulnerability of nuclear power reactors to sabotage identified actions which could lead to the release of radioactive material beyond plant boundaries. It was concluded that the design and operating features of nuclear power plants and their engineered safety features provide inherent protection against acts of sabotage. Nevertheless, recommendations were made for further reduction of power plant vulnerability.[1] Other studies sponsored by the United States Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) provided data and models useful in evaluating reactor safeguards.[2,3] Starting with this

ENS/ANS international topical meeting on nuclear power reactor safety, Brussels, 16-18 October 1978

background, we developed a general framework for evaluation of reactor safeguards systems.[4]

There are several possible sources of radioactive material at a power reactor plant: the core, the spent fuel pool, the new fuel storage vault, spent fuel shipping casks, and the radioactive waste system. The physical form, chemical composition, and radiation level associated with materials from these sources make theft of radioactive material from light water reactors an unlikely terrorist goal. For this study the primary safeguards concern was sabotage as a result of forcible attack by a group of outsiders leading to release of significant quantities of radioactive material. The methodology developed to evaluate the effectiveness of a reactor safeguards system against this type of attack and its application are discussed below.

METHODOLOGY

Figure 1 illustrates the major steps in the methodology developed in this study. The fundamental analytical tools used are fault tree analysis, an extension of basic fault tree techniques called vital area analysis, graph-theoretic modeling, and system simulation modeling. The role of each of these mathematical techniques in the effectiveness evaluation process is discussed below.

Fault Tree Analysis

Nuclear power reactors are designed with redundant and diverse systems to prevent release of radioactive material. To define the many possible combinations of events which could cause a significant release from the plant requires the application of a systematic analytic method. Fault tree analysis has been found to be an appropriate tool for this purpose.

A fault tree is a logic diagram which graphically represents the combinations of component and subsystem events that can result in a specified undesired system state. The undesired state (or event) is the release of significant amounts of radioactive material from the plant as a result of sabotage. In the fault tree analysis, this undesired event is developed into logical combinations of contributing events, each of which is further developed in turn until primary events terminate each branch of the tree. Primary events are individual sabotage acts such as disabling a pump or severing a pipe.

A logic equation, equivalent to the fault tree, is obtained by successive substitution of events lower in the tree for ones higher until the undesired event is expressed solely in terms of primary events. Each combination of primary events sufficient to cause release appears as a term in the logic equation representing the tree. Boolean algebraic manipulation of the equation provides a powerful analytic tool for determining protection requirements.

Vital Area Analysis

The primary events in the fault trees are sabotage actions which in certain combinations (as specified by the logic of the tree) can lead to release of radioactive material from the plant. It is also important to know where in the plant the adversary must go to accomplish these acts in order to ensure that the safeguards system design includes protective mechanisms for the buildings, rooms, and compartments within which the sabotage actions can be accomplished. In this step in the modeling process each primary event in the system fault tree is replaced by the location or logical combination of locations where the action can be accomplished. This amounts to a transformation of variables in the event equation described above to obtain a location equation for the undesired event. This location equation represents the combinations of locations to which the adversary must gain access in order to cause

the undesired event. Each combination of locations (each term in the location equation) may represent a single combination or thousands of combinations of primary events, depending upon how many events can be accomplished at each location and how the events combine to produce release. There are usually fewer locations than primary events; therefore, the location equation is typically much simpler than the event equation.

The location equation can be processed further to identify a minimum set of locations (critical location set) the protection of which will interrupt all possible sequences leading to release. This is done by taking the Boolean complement (logical NOT) of the location equation. If access is denied to all the locations in one term of the complement equation, then none of the event combinations leading to release can be accomplished. The terms in the complement equation can be ordered according to the number of locations in each term or any quantitative value (such as cost of protection or impact on operability) which can be associated with each location.

Minimum Path Analysis

The previous portion of the analysis identified a set of plant locations which the safeguards system must protect. 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 of greatest interest are those which optimize the adversary's probability of success and therefore place the greatest stress on the safeguards system.

