2
9-12-77

SAND77-0410C
Unlimited Release

3151 - W. L. Garner (3)
For ERDA/TIC (Unlimited Release)

CONF-770656--21

The Use of ISEM in Studying the Impact of Guard Tactics on Facility Safeguards System Effectiveness

Dennis Engi, Drayton D. Boozer

SF 2900 Q(7-73)

THE USE OF ISEM IN STUDYING THE IMPACT OF GUARD TACTICS ON FACILITY SAFEGUARDS SYSTEM EFFECTIVENESS*

Dennis Engi
and
Drayton D. Boozer
Sandia Laboratories
Albuquerque, New Mexico 87115

Abstract

The Insider Safeguards Effectiveness Model (ISEM) is a stochastic, discrete event, Monte-Carlo Simulation Model used to assess the effectiveness of physical protection systems for facilities which store, process, or use SNM. ISEM simulates the interaction of a group of insiders (adversaries who are guards or other employees having authorized access to the facility) with the facility's safeguards system.

The facility is described in terms of a set of areas, portals, and barriers. These facility entities are assigned attributes such as number of employees, number and type of sensors, detection probabilities, and delay times. The sensor control and alarm locations are correlated with the authorized access areas of the insider(s) and, if the insider has the appropriate access, the probability of an insider successfully defeating a sensor control or alarm is computed based upon the surveillance subsystems and the insider's attributes.

Following an alarm and an assessment, actions are initiated by the safeguards system. These actions typically involve dispatching guards to specific locations within the facility. Since the specific guard responses must be predetermined, a safeguards system should be evolved from a consideration of a wide spectrum of feasible adversary strategies.

The sensitivity of safeguards system effectiveness to a variety of guard tactics is explored in this paper. The evolution of comprehensive guard tactics for protecting a hypothetical facility is demonstrated. Attention is focused on the potential threat posed by insiders and the necessity of well conceived guard tactics in dealing with this threat.

Introduction and Summary

The guard force is an integral part of the safeguards system at nuclear facilities. Moreover, the tactics employed by guards in countering attacks against the facility are vital in determining the effectiveness of the safeguards system. The purpose of this paper is to provide a structure for analyzing the impact of guard tactics on the effectiveness of safeguards systems.

In order to carry out the proposed study, it is necessary to measure the effectiveness of a safeguards system. The Insider Safeguards Effectiveness Model (ISEM) is used in this

*Presented at the 18th Annual Meeting of the Institute of Nuclear Materials Management, Washington, DC, June 28-30, 1977.

paper to provide this measure. ISEM is a Monte-Carlo simulation model which was developed to treat specifically those insider attacks in which the time relationship among events is important. Documentation for ISEM can be found in references (1), (2), and (3).

The sensitivity of effectiveness to guard tactics is demonstrated by computing the effectiveness measure for a variety of guard tactics employed against a number of distinct insider paths through the facility. For the paths considered, the insider has either theft or sabotage as his objective and can perform covert as well as overt activities. Each path represents a unique insider strategy. The guard tactics employed range from sending a single guard for assessment to collecting the guards en masse prior to dispatching them to confront the insider.

The methodology presented herein provides a structured approach for the decision maker in his quest for improving guard tactics. Alternative criteria are suggested which can be used. Perhaps the primary contribution of the methodology is that it provides a structure through which the analyst can gain valuable insights into interrelationships among elements of the safeguards system.

Model Description

ISEM was developed to treat specifically those insider attacks in which the time relationship among events is important. The concept of attack detection leading to a safeguards system response is central to the model. The set of events for one attack may include events from the material control, material accounting, and personnel control systems; however, there is no distinction made between these major safeguards subsystems within the model. An important class of insider scenarios treated by ISEM is that in which some response by security guards is required to prevent the successful completion of the insiders' attack. ISEM can model either theft or sabotage attacks which consist of both covert and overt insider actions. An insider scenario is used to denote a broad class of events, a subset of which constitutes the insider's path.

Among the effectiveness measures which can be obtained from ISEM are estimates of (1) the probability of at least one alarm along the insider's path, (2) the probability the insider's path is interrupted by guards, (3) the probability the insider's path is interrupted given a detection, and (4) the probability that the insider is neutralized along his path either by encounters with guards or by being caught in portals. For all measures the results are conditioned on an attack by the insider.

The facility is represented in ISEM by three basic entities: AREAS, PORTALS, and BARRIERS. Detection elements such as area, point, or line sensors can be located at these facility entities. Area sensors are used to detect living and inanimate objects within given areas while point sensors generate alarms at specific locations. Line sensors detect

intrusions across a given line such as one extending along a perimeter fence.

