UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

AUG 5 1980

MEMORANDUM FOR: William J. Dircks, Director
Office of Nuclear Material Safety
and Safeguards

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

Victor Stello, Jr., Director
Office of Inspection and Enforcement

Robert B. Minoque, Director
Office of Standards Development

FROM: Robert J. Budnitz, Director
Office of Nuclear Regulatory Research

SUBJECT: RESEARCH INFORMATION LETTER NO. 93 "ISEM"
ADVERSARY SEQUENCE EVALUATION MODEL

Introduction

This memorandum transmits the computer program and documentation (Ref. 1) of completed research on the Insider Safeguards Effectiveness Model (ISEM), which is part of a continuing NRC research activity entitled "Effectiveness Evaluation Methods for Fixed-Site Physical Protection." The study was performed by Sandia National Laboratories, Albuquerque, New Mexico, and was jointly sponsored by the NRC and the DOE. Support of this work by the Office of Nuclear Regulatory Research (RES) was motivated by a research request (NMSS-77-1) coordinated among your offices, identifying a need for evaluative methods for fixed-site theft and sabotage prevention systems. Documentation (Refs. 2-5) concerning ISEM during its development has previously been made available throughout the NRC.

The purpose of this study was to develop a methodology for analyzing fixed-site security systems as to their effectiveness against threats posed by insiders (i.e., adversaries having authorized access to the facility), only one of whom may take forcible action. Analysis considerations may include trade-offs involving on-site and off-site response forces and response times, perimeter system alarms, barrier configurations, and the sensitivity of system effectiveness to guard utilization (numbers, stationing, weaponry, competence, and deployment in response to alarms). The model provides a framework for performing

inexpensive studies related to fixed-site security systems, for evaluating alternative decisions, and for estimating the relative cost effectiveness associated with these decision policies.

Discussion

ISEM is a discrete-event Monte-Carlo simulation of the interaction between one adversary (either insider or outsider) and the physical protection system of a nuclear facility as the adversary traverses a prescribed entry or exit path. The physical layout of the facility is treated as an arrangement of AREAS, BARRIERS, and PORTALS, which are called entities. An adversary path is an ordered sequence of entities. Provision is made for additional inside adversaries who may covertly tamper with the sensor systems to which they have access. These covert insiders who tamper with the sensors do not play an active role during the simulation.

A sensor system consists of a sensor and a serially connected set of (from 0 to 2) logic points which connect in parallel to a set of (from 1 to 3) alarm points. Each sensor system has one sensor, and there is no explicit maximum number of sensor systems. Defeat of any logic point ensures the defeat of all alarms from the sensors connected to it. The defeat of an alarm point interrupts alarms only to that point; there is no effect on any other alarm points. Sensors are not attacked, but logic and alarm points can be attacked. Guards (who may be insiders) may have access to logic or alarm points located in AREAS and PORTALS. Employees (who may be insiders) have access only to logic or alarm points located in AREAS. Success probabilities for tampering are specified separately for logic points and alarm points. Each tampering attempt is assumed to be independent.

Proceeding along the path, each entity is checked to see if an alarm would have occurred had there been no tampering. If so, a check is made to see whether tampering, if any, defeated the alarm. [The likelihood of successful tampering is diminished by a sufficient population density of employees in the entity and by the presence of a closed-circuit television (CCTV) assessment system.]

Intrusion detection is based upon a probability of detection associated with entering the effective region of an area sensor, crossing a line sensor, or being scanned by or directly activating a local sensor. Scanning sensors have been modeled in some detail; these include SNM detectors (gamma and neutron flux), high explosives detectors, and metal detectors.

If the insiders were unsuccessful in defeating the sensor system and an alarm annunciates, an assessment delay occurs, followed by the deployment of guards to specific PORTALS from their normal stations in specific AREAS. It is assumed that the assessment is made correctly and that the adversary in unauthorized possession of material is identified on sight as the adversary.