Rather than evaluating every term in the location equation independently, the approach taken here is to determine an upper bound on the likelihood of adversary success. To conservatively evaluate the safeguards systems, we have assumed that the adversary will optimize his action sequence; thus, it is necessary to know what paths through the plant are optimal for the adversary. Given the critical locations, identified by

means of the above fault tree and vital area analyses, the approach used in this study is to find one or more minimum-time paths to each critical location. Minimizing time does not necessarily maximize probability of adversary success in all cases. But in the facility analyzed in this study, detection systems are deployed uniformly around the targets. As a result, minimum time paths are generally ones which also minimize detection probability and maximize probability of adversary success. Techniques are under development which will allow computation of paths that are truly optimum for the adversary.

Graph-Theoretic Modeling: For purposes of pathfinding, a discrete model of the plant layout, called a graph, is developed. A graph is simply a network of nodes and arcs. The nodes represent locations on the boundary, on the internal barriers, and at targets, while the arcs represent ways to travel between locations. Both the nodes and the arcs are assigned weights which are measures of some quantity to be minimized. Here, the node weights represent barrier and boundary penetration times or sabotage times, and the arc weights represent transit times. Thus, the shortest paths are those which minimize time. Other measures of path length, such as distance or detection probability can be used but only shortest-time paths were considered in this study.

A very efficient shortest path algorithm has been adapted and applied to the sabotage problem.[5] This algorithm finds the lengths of the shortest paths from one node to all others. The efficiency of the algorithm stems from the fact that it gathers information only about the shortest paths and thereby avoids wasting time on the vast number of non-shortest paths.

Computer Graphics Display System: An interactive computer graphics program has been developed to display the shortest paths in a graph 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.

Simulation Model

A dynamic simulation model, the Forcible Entry Safeguard Effectiveness Model (FESEM), was developed in an earlier study to simulate the complex interactions between adversaries and security system components.[6] The purpose of the model is to explore the relative importance to safeguards system effectiveness of various characteristics (such as probability of intrusion detection, delay times, and guard force characteristics), adversary attributes, and attack paths. The model requires as input the characteristics of the fixed-site to be evaluated including: (1) the number, size, and response time for the response forces and probability of their receiving valid communication of attacks, (2) the number, type, and thickness of barriers, and the probability of detection at alarmed barriers, (3) the distance between barriers, and (4) the probability of a high explosive (HE) detonation being detected if the adversary uses HE to penetrate a barrier. The information for items (2) and (3) can be obtained from the data used or generated in the minimum path analysis.

Given these inputs, along with the adversary characteristics, the FESEM can simulate adversary attacks against the site design. Barrier breaks, delays provided by barriers, crossing times between barriers, and advancements along the paths are simulated by a random sample from input probability distributions. An engagement simulation model is used to predict the outcome of armed confrontations between the adversary and the guard force. After a large number of attacks has been simulated, statistics are accumulated to determine the relative effectiveness of the safeguards system against the assumed threat.

The primary output of the simulation model is the probability of adversary defeat, P_{SI}, which represents the probability that the safeguards system functions properly and prevents the adversary from completing his intended malevolent action. In principle, a P_{SI} could be computed for every forcible adversary action sequence which might result in release of material; in practice, it is possible to consider only a small fraction of the very large set of possible sequences. Thus, the simulation modeling was limited to sequences along the shortest-time paths to each of the critical locations. This procedure determines an approximate lower bound on P_{SI} for all sequences because one or more of the critical locations must be visited in every sequence.

APPLICATION OF THE METHODOLOGY TO A TYPICAL LWR PLANT

To evaluate different safeguards system options and to verify the applicability of the method described in the previous section, a detailed, conceptual study was performed for a typical nuclear power reactor plant. This typical plant provided a physical model for the structural characteristics and equipment layout. A safeguards system was proposed for the typical plant, and the effectiveness of the system was evaluated by application of the methodology discussed above. The elements of the safeguards system which contribute most to overall system effectiveness were identified by examining in the simulation model the sensitivity of the effectiveness measure (P_{SI}) to changes in the system paramaters.