Each sensor has a specified facility location, and associated with each sensor is a set of logic points and alarm points. Logic points are those locations where sensor information flow can be interrupted. Examples of logic points are sensor threshold control points (e.g., a potentiometer in a portal) and computer logic and memory points (e.g., a microprocessor used to control sensor alarms). The sensor communication lines which connect sensors, logic points, and alarms are assumed to be secure; but the logic points are susceptible to degradation by insiders. Alarm points are locations where a sensor alarm annunciates. For example, a buzzer in the security control area sounds in response to a door opening on a facility's exterior.

Insider access areas are compared with both logic and alarm points to determine which sensors might be degraded by the insider. The defeat of any logic point for a particular sensor insures defeat of all alarm points for that sensor. The defeat of any alarm point for a particular sensor is considered to be independent of the defeat of all other alarm points. If an insider has appropriate access, outcomes based on input point probability assignments are used to determine if the logic or alarm points are defeated. The probability of successful tampering is also affected by the personnel density and the existence of surveillance sensors in the area.

The gamma and neutron SNM sensor models consider the amount, type, composition, enrichment, burn-up, shielding, and location of the SNM on the insider. SNM sensor characteristics and local environmental conditions are used to determine the background count rate which, in turn, determines the sensor threshold. Metal and explosive sensors are modeled using functional relationships between the effective mass of material and the alarm probability. Sources of metal include weapons and shields for explosives and SNM. The effect of the shield on the operation of the SNM and explosive sensors is described by attenuation factors.

In general, the insider threat is subdivided into insider guards and other employees. It is assumed that the strategy of the insider(s) is to attack the sensor system elements covertly before the potentially overt actions are taken during the interaction phase of the scenario. It is further assumed that only one insider carries the SNM, explosives, firearms, tools, and other materials. Under this assumption, only one insider (either guard or employee) can become involved in an engagement with the guard forces. The only difference in the effect on the scenario caused by an insider employee and an insider guard is that guards have access to sensor alarm and logic points located in both areas and portals, whereas employees have access only to sensor alarm and logic points located in areas. Therefore, insider guards can defeat sensor system elements located in portals but insider employees cannot. Insider guards covertly attack the sensor system but

at most one guard may interact overtly with the guard response force.

ISEM requires that an insider path be specified. Generally, only a subset of facility entities and sensors is involved in a particular insider path; however, ISEM is structured so that facility data can be stored initially and then used for any path chosen for analysis.

The actual confrontation between guards and the insider is modeled as a discrete-state/continuous-time stochastic process (4). The states are the number of combatants actively involved in the confrontation. Transition times between states are assumed to be continuous random variables which are a function of the force size, weapons, and competence of the opposing forces. Distributions of the transition times, along with a count of the number of guard arrivals at the confrontation site, completely determine the engagement process. For example, in an encounter involving two guards and an insider, three initial transitions from this initial state are possible. One guard can be disabled; the insider can be disabled; or another guard can arrive at the encounter site. The states of the model change until either all guards or the insider are disabled.

Analysis of a Hypothetical Facility

Facility Description. The facility that was modeled for this paper is depicted in Figure 1. Areas 5, 8, and 9 of the facility are the vault, work area, and reactor cell, respectively. Area 10 is an administrative office building. The guard stations are located in Areas 3 and 4. Area 6 contains the emergency power generators. The remainder of the areas (1, 2, and 7) are the facility grounds and are bordered by chain-link fences.

Thirty-nine sensor systems are located throughout the facility. Upon activation a sensor may trigger an alarm in either or both of the guard stations.

There are two types of portals modeled. Portals 1 and 5 are vehicle portals. The assumed procedures for the vehicle portals require the presence of guards when vehicles are passing through. For the personnel portals (3 and 4) the sensors operate automatically and the guards may or may not be present.

Description of Insider Paths and Guard Tactics. In ISEM the insider paths are described in terms of a spatial ordering of the appropriate facility entities: AREAS, PORTALS, and BARRIERS. As an example, one of the insider paths considered begins with the theft of SNM from the work area (Area 8), and involves carrying the material through the reactor cell, out the breakout door and eventually through the perimeter fences. In ISEM this path would be described as follows: (Area 8, Portal 6, Area 9, Portal 15, Area 7, Portal 14, Area 2, Barrier 2, Area 1, Barrier 1). For illustrative purposes five specific insider paths were considered in this paper. A brief generic description of these paths is given in Table I(a).

