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

APR 10 1978

MEMORANDUM FOR: Clifford V. Smith, Jr., Director
Office of Nuclear Material Safety
and Safeguards

FROM: Saul Levine, Director
Office of Nuclear Regulatory Research

SUBJECT: RESEARCH INFORMATION LETTER NO. 24 - "FESEM" ADVERSARY SEQUENCE EVALUATION MODEL

Introduction

This memorandum transmits the results* of completed research on the Forcible Entry Safeguards Effectiveness Model (FESEM), which is part of a continuing NRC research activity entitled "Effectiveness Evaluation Methods for Fixed-Site Physical Protection." The study was performed by Sandia Laboratories, Albuquerque, New Mexico, for the Office of Nuclear Regulatory Research (RES) in response to a research request (NMSS-77-1) from your office, identifying a need for evaluative methods for fixed-site theft and sabotage prevention systems.

The purpose of this study was to develop a methodology for analyzing fixed-site security systems as to their effectiveness against a forcible attack by an adversary intent on creating an act of sabotage or theft. Analysis may include trade-offs involving on-site and off-site response forces and response times, perimeter system alarms, barrier configurations, and varying levels of forcible attacks by an adversary. The model provides a framework for performing inexpensive experiments related to fixed-site security systems, for testing alternative decisions, and for determining the relative cost effectiveness associated with these decision policies.

Discussion

FESEM is a Monte Carlo simulation model which can be applied to problems of forcible entry, for any assumed path, with an adversary having a variety of attributes, and gives an estimate of adversary success probability. The model includes essential elements of the fixed-site safeguards system which are related to the protective barriers for delay, sensors and alarms for detection, viewing and decision devices for

24

*Chapman, L. D., G. A. Kinemond, and D. W. Sasser, "Users Guide for Evaluating Alternative Fixed-Site Physical Protection Using "FESEM"," Sandia Laboratories, Albuquerque New Mexico, SAND77-1367, November 1977.

assessment, communication methods, and engagement with the adversary. Certain estimates of the functional capability of each of these elements are necessary inputs to FESEM. In general, most of these data can be obtained directly from the facility to be analyzed. Once potential adversary targets and likely physical paths to these targets have been identified, fixed-site characteristics and barrier specifications can be generated for each physical path. Adversary attributes which affect the engagement model are randomly selected, based on attribute limits specified by the user.

Given the required input data, FESEM simulates an adversary action sequence using an analytical security force/adversary force engagement model. One of four possible types of attack may be specified (or selected at random) for each simulation: (1) external attack-sabotage; (2) external attack-theft; (3) internal assisted attack sabotage; and (4) internal assisted attack-theft. Internal attack implies that a worker at the fixed site may be an ally of the attackers and may, either by intent or under duress, degrade the alarm and/or communication systems. External attack implies that the attackers do not have internal assistance.

After the site characteristics have been selected, adversary attributes are generated, and an attack is simulated against the fixed site. Internally aided attacks may serve to degrade the alarm and communication systems. Upon the arrival of a guard force meeting the minimum force requirements, a battle or engagement is initiated with the adversary. During the engagement simulation, the adversary advancement is assumed to be interrupted. If the adversary wins the battle, then his advancement continues until interrupted by the arrival of either on-site or off-site guard forces or completion of the theft or sabotage. This ends one simulation. Generally, between 500 - 1000 such simulated attacks 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.

Results

The results of the FESEM analysis include estimates of the probability of sabotage or theft wins (and losses) based on attack force size, attack mobility, and type of attack; collected statistics associated with each variable (e.g., means, standard deviations, extreme values, etc.); and 15 optional histograms (e.g., number of wins by defenders and by attackers for successful sabotage or theft, alarm types for all runs, time required for successful sabotage or completion of theft, etc.).

The FESEM is written in the GASP IV simulation language (FORTRAN-based) and processes both discrete and continuous events. The code uses the SCOPE system for the CDC-6600 computer and is operational on the BATCH mode on Sandia's SCOPE operating system and the time-sharing mode on Sandia's NOS operating system. The computer memory requirement is approximately 100K octal and a single replication takes about 0.2 CPU second.

The program is currently available for NRC use via an access code number to Sandia's computer. A training program was given in February 1978 to interested NRC personnel and potential users.

In the latter stages of Sandia's development and testing, numerous applications of FESEM were carried out. Assessments were made at 21 ERDA facilities, including Argonne, Battelle, Hanford, Livermore, Los Alamos, Oak Ridge, and Savannah River. Detailed studies were done at six ERDA facilities.

Recommendations

It is recommended that the FESEM model be used by NMSS and other offices as an ancillary aid in formulating regulatory requirements, licensing, inspection and other monitoring operations. One output from FESEM provides the user with information that illustrates where the weaknesses are in the security system. Sensitivity analyses can be made to determine the worth of upgrading individual physical protection system components. One can then determine appropriate upgrade actions and provide a cost/benefit analysis of the system improvements. There are numerous time-sharing terminals available throughout the NRC and technical questions regarding FESEM may be referred to R. C. Robinson of the Technical Support Branch.

Saul Levine

Saul Levine, Director
Office of Nuclear Regulatory Research