Fault Tree and Vital Area Analysis Results

There are approximately 250 primary events in the fault tree for sabotage of the example plant and a large number of ways these events can combine to cause release of radioactive

material from the plant. When the basic events in the fault tree were replaced with the locations at which they can be accomplished, thirty-six vital areas were identified for the 250 primary events. The complement of the location equation for the typical plant contains many terms (combinations of locations) each with 15 or more literals (locations). Thus, preventing adversary access to as few as 15 of the 36 target areas would assure interruption of all adversary action sequences for the example plant.

Graph Model of the Plant

A graph of the example plant was developed for use in the process of path selection. The coordinates of all points of interest were obtained from scaled plot plans of the facility, and the graph was constructed to give an accurate visual representation of the site.

Five boundary nodes were arbitrarily selected as penetration points in the perimeter fence to give representative cases for adversary access to the site. The algorithm described earlier was used to find the shortest-time paths from these nodes to each of the vital areas. Barrier sequences, penetration times, and transit times were extracted from the shortest path data for use in the simulation modeling.

Simulation Modeling

The sensitivity of P_{SI} to changes in the safeguards system characteristics was evaluated using FESEM. Alarm system performance and composition, barrier delay times, on-and-off site response force characteristics and communications reliability were examined in the evaluations. The results of the parameter variation studies are summarized below.

Intrusion alarms form an important part of the physical protection system. The sensitivity of P_{SI} to the probability

of detection by the perimeter alarm system and the interdependence of perimeter and building alarms are illustrated in Figure 2. The points on the ordinate show the variation with door alarm probability when there is no fence alarm system. P_{SI} drops from about 0.95 for the case of high door alarms to about 0.4 with the door alarm reduced to a low value (0.1) as might be the case if the alarm could be defeated.

With high (0.97) probability of detection of the door alarms, increasing the perimeter alarm probability does not significantly improve P_{SI}, but it makes a dramatic improvement in system performance if the door alarms function in the medium to low range. One might conclude that a high door alarm probability is sufficient for intrusion detection in the physical protection system. However, another factor should be considered, namely, the locations at which engagements between adversary and response forces occur. Because both forces are armed and pitched battles are assumed probable, it is desirable that engagements occur outside of buildings to prevent collateral damage. The effect of the perimeter alarm on the location of engagements is illustrated in Figure 3. With no perimeter alarm, less than 30 percent of the engagements occur outside of buildings, but with a high alarm probability at the fence, practically all of them do.

Barrier delay times are difficult to estimate and will vary widely with the abilities and resources of the adversary as well as with the condition of the plant. The sensitivity of P_{SI} to changes in barrier delay is illustrated in Figure 4. If the barrier delay is not at least as long as the guard response time (2 minutes for the model), P_{SI} is adversely affected.

Reliable communications between the alarm station and the on-site guards and between the plant and the off-site response force are essential. Figure 5 illustrates the dependence of P_{SI} on the communications probabilities.

The off-site response force, made up of local law enforcement officers or off-duty guards, supplements the on-site force and constitutes the final line of defense for the plant. With the baseline system, P_{SI} was not very sensitive to changes in the response time of the off-site force. Doubling the off-site response time reduced P_{SI} by about 10 percent. Thus, time of arrival of the off-site force was not critical, given the assumed size of the on-site and adversary forces.

ADVANCED METHODOLOGY

More recent work has dealt with the simplification and refinement of the evaluation process. An automated approach called Safeguards Automated Facility Evaluation (SAFE)[7] has been developed to speed safeguards system evaluation and to provide improved analytical capabilities. SAFE consists of several operational modules for facility characterization, selection of critical paths, and evaluation of safeguards effectiveness along these paths. It has been implemented on an interactive computer time-sharing system and uses computer graphics for the processing and presentation of information. The modular form of SAFE makes it possible to substitute other functionally equivalent modules as they are developed. One of the major advances in SAFE is the ability to perform parameter variation studies very rapidly and comprehensively. The SAFE procedure should be useful to system designers and licensing bodies in the nuclear facility safeguards field as well as to those dealing with security problems in other fields.