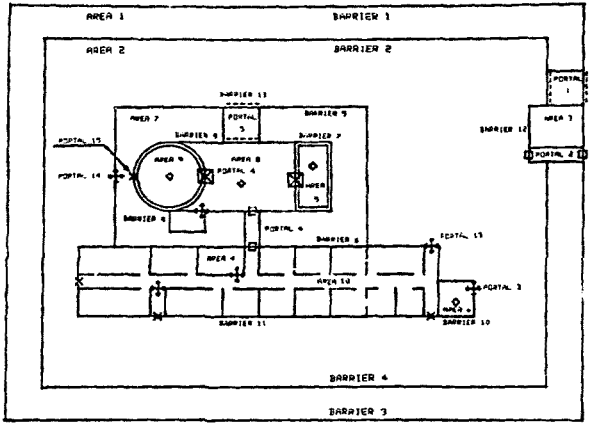

Figure 1. Conceptual Facility Layout

Specifications for guard tactics are required to complete the description of the safeguards system. That is, for each alarm in the facility a dispatching rule is prespecified. These rules involve sending guards from their duty stations to other locations within the facility. For example, if a microwave sensor in Area 1 were activated and resulted in an alarm being sounded in Area 3, the response could involve sending a guard from Area 2 to make an assessment. In a similar fashion, each sensor in the facility would have a specific response associated with it prior to running ISEM. Table I(b) gives a brief description of the tactics studied in this paper.

Sensitivity of Safeguards System Effectiveness to Guard Tactics

The concept of effectiveness can be cast in the context of performance measures of certain portions of the safeguards system. The measure may be a composite of many interacting subsystems of the overall safeguards system, e.g., sensors, personnel controls, guard force, etc. The focus for this paper is the effect of guard tactics on safeguards system effectiveness. The other parameters of the safeguards system description were held constant. The effectiveness measure considered is the

Table I. Description of Insider Paths and Guard Tactics

(a)

Path	Description
P_1	Theft of SNM from work area. Breakout through fence. (AREA 8, PORTAL 6, AREA 9, PORTAL 15, AREA 7, PORTAL 14, AREA 2, BARRIER 2, AREA 1, BARRIER 1)
P_2	Theft of SNM from work area. Covert traversal through personnel control system. (AREA 8, PORTAL 4, AREA 10, PORTAL 13, AREA 2, PORTAL 2)
P_3	Sabotage reactor with high explosives which are smuggled through the personnel control system. (PORTAL AREA 2, PORTAL 13, AREA 10, PORTAL 4, AREA 8, PORTAL 6, AREA 9)
P_4	Sabotage emergency power station with high explosives which are smuggled through the personnel control system. (PORTAL 2, AREA 2, PORTAL 3, AREA 6)
P_5	Procurement of SNM in work area. Dispersal in protected area. (AREA 8, PORTAL 6, AREA 9, PORTAL 15, AREA 7, PORTAL 14, AREA 2)

(b)

Tactics	Description
T_1	A single guard travels to location of activated sensor to make an assessment. Other actions are minimal.
T_2	Guards attempt to seal the personnel control system.
T_3	At least two guards meet at a common "homing point" then search-out the insider.
T_4	Some of the guards seal the personnel control system, others search-out the insider.

probability that the insider is neutralized, conditioned on the event that a detection of unauthorized activities occurs. The conditioning criterion is introduced to eliminate the effect of inadequate performance of the sensor system. Clearly, if there is no detection, the guards cannot react to intercept the insider.

The results of the ISEM runs are shown in Table II. Table II(a) contains the results for each combination of insider and guard tactics considered. For example, path 5 consists of an insider taking the SNM from the work area (Area 8), passing through the reactor cell and into the protected area where he disperses the material. When this path is simulated with guard tactics T_3 and T_4 the results are dramatically different (0.01 vs 0.83, respectively). The reason for this becomes apparent when the tactics are described in more detail. The T_3 set of tactics consists of collecting two or more guards at some common homing point, then dispatching them as a group to interdict the insider. The motivation for devising this particular set of tactics was to provide the guards with supportive firepower if necessary. In contrast, tactics set T_4 dispatches guards individually and as quickly as possible to interdict the insider. In light of these quite distinct

objectives the predicted outcomes are intuitively consistent. That is, with the P_5 vs T_3 case, by the time the guards come together to respond there is insufficient time to stop the insider. On the other hand, in the P_5 vs T_4 case the response time is sufficiently short for the guards to stop the insider a large portion of the time.

Note that the paths which were chosen for study fall into one of two categories - theft or sabotage. Paths 1 and 2 are theft oriented and paths 3, 4, and 5 have sabotage as the insider's objective. The data in Table II(b) depict a theft vs sabotage reduction of the data in Table II(a). This reduction involves averaging path data within each of the two insider goals.