If the adversary is within a PORTAL when a guard arrived, it is assumed that the adversary is defeated for that particular interaction. If the adversary has left the PORTAL by the time a guard arrives and is in or at an adjacent entity, there is a probability that the guard will call for maximum reinforcement. If the adversary arrives at the PORTAL after a guard has reached it, an encounter ensues. In a call for reinforcement, guards are individually redeployed to the location of the encounter.

The encounter between guards and the adversary is modeled as a discrete-state, continuous-time stochastic process. The encounter is described by the weapon and competence levels of the opposing forces (recall that only one adversary may be armed), along with the number of guards that have arrived at the encounter point. Competence and weapon levels are assumed to remain fixed throughout the encounter. The encounter is concluded when either the adversary or the guard force has been eliminated. If the adversary is eliminated, the physical protection system wins; if the guards are eliminated, subsequent encounters are still possible. The adversary can win only if his entire path is successfully traversed.

Since ISEM simulates either an entry or an exit path for one run, it is necessary to make two runs to simulate a scenario that requires both entrance and exit paths. Proper conditioning of the input allows a system response to be initiated along the entrance path and continued along the exit path. Generally, between 500 - 1000 simulated interactions are randomly generated against the site for each scenario. The model collects statistics on various aspects of each scenario that may be utilized by the decision maker as an aid in evaluating or upgrading a physical protection system.

The input data required in the model consist of detailed information related to (1) facility areas, (2) facility barriers, (3) facility portals, (4) facility sensors, (5) insiders, both guards and other employees, (6) the description of Special Nuclear Materials, (7) the description of explosives, and (8) security forces, including descriptions, tactics and data on adversaries.

The three principal types of output information available from ISEM are (1) event sequences which illustrate how events occur with time along a path, (2) twenty-two statistical variables which summarize simulation results, and (3) fifteen histograms which pictorially represent and further expand the statistical results.

Results

The primary product of this research is a computer program and its documentation, which is hereby transmitted. ISEM is written in the GASP IV simulation language which is a package of FORTRAN subroutines. It is operational in the "batch" mode on Sandia's SCOPE operating system and in the time-sharing mode on Sandia's NOS operating system. The batch version requires approximately 100K octal words of central memory and a single replication takes about 0.1 CPU second. The user's manual (Ref. 1) describes the batch version, which should be readily adaptable to

any computer having the GASP IV package, a FORTRAN compiler, and the required central memory. The time-sharing version is not easily adaptable to other computers.

In the latter stages of Sandia's development and testing, applications of ISEM were carried out at seven (DOE and/or NRC) facilities, including Rocky Flats and Savannah River. Since its completion, the capability for applying ISEM as well as EASI (RIL #23) and FESEM (RIL #24) has been requested by industry and other government agencies.

The program is currently available for NRC use via an access code number to Sandia's CDC-6600 computer. The Tektronix 4054 intelligent terminal purchased for the recently established Application and Development Facility (ADF) provides NMSS with convenient access to this model. A training program was given in April 1978 to a few NRC potential users. This can be repeated for other interested users given sufficient requests.

The ISEM model was included in the user tests conducted within the NMSS "Test of Evaluation Methods" program. This program made trial applications of several safeguards system evaluation computer programs.

Recommendations

ISEM is a first-generation model suitable for the study of physical protection system interaction with a single adversary following a prescribed path, preceded by a covert attack on sensor system elements by a group of insiders. It is recommended that until second-generation models are tested and approved, the ISEM model may be used by NMSS and other offices as an ancillary aid in formulating regulatory requirements, licensing, inspection and other monitoring operations related to the insider problem. The model permits a reasonably detailed study of guard tactics and procedures at a facility. One output from ISEM provides the user with information that illustrates where the security system may be vulnerable to the particular scenario analyzed. Sensitivity analyses can be made on most components along the adversary's path to determine the worth (for a particular scenario) of upgrading individual physical protection system components. One can then, in conjunction with the analyses of other scenarios, determine appropriate upgrade actions and provide a cost/benefit analysis of the system improvements. There are numerous time-sharing terminals available throughout NRC from which the Sandia NOS interactive system can be accessed. Technical questions regarding ISEM may be referred to R. C. Robinson of the Safeguards Research Branch.