CONCLUSION

The methodology developed in this study provides several advances in safeguards system effectiveness modeling. It provides a systematic means of identifying the areas of the plant which

must be protected to prevent sabotage leading to release of radioactive material. The concept of identifying a minimum set of locations whose protection will assure the interruption of all adversary action sequences should be very useful in minimizing costs and adverse operational impacts of reactor safeguards. The demonstration of the usefulness of graph-theoretic techniques in selecting adversary paths in facilities of the size and structural complexity of power reactors is another important advancement. A related development, the use of an interactive computer graphics system to display plant layout and path data, provides many advantages for the analyst in terms of input data preparation and visualization of results of the analysis.

REFERENCES

1. Safety and Security of Nuclear Power Reactors to Acts of Sabotage, SAND75-0504, Sandia Laboratories, Albuquerque, New Mexico, March 1976.

2. Physical Protection of Special Nuclear Material in the Commercial Fuel Cycle (U), SAND75-0457, Sandia Laboratories, Albuquerque, New Mexico, March 1976.

3. The initial development of pathfinding algorithms was sponsored by the DOE program titled "Physical Protection of Nuclear Materials at Fixed Facilities".

4. G. B. Varnado, D. M. Ericson, Jr., S. L. Daniel, H. A. Bennett, B. L. Hulme, Reactor Safeguards System Assessment and Design, Volume I, SAND77-0644, Sandia Laboratories, Albuquerque, New Mexico, June 1978.

5. B. L. Hulme, Pathfinding in Graph-Theoretic Sabotage Models. 1. Simultaneous Attack by Several Teams, SAND76-0314, Sandia Laboratories, Albuquerque, New Mexico, July 1976.

6. L. D. Chapman, Effectiveness Evaluation of Alternative Fixed-Site Safeguard Security Systems, SAND75-6159, Sandia Laboratories, Albuquerque, New Mexico, presented at the 1976 Summer Computer Simulation Conference, July 12-14, 1976, Washington, DC.

7. L. D. Chapman, L. M. Grady, H. A. Bennett, D. W. Sasser, and D. Engi, Safeguards Automated Facility Evaluation (SAFE) Methodology, SAND78-0378, Sandia Laboratories, Albuquerque, New Mexico, August 1978.

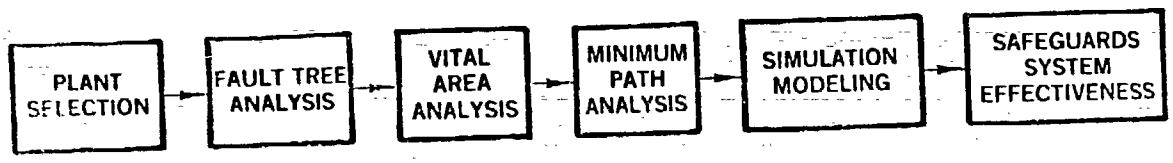

FIGURE 1. MAJOR STEPS IN METHODOLOGY.

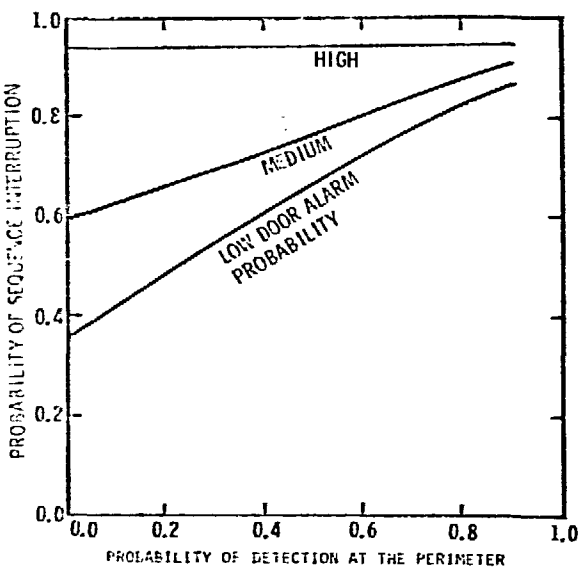

FIGURE 2. SENSITIVITY OF OVERALL SYSTEM PERFORMANCE TO CHANGES IN PROBABILITY OF DETECTION AT THE PLANT PERIMETER.

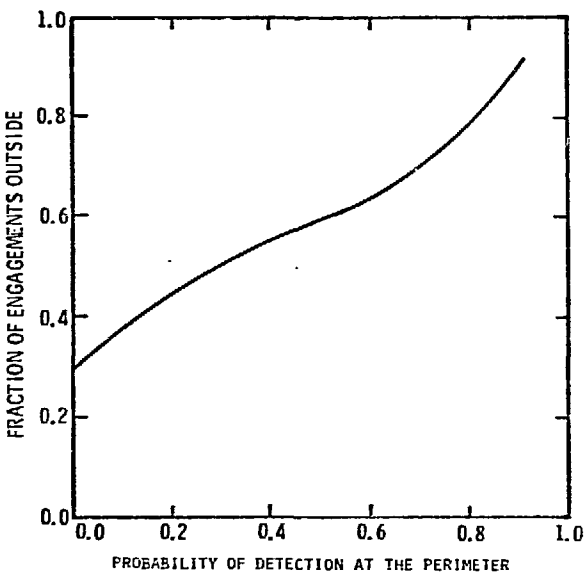

FIGURE 3. VARIATION IN THE LOCATION OF ENGAGEMENTS WITH CHANGES IN PROBABILITY OF DETECTION AT THE PLANT PERIMETER.

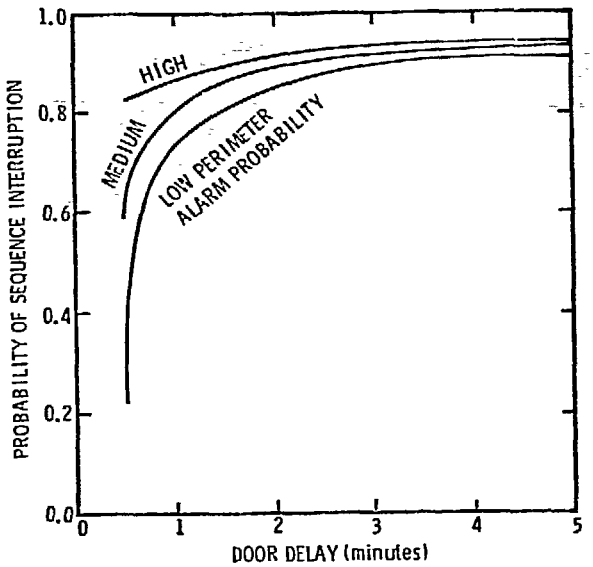

FIGURE 4. SENSITIVITY OF OVERALL SYSTEM PERFORMANCE TO CHANGES IN PENETRATION TIME FOR LOCKED STEEL DOORS.

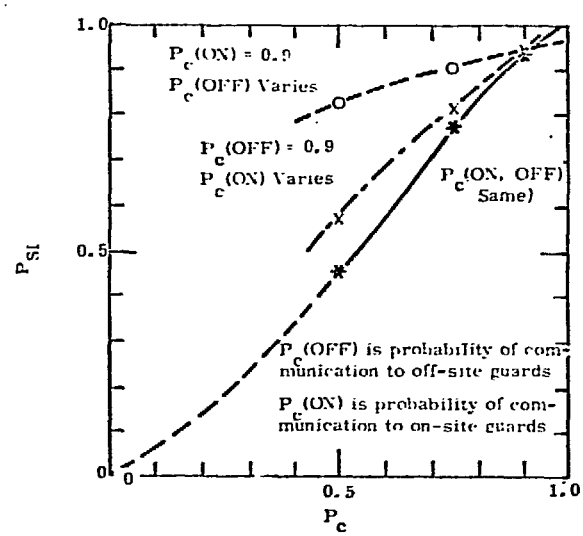

FIGURE 5. SENSITIVITY OF OVERALL SYSTEM PERFORMANCE TO CHANGES IN COMMUNICATIONS PROBABILITIES.