Table II. Probability of System Win Given a Detection

(a) Paths vs Tactics

		T_1	T_2	T_3	T_4
Theft	P_1	0.15	0.66	0.06	0.60
	P_2	1.0	1.0	0.93	0.90
Sabotage	P_3	0.61	0.4[illegible]	0.49	0.84
	P_4	0.59	0.5[illegible]	0.10	0.59
	P_5	0.58	0.10	0.01	0.13
	Mean	0.59	0.55	0.32	0.75†
	Maximin	0.15	0.10	0.01	0.59*

(b) Goals vs Tactics

	T_1	T_2	T_3	T_4
Theft	0.58	0.83	0.50	0.75
Sabotage	0.44	0.36	0.20	0.73
Mean	0.51	0.60	0.35	0.74

Examination of the data in Table II(a) yields some interesting observations. Suppose that each of the insider paths is thought to be equally likely. Then the arithmetic mean for each column provides a composite measure for the probability that a specific set of guard tactics will be successful in stopping the insider (cf. row 6 of Table II(a)). In the terminology of game theory this a two-person, zero-sum game with mixed strategies. The optimal decision with respect to this information is to choose tactics set T_4 since this would maximize the composite probability of system win. Unfortunately, if the insider has information regarding the set of tactics utilized, he can choose the path that maximizes his chances of succeeding based upon the specific set of guard tactics that have been instituted. So in this instance he might be led to choose path P_4 because it minimizes the probability that the safeguards system successfully stops him, given that tactics T_4 are used.

† The optimal solution for selection criterion is based on mean values.

* The optimal solution for selection criterion is based on the maximum probability of safeguards system win given detection for worst case path (maximin).

Another criterion that is potentially useful is to select the set of tactics that maximizes the probability of a system win for the worst case path. This is accomplished by first finding the minimum value for each column (set of tactics) then selecting the set of tactics that has the maximum of these minimum values. This is a two-person, zero-sum game with strategies not mixed. In this example T_4 would be selected because it contains the maximum value.

The data in Table II(b) could also be used in selecting tactics. Again, the optimal choice of tactics appears to be T_4 when the composite average is the criterion. Note also that T_4 offers a balance of protection against sabotage and theft in that the effectiveness results are the same. However, T_4 is not necessarily the optimal choice of tactics. For example, if theft is considered to be more significant than sabotage, T_2 may be the choice of tactics since it maximizes the probability of a safeguards system win given a detection for theft paths.

Conclusions and Recommendations

This paper demonstrates a methodology within which the sensitivity of safeguards system effectiveness to a variety of guard tactics can be analyzed. The measure of effectiveness chosen for this study was the probability that the safeguards system successfully neutralizes an attack by an insider given that the insider is detected somewhere during his attempt. Although not treated here, other effectiveness measures may be more appropriate in certain circumstances. Consequently, the analyst should be circumspect in the selection of a measure or set of measures which is most useful for his specific situation. However, in the judgment of the authors, the measure used in this paper is the most relevant for the problem studied.

For illustrative purposes five insider paths were played against four sets of guard tactics. In practice, considerably more insider paths and/or guard tactics would be necessary to cover the spectrum of contingencies that may be relevant.

Different criteria for selecting the optimal set of guard tactics from those considered were presented. The criterion, or set of criteria, that are actually used in the optimization performed on the effectiveness data are, perhaps, not as important as the insights that can be gained by performing the optimization. That is, the methodology presented provides a structure through which an analyst may choose guard tactics which complement the other portions of the safeguards system in combating the perceived threat. Although ISEM was used to generate the effectiveness results used in this paper, the methodology is not dependent on the particular effectiveness model employed nor on the assumption that the adversary is an insider.

Acknowledgements

The authors wish to express their appreciation to other members of the Sandia Laboratories staff who supported this effort. In particular, thanks are due J. L. Todd and L. M. Grady for their assistance in designing the conceptual facility and in digitizing the facility layout.

References

1. Boozer, Drayton D. and Dennis Engi, Simulation of Personnel Control Systems with the Insider Safeguards Effectiveness Model (ISEM), SAND76-0682, Sandia Laboratories, Albuquerque, NM, April 1977.

2. Boozer, Drayton D. and Dennis Engi, Insider Safeguards Effectiveness Model (ISEM): Sandia User's Guide, SAND77-0043, Sandia Laboratories, Albuquerque, NM, to be published.

3. Boozer, Drayton D. and Dennis Engi, "Nuclear Facility Safeguards System Modeling Using Discrete Event Simulation," Proceedings of the Eighth Annual Pittsburgh Conference on Modeling and Simulation, April 1977.

4. Engi, Dennis, A Small-Scale Engagement Model with Arrivals: Analytical Solutions, SAND77-0054, Sandia Laboratories, Albuquerque, NM, April 1977.