T. F. Murley/acting

Robert J. Budnitz, Director
Office of Nuclear Regulatory Research

References

1. Boozer, D. D., & D. Engi, "Insider Safeguards Effectiveness Model (ISEM) Users Guide," Sandia Laboratories, Albuquerque, New Mexico, SAND77-0043, November 1977.

2. Engi, D., & D. D. Boozer, "The Use of ISEM in Studying the Impact of Guard Tactics on Facility Safeguards System Effectiveness," Sandia Laboratories, Albuquerque, New Mexico, SAND77-0410C, July 1977.

3. Boozer, D. D., & D. Engi, "Simulation of Personnel Control Systems with the Insider Safeguards Effectiveness Model (ISEM)," Sandia Laboratories, Albuquerque, New Mexico, SAND76-0682, April 1977.

4. Boozer, D. D., & D. Engi, "Nuclear Facility Safeguards Systems Modeling Using Discrete Event Simulation," Sandia Laboratories, Albuquerque, New Mexico, SAND77-0075, July 1977.

5. Engi, D., "A Small Scale Engagement Model with Arrivals: Analytical Solutions," Sandia Laboratories, Albuquerque, New Mexico, SAND77-0054, April 1977.

any computer having the GASP IV package, a FORTRAN compiler, and the required central memory. The time-sharing version is not easily adaptable to other computers.

In the latter stages of Sandia's development and testing, applications of ISEM were carried out at seven (DOE and/or NRC) facilities, including Rocky Flats and Savannah River. Since its completion, the capability for applying ISEM as well as EASI (RIL #23) and FESEM (RIL #24) has been requested by industry and other government agencies.

The program is currently available for NRC use via an access code number to Sandia's CDC-6600 computer. The Tektronic 4054 intelligent terminal purchased for the recently established Application and Development Facility (ADF) provides NMSS with convenient access to this model. A training program was given in April 1978 to a few NRC potential users. This can be repeated for other interested users given sufficient requests.

The ISEM model was included in the user tests conducted within the NMSS "Test of Evaluation Methods" program. This program made trial applications of several safeguards system evaluation computer programs.

Recommendations

ISEM is a first-generation model suitable for the study of physical protection system interaction with a single adversary following a prescribed path, preceded by a covert attack on sensor system elements by a group of insiders. It is recommended that until second-generation models are tested and approved, the ISEM model may be used by NMSS and other offices as an ancillary aid in formulating regulatory requirements, licensing, inspection and other monitoring operations related to the insider problem. The model permits a reasonably detailed study of guard tactics and procedures at a facility. One output from ISEM provides the user with information that illustrates where the security system may be vulnerable to the particular scenario analyzed. Sensitivity analyses can be made on most components along the adversary's path to determine the worth (for a particular scenario) of upgrading individual physical protection system components. One can then, in conjunction with the analyses of other scenarios, determine appropriate upgrade actions and provide a cost/benefit analysis of the system improvements. There are numerous time-sharing terminals available throughout NRC from which the Sandia NOS interactive system can be accessed. Technical questions regarding ISEM may be referred to R. C. Robinson of the Safeguards Research Branch.

Original Signed by
T. E. Murley

Robert J. Budnitz, Acting Director
Office of Nuclear Regulatory Research

RJBudnitz
06/5/80

OFFICE ►	SAFER:RES	SAFER:RES	SAFER:RES	SAFER:RES	SAFER:RES	RES
SURNAME ►	R.Robinson:jh	Tomlin	Durst	Bassett	Arsenault	Larkins
DATE ►	06/03/80	06/5/80	06/5/80	06/9/80	06/24/80	6/3/80

NRC Form 318B (4-79) NRCM 0240 ★U.S. GOVERNMENT PRINTING OFFICE: 1979—